Novell ZENworks® Server Management

6.5

www.novell.com

管理ガイド

2004 年 2 月 11 日



Novell®

法的通知

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っていません。また本書の商品性および特定の目的への適合性について、いかなる黙示の保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っていません。またノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる黙示の保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、Novell 製ソフトウェアの内容を変更する権利を常に留保します。

米国輸出規制または当該国の法律を含む (これに限られません) 該当する法律や規制に違反して、この製品を輸出または再輸出することはできません。

Copyright ヮ 1999-2005 Novell, Inc. All rights reserved. 本書の一部または全体を無断で複写・転載することは、その形態を問わず禁じます。

米国 Novell, Inc. およびノベル株式会社は、このガイドに記載されている製品で具体的に示されているテクノロジに関する知的所有権を有しています。特に、これらの知的所有権には、Novell Legal Web サイト (http://www.novell.com/company/legal/patents/) に記載されている 1 つまたは複数の米国特許、米国および他の国における 1 つまたは複数のその他の特許または係属特許のアプリケーションを含んでいます (ただし、これらに限定されません)。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Novell ZENworks 6.5 Server Management 管理ガイド
2004 年 2 月 11 日

オンラインドキュメント： この製品およびその他の Novell 製品のオンラインドキュメントやアップデート版を入手するには、www.novell.com/documentation を参照してください。

Novell の商標

ConsoleOne は、米国 Novell Inc. の米国ならびに他の国における登録商標です。
eDirectory は、米国 Novell, Inc. の商標です。
GroupWise は、米国 Novell Inc. の米国ならびに他の国における登録商標です。
IPX は、米国 Novell, Inc. の商標です。
NCP は、米国 Novell, Inc. の商標です。
NDS は、米国 Novell, Inc. の米国ならびに他の国における登録商標です。
NetExplorer は、米国 Novell, Inc. の商標です。
NetWare は、米国 Novell Inc. の米国ならびに他の国における登録商標です。
NetWare Core Protocol は、米国 Novell, Inc. の商標です。
NetWare Management Agent は、米国 Novell, Inc. の商標です。
NetWare SFT III は、米国 Novell, Inc. の商標です。
NLM は、米国 Novell, Inc. の商標です。
Novell は、米国 Novell Inc. の米国ならびに他の国における登録商標です。
Novell Client は、米国 Novell, Inc. の商標です。
Novell Technical Services は、米国 Novell, Inc. のサービスマークです。
SPX は、米国 Novell, Inc. の商標です。
SUSE は、ノベルの傘下である SUSE LINUX AG. の登録商標です。
ZENworks は、米国 Novell Inc. の米国ならびに他の国における登録商標です。

Third-Party Materials

すべてのサードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて 21

パート I Policy and Distribution Services

1 インストール後の設定 25

配布システムの計画 25
概要 26
Distribution の選択 28
ネットワークトポロジの理解 33
追加の Distributor の必要性 34
他の Subscriber のイントールの必要性 37
配布フローの決定 38
Distribution のセキュリティの理解 40
Distribution の Channel の決定 42
Subscriber の登録の決定 43
配布スケジュールの決定 44
配布システムの設定 46
追加の Distributor、データベース、および Subscriber のインストール 47
追加の配布セキュリティのセットアップ 50
配布フローの設定 52
Distribution および関連 Channel の作成 54
Distribution への登録 56
Distribution の送信 57
配布システムの管理 58
設定計画ワークシート 58

2 Novell iManager 69

iManager の ZENworks Server Management の役割へのアクセス 70
iManager へのログイン 70
インタフェースの理解 71
役割とタスクの表示 72
Tiered Electronic Distribution オブジェクトの管理 73
iManager での Tiered Electronic Distribution オブジェクトの作成 74
iManager での Tiered Electronic Distribution オブジェクトプロパティの編集 75
iManager での Tiered Electronic Distribution オブジェクトの削除 75
配布プロセスの監視 76
[Tiered Distribution] ビューの使用 76
[Subscriber Distribution] ビューの使用 77
Remote Web Console によるエージェントの管理 79
Distributor Agent の管理 80
Policy/Package Agent の管理 82
複数の Remote Web Console ウィンドウの表示 84
iManager の ZENworks Server Management の役割と ConsoleOne 機能の比較 84

3 Tiered Electronic Distribution 87
一般的な配布タスク . . . 87
Tiered Electronic Distribution の理解 . . . 89
Tiered Electronic Distribution による配布管理 . . . 90
基本配布プロセス . . . 90
Tiered Electronic Distribution の eDirectory オブジェクト . . . 91
Tiered Electronic Distribution オブジェクトの関係 . . . 91
物理ネットワーク接続 . . . 92
配布フローの詳細 . . . 92
Tiered Electronic Distribution のプロセス . . . 93
階層配布モデル . . . 95
Tiered Electronic Distribution の重要なコンポーネント . . . 96
Distributor . . . 96
Distributor の理解 . . . 97
配布ルーティングの理解 . . . 99
Distributor の作成 . . . 107
Distributor の設定 . . . 108
Distributor の更新 . . . 111
Distributor オブジェクトの削除と Distribution への影響 . . . 112
Distribution . . . 112
Distribution の理解 . . . 112
Distribution に関する問題 . . . 116
Distribution の決定 . . . 119
Distribution の作成 . . . 125
Distribution の優先度 . . . 128
Distribution の前後の処理 . . . 129
他の Distributor への Distribution の再割り当て . . . 135
Distribution の削除 . . . 139
Distribution オブジェクトの削除 - 一時ファイルの自動削除 . . . 139
孤立した Distribution の処理 . . . 142
手動による Distribution のインポートとエクスポート . . . 143
Distribution ウィザードの使用 . . . 146
Channels . . . 147
Channel の理解 . . . 147
Channel の作成と設定 . . . 148
Channel からの強制送信 . . . 150
Subscriber . . . 150
Subscriber の理解 . . . 150
Subscriber の作成 . . . 152
Subscriber の設定 . . . 153
Subscriber 設定の更新 . . . 156
Subscriber と Channel の関連付け . . . 157
Distributor のルーティング階層に属する Subscriber オブジェクトの削除 . . . 158
Subscriber Group . . . 158
Subscriber Group の理解 . . . 158
Subscriber Group の作成と設定 . . . 159
External Subscriber . . . 160
External Subscriber の理解 . . . 160
External Subscriber による別のツリーへの配布 . . . 166
External Subscriber の作成と設定 . . . 168
複数の Tiered Electronic Distribution オブジェクトの設定 . . . 169
複数の Tiered Electronic Distribution オブジェクトプロパティの変更に関する問題 . . . 170
複数の Tiered Electronic Distribution オブジェクトのプロパティの変更 . . . 171
複数のオブジェクトの変更に使用するプロパティタブ . . . 172
Distribution の送信 . . . 176
配布プロセスの理解 . . . 176

単一の Distribution の強制送信 . . . 178
親 Subscriber による Distribution の送信 . . . 178
ツリー間の Distribution の送信 . . . 179
Tiered Electronic Distribution に関するその他の問題 . . . 180
File Distribution のディレクトリ同期の細分性 . . . 180
Tiered Electronic Distribution の依存関係の理解 . . . 185
システムリソースとサーバの動作 . . . 185
I/O レートと同時に実行可能な Distribution の制御 . . . 186
メッセージトラフィックの極小化 . . . 187
Tiered Electronic Distribution サーバの DNS 名または IP アドレスの変更 . . . 188
Tiered Electronic Distribution プロセスのエラー . . . 189
作業ディレクトリ . . . 190
NetWare Distributor のディレクトリ . . . 190
NetWare Subscriber のディレクトリ . . . 191
Windows Distributor のディレクトリ . . . 192
Windows Subscriber のディレクトリ . . . 193
Linux Distributor または Solaris Distributor のディレクトリ . . . 193
Linux Subscriber または Solaris Subscriber のディレクトリ . . . 193
Tednode.properties ファイルの編集 . . . 194

4 Server Policies（サーバポリシー） 197

サーバポリシーについて . . . 197
サーバポリシーによる設定および動作の管理 . . . 198
サーバポリシーとポリシーパッケージ . . . 198
ポリシーの特性 . . . 199
サーバポリシーのアーキテクチャ . . . 200
ポリシーの適用 . . . 203
サーバポリシーの説明 . . . 205
ポリシーパッケージの作成 . . . 208
ポリシーコンテナの作成 . . . 209
ポリシーパッケージオブジェクトの作成 . . . 209
サーバポリシーの設定 . . . 210
Zentrap.mib のコンパイル . . . 210
Container Package ポリシーの設定 . . . 210
Service Location Package ポリシーの設定 . . . 212
Distributed Server Package ポリシーの設定 . . . 219
ポリシーを使用したカスタムログファイルの作成 . . . 235
ポリシーの有効化 . . . 236
ポリシーの配布 . . . 236
ポリシーの関連付け . . . 237
Distributor オブジェクトへのポリシーパッケージの関連付け . . . 237
ポリシーパッケージへの Distributor オブジェクトの関連付け . . . 237
ポリシーのスケジュール設定 . . . 238
有効なポリシーの表示 . . . 238
ポリシー適用の変更 . . . 238
適用されるポリシーの変更 . . . 238
特定のポリシーの適用の停止 . . . 239
特定の Subscriber に関するポリシー適用の削除 . . . 239
Policy Package Distribution の適用の停止 . . . 240

5 Server Software Package に関する問題 241

Server Software Packages によるソフトウェアの管理 . . . 241
Server Software Packages の理解 . . . 242
Server Software Packages およびコンポーネントの理解 . . . 242
ソフトウェアパッケージとコンポーネントの環境設定の理解 . . . 243
ソフトウェアパッケージをインストールする順序の決定 . . . 244
抽出したファイルの実行 . . . 245

ソフトウェアパッケージのコンパイル . . . 245
ソフトウェアパッケージへのアクセス . . . 246
ソフトウェアパッケージの配布 . . . 247
クラスタへのソフトウェアパッケージの配布 . . . 247
Server Software Package の管理 . . . 248
ソフトウェアパッケージのインストールの失敗 . . . 254
ソフトウェアパッケージのインストールのロールバック . . . 254
Server Software Packages のプランニング . . . 255
どのファイルまたはアプリケーションを配布する必要があるか . . . 255
どのようなソフトウェアパッケージコンポーネントが必要であるか . . . 256
必要な最小限の要件は何か . . . 256
Server Software Package の設定 . . . 257
複数のワークステーションによる Server Software Package の管理の設定 . . . 257
Server Software Package の作成 . . . 261
Server Software Package の環境設定 . . . 262
ソフトウェアパッケージコンポーネントの作成 . . . 262
ソフトウェアパッケージコンポーネントの環境設定 . . . 263
ソフトウェアパッケージのコンパイル . . . 274
ソフトウェアパッケージの配布 . . . 275
古いバージョンの Server Software Package の ZENworks 6.5 Server Management への変換 . . . 275
Server Software Packages によるサーバ上のディレクトリの削除 . . . 277
Server Software Package で使用する変数の設定 . . . 277
Server Software Package の作成 . . . 278
Server Software Package コンポーネントの作成と環境設定 . . . 279
Server Software Package のコンパイル . . . 280
ディレクトリの削除の手動によるテスト . . . 281
次のタスク . . . 281

6 Desktop Application Distribution 283

Desktop Application Distribution の理解 . . . 283
Desktop Application Distribution の目的 . . . 283
配布されたアプリケーションの問題 . . . 286
その他の問題 . . . 297
要件 . . . 299
Desktop Application Distribution の作成 . . . 300
Desktop Application Distribution ウィザードの理解 . . . 301
Distribution の作成 . . . 301
Desktop Application Distribution の再構築 . . . 308
すべての属性の更新 . . . 308
再構築のトリガ . . . 308
Desktop Application Distribution ファイルのクリーンアップ . . . 310
ツリー間での Desktop Application Distribution の送信 . . . 310

7 Policy and Distribution Services のセキュリティ 313

署名付き証明書とダイジェストを使用した配布のセキュリティ . . . 313
ダイジェストについて . . . 314
Policy and Distribution Services での証明書の使用について . . . 314
証明書に関する重要な点 . . . 315
ConsoleOne ユーザの権利と証明書のコピー . . . 317
証明書ファイルの場所 . . . 317
証明書の解決 . . . 317
無効な証明書の処理 . . . 318
証明書とプライベートキーのディレクトリ . . . 322
暗号化されていない Distribution 用のセキュリティ証明書の作成 . . . 322
暗号化されていない Distribution 用の証明書の手動によるコピー . . . 323
暗号化を使用した Distribution のセキュリティ . . . 324
暗号化証明書の作成とコピー . . . 324

暗号化された Distribution の送信 . . . 327
暗号化された Distribution の抽出 . . . 327
セキュリティ保護されていない接続でのサーバ間通信のセキュリティ . . . 328
この節で使用される用語 . . . 329
セキュリティ証明書 . . . 329
SSL の使用 . . . 329
パスワードファイルの形式 . . . 330
TCP/IP アドレスと DNS 名 . . . 330

8 スケジュール設定 331

Policy and Distribution Services でのスケジュール設定の理解 . . . 331
配布にスケジュール設定が必要な理由 . . . 331
スケジュール設定を必要とするサーバポリシー . . . 332
サーバポリシーと Tiered Electronic Distribution のスケジュール設定の相違点 . . . 332
Tiered Electronic Distribution ポリシーの優先設定 . . . 333
スケジュール設定と Tiered Electronic Distribution オブジェクト . . . 333
Tiered Electronic Distribution オブジェクトおよびスケジュールの理解 . . . 334
Tiered Electronic Distribution のスケジュール間の相互関係 . . . 339
スケジュール設定に影響する 3 つの時間要因 . . . 340
スケジュール設定の指針 . . . 344
スケジュール設定に関する問題 . . . 346
スケジュール設定とサーバポリシー . . . 353
ポリシースケジュールと Distribution スケジュールの比較 . . . 353
サーバポリシーのスケジュール設定 . . . 354
デフォルトパッケージスケジュールの編集 . . . 354

9 変数 355

変数の理解 . . . 355
変数を使用する理由 . . . 355
変数の使用 . . . 356
変数の使用方法の違い . . . 358
使用する変数を決定する際の優先順位 . . . 358
Distribution の変数の例 . . . 358
変数の種類 . . . 359
定義済みの変数 . . . 359
ユーザ定義変数 . . . 360
変数の定義 . . . 361
すべての Subscriber に関するデフォルトの変数の定義 . . . 361
特定の Subscriber の変数の定義 . . . 362
Server Software Package の変数の定義 . . . 362
iManager でのすべての変数の表示 . . . 363
変数を使用した Subscriber のコンソールプロンプトの変更 . . . 363
変数を使用したファイルの抽出の制御 . . . 363

10 ZENworks Database 365

ZENworks データベースの理解 . . . 365
データベースエンジン . . . 365
データベースファイル . . . 365
データベースオブジェクト . . . 366
データベースの実行 . . . 366
データベースのキャッシュ . . . 366
データベース情報 . . . 366
データベースの共存 . . . 367
必要なデータベースの数の決定 . . . 368
データベースのログの記録と Tiered Electronic Distribution のレポーティング . . . 368
複数のデータベース . . . 369

Server Management データベースのインストールと接続 371
データベースのインストール 372
データベースへの接続 373
ZENworks データベースオブジェクトの作成 374
データベースのパージ 375
Tiered Electronic Distribution の情報 375
サーバポリシー情報 375

11 レポート機能 379
Policy and Distribution Services のレポーティングの理解 379
レポーティングカテゴリ 379
レポーティングスコープ 380
レポートへのアクセス 380
レポート情報の作成と保存 380
レポートの説明 381
Tiered Electronic Distribution レポート 381
サーバポリシーレポート 383
レポートの生成 386
カスタマイズしたレポートの作成 387
デフォルトの Sybase データベースのユーザ ID およびパスワード 387
サーバポリシーデータベースの内容 388
Tiered Electronic Distribution データベースの内容 394

A Distribution のタイプ 399
Desktop Application 399
File 400
New Target 400
Add Directory 400
Add Files 401
削除 401
Synchronize Directories 401
Verify Distributions 401
Retry __ Times 402
Kill Connection on Open Files 402
Maintain Trustees 402
Error Handling 402
FTP 402
New FTP Source 403
New Target 403
Add Directory 403
Add Files 403
削除 403
プロパティ 403
Files To Be Distributed 403
Binary Transfer 404
Include Symbolic Link Files 404
HTTP 404
New Target 404
Add Directory 404
Add Files 404
削除 405
Files To Be Distributed 405
MSI 405
追加 405
削除 405
設定 405
並べ替え 408

ポリシーパッケージ . . . 408
Up/Down . . . 408
Add . . . 409
削除 . . . 409
プロパティ . . . 409
The Following Policy Packages Will Be Distributed . . . 409
RPM . . . 409
Up/Down . . . 409
Add From Distributor . . . 409
Add From FTP Site . . . 409
削除 . . . 409
Selected Packages . . . 410
Installation Parameters . . . 410
Software Package . . . 410
Up/Down . . . 410
Add . . . 410
削除 . . . 410
Selected Software Packages . . . 410

B スケジュールタイプ 411
曜日 . . . 412
イベント . . . 412
間隔 (Interval) . . . 413
月 . . . 413
Never . . . 413
パッケージスケジュール . . . 413
相対 (Relative) . . . 414
すぐに実行 (Run Immediately) . . . 414
Time . . . 414
週 . . . 415
年 . . . 415

C サーバコンソールコマンド 417
ZENworks Server Management コンソールコマンド . . . 417
Java コンソールコマンド . . . 420

D ロード / アンロードアクション 421
Load NLM/Process . . . 421
Load Java Class . . . 422
Unload Process . . . 422
Start Service . . . 422
Stop Service . . . 422

E Server Software Packages の要件 423
オペレーティングシステム . . . 423
Memory (RAM) . . . 426
ディスク領域 . . . 426
SET Commands . . . 427
レジストリ . . . 427
File . . . 428
Products.dat . . . 428

F Server Software Package コンポーネントのレジストリエントリ 429
Key . . . 429
Binary . . . 430
Expand String . . . 430
(Default) . . . 431
DWord . . . 431

Multi-Value String 431
String 432

G ドキュメントの更新 433
2004年2月11日 433
インストール後の設定 433
Novell iManager 434
Tiered Electronic Distribution 434
Desktop Application Distribution 435
レポート機能 435
Distributionのタイプ 435
2004年11月10日 435
Desktop Application Distribution 435
2004年9月2日 436
2004年7月28日 436
Tiered Electronic Distribution 436
Server Policies（サーバポリシー） 436

パート II Server Inventory

12 Server Inventoryの理解 439
Server Inventory用語 439
Server Inventoryのコンポーネントの概要 441
Inventory Scanner 441
インベントリサーバ上のインベントリコンポーネント 441
Inventory Database 442
管理コンソール 442
インベントリスキャンサイクルの理解 442
インベントリサーバの役割の理解 443
ルートサーバ 443
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ） . . . 444
中間サーバ 445
データベースが接続されている中間サーバ 446
Intermediate Server with Inventoried Servers
（インベントリ対象サーバが接続されている中間サーバ） 447
Intermediate Server with Database and Inventoried Servers
（データベースとインベントリ対象サーバが接続されている中間サーバ） 448
リーフサーバ 449
データベースが接続されているリーフサーバ 450
スタンドアロンサーバ 451
インベントリサーバの役割の早見表 452

13 Server Inventoryのセットアップ 453
Server Inventoryの展開 453
単純な展開 453
高度な展開 457
Server Inventoryのインストールの効果の理解 474
Inventory Serviceの開始と停止 476
インベントリサーバの役割変更 478
インベントリデータベースのセットアップ 487
Sybaseインベントリデータベースのセットアップ 488
Oracle 8iインベントリデータベースの設定 494
Oracle 9iインベントリデータベースのセットアップ 498
MS SQL Server 2000インベントリデータベースのセットアップ 502
Inventory Serviceオブジェクトの設定 507
データベース場所ポリシーの設定 508
Server Inventoryポリシーの設定 509

ロールアップポリシーの設定 . . . 511
ディクショナリ更新ポリシーの設定 . . . 513
ディクショナリの配布の設定 . . . 514

14 Server Inventory コンポーネントの理解 517
Inventory Service Manager の理解 . . . 517
サービスのリスト . . . 517
NetWare インベントリサーバ上のサービス . . . 518
Windows インベントリサーバ上のサービス . . . 519
Server Configuration Service の理解 . . . 520
Inventory Scanner の理解 . . . 520
インベントリスキャンプロセス . . . 520
NetWare インベントリ対象サーバに対するスキャン . . . 521
Windows インベントリ対象サーバに対するスキャン . . . 523
Sender-Receiver の理解 . . . 527
Sender の理解 . . . 529
Receiver の理解 . . . 530
圧縮されたスキャンデータファイルの理解 . . . 530
Sender-Receiver のディレクトリ . . . 531
Selector の理解 . . . 532
Storer の理解 . . . 534
Dictionary Provider と Dictionary Consumer について . . . 534
Upgrade Service の理解 . . . 535
インベントリサーバ上のインベントリコンポーネントの概要 . . . 535
インベントリデータベースの理解 . . . 536

15 ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解 537
概要 . . . 537
CIM スキーマ . . . 538
CIM 対リレーショナルマッピング . . . 541
ZENworks 6.5 Server Management のインベントリデータベーススキーマ . . . 545
ZENworks 6.5 Server Management での CIM スキーマ実装のケーススタディ . . . 545
スキーマ図の凡例 . . . 548
ZENworks 6.5 Server Management の CIM と拡張スキーマのスキーマ図 . . . 549
ソフトウェアインベントリのスキーマ . . . 556
インベントリデータベースの照会例 . . . 561

16 インベントリ情報の管理 571
インベントリ用に配備されたインベントリサーバの表示 . . . 571
スキャンするハードウェアインベントリ情報のカスタマイズ . . . 572
DMI を使ったベンダ固有の資産情報のスキャン . . . 572
Jaz および Zip ドライブベンダのハードウェアスキャン情報のカスタマイズ . . . 574
モニタのサイズに関するハードウェア情報のカスタマイズ . . . 575
ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ . . . 576
ZENworks ソフトウェアディクショナリとは . . . 577
ソフトウェアディクショナリルールとは . . . 578
ソフトウェア識別情報とは . . . 578
キー ID とは . . . 578
不明なソフトウェアとは . . . 578
継承されたルールとは . . . 578
優先されるルールとは . . . 579
ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解 . . . 579
ソフトウェアディクショナリパターンタイプについて . . . 585
ソフトウェアディクショナリのルールの設定 . . . 586
ファイルとソフトウェアのデフォルトマッピングルールの無視 . . . 589
ソフトウェアディクショナリ (Software Dictionary) . . . 589
[Report Files with These File Extensions As Unidentified Software] . . . 593

[Manage Unidentified Software] . . . 594
複数のソフトウェアバージョンのレポート . . . 595
[Report Disk Space Used by File Extensions] . . . 598
ソフトウェアスキャンフィルタ - [Drives and Directories] . . . 599
ソフトウェアスキャンフィルタ - [File Extensions] . . . 603
ソフトウェアスキャンフィルタ - [Files] . . . 605
ソフトウェアスキャンフィルタ - [Software] . . . 606
ディスク使用状況スキャンフィルタ - [Drives and Directories] . . . 607
ディスク使用状況スキャンフィルタ - [Files] . . . 611
[Vendor Name Aliases] . . . 613
[Software Name Aliases] . . . 614
[Reconcile Software] . . . 615
テーブル内のエントリのソート . . . 616
テーブル内のエントリのフィルタ処理 . . . 616
テーブル内のエントリの更新 . . . 617
ソフトウェアディクショナリの展開に関する基準の設定 . . . 617
[Inventory Summary] でのソフトウェアインベントリ情報の表示 . . . 619
ソフトウェアインベントリレポートの生成 . . . 619
ZENworks for Servers 3.*X*インベントリ対象サーバのスキャン対象ソフトウェアインベントリ情報のカスタマイズ . . . 621
インベントリデータベースからの重複するインベントリ対象サーバの削除 . . . 621
Inventory Removal Service プロセスについて . . . 622
Inventory Removal Service を使用した同期 . . . 622

17 インベントリ情報の表示 625

ConsoleOne を使用したインベントリ情報の表示 . . . 625
インベントリデータベースの設定 . . . 625
インベントリ対象サーバのインベントリサマリの表示 . . . 626
データベース照会によるインベントリ対象サーバのインベントリ情報の表示 . . . 638
インベントリレポートの実行 . . . 641
インベントリ情報のエクスポート . . . 653
インベントリ情報のエクスポート手順 . . . 653
既存の環境設定ファイルのロード . . . 656
インベントリサーバからの Data Export プログラムの実行 . . . 657
XML の概要と XML ファイルの内容 . . . 658
CIM スキーマを使用しないインベントリデータベースからのインベントリ情報の取得 . . . 660
インベントリビューのリスト . . . 661
インベントリビューの使用方法 . . . 684

18 ステータスログによる Server Inventory の監視 685

インベントリ対象サーバのスキャンステータスの表示 . . . 685
インベントリサーバのロールアップ履歴の表示 . . . 686
インベントリサーバのインベントリコンポーネントのステータス表示 . . . 686
インベントリ対象サーバでの最新スキャンステータスの表示 . . . 687
インベントリサーバのロールアップログの表示 . . . 687
インベントリステータスログファイルのエクスポート . . . 688
ステータスログおよびスキャンログの概要 . . . 688
XML 形式でのステータスログの表示 . . . 689

H パフォーマンスに関するヒント 691

データベースパラメータの調整に関するヒント . . . 691
NetWare および Windows 環境の Sybase . . . 691
Windows 環境の Oracle . . . 693
Oracle データベースのパフォーマンスの最適化 . . . 694
Windows 環境の MS SQL . . . 695
Inventory ConsoleOne ユーティリティのパフォーマンスに関するヒント . . . 695
Inventory Reports のパフォーマンスに関するヒント . . . 696

Inventory Data Export のパフォーマンスに関するヒント 696
インベントリ照会のパフォーマンスに関するヒント 696
参考資料 697

I Inventory Scanner で収集されるハードウェア情報 699
NetWare インベントリ対象サーバで収集されるハードウェア情報 699
Windows インベントリ対象サーバで収集されるハードウェア情報 704

J ZENworks 6.5 Server Management の Inventory 属性 715

K 列挙値 733
General-System Information-Management Technology の列挙値 733
General-Inventory Information-Scan Mode の列挙値 734
Software-Operating Systems-Windows - Name の列挙値 734
Installation Repository の列挙値 734
Hardware-Display Adapter-Video Architecture の列挙値 734
Hardware-Display Adapter-Video Memory Type の列挙値 735
Hardware-Pointing Device-Name の列挙値 735
Hardware-Battery-Chemistry の列挙値 735
Hardware-Processor-Processor Family の列挙値 735
Hardware-Processor-Upgrade Method の列挙値 736
Hardware-Chassis-Chassis Type の列挙値 736
Hardware-Bus-Protocol Supported の列挙値 736
Hardware-Processor-Role の列挙値 736
System-System Cache-Level の列挙値 737
System-System Cache-Cache Type の列挙値 737
System-System Cache-Replacement Policy の列挙値 737
System-System Cache-Read Policy の列挙値 737
System-System Cache-Write Policy の列挙値 737
System-System Cache-Associativity の列挙値 737
System-System IRQ-Availability の列挙値 738
System-System IRQ-IRQ Trigger Type の列挙値 738
System-System DMA-Availability の列挙値 738
Language の列挙値 738

L ドキュメントの更新 743
2005 年 2 月 11 日 743
2004 年 11 月 10 日 744
2004 年 9 月 2 日 745
2004 年 7 月 28 日 745

パート III Remote Management（リモート管理）

19 NetWare サーバのリモート管理 749
RConsoleJ コンポーネントの概要 749
RConsoleJ クライアント 749
RConsoleJ Agent 750
RConsoleJ Proxy Agent 750
RConsoleJ の設定 750
RConsoleJ Agent のロード 750
RConsoleJ Client の実行 751
プロキシサーバへの RConsoleJ Proxy Agent のロード 751
RConsoleJ 752
シナリオ 1:IP NetWare サーバを制御する IP クライアント 752
シナリオ 2:IPX NetWare サーバを制御する IP クライアント 754
起動時のエージェントのロード 755
起動時の RConsoleJ Agent のロード 755

起動時の RConsoleJ Proxy Agent のロード 756
RConsoleJ のセキュリティの設定 756
リモート NetWare サーバの管理 756
サーバのネイティブ言語でのコンソールコマンドの送信 757
RConsoleJ Client とターゲット NetWare 画面との同期 757

20 Windows サーバのリモート管理 759

Remote Management の用語 759
Windows サーバのリモート管理の理解 760
Remote Management のセキュリティの設定 761
Remote Management ポリシーの設定 761
管理対象サーバでのエージェントのパスワードの設定 764
リモート Windows サーバの管理 765
Remote Management セッションの開始 765
Windows XP SP2 での動作 767
Remote Management ポートの設定 767
Remote View セッションの管理 768
Remote Control セッションの管理 771
リモートオペレータ識別情報の表示 779
Remote Management セッションの監査ログの表示 779
Remote Management のパフォーマンスの向上 779
Remote Management Agent のシャットダウンと再起動 780

M ドキュメントの更新 783

2005 年 2 月 11 日 783
Windows サーバのリモート管理 784
2004 年 9 月 2 日 784

パート IV [Management and Monitoring Services]

21 Management and Monitoring Services の設定 787

Management and Monitoring Services の理解 787
Management Site Services 787
Server Management 791
Traffic Analysis 791
Novell ConsoleOne 792
設定の計画 792
必要な管理情報の定義 793
ネットワーク管理戦略の計画 793
役割ベース管理 795
Novell ZENworks の管理サイト 796
Novell ZENworks Server Management の一般的な役割 797
Novell ZENworks Server Management の役割ベースモジュールと役割 798
役割ベース管理の設定 809
Management and Monitoring Services の設定 811
Management and Monitoring Services の停止と起動 812
検出プロセスのセットアップとバックエンドプロセスの起動 812
アラーム管理システムのセットアップ 813
監視のセットアップ 814
Traffic Analysis Agent のセットアップ 814

22 Novell ConsoleOne での Management and Monitoring Services の使用 817

Novell ZENworks Server Management のネームスペースについて 817
Novell ZENworks Server Management のオプションの選択 819
ビュー 819
プロパティ 820
アクション 820

ビューの使用 . . . 821
ビューの外観の変更 . . . 821
列の変更 . . . 822
ビューのフィルタ処理 . . . 823
ビューのソート . . . 824
ビューの印刷 . . . 825
ビューのエクスポート . . . 825
ビューの保存 . . . 825
カスタムビューの削除と名前の変更 . . . 826
Novell ConsoleOne のビューへの複数ビューの表示 . . . 826

23 ネットワーク検出とアトラス管理の理解 829

ネットワーク検出の理解 . . . 830
Discovery コンポーネント . . . 830
検出プロセス . . . 840
検出されるネットワークオブジェクト . . . 847
ファイルベースの検出 . . . 855
Discovery Console . . . 857
マップに反映される検出結果 . . . 860
検出のセットアップ . . . 862
検出の開始 . . . 864
初期検出のステータスの確認 . . . 864
検出結果の確認 . . . 865
デフォルト設定の変更 . . . 866
Java プロセスの設定 . . . 872
管理サーバのアンロード . . . 874
アトラスの管理 . . . 874
アトラスの使用 . . . 874
統合ビューの使用 . . . 881

24 アラーム管理の理解 883

アラーム管理システムの理解 . . . 883
アラーム管理システムのコンポーネント . . . 884
アラーム管理システムの管理 . . . 887
アラームインジケータの認識 . . . 888
アラームの表示 . . . 888
アラームの有効化と無効化 . . . 893
アラームの解決 . . . 893
アラームの削除 . . . 896
アラームに関するアクションの実行 . . . 897
アラーム管理システムの維持 . . . 906
アラーム管理システムのトラブルシューティング . . . 906

25 サーバ管理の理解 907

サーバ管理の理解 . . . 908
SNMP ベースのサーバ管理 . . . 909
SNMP エージェントの機能 . . . 910
サーバ管理の計画 . . . 910
通常のサーバアクティビティ基準の作成 . . . 911
基準ドキュメントの使用 . . . 911
サーバ基準ドキュメントに関するヒント . . . 911
サーバ管理の最適化 . . . 913
デフォルトのトレンドとしきい値の設定 . . . 913
アラーム生成の管理 . . . 917
SNMP アラームの受信先の定義 . . . 919
サーバの管理 . . . 920
サーバ設定情報の表示 . . . 920
概要データの表示 . . . 921

トレンドデータの表示 922
トレンドデータのサンプル収集の管理 925
サーバのパラメータの設定 926
サーバコマンドの実行 927
Management Site Server のステータス 928
オブジェクトの階層構造とビューの詳細 929
オブジェクトの階層構造 929
オブジェクトビューの詳細 930

26 MIB ツールの使用 951

MIB ツールの理解 951
MIB について 951
SNMP MIB Compiler の理解 952
SNMP MIB Browser の理解 953
MIB ツールを使ったデバイスの管理 955
トラップの定義 956
MIB の設定と MIB ツールのセットアップ 961
Novell ZENworks Server Management と統合するためのサードパーティ MIB の注釈付け 961
SNMP 対応ノードの MIB のコンパイル 962
MIB Browser の使用 963
MIB ツリーの参照 964
オブジェクトとその子ノードの値の表示 965
オブジェクト値のセットアップによるノードの設定 966
SNMP 初期設定の変更 967
SNMP テーブルのインスタンスの変更 967
スカラオブジェクトのテーブルの作成 970
SNMP リクエスト結果のグラフ表示 971
テーブルおよびグラフへのプロファイルの使用 972
MIB の保持 973

27 Monitoring Services 975

Monitoring Services の理解 975
Monitoring Services の使用に関する役割ベースのサービス 977
ターゲットノード上のサービスの監視 977
サービスを監視するターゲットノードの定義 978
テスト結果データの表示 979
ノードのテストオプションの変更 980
監視するサービスの追加 980

28 トラフィック分析の理解 981

トラフィック分析の理解 981
トラフィック分析コンポーネント 981
トラフィック分析コンポーネント間の通信 983
トラフィック分析機能 984
トラフィック分析の基礎知識 985
セグメント監視の計画 995
通常のセグメントアクティビティ基準の作成 995
基準ドキュメントの使用 996
セグメント基準ドキュメントに関するヒント 997
ネットワークトラフィックの分析の準備 998
優先 RMON エージェントの選択 998
SNMP パラメータの設定 999
ネットワークトラフィックの分析 1000
セグメントのトラフィックの分析 1001
セグメントに接続されたノードのトラフィックの分析 1010
パケットのキャプチャ 1017
キャプチャされたパケットの表示 1021

ネットワークのプロトコルによって生成されたトラフィックの分析 . . . 1028
スイッチ上のトラフィックの分析 . . . 1032
トラフィック分析の最適化 . . . 1034
セグメント上のステーションを表示するオプションの選択 . . . 1034
トレンド統計を表示するオプションの選択 . . . 1036
上位ノードグラフを表示するオプションの選択 . . . 1039
[Unified Port Traffic] ビューで表示する統計を選択する . . . 1040
キャプチャされたパケットを表示するオプションの選択 . . . 1041
[Set Alarm] ダイアログボックスでのアラームオプションの設定 . . . 1041
[Monitor Nodes for Inactivity] ビューの設定 . . . 1044
Traffic Analysis Agent の理解 . . . 1045
NetWare 版 Traffic Analysis Agent の使用 . . . 1047
NetWare 版 Traffic Analysis Agent のインストール計画 . . . 1048
NetWare 版 Traffic Analysis Agent のパフォーマンスの最適化 . . . 1048
NetWare 版 Traffic Analysis Agent のコンソールユーティリティの使用 . . . 1056
Windows 版 Traffic Analysis Agent の使用 . . . 1062
インストール時の変更 . . . 1063
Windows 版 Traffic Analysis Agent のインストール計画 . . . 1064
Windows 版 Traffic Analysis Agent の最適化 . . . 1067
LANZCON の使用 . . . 1070

29 エージェントの環境設定のカスタマイズ 1073

エージェントのファイル . . . 1073
NetWare 版 Management Agent のファイル . . . 1073
Windows サーバ版 Management Agent のファイル . . . 1075
NetWare 版 Management Agent のカスタマイズ . . . 1076
servinst.nlm のロードパラメータ . . . 1076
hostmib.nlm のロードパラメータ . . . 1077
ntrend.nlm のロードパラメータ . . . 1077
Windows サーバ版 Management Agent のカスタマイズ . . . 1078
Windows サーバ版 Management Agent の設定 . . . 1079
カスタムイベントログタイプからのイベント収集 . . . 1079
Nttrap.ini ファイルにおける否定のフィルタ条件の指定 . . . 1080
サードパーティのエージェントの設定 . . . 1080
トラップを受信できることの確認 . . . 1080
ベンダ固有の SNMP トラップの統合 . . . 1080
Advanced Trending Agent . . . 1081
Advanced Trending Agent について . . . 1081
トレンド変数の設定 . . . 1081
Linux 上での Advanced Trending Agent の設定 . . . 1082
すべてのプラットフォーム上での Advanced Trending Agent の設定 . . . 1083
クイックリファレンステーブル . . . 1084
設定の更新 . . . 1085
Advanced Trending Agent のインストール . . . 1086
Management and Monitoring Services for Linux . . . 1086
リアルタイム統計情報の提供 . . . 1086
システムイベントのトラップの生成 . . . 1087
履歴収集情報の提供 . . . 1089
[Linux Management] ビュー . . . 1090
Linux Server Health Report . . . 1090

30 Novell ZENworks Server Management でサポートされるプロトコルデコードスイート 1091

Novell NetWare プロトコルスイート . . . 1091
Network File System プロトコルスイート . . . 1093
Systems Network Architecture プロトコルスイート . . . 1094
AppleTalk プロトコルスイート . . . 1094
TCP/IP プロトコルスイート . . . 1096

31 Novell ZENworks Management and Monitoring Services データベース 1101
Novell ZENworks Server Management データベースの理解 1101
データベースの実行 1101
データベースのキャッシュ 1102
データベースのバックアップ 1102
トポロジ / アラームデータベースのバックアップ 1102
データベースパスワードの変更 1102
データベースを空にする 1103

32 Management and Monitoring Services でのレポートの使用 1105
Management and Monitoring Services のレポートの理解 1105
トポロジレポートについて 1105
アラームレポートについて 1108
ヘルスレポートについて 1109
レポートの管理 1111
トポロジレポートの管理 1111
Server Management のヘルスレポートの管理 1112

33 SNMP コミュニティ文字列の使用 1119
SNMP コミュニティ文字列について 1119
SNMP のセキュリティ 1120
SNMP コミュニティ文字列の設定 1120
SNMP コミュニティ文字列の設定 :Novell NetWare サーバ 1120
SNMP コミュニティ文字列の設定 :Novell ConsoleOne 1122
個々のノードのコミュニティ文字列の設定 1123
SNMP コミュニティ文字列の設定 :Windows: 1123

34 View Builder の理解 1125
Name-Value Pairs View コンポーネントの作成 1127
名前と値のペアの追加 1128
Name-Value Pairs View コンポーネントの編集 1129
Name-Value Pairs View の削除 1129
Alarm View コンポーネントの作成 1129
Alarms View コンポーネントの編集 1130
Alarm View コンポーネントの削除 1130
Table View コンポーネントの作成 1130
Table View の編集 1131
Table View の削除 1131
Graph View コンポーネントの作成 1132
グラフの詳細の追加 1132
Graph View コンポーネントの編集 1133
Graph View コンポーネントの削除 1133
ビューを表示する条件の設定 1133

N ドキュメントの更新 1135
2004 年 9 月 2 日 1135
2004 年 7 月 28 日 1135

このガイドについて

このガイドでは、Novell® ZENworks® 6.5 Server Management を管理する方法について説明します。このガイドはネットワーク管理者を対象としており、次の章で構成されています。

- 23 ページの「Policy and Distribution Services」
- 437 ページの「Server Inventory」
- 747 ページの「Remote Management（リモート管理）」
- 785 ページの「[Management and Monitoring Services]」

表記規則

Novell のマニュアルでは、大なり記号 (>) を使用して、手順説明の個々の操作や、相互参照パスの項目を区切ります。

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は、サードパーティの商標であることを示します。

プラットフォームによってバックスラッシュで表記する場合とスラッシュで表記する場合があるパス名は、バックスラッシュで表記します。Linux*、UNIX* など、スラッシュを使う必要があるプラットフォームを使用しているユーザは、必要に応じてスラッシュを使用してください。

ご意見の宛先

本マニュアルおよび本製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインドキュメントの各ページの下部にある「ご意見の宛先」機能をご利用いただくか、www.novell.com/documentation/feedback.html にアクセスして、ご意見をご記入ください。

ドキュメントの更新

このガイドに対する更新の日付入りリストは、次の項を参照してください。

- Policy and Distribution Services: 433 ページの付録 G、「ドキュメントの更新」
- Server Inventory: 743 ページの付録 L、「ドキュメントの更新」
- リモート管理：783 ページの付録 M、「ドキュメントの更新」
- Management and Monitoring Services: 1135 ページの付録 N、「ドキュメントの更新」

このガイドの最新バージョンについては、ZENworks 6.5 Web サイト (http://www.novell.com/documentation/zenworks65/index.html) を参照してください。

関連ドキュメント

ZENworks 6.5 Server Management のインストールおよび実行に関する最新の情報については、『*ZENworks 6.5 Server Management インストールガイド* (http://www.novell.com/documentation/zenworks65/index.html)』を参照してください。

Policy and Distribution Services

Novell® ZENworks® 6.5 Server Management Policy and Distribution Services は、サーバのソフトウェア、環境設定、および動作の管理システムです。Policy and Distribution Services を使用して、以下の作業を行うことができます。

- ネットワーク全体のサーバにインストールされているソフトウェアのバージョンを管理する
- 特定のサーバのセットについて標準的な環境設定を定義して適用する
- サーバの停止、ボリュームのバックアップ、しきい値を超過した場合の管理など、特定の状況でのサーバの動作を制御する

Policy and Distribution Services は、次の 3 つのコンポーネントで構成されています。

- **Tiered Electronic Distribution:** データの配信およびサーバポリシーの適用を容易にします。
- **Server Policies:** サーバの環境設定および管理を容易にします。
- **Server Software Packages:** ソフトウェアのインストールを容易にします。

Policy and Distribution Services を管理するには、次のいずれかを使用します。

- **ConsoleOne 1.3.6。** ZENworks Server Management オブジェクトを作成および設定したり、Policy and Distribution Services の管理タスクを実行したりできます。
- **Novell iManager 2.0.2 の ZENworks Server Management の役割。** Internet Explorer 5.5 以降を使用できる任意のワークステーションから iManager を使用して Policy and Distribution Services の管理タスクを実行できます。

Policy and Distribution Services のドキュメントは次の章で構成されています。

- 1 章 25 ページの「インストール後の設定」(ZENworks 6.5 Server Management をはじめてインストールした場合は、この章を参照してポリシーおよび配布システムを設定してください。)
- 2 章 69 ページの「Novell iManager」
- 3 章 87 ページの「Tiered Electronic Distribution」
- 4 章 197 ページの「Server Policies (サーバポリシー)」
- 5 章 241 ページの「Server Software Package に関する問題」
- 6 章 283 ページの「Desktop Application Distribution」
- 7 章 313 ページの「Policy and Distribution Services のセキュリティ」
- 8 章 331 ページの「スケジュール設定」
- 9 章 355 ページの「変数」

- 10 章 365 ページの「ZENworks Database」
- 11 章 379 ページの「レポート機能」
- 399 ページの付録 A、「Distribution のタイプ」
- 411 ページの付録 B、「スケジュールタイプ」
- 417 ページの付録 C、「サーバコンソールコマンド」
- 421 ページの付録 D、「ロード / アンロードアクション」
- 423 ページの付録 E、「Server Software Packages の要件」
- 429 ページの付録 F、「Server Software Package コンポーネントのレジストリエントリ」
- 433 ページの付録 G、「ドキュメントの更新」

1 インストール後の設定

Novell® ZENworks® Server Management の Tiered Electronic Distribution 機能を効果的に使用するには、ネットワークにコンポーネントを正しくインストールして設定する必要があります。まず、Policy and Distribution Services の基本的なインストールを実行します（『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」を参照してください。

ポリシーの設定については、4 章 197 ページの「Server Policies（サーバポリシー）」を参照してください。

この章では、Tiered Electronic Distribution システムを設定する際に役立つ概念、計画ワークシート、および設定手順について説明します。詳細については、3 章 87 ページの「Tiered Electronic Distribution」を参照してください。

次の節の情報を利用して、必要に応じた新規 Distributor の追加と Subscriber ソフトウェアのインストール、Distributor のルーティング階層の設定、および Distribution の作成と送信を行うことができます。

- 25 ページの「配布システムの計画」

  この節では、計画ワークシートを使用して決定事項を管理します。この計画ワークシートの情報を使用することで、設定を計画どおりに簡単に実行できます。

- 46 ページの「配布システムの設定」

  この節では、配布システムの設定手順について説明します。

- 58 ページの「配布システムの管理」

  この節では、Novell ConsoleOne® と Novell iManager を使用した配布システムの管理方法について概要を説明します。

- 58 ページの「設定計画ワークシート」

  計画ワークシートには、各ワークシート項目の基本的な情報が含まれています。また、ワークシート項目のより詳しい情報を参照するためのリンクも含まれています。

  ワークシートには計画情報のみが含まれ、計画されない手順の情報は含まれないため、ワークシートを46 ページの「配布システムの設定」の手順の代わりに使用することはできません。

配布システムの計画

次の節を順に参照してください。

1. 26 ページの「概要」
2. 28 ページの「Distribution の選択」
3. 33 ページの「ネットワークトポロジの理解」

4. 34 ページの「追加の Distributor の必要性」
5. 37 ページの「他の Subscriber のイントールの必要性」
6. 38 ページの「配布フローの決定」
7. 40 ページの「Distribution のセキュリティの理解」
8. 42 ページの「Distribution の Channel の決定」
9. 43 ページの「Subscriber の登録の決定」
10. 44 ページの「配布スケジュールの決定」

概要

Policy and Distribution Services は、次の 3 つのコンポーネントで構成されています。

- **Tiered Electronic Distribution:** ネットワーク用の配布システムです。
  - サーバ間で電子データを配布して、ネットワークサーバを管理する方法です。
  - 効率的な配布のために、階層アーキテクチャを使用します。たとえば、1 つのサーバが他の多数のサーバを処理し、それらの各サーバもさらに多くのサーバを処理するというような、多階層による負荷の共有などを使用します。
  - オフピーク時の配布など、帯域幅の効率的な利用を目的とした Distribution のスケジュールが可能です。
  - Distribution に対して未承認の変更が加えられることを防ぎます。
- **Server Policies:** サーバの設定および動作を管理するためのシステムです。
- **Server Software Packages:** ソフトウェアのサーバへのインストールおよびアップグレードを自動化する機能です。

大半のポリシーおよびすべての Server Software Package は配布されるため、これらのコンポーネントのいずれかを使用する場合は、通常 Tiered Electronic Distribution が必要になります。したがって、この章では主に Tiered Electronic Distribution を理解し、設定するための情報を提供します。Policy and Distribution Services を構成する他の 2 つのコンポーネントの詳細については、次の各章を参照してください。

- 4 章 197 ページの「Server Policies（サーバポリシー）」
- 5 章 241 ページの「Server Software Package に関する問題」

次の節では、Tiered Electronic Distribution を理解し、設定するうえで必要な基本的情報について説明します。

- 26 ページの「配布可能なデータ」
- 27 ページの「データの配布方法」
- 27 ページの「配布システムの計画に必要な情報」

配布可能なデータ

Tiered Electronic Distribution を使用して、次の種類の電子データを配布できます。

Distribution タイプ	配布内容
Desktop Application	ZENworks Desktop Management で作成されたデスクトップアプリケーションオブジェクトおよびファイル

Distribution タイプ	配布内容
File	Distributor サーバのファイルシステム内にあるファイルとディレクトリ
FTP	FTP ソースのファイルとディレクトリ
HTTP	HTTP ソースのコンテンツ
MSI	MSI エンジンによって Windows* 環境にインストールされるソフトウェア
ポリシーパッケージ	サーバを制御するポリシー
RPM	Linux および Solaris* サーバの RPM パッケージ（RPM が Solaris コンピュータにインストールされている場合は Solaris のみ）
Software Package	ソフトウェアを自動的にサーバにインストールまたはアップグレードするための Server Software Packages

このリストから、サーバに配布できる電子データにはさまざまなタイプがあることがわかります。

データの配布方法

Tiered Electronic Distribution では、Distribution ファイルが Distributor サーバから Subscriber サーバに送信されます。基本的な配布プロセスは次の通りです。

1. 配布するデータを決定します。
2. Distribution を作成します。
3. Distribution の Channel を作成します。
4. この Distribution を必要とする Subscriber を決定します。
5. Subscriber サーバを Distribution の Channel に登録します。
6. 適切なスケジュールが設定されていることを確認します（構築、送信、および抽出）。
7. Distributor を更新して、Distribution を送信します。これにより、Distribution が Distribution の構築スケジュールに基づいて構築され、Channel の送信スケジュールに基づいて送信されます。
8. Subscriber の抽出スケジュールに基づいて Subscriber サーバで Distribution が抽出されます。
9. Distribution タイプに基づいて、Subscriber サーバで Distribution が使用されます。

このプロセスから、いくつかの Tiered Electronic Distribution コンポーネントを作成および設定する必要があることがわかります。詳細については、90 ページの「基本配布プロセス」および 176 ページの「配布プロセスの理解」を参照してください。

配布システムの計画に必要な情報

- 必要な Distribution。次に例を示します。
  - サーバファイル、HTTP コンテンツ、FTP コンテンツ、または RPM パッケージのいずれを配布するか

- デスクトップアプリケーションを配布するかどうか(複数のツリーがある場合、Subscriber オブジェクトの設定方法に影響します)
- サーバ管理に必要なポリシー
- インストールを自動化する必要があるサーバソフトウェア

- 追加の Distributor が必要かどうか
- 環境内にNovell eDirectory™ 8.7.3とNDS® 6.*x*または7.*x*が混在しているかどうか(両方が存在すると Distributor に悪影響を及ぼしますが、回避策はあります)
- レポート目的で必要なデータベース数
- Subscriber ソフトウェアをサーバにインストールする必要があるかどうか
- どの Subscriber にどの Distribution が必要か
- ネットワークのトポロジ(サーバプラットフォーム、低速 WAN、ファイアウォール、NAT(Network Address Translation)、複数のツリーなど)
- Tiered Electronic Distribution によって生じる可能性のあるシステムリソース問題とサーバの動作問題
- 特定のサーバ用に Distribution を暗号化する必要があるかどうか
- Distribution のチャネリングに Subscriber Group を使用できるかどうか
- Distribution の Subscriber サーバへの送信方法(階層配布モデル)
- ネットワークトラフィックを最小化するための配布プロセスのスケジュール方法(業務時間内など)

これらの情報を決定するには、28 ページの「Distribution の選択」に進みます。

Distribution の選択

この節では、各 Distribution タイプの基本的な情報について説明します。

Distribution を追加してから必要な Distributor を追加することで、配布システムを徐々に構築できます。新しい Distribution を追加する場合は、いつでもこのプロセスを繰り返すことができます。

58 ページの「設定計画ワークシート」を印刷してください。計画に関する節では、このワークシートに記入するよう求められます。

Distribution タイプに関する次の節を参照し、今回作成する種類を選択してください。計画ワークシートの項目は、各 Distribution タイプに用意されています。

- 29 ページの「Desktop Application」
- 29 ページの「File」
- 29 ページの「FTP」
- 30 ページの「HTTP」
- 30 ページの「MSI」
- 30 ページの「ポリシーパッケージ」
- 32 ページの「RPM」
- 32 ページの「Software Package」

Desktop Application

この Distribution タイプを使用すると、eDirectory ツリーとターゲット Subscriber サーバ上の指定の場所に、アプリケーションオブジェクトと関連ファイルを配布できます。

Desktop Management との統合については、6 章 283 ページの「Desktop Application Distribution」を参照してください。

Desktop Application タイプの Distribution については、120 ページの「Desktop Application」を参照してください。

Desktop Application Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート

Distribution でトラスティ権利を保持する場合、項目 3 および項目 20 に、Desktop Application タイプの Distribution を作成するため、Desktop Application Distribution を受信する各サーバで Subscriber オブジェクトと NCP™ サーバオブジェクトを同じツリーに配置する必要があることを記入します。

項目 19 に、作成する Distribution の種類として「Desktop Application」と記入します。また、次の情報も指定してください。

- 目的を表した Distribution の名前
- Desktop Application Distribution を必要とするサーバの名前

File

この Distribution タイプでは、Distributor サーバのファイルシステムからファイルまたはディレクトリを選択し、Subscriber サーバのファイルシステム上の選択した場所に配布できます。

Distribution ウィザードを使用して、File および FTP タイプの Distribution の作成プロセスを自動化できます。詳細については、146 ページの「Distribution ウィザードの使用」を参照してください。

File タイプの Distribution については、120 ページの「File」を参照してください。

File Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート

項目 19 に、作成する Distribution の種類として「File」と記入します。また、次の情報も指定してください。

- 目的を表した Distribution の名前
- File Distribution を必要とするサーバの名前

FTP

この Distribution タイプでは、1 つまたは複数の FTP ソースのファイルで構成される Distribution を作成できます。各ソースには、1 つまたは複数のディレクトリやファイルを含めることができます。

Distribution ウィザードを使用して、File および FTP タイプの Distribution の作成プロセスを自動化できます。詳細については、146 ページの「Distribution ウィザードの使用」を参照してください。

FTP タイプの Distribution については、121 ページの「FTP」を参照してください。

FTP Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート
項目 19 に、作成する Distribution の種類として「FTP」と記入します。また、次の情報も指定してください。 ◆ 目的を表した Distribution の名前 ◆ FTP Distribution を必要とするサーバの名前

HTTP

この Distribution タイプでは、1 つまたは複数の HTTP ソースで構成される Distribution を作成できます。各ソースには、1 つまたは複数のターゲットエントリを含むことができます。

HTTP タイプの Distribution については、122 ページの「HTTP」を参照してください。

HTTP Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート
項目 19 に、作成する Distribution の種類として「HTTP」と記入します。また、次の情報も指定してください。 ◆ 目的を表した Distribution の名前 ◆ HTTP Distribution を必要とするサーバの名前

MSI

これは MSI エンジンによって Windows 環境にインストールされる MSI パッケージの Distribution です。

MSI タイプの Distribution については、122 ページの「MSI」を参照してください。

MSI Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート
項目 19 に、作成する Distribution の種類として「MSI」と記入します。また、次の情報も指定してください。 ◆ 目的を表した Distribution の名前 ◆ MSI Distribution を必要とするサーバの名前

ポリシーパッケージ

この Distribution タイプは、Subscriber サーバに次のいずれかのポリシーを適用するメカニズムを提供します。

ポリシー	説明
Copy Files	ポリシー設定を使用して、サーバ上のファイルを特定の場所から別の場所にコピーできるようにします。
NetWare Set Parameters	サーバまたはサーバグループに対して、選択されている NetWare® 設定パラメータを指定および最適化します。
Prohibited File	指定したボリューム / ドライブまたはディレクトリ / フォルダからの許可されていないファイルの削除や移動を監視および強制します。
Scheduled Down	サーバを停止するタイミングをスケジュールしたり、停止したサーバを自動的に再起動するかどうかを指定します。
Scheduled Load/Unload	選択したサーバおよび Windows サービスの起動や停止のための NLM™ および Java* クラスプロセスをロード / アンロードする順序を自動化します。
Search	Distributor Agent を有効にして Service Location Package 内のポリシーを検出および使用するために、ZENworks Server Management で使用されます。
Server Down Process	サーバを停止する前に従うプロセスや満たす必要がある条件を制御します。
Server Scripts	サーバ上でのスクリプトの使用を自動化します。
SMTP Host	外部に発信されるインターネット電子メールを処理するリレーホストの TCP/IP アドレスを設定します。
SNMP Community Strings	SNMP 要求を受信し、応答できるようにします。
SNMP Trap Targets	レポート目的のために、関連付けられている eDirectory オブジェクトの SNMP トラップターゲットを設定します。
Text File Changes	テキストファイルの変更を自動化します。
Tiered Electronic Distribution	Distributor オブジェクトと Subscriber オブジェクトのデフォルト値を設定します。
ZENworks Database	ZENworks データベースオブジェクトとデータベースファイルへのパスを特定するための DN を設定します。データベースは、成否のログを記録するために Policy and Distribution Services で使用され、このログを使用してレポートが作成されます。 インストール時に指定されたデータベースの場所は、このポリシーを作成して有効化することにより変更できます。
ZENworks Server Management	ステータスログの記録、Policy/Package Agent のサーバコンソールプロンプトの定義、作業パスの設定、データベースのパージ範囲の設定など、Policy and Distribution Services の基本的な環境設定パラメータが含まれています。

各ポリシーの詳細については、205 ページの「サーバポリシーの説明」を参照してください。

ポリシーおよびポリシーパッケージについては、4 章 197 ページの「Server Policies（サーバポリシー）」を参照してください。

Policy Package タイプの Distribution については、123 ページの「ポリシーパッケージ」を参照してください。

Policy Package Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート

項目 19 に、作成する Distribution の種類として「Policy Package」と記入します。また、次の情報も指定してください。

- ポリシーの名前
- 各ポリシーについて、そのポリシーが必要なサーバの名前

RPM

これは、Linux または Solaris プラットフォームの Distribution です。RPM Distribution を使用して、RPM (Red Hat* Package Manager) パッケージを配布できます。

RPM タイプの Distribution については、124 ページの「RPM」を参照してください。

RPM Distribution を今回作成するかどうかを決定してください。

設定計画ワークシート

項目 19 に、作成する Distribution の種類として「RPM」と記入します。また、次の情報も指定してください。

- 目的を表した Distribution の名前
- RPM Distribution を必要とするサーバの名前

Software Package

この Distribution タイプを使用すると、ConsoleOne の Server Software Package ネームスペースで作成した Server Software Package を配布できます。まず .spk ファイルを作成し、その後に .cpk ファイルにコンパイルして配布します。

Server Software Packages の詳細については、5 章 241 ページの「Server Software Package に関する問題」を参照してください。

Software Package Distribution タイプについては、124 ページの「Software Package」を参照してください。

今回作成するソフトウェアパッケージを決定してください。

設定計画ワークシート

項目 19 に、作成する Distribution の種類として「Software Package」と記入します。また、次の情報も指定してください。

- 目的を表した Distribution の名前
- Software Package Distribution を必要とするサーバの名前

ネットワークトポロジの理解

配布システムを効率的に管理するには、ネットワークトポロジについて理解する必要があります。たとえば、次のように入力します。

- 使用しているサーバプラットフォーム。
- プラットフォームあたりのサーバ数。
- WAN リンクおよびファイアウォールに対するサーバの位置。
- NAT(Network Address Translation) の使用の有無。
- 低速ネットワークリンクの場所。

この種の情報は、ネットワークに最良の配布管理ソリューションを設定するために役立ちます。

ネットワークに関する情報を取得するには

1 Server Management のスキーマを拡張したツリーをメモします。

設定計画ワークシート
項目 1 で、Server Management のスキーマを拡張したネットワーク内のツリー名を指定します。

2 ネットワーク構造の図を作成します。

この図は、後で配布ルートを決定するときに使用します。

図には次の情報を示します。

- 低速リンクの場所
- 各 LAN 上のサーバ数
- ファイアウォール外のサーバ数
- NAT を使用しているサーバ数

3 現在のツリー構成を示す図を作成します。次のような主なコンテナを示します。

- 地理的な位置を示すコンテナ (物理的ツリー設計)
- 事業組織を示すコンテナ (論理的ツリー設計)
- サーバが存在するコンテナ (Distributor および Subscriber 用)

4 次の情報をツリー図に示します。

- Distributor 候補のサーバの場所 (Server Management の最低要件を満たす NetWare、Windows、Linux、または Solaris サーバ)
- 低速ネットワーク接続が存在するコンテナ

  これはネットワーク図で示した低速接続の場所と一致している必要があります。

5 次の情報をネットワーク図に示します。

- Distributor 候補のサーバの場所 (ツリー図で示した場所)

追加の Distributor の必要性

Policy and Distribution Services をはじめてインストールした場合、Distributor とデータベースファイルは 1 つずつインストールされます。通常、追加の Distributor は企業構造や地理的な場所に応じて必要になります。

Distributor の必要数は、Distributor サーバの負荷 (Distribution の構築作業を完了できるかどうかなど) によって決まります。たとえば、オフピーク時に構築する大規模な Distribution と、ウィルスパターンの Distribution があり、いずれもただちに送信する必要がない場合は、これらの Distribution が予定どおりに構築、送信されるように、日ごとの更新スケジュールが設定された Distributor(Distribution を 1 日に 1 度作成するため) と、新しいウィルスパターンの発見用に頻繁な更新スケジュールが設定された Distributor の、2 種類の Distributor が必要になります。

作成した図を使用して、追加の Distributor をインストールする必要があるかどうかを決定してください。

設定計画ワークシート
項目 2 で、Distributor ソフトウェアをインストールするサーバ名を指定します。

Distributor サーバで Distribution の構築と送信の負荷がどのように処理されるかを確認してから、Distributor を追加して負荷を分散するかどうかを決定できます。

Distributor ごとに、次の情報も決定する必要があります。

- 34 ページの「Distributor プロパティ」
- 35 ページの「ソフトウェアのインストールパス」
- 35 ページの「Distributor サーバで Server Management データベースをホストするかどうか」
- 36 ページの「Distributor を混在 eDirectory 環境で実行できるかどうか」

Distributor プロパティ

インストール時に、Distributor プロパティをデフォルトから次のように変更できます。

- **[Object Name]** : Distributor オブジェクトの名前を変更する場合は、そのサーバが Distributor であることなど、サーバの識別情報を名前に保持することをお勧めします。
- **[Container]** : Distributor オブジェクトがインストールされているコンテナの使用について計画します。

  Distributor として使用する Windows 2000/2003 サーバに eDirectory がインストールされていない場合、そのサーバのデフォルトのコンテナオブジェクトはインストール中に表示されません。したがって、その Distributor オブジェクトのコンテナを決定します。
- **[Working Directory]** : Distributor の作業ファイルには、デフォルトのパス以外のボリューム、ドライブ、またはディレクトリパスを使用できます。

  作業ディレクトリは、Distribution のサイズに応じてかなり大きくなる可能性があるため、十分なディスク容量を確保しておく必要があります。

  NetWare サーバのデフォルトのボリュームは sys: です。NetWare サーバでは、別のボリュームを指定することを強くお勧めします。

NetWare および Windows サーバのデフォルトの作業ディレクトリパスは、次のとおりです。

```
\zenworks\pds\ted\dist
```

Linux または Solaris サーバのパスを次に示します。

```
/var/opt/novell/zenworks/zfs/pds/ted/dist
```

Distributor の作業ディレクトリは、Distribution の作成時にも使用されます。Distribution オブジェクトの DN を使用して、作業ディレクトリの下位にサブディレクトリが作成されます。

作業ディレクトリの詳細については、190 ページの「作業ディレクトリ」を参照してください。

設定計画ワークシート
項目 7 で、デフォルトから変更する Distributor のプロパティ情報を指定します。これには、オブジェクト名、オブジェクトのコンテナ、および作業ディレクトリが含まれます。

ソフトウェアのインストールパス

Server Management では、次のデフォルトのインストールパスが使用されます。

- [NetWare] : sys:

  別のボリュームを選択できます。

- [Windows] : C:

  別のドライブを選択できます。

Linux または Solaris のパスは変更できません。

設定計画ワークシート
Distributor のインストールパスをデフォルトから変更する場合は、項目 5 でパスを指定します。パス情報には、インストールパスを変更する Distributor の識別情報を含めます。 Subscriber のインストールパスをデフォルトから変更する場合は、項目 6 でパスを指定します。パス情報には、インストールパスを変更する Subscriber の識別情報を含めます。

Distributor サーバで Server Management データベースをホストするかどうか

Server Management データベースは、ツリー内に複数保持することができ、NetWare および Windows サーバの両方にインストールできます。

データベースは、Server Policies または Tiered Electronic Distribution コンポーネントの成功と失敗をログに記録するために、Policy and Distribution Services によって使用されます。Policy and Distribution Services は、データベースを使用しなくても正常に機能します。これは、レポート用の情報を記録するためにのみ zfslog.db ファイルを使用するからです。Policy and Distribution Services の zfslog.db には、環境設定情報は含まれていません。

各 Distributor で専用のデータベースを使用するか、またはすべての Distributor で同じデータベースを共有するかどうかを決定するには、情報のレポート方法を決定する必要があります。ツリー内にいくつのデータベースが必要であるかを判断するには、次の点を検討します。

- **WAN トラフィック：** Tiered Electronic Distribution は大量のデータベースの更新を実行しないので、システムリソースに対する実際の影響は最小限です。最も大きな影響は、トランザクションの実行にかかる時間です。ただし、WAN 接続が低速である場合、WAN を介してデータベースのログの記録を実行しないことも可能です。
- **複数の Distributor：** ツリー内に複数の Distributor がある場合、それぞれに 1 つのデータベースを使用することも、1 つ以上のデータベースを共有させることもできます。必要な Distributor のレポーティングのタイプによって、それぞれに個別のデータベースを使用するかどうかが決まります。たとえば、Distributor が、送信する Distribution のタイプ専用であるかどうかなどです。
- **統合されたレポーティング：** すべての Tiered Electronic Distribution 情報についてレポートを 1 つだけ生成する場合は、WAN トラフィックの注意事項に関係なく、データベースオブジェクトとファイルを 1 つだけインストールし、すべての Tiered Electronic Distribution の Distributor ログをそのファイルに記録します。ZENworks データベースポリシー (Service Location Package) を使用して、すべての Distributor がそのデータベースファイルを使用するように指定します。
- **特殊なレポーティング：** サーバの特定の領域やグループに固有のレポートが必要になる場合があります。データベースオブジェクトとファイルを各領域にインストールし、Distributor でその領域またはサーバグループのログをそのデータベースに記録することができます。個別の ZENworks データベースポリシー (Service Location Package) を使用して、各 Distributor が適切なデータベースファイルを使用するように指定します。

詳細については、10 章 365 ページの「ZENworks Database」を参照してください。

重要： [Subscriber/Policies] オプションをインストールしているデータベースのサーバを選択していることを確認します。ZENworks Server Management ポリシー (Distributed Server Package) の [Purge Database] オプションが機能するのは、Policy/Package Agent ソフトウェアと zfslog.db ファイルが同じサーバ上にある場合だけです。

設定計画ワークシート

作成する各データベースオブジェクトについて、次の情報を指定してください。

- 項目 4 で、Server Management データベースファイルをホストする Distributor サーバの名前を指定します。
- 項目 9 で、デフォルトのパスと異なるインストールパス情報を指定します。
- データベースオブジェクトの名前をデフォルトから変更する場合は、項目 10 で名前を指定します。
- 項目 11 で、データベースオブジェクトを作成する eDirectory コンテナを指定します。

Distributor を混在 eDirectory 環境で実行できるかどうか

Server Management は、混在 eDirectory 環境で実行できます。たとえば、ネットワークに eDirectory 8.*x* と NDS® 6.*x* または 7.*x* の両方がインストールされている場合があります。

ただし、Server Management では、製品のインストール時にツリーにオブジェクトを配置できるように、eDirectory 8.*x* (8.6.2、8.7.1、または 8.7.3 以降のみ) が必要です。eDirectory はマスタレプリカと共にネットワーク内の任意の場所にインストールされている必要がありますが、Server Management ソフトウェアをインストールするサーバにインストールする必要はありません。

また、ZENworks 6.5 Distributor サーバで eDirectory 8.*x* が実行されている必要があります。

Server Management サーバの要件は、(NCP サーバオブジェクトが存在するパーティションの)eDirectory マスタレプリカがインストールされているサーバと通信できることだけです。したがって、Server Management をインストールする各サーバに eDirectory をインストールする必要はありません。

eDirectory 8.*x* を使用しているツリー内のサーバの IP アドレスを選択してください。サーバで eDirectory 8.*x* が実行されている場合は、Distributor サーバ自体の IP アドレスになる可能性があります。

設定計画ワークシート
項目 12 で、eDirectory 8.*x* を使用しているサーバの IP アドレスを指定します。

他の Subscriber のイントールの必要性

Policy and Distribution Services をはじめてインストールした場合、このソフトウェアはすべてのサーバにはインストールされていません。Subscriber ソフトウェアをサーバに徐々に追加してインストールする場合は、この時点で次の段階を完了できます。

インストール時に、Subscriber プロパティをデフォルトから次のように変更できます。

- [Object Name]：Subscriber オブジェクトの名前を変更する場合は、そのサーバが Subscriber であることなど、サーバの識別情報を名前に保持することをお勧めします。
- [Container]：Subscriber オブジェクトがインストールされているコンテナの使用について計画します。

  Subscriber サーバオブジェクトは、オペレーティングシステムと一致するコンテナに配置する必要があります。たとえば、NetWare サーバの場合は NetWare コンテナに、Windows サーバの場合は Windows コンテナに配置します。

  Subscriber として使用する Windows 2000/2003 サーバに eDirectory がインストールされていない場合、そのサーバのデフォルトのコンテナオブジェクトはインストール中に表示されません。したがって、その Subscriber オブジェクトのコンテナを決定します。
- [Working Directory]：Subscriber の作業ファイルには、デフォルトのパス以外のボリューム、ドライブ、またはディレクトリパスを使用できます。

  作業ディレクトリは、Distribution のサイズに応じてかなり大きくなる可能性があるため、十分なディスク容量を確保しておく必要があります。NetWare サーバのデフォルトのボリュームは sys: です。NetWare サーバでは、別のボリュームを指定することを強くお勧めします。

  Subscriber サーバで別のパスを指定する必要がある場合があります。たとえば、NetWare サーバでは sys: を、Windows サーバでは D: を指定します。パスデータには、ボリューム / ドライブ指定などの変数を使用できます。詳細については、9 章 355 ページの「変数」を参照してください。

  NetWare および Windows サーバのデフォルトの作業ディレクトリパスは、次のとおりです。

  ```
  \zenworks\pds\ted\sub
  ```

  Linux および Solaris サーバのパスは、次のとおりです。

  ```
  /var/opt/novell/zenworks/zfs/pds/ted/sub
  ```

作業ディレクトリの詳細については、190 ページの「作業ディレクトリ」を参照してください。

設定計画ワークシート
項目 3 で、今回 Subscriber ソフトウェアをインストールするサーバ名を指定します。
項目 8 で、デフォルトから変更するプロパティ情報を、インストールする Subscriber ごとに指定します。これには、オブジェクト名、オブジェクトのコンテナ、および作業ディレクトリが含まれます。

配布フローの決定

次の節では、配布ルートの決定に関する情報について説明します。

- 38 ページの「配布ルートの理解」
- 39 ページの「配布ルートに対する Subscriber の選択」
- 40 ページの「配布ルートの設定」

詳細については、99 ページの「配布ルーティングの理解」を参照してください。

配布ルートの理解

各 Distributor には、Distribution を送信するための階層型のパスを提供するルーティング階層があります。ルーティング階層は、Subscriber のリストで構成されます。Subscriber の階層は、多レベルの深い階層にすることができます。

また、Distributor のルーティング階層内の Subscriber を、その Distributor からの Distribution の受信先にする必要はありません。Subscriber は、Distributor が Distribution を他の Subscriber に渡すためのプロキシの役割を果たすに過ぎません。

必ずしもすべての Subscriber がルーティング階層内に存在する必要はありません。ルーティング階層内に存在する必要があるのは、Distribution を他の Subscriber サーバに渡すために使用される Subscriber のみです。ネットワークの Subscriber サーバのほとんどは、Distribution を受信して抽出するだけのエンドノード Subscriber です。

Distributor は、特定の Subscriber への最も効率的なルートを次のように判断します。

1. Distributor は、Distribution を受信する Subscriber を識別します。
2. Distributor は、その Subscriber に親 Subscriber があるかどうかを判断します。
3. Subscriber に親 Subscriber がある場合、Distributor はその親 Subscriber のルーティング階層をチェックします。
   a. 親 Subscriber がルーティング階層内にある場合、Distributor はそのルートを使用して Subscriber に Distribution を送信します。
   b. 親 Subscriber がルーティング階層内にない場合、Distributor はターゲットのエンドノード Subscriber の親 Subscriber に直接 Distribution を送信します。
4. Subscriber に親 Subscriber がない場合、Distributor はその Subscriber のルーティング階層をチェックします。
   a. Subscriber がルーティング階層内にある場合、Distributor はそのルートを使用して Subscriber に Distribution を送信します。
   b. Subscriber がルーティング階層内にない場合、Distributor は Subscriber に直接 Distribution を送信します。

言い換えると、Distributor がルーティング階層を使用した Distribution の送信ルートを検出した場合は、その階層内のパスを使用して Distribution を Subscriber に送信し、それ以外の場合は、Subscriber(またはその親 Subscriber) に直接 Distribution を送信します。

このため、Distributor から定期的に Distribution を受信する Subscriber はすべて、Distributor のルーティング階層と何らかの形で接続している必要があります。この接続は、Subscriber を階層のリストに加えたり、階層内の Subscriber の 1 つを親 Subscriber にすることで確立できます。

ルーティング階層の第 1 層にある Subscriber に対して Distribution を送信するとき以外、Distributor は通常、WAN リンクを介して Distribution を送信することはできません。

Distributor のルーティング階層を設計する場合は、次の点を考慮してください。

- **エンドノード Subscriber:** ルーティング階層に追加する必要がある Subscriber は、Distribution を渡す際に使用する Subscriber のみです。Distribution を受信するだけで渡すことがないエンドノード Subscriber は、ルーティング階層に追加する必要はありません。
- **配布ルートの設定：** 配布ルートを作成するには、ネットワークの設計と各 LAN 上の Subscriber 数を考慮してください。その後、ネットワークトポロジに似たルーティング階層を設計します。
- **複数の Subscriber の選択：** 階層の作成時に、1 つの Distributor または Subscriber の下の同じ層に、複数の Subscriber を配置できます。

  重要： 各層に多数の Subscriber を配置して層数を少なく抑えるよりも、Subscriber が少ない層を多数作成した方がルーティング階層としては効率的です。したがって、各層で多数の Subscriber を選択しないようにしてください。これにより、Distribution を他の Subscriber サーバに送信する Distributor または Subscriber サーバの負荷が最小限に抑えられます。階層を作成すると、ネットワーク内での Distribution の送信によって生じる負荷が共有されます。
- **複数の Distributor の使用:** 複数の Distributor で同じ Subscriber のルーティング階層を使用すれば、各 Distributor で同じ配布ルートを使用できます。
- **Subscriber の再利用：** ルーティング階層内の 1 つの親 Subscriber サーバで複数の Distributor を処理する場合、Subscriber サーバに過重負荷が生じないかどうかを考慮してください。

配布ルートに対する Subscriber の選択

Distributor のルーティング階層の目的は、Subscriber への最も効率的な配布方法を作成することです。ルーティング階層内の Subscriber に最も適したサーバと、その階層内に含むサーバ数を決定する必要があります。

物理的設定において堅牢なサーバを選択してください。たとえば、高速な CPU、十分な RAM、十分なハードディスクの空き容量 (特に NetWare サーバの sys: 以外のボリューム) を持つサーバです。

次の条件を使用して、Distributor のルーティング階層に含める Subscriber を決定してください。

- Distributor の負荷を最小限にするためにその Subscriber が必要かどうか。
- 特定の LAN 上にある親 Subscriber の負荷を共有するために他の Subscriber が必要かどうか。
- ネットワークトラフィック (WAN またはファイアウォール経由など) を軽減するためにその Subscriber が必要かどうか。

Distributor のルーティング階層で使用する Subscriber サーバを識別するには、Distributor のルーティング階層内で親 Subscriber として使用するサーバのリストを作成します。

ネットワークトラフィックを最小限にするには、各 LAN で最低 1 つのサーバを選択してください。

Distributor のルーティング階層内で親 Subscriber として使用するサーバオブジェクトを識別してください。

設定計画ワークシート
項目 16 で、親 Subscriber サーバの名前（完全なコンテキスト）を指定します。

配布ルートの設定

ネットワーク図に次の情報を指定してください。

設定計画図
WAN リンクまたはファイアウォールによって Distributor の場所から分離されている各場所の横に「親 =1」と記入します（その場所に Subscriber が 1 つしかない場合は除く）。 Subscriber 数が多く追加の親 Subscriber が必要な場所については、「親 =1」を「親 =#」に変更します。# は負荷分散のためにその場所で必要な親 Subscriber の数です。 Distribution を受信して指定の場所の他の親 Subscriber に渡すために、その場所の Subscriber の 1 つをプライマリ親 Subscriber（ルーティング階層のその場所で唯一）として使用するかどうかをメモします。 必要に応じて、Distributor の場所の親 Subscriber を含めてください。

ネットワーク図の情報を使用して、選択した Subscriber を使った Distributor のルーティング階層を設計してください。

設定計画ワークシート
項目 15 で、Distributor の各ルーティング階層の階層を作成します。異なる Distributor の階層の Subscriber サーバを再利用できます。

Distribution のセキュリティの理解

Server Management では、セキュリティで保護されているネットワーク内で送信される Distribution に対して、証明書を使用して適切なセキュリティ機能を提供します。ただし、Server Management で利用可能な追加のセキュリティ処理が必要になる場合があります。

セキュリティの詳細については、7 章 313 ページの「Policy and Distribution Services のセキュリティ」を参照してください。

次の説を参照して、Distribution に追加のセキュリティが必要かどうか判断してください。

- 41 ページの「サーバ間通信セキュリティの必要性の判断」
- 41 ページの「Windows サーバに対する暗号化セキュリティの必要性の判断」

サーバ間通信セキュリティの必要性の判断

Policy and Distribution Services では、通常のサーバ間通信に XMLRPC (Extensible Markup Language Remote Procedure Call) を使用します。XMLRPC は、オプションで、セキュリティ保護されていない接続での通信に対してセキュリティを提供します。

Policy and Distribution Services では、セキュリティ保護されていない接続でのサーバ間の通信や、セキュリティ保護されていない接続での管理ワークステーションとサーバの間の通信に、このセキュリティを使用します。たとえば、ファイアウォール、イントラネット、NAT 設定などです。

このサーバ間通信のセキュリティによって、セキュリティで保護されていない接続を介して受信したデータが信頼されるソースから送信されたものであり、途中で改ざんされておらず、受信したデータは他のコンピュータでも信頼できることが保証されます。これは、署名付きのセキュリティ証明書とデジタル署名を使用することによって実現されます。

このセキュリティでは特定のテキストファイルを編集する必要があり、Server Management ウィザードを使用してインストールされます。

サーバ間通信のセキュリティが必要になるのは、次のような場合です。

- **ConsoleOne の管理：** ワークステーションを使用して、セキュリティで保護されていない接続を介して Distributor サーバを管理する場合。
- **パラメータ：** SET Parameterポリシーや SETパラメータのソフトウェアパッケージを作成する場合、ターゲットサーバの SET パラメータ情報を提供するためにサーバ間通信が行われます。この通信は、セキュリティで保護されていない接続を介する場合があります。
- **Server Down Policy:** このポリシーを使用してサーバを停止する場合、停止するサーバとそのサーバが再び稼動するのを監視する別のサーバとの間の通信がセキュリティで保護されていない接続を介することがあります。

詳細については、328 ページの「セキュリティ保護されていない接続でのサーバ間通信のセキュリティ」を参照してください。

設定計画ワークシート
項目 13 で、サーバ間通信セキュリティソフトウェアをインストールする NetWare および Windows サーバ名を指定します。

Windows サーバに対する暗号化セキュリティの必要性の判断

通常、セキュリティで保護されているネットワーク内で送信される Distribution を暗号化する必要はありません。ただし、ネットワーク外に Distribution を送信する場合は、暗号化を使用してセキュリティを強化することができます。Distribution の暗号化には、NICI ソフトウェアが使用されます。

NetWare サーバによっては、オペレーティングシステムと共に NICI 2.6 が自動的にインストールされます。ただし、ZENworks 6.5 Server Management でサポートされているのはバージョン 2.6.4 です。NetWare バージョンの NICI は、アップグレードする必要があります。バージョン 2.6.4 は、ZENworks 6.5 に同梱されており、ZENworks for Servers 3.0.2(バージョン 3 SP2 を含む) にも同梱されています。

Windows、Linux、および Solaris サーバでは、暗号化された Distribution を構築する Distributor および抽出する Subscriber サーバに、NICI 2.6.4 をインストールする必要があります。

重要： ネットワークで NICI 2.4.6 を実行している場合は、NICI 2.6.4 へのアップグレードは省略可能です。両バージョン間には互換性があります。

Windows、Linux、および Solaris サーバに NICI ソフトウェアをインストールする場合は、ネットワーク内のすべての Distributor および Subscriber サーバにも同じバージョンをインストールする必要があります。ネットワーク内に異なるバージョンの NICI がインストールされていると、暗号化が正常に機能しません。

Distribution の暗号化については、324 ページの「暗号化を使用した Distribution のセキュリティ」を参照してください。

設定計画ワークシート
項目 14 で、NICI ソフトウェアをインストールする必要がある Windows、Linux、および Solaris サーバ名を指定します。

Distribution の Channel の決定

Channel は、Distribution をグループ化する場合、Distributor の Distribution を Subscriber へ渡すスケジュールを確立する場合、および Distributor が Distribution ファイルの物理的な送信先を判断できるように、Channel に登録する Subscriber のリストを作成する場合に使用されます。

特定の Distribution の使用目的（ウィルスパターンファイル、オペレーティングシステムのサポートパック、またはポリシーパッケージなど）用、または特定の Distribution 時間（オフピーク時の Distribution）用の Channel を作成することができます。

複数の Distributor の Distribution を 1 つの Channel に関連付けることができます。1 つの Channel に複数の Subscriber を登録できます。

特定の Distribution を受信するよう Subscriber を Channel に登録します。Distributor の Distribution を Channel に関連付けて、登録された Subscriber がその Distribution を受信できるようにします。

複数の Distributor をインストールしている場合は、それらの Distributor で Distribution の Channel を共有できます。たとえば、Distributor A と Distributor B から同じ Subscriber のセットに Distribution を送信する場合、両方の Distributor で同じ Channel を共有できます。

Channel は、Subscriber に Distribution を送信するときに使用されます。次の点を考慮してください。

- Channel は特定の Distributor に占有されません。
- Distributor によって Distribution が Channel に関連付けられます。
- Channel には複数の Distributor の Distribution を関連付けることができます。
- Channel を使用して、関連付けられた Distribution をグループ化できます。
- Channel のスケジュールによって、リストされた Distribution が送信されるタイミングが決まります。

- Subscriber は、登録された Channel（複数可）にリストされているすべての Distribution を受信することができます。
- Subscriber は、Channel にリストされている Distribution から個別に Distribution を選択することはできません（必ずその Channel の Distribution をすべて受信します）。

Channel に名前を付けるときは、わかりやすい名前を使用してください。たとえば、次のように入力します。

```
VirusProtect
VProtectPatterns
VirusProtection
NW51patch4
NW6patch1
AUTOEXECNCF000326
```

次のように名前を決めると、Channel をより簡単に管理できます。

- 目的に合った名前を使用する
- Channel と Distribution に類似した名前を使用する

設定計画ワークシート

項目 21 で、Channel 名を指定します。関連付けられている Distribution が識別しやすいように、一意の名前を付けてください。

通常、作成した Channel には 1 つ以上の Distribution が関連付けられます。ただし、配布を柔軟に行うために、配布するアプリケーションごとに Channel を 1 つ作成することもできます。

設定計画ワークシート

項目 22 で、各 Channel が所有する Distribution を指定します。

管理を容易にするために、他の Tiered Electronic Distribution オブジェクト（特に Distribution オブジェクト）と同じコンテキストに Channel オブジェクトを作成することを計画してください。

設定計画ワークシート

項目 20 で、Channel オブジェクトを作成する eDirectory コンテキストを指定します。

Subscriber の登録の決定

Subscriber で Distribution を受信する前に、Subscriber を Channel に登録する必要があります。これは、Subscriber または Subscriber Group を、必要な Distribution が関連付けられた Channel に登録することによって行います。

- 44 ページの「Subscriber」
- 44 ページの「Subscriber Group」

Subscriber

Subscriber は eDirectory にアクセスしないため、Subscriber オブジェクトのプロパティ内の設定情報はすべて、設定元の Distributor から必要に応じて転送されます。これには、作業ディレクトリ、ログファイルのレベルと場所、コンソールのメッセージレベル、変数などの情報が含まれます。

Subscriber オブジェクトのプロパティに加えられた変更は、Distributor が再度 eDirectory を読み込み、新しい Distribution と設定情報を Subscriber に転送するまで有効になりません。

Channel ごとに、特定の Distribution を必要とする Subscriber を決定してください。

設定計画ワークシート
Under 項目 24 で、Distribution の Channel 名（項目 22）を指定し、その Distribution を必要とする Subscriber のリストを作成します。項目 21 で指定した Channel ごとにこれを繰り返します。

Subscriber Group

Subscriber Group は、同じ Distribution を必要とする Subscriber のグループ化に使用されます。

Subscriber Group は、異なる複数の Distribution を同じ Subscriber のグループに送信する場合に役立ちます。Subscriber が 1 つの Channel にだけ関連付けられている場合は、Subscriber Group を作成する必要はありません。

たとえば、Channel A は Distribution A を含み、Channel B は Distribution B を含むという構成の複数の Channel があるとします。この場合、Subscriber Group を使用しないと、各 Subscriber を Channel A に登録し、さらに Channel B にも登録するというように、長いプロセスが必要になります。Subscriber Group を使用すると、グループを作成して複数の Subscriber を追加し、そのグループを各 Channel に登録するだけで済みます。

Subscriber Group の別の使用法として、グループが複数の Channel に関連付けられている場合は、グループのメンバーシップを編集すると、より簡単に複数の Channel に同じ変更を加えることができます。たとえば、Subscriber Group から Subscriber を削除するには、グループのプロパティを編集するだけです。複数の Channel から同じ Subscriber を削除するには、各 Channel のプロパティを編集する必要があります。

設定計画ワークシート
項目 17 で、Subscriber Group の一意の名前を指定します。 項目 18 で、そのグループが登録される Channel の Distribution（項目 21 および項目 22）を必要とする Subscriber の一覧を指定します。 項目 24 で、グループ内のすべての Subscriber が受信する Distribution の Channel 名を指定します。

配布スケジュールの決定

多様な配布プロセスに対応できるように、Tiered Electronic Distribution には複数のスケジュールが用意されています。詳細については、8 章 331 ページの「スケジュール設定」を参照してください。

Tiered Electronic Distribution のスケジュールを計画するには、次の節を参照してください。

- 45 ページの「Tiered Electronic Distribution のスケジュール作成の理解」
- 45 ページの「Distributor の更新スケジュールの決定」
- 46 ページの「Distribution の構築スケジュールの決定」
- 46 ページの「Channel の送信スケジュールの決定」
- 46 ページの「Subscriber の抽出スケジュールの決定」

Tiered Electronic Distribution のスケジュール作成の理解

Tiered Electronic Distribution オブジェクトと個別の Server Policies の両方のスケジュールを作成できます。

Tiered Electronic Distribution では、Distributor を更新、および Distribution を構築、送信、抽出するタイミングを制御するスケジュールを使用します。スケジュールは Distribution で使用されるリソース全体には影響しませんが、リソースがいつ使用されるかに影響します。

一部のポリシーでは、ポリシーが有効になる前にスケジュールを作成する必要があります。有効にしたポリシーに対してまだスケジュールを設定していない場合は、デフォルトのスケジュールを提供する Default Package Schedule で指定されているスケジュールに応じて、ポリシーが実行されます。デフォルトのスケジュールは、[Run At System Startup] です。

複数のポリシーに同じスケジュールを設定した場合、実行される順序はポリシーを作成した時点のタイムスタンプによって決まります。したがって、ポリシーのリストを表示したときの順序が実行される順序になります。

特定のポリシーを実行する順序を制御する場合は、実行のタイミングを決めるタイムスタンプに頼るのではなく、そのスケジュールを変更します。したがって、ポリシーのスケジュールを設定する場合は、選択する Tiered Electronic Distribution スケジュールを十分に考慮し、不要な重複や、スケジュール設定した項目で失敗を引き起こす可能性のある順序外のイベントなどがないように注意します。

次の問題について理解しておく必要があります。

- タイムゾーンがスケジュール設定に与える影響
- 配布スケジュールがポリシースケジュールに与える影響
- Server Management以外を使用していないDistributorまたはSubscriberサーバが配布スケジュールに与える影響
- Randomly Dispatch オプションがスケジュール設定に与える影響
- Tiered Electronic DistributionオブジェクトのActiveおよびInactiveオブジェクトのオプションがスケジュール設定と配布フローに与える影響

Distributor の更新スケジュールの決定

更新スケジュールによって、Distributor が eDirectory から設定の変更を読み込むタイミングが決定します。

これにより、Distribution の構築要求に対する Distributor の応答が可能になります。Distributor は、eDirectory 内の設定の変更を検出すると Distribution を再構築します。

また、このスケジュールはデフォルトでは［Never］に設定されているため、Distributor を手動で更新して配布プロセスを開始するよう要求されます。このスケジュールは、必要に応じて、後で変更できます。

Distribution の構築スケジュールの決定

構築スケジュールによって、Distribution の各構成要素の構築を Distributor に対して要求するタイミングが決定します。

Distribution が構築後直ちに送信されるよう、設定時に各 Distribution の構築スケジュールを設定するよう要求されます。

Channel の送信スケジュールの決定

送信スケジュールによって、Distributor が Distribution を Subscriber に送信する時間帯が決定します。

設定時に、各 Channel の送信スケジュールを 5 分間隔に設定すると、スケジュール開始後、Distribution は Distributor から 5 分間隔で送信されます。

Subscriber の抽出スケジュールの決定

抽出スケジュールによって、Subscriber が受信した Distribution を抽出するタイミングが決定します。

Subscriber では、受信した Distribution を使用する前に抽出する必要があります。したがって、Distribution を送信する前に、Subscriber の抽出スケジュールを設定する必要があります。

各 Subscriber サーバについて Distribution を抽出するスケジュールを決定してください。Distribution のサイズによっては、オフピーク時の抽出が最適な場合があります。スケジュール設定に関するタイムゾーンの問題については、346 ページの「スケジュール設定に関する問題」、および 348 ページの「時差の計算」を参照してください。

設定計画ワークシート
項目 23 で、Subscriber の抽出スケジュールを指定します。

配布システムの設定

次の節を順に参照してください。

1. 47 ページの「追加の Distributor、データベース、および Subscriber のインストール」
2. 50 ページの「追加の配布セキュリティのセットアップ」
3. 52 ページの「配布フローの設定」
4. 54 ページの「Distribution および関連 Channel の作成」
5. 56 ページの「Distribution への登録」
6. 57 ページの「Distribution の送信」

追加の Distributor、データベース、および Subscriber のインストール

Policy and Distribution Services をはじめてインストールした場合、Distributor とデータベースファイルは 1 つずつインストールされます。Distributor またはデータベースを追加でインストールする場合は (97 ページの「Distributor の理解」と 368 ページの「必要なデータベースの数の決定」を参照)、インストールをここで実行する必要があります。

Policy and Distribution Services をはじめてインストールした場合、Subscriber ソフトウェアはすべてのサーバにはインストールされていません。Subscriber ソフトウェアを別のサーバにもインストールする場合は、ここでインストールを実行する必要があります。

重要： Subscriber ソフトウェアがインストールされていないサーバは、ここで作成および配布を計画した Distribution を受信できません。ただし、後で Subscriber ソフトウェアをサーバにインストールするときに、Distribution を受信するように既存の Channel に登録することができます。

追加の Distributor、データベース、および Subscriber ソフトウェアを別のサーバにインストールするには、次の操作を順に実行してください。

1. 47 ページの「インストールの準備」
2. 47 ページの「インストールプログラムの起動」
3. 48 ページの「Distributor および Subscriber サーバの選択と設定」
4. 50 ページの「インストールの完了」

インストールの準備

1 ターゲットの Distributor および Subscriber サーバが、必要条件をすべて満たしていることを確認します。

詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「サーバの要件」を参照してください。

2 Distributor および Subscriber のインストールに使用するワークステーションを選択します。

3 Server Management オブジェクトを作成する eDirectory ツリーにログインしていない場合は、ログインします (ワークシートの項目 1)。

これは、ZENworks 6.5 Server Management のスキーマを拡張したツリーと同じである必要があります。

インストール中は、すべての NetWare ターゲットサーバに対して自動的に認証が行なわれます。これらのサーバ以外に、別のツリーまたはドメインのサーバを選択して Policy and Distribution Services ソフトウェアをインストールすることもできます。ただし、これは選択された各サーバのすべての Server Management オブジェクトがインストールされているツリーです。

4 47 ページの「インストールプログラムの起動」に進みます。

インストールプログラムの起動

1 インストールを実行するワークステーションに、*ZENworks 6.5 Server Management Program* CD を挿入します。

起動画面が表示されます。CD 挿入後、起動画面が自動的に表示されない場合は、CD のルートにある winsetup.exe を実行すると起動できます。

重要： リモートサーバでの CD によるインストールは、ワークステーション上のドライブがそのリモートサーバにマッピングされていないかぎりサポートされません。たとえば、Windows サーバの CD ドライブに CD を挿入してワークステーションからインストールを実行する場合、ワークステーション上のドライブをその Windows サーバの CD ドライブにマッピングしておく必要があります。

2 [Server Management] を選択し、次に [Policy-Enabled Server Management] を選択します。

これにより、インストールプログラムが開始します。

3 ソフトウェアの使用許諾契約に同意する場合は、[Accept] をクリックし、[Next] をクリックします。

4 [Installation Type] ページで [New Installation] をクリックし、[Next] をクリックします。

5 [Installation Options] ページで、3 つすべてのチェックボックスがオンになっていることを確認します。

6 [eDirectory Tree for Creating Objects] ページで、ツリーを選択します (ワークシートの項目 1)。

これは、最初に Server Management オブジェクトを作成したツリーです。

7 48 ページの「Distributor および Subscriber サーバの選択と設定」に進みます。

Distributor および Subscriber サーバの選択と設定

1 [Server Selection] ページで、[Add Server] をクリックします。

2 Distributor サーバ (ワークシートの項目 2) と Subscriber サーバ (ワークシートの項目 3) を参照して選択し、[OK] をクリックします。

3 このページに表示された各サーバを設定し、次に [Next] をクリックして [File Locations and Options] ページに進みます。

ヒント： 1 つまたは複数のサーバの特定の役割または役割のセットを簡単に設定するには、サーバを選択し、選択したサーバを右クリックしてサーバの役割を選択します。その役割に適用されるオプションは自動的に選択されます。他の役割についてもこの手順を繰り返します。

[ZENworks Policy-Enabled Management Services]

デフォルトでは、次の 3 つのオプションはすべて選択されています。Inventory Agent をインストールする場合は、Policy and Distribution Server もインストールすることを選択する必要があります。

- **[Policy and Distribution Server]：** Subscriber にする各サーバについて、このチェックボックスをオンにします。

Tiered Electronic Distribution の目的には、次の 4 つを選択解除できます。

[Inventory Agents]
Remote Management (リモート管理)

[Additional Options]

インストールプログラムによって、これらのオプションがターゲットサーバにすでにインストールされているかどうかが検出され、インストールされているオプションのラベルは淡色表示されます。このチェックボックスをオンにして、コンポーネントを再インストールすることもできます。

- **Distributor:** Subscriber サービスはすべてのターゲットサーバに自動的にインストールされます。Distributor サーバの作成を計画した場合は、このチェックボックスを選択します。

- **[Server Management Database]：** これは、Distributor がサーバにログを記録する Policy and Distribution Services データベースです（ワークシートの項目 4）。データベースのログの記録によるネットワークトラフィックを最小限に抑えるには、このデータベースを Distributor と同じサーバにインストールしてください。

  重要： インストールプログラムを実行するたびに複数のサーバにデータベースをインストールできますが、サーバごとにインストールできるデータベースは 1 つだけです。[Database Settings] ページで、インストールされる各データベースを個別に設定できます。[Database Logging] ページで、インストールするデータベースの中で、初期のログの記録に使用するデータベースを指定します。

Tiered Electronic Distribution の目的には、次の 4 つを選択解除できます。

Inventory Database
Inventory Server
Inventory Proxy Server
ConsoleOne Snap-Ins

ヒント： サーバのグループを選択し、そのグループを右クリックすることによって、選択したグループに同じオプションを設定できます。これによって、[Custom Selection] ダイアログボックスが表示されます。

4 [File Locations and Options] ページで、次の操作を行います。

4a Distributor サーバのデフォルトのインストールパスを使用しない場合は、各 Distributor サーバのインストールパスを編集します（ワークシートの項目 5）。

すべての Distributor サーバで同じインストールパスを使用する場合は、すべてのサーバを選択してパスを編集します。

4b Subscriber サーバのデフォルトのインストールパスを使用しない場合は、各 Subscriber サーバのインストールパスを編集します（ワークシートの項目 6）。

すべての Subscriber サーバで同じインストールパスを使用する場合は、すべてのサーバを選択してパスを編集します。

4c サーバの起動時に Policy and Distribution Services コンポーネントを起動するには、チェックボックスをオンにします。

4d インストールの完了時にサービスを開始するには、チェックボックスをオンにして、[Next] をクリックします。

5 [Distributor Object Properties] ページで、必要に応じてプロパティを編集し（ワークシートの項目 7）、[Next] をクリックします。

6 [Subscriber Object Properties] ページで、必要に応じてプロパティを編集し（ワークシートの項目 8）、[Next] をクリックします。

7 [Database Settings] ページで、次の操作を行います。

7a データベースファイルのデフォルトのパスを使用しない場合は、パスを編集します（ワークシートの項目 9）。

データベースファイルはサイズが非常に大きくなる可能性があるため、NetWare のデフォルトのボリュームを、sys: からそのサーバ上の別のボリュームに変更することをお勧めします。

7b 必要に応じて、データベースオブジェクトの名前を編集します（ワークシートの項目 10）。

7c 必要に応じて、データベースオブジェクトのコンテナを編集します（ワークシートの項目 11）。

8 Policy and Distribution Services データベースをインストールすることを選択した場合は、[Log to a Server Management Database That Will Be Installed] オプションが選択されています。[Next] をクリックして [Summary] ページを表示します。

9 50 ページの「インストールの完了」に進みます。

インストールの完了

1 現在のインストール設定を保存して将来 Distributor のインストールで再利用できるようにするには、[Summary] ページで、[Save the Following] チェックボックスをオンにします。

2 テンプレートファイルのパスとファイル名を指定します。

[Finish] をクリックせずにインストールプログラムを終了しようとすると、現在のインストール設定をインストールのテンプレートファイルに保存するよう要求するメッセージが表示されます。

このテンプレートを再利用すると、将来 Distributor または Subscriber をインストールする際に、インストールページの入力に要する時間が短縮されます。

3 [Finish] をクリックしてインストールプロセスを開始します。

4 インストールプログラムが終了したら、インストールログファイルを調べて、インストールに失敗したコンポーネントがないかどうかを確認します。

ログファイルは次の場所にあります。

`%TEMP%\_res`*`number`*`.txt`

number は 3 桁の数値で、新しいログファイルが作成されるたびに増えます。

5 必要に応じて、インストールプログラムを再実行します。

インストールに失敗したコンポーネントだけを選択します。

6 インストールするデータベースごとに、インストールプログラムを実行します (ワークシートの項目 4)。

[Server Selection] ページで、データベースをインストールする予定の Distributor の中からまだインストールしていない Distributor を 1 つだけ追加します。次に、そのデータベースの Distributor サーバの [Database] 列のみをクリックし、残りのインストールページで適切な情報を指定します。

7 追加の配布セキュリティをセットアップする場合は、50 ページの「追加の配布セキュリティのセットアップ」に進みます。それ以外の場合は、52 ページの「配布フローの設定」に進みます。

追加の配布セキュリティのセットアップ

Distribution のセキュリティを強化するために、必要に応じて次の操作を行ってください。

- 51 ページの「NICI 2.6.4 のインストール」
- 52 ページの「サーバ間通信セキュリティのセットアップ」

NICI 2.6.4 のインストール

特定の NetWare、Windows、Linux、または Solaris の Subscriber サーバで Distribution の暗号化が必要な場合、ZENworks 6.5 Server Management では、NICI 2.6.4 がサポートされています。NICI 2.6.4 が不要な場合は、52 ページの「配布フローの設定」に進みます。

ZENworks for Servers 3 SP2 を使用してサーバを NICI 2.6.4 にアップデートしている場合は、52 ページの「配布フローの設定」に進みます。

重要： 暗号化された Distribution を送信および受信するすべてのサーバで、同じバージョンの NICI を実行する必要があります。異なるバージョンが実行されていると、いずれのサーバでも暗号化された Distribution は失敗します。

NICI 配布のためのソフトウェアパッケージ用に選択する Channel に登録されたすべての Subscriber に、NICI 2.6.4 をインストールする必要があります。また NICI 2.6.4 は、暗号化された Distribution を作成するすべての Distributor サーバ上で実行される必要があります。

ただし、NICI 2.4.6 をインストール済みである場合は、NICI 2.6.4 へのアップグレードは省略可能です。両バージョン間には互換性があります。

NICI のアップデートは、*ZENworks 6.5 Companion 2* CD に含まれています。これは、[Novell International Cryptographic Infrastructure (NICI)] メニューオプションを使用して、Windows サーバにインストールされます。

NICI 2.6.4 用のソフトウェアパッケージアップデートも、*ZENworks 6.5 Companion 2* CD に含まれています。

NICI 2.6.4 のインストール時に、NICI がすでにインストールされているかどうかはインストールプログラムでチェックされません。

適切なインストール方法を選択してください。

- 51 ページの「Windows サーバへの NICI のインストール」
- 51 ページの「Server Software Package を使用した NICI のインストール」

Windows サーバへの NICI のインストール

Windows サーバに NICI 2.6.4 をインストールするには

1. Windows ワークステーションに、*ZENworks 6.5 Companion 2* CD を挿入します。
2. [Companion Programs and Files] オプションを選択し、>> をクリックして *Companion 2* CD のメニューを表示します。
3. [Novell International Cryptographic Infrastructure (NICI)]メニューオプションを選択します。
4. インストール手順に従います。
5. 52 ページの「配布フローの設定」に進みます。

Server Software Package を使用した NICI のインストール

サポートされている任意のサーバに NICI 2.6.4 をインストールするには

1. Windows ワークステーションに、*ZENworks 6.5 Companion 2* CD を挿入します。
2. CD の ¥NICI ディレクトリから nici265.exe ファイルをワークステーションにコピーして、ファイルを抽出します。
3. NICI 2.6.4 のインストール用に Software Package Distribution を作成する Distributor サーバ上の場所に、抽出した nici264.cpk ファイルをコピーします。

4 Distribution を作成して、暗号化された Distribution を受信する各 Subscriber サーバに送信します。

Software Package Distribution の作成および送信については、125 ページの「Distribution の作成」を参照してください。

5 52 ページの「配布フローの設定」に進みます。

サーバ間通信セキュリティのセットアップ

セキュリティで保護されたネットワークの外部にあるサーバに配布する場合は (ワークシートの項目 13)、サーバ間通信セキュリティのセットアップ手順について、328 ページの「セキュリティ保護されていない接続でのサーバ間通信のセキュリティ」を参照してください。

配布フローの設定

Distribution の送信時にネットワークを最も効率的に使用するには、Distributor のルーティング階層を作成して配布システムを設定する必要があります。これは、Policy and Distribution Services のインストール時にすべての Distributor に対して実行されるわけではありません。

配布システムを設定するには

- 52 ページの「Distributor のルーティング階層の設定」
- 53 ページの「親 Subscriber の設定」
- 53 ページの「Subscriber Group の設定」

Distributor のルーティング階層の設定

1 ConsoleOne で、Distributor オブジェクトを右クリックし (ワークシートの項目 2)、[Properties] をクリックします。

2 [Routing] タブを選択し、次の操作を行います。

2a [Add] をクリックして第 1 層の Subscriber サーバを参照し (ワークシートの項目 15)、[Select] をクリックして [OK] をクリックします。

これにより、第 1 層の Subscriber が設定されます。この Subscriber は、Distributor から直接 Distribution を受信します。

2b ルーティングツリーの第 1 層の Subscriber から 1 つを選択し、[Add] をクリックしてその Subscriber の下位に来る次の層の Subscriber サーバを参照します (ワークシートの項目 15)。次に、[Select] をクリックして [OK] をクリックします。

これにより、選択した Subscriber の第 2 層の Subscriber サーバが設定されます。この第 2 層の Subscriber は、Distributor から階層内の上位の Subscriber を介して間接的に Distribution を受信します。

2c 第 1 層の Subscriber ごとにステップ 2b を繰り返し、第 2 層の Subscriber をすべて選択します。

2d ルーティングツリーの第 2 層の Subscriber から 1 つを選択し、[Add] をクリックしてその Subscriber の下位に来る次の層の Subscriber サーバを参照します (ワークシートの項目 15)。次に、[Select] をクリックして [OK] をクリックします。

2e 第 2 層の Subscriber ごとにステップ 2d を繰り返し、第 3 層の Subscriber をすべて選択します。

2f このプロセスを階層ごとに繰り返して、現在の Distributor のルーティング階層を計画どおりに作成します。

3 他の Distributor に対して、ステップ 1 からステップ 2 を繰り返します。

4 ルーティング階層の作成が終了したら、[OK] をクリックします。

5 53 ページの「親 Subscriber の設定」に進みます。

親 Subscriber の設定

すべての Subscriber が Distributor から直接 Distribution を受信するわけではありません。Distributor のルーティング階層により、Distribution の送信時における Distributor の負荷を最小限に抑えることができます。

ルーティング階層を使用して Subscriber サーバで Distribution を受信するには、各エンドノード Subscriber(Distribution を受信する Subscriber) に対して、ルーティング階層内にある親 Subscriber を識別する必要があります。これにより、エンドノード Subscriber は Distributor から直接 Distribution を受信するのではなく、ルーティング階層を使用して Distribution を受信できるようになります。

Distributor のルーティング階層内にある Subscriber には、その Distributor から Distribution を受信するための親 Subscriber は必要ありません。Distributor はまずルーティング階層をチェックし、次に親 Subscriber をチェックします。

Subscriber を親 Subscriber に関連付けるには

1 ConsoleOne で、特定の親 Subscriber で処理するサーバの Subscriber オブジェクトのグループを選択し (ワークシートの項目 16)、選択したグループを右クリックして [Properties of Multiple Objects] をクリックします。次に、[Parent Subscriber] フィールドで親 Subscriber オブジェクトを参照し、[OK] > [OK] の順にクリックします。

eDirectory オブジェクトは複数編集が可能です。したがって、1 つの親 Subscriber が処理する Subscriber をすべて選択し、それらすべての Subscriber に対して [Parent Subscriber] フィールドを一度に編集できます。

2 すべてのエンドノード Subscriber に対して、このプロセスを繰り返します。

3 53 ページの「Subscriber Group の設定」に進みます。

Subscriber Group の設定

Subscriber Group を作成するには

1 ConsoleOne で、Subscriber Group オブジェクトを格納するコンテナを選択し、[File] > [New] > [Object] の順にクリックして、[TED Subscriber Group] を選択します。

2 [New TED Subscriber Group] ダイアログボックスで、Subscriber Group 名を指定し (ワークシートの項目 17)、[Define Additional Properties] をクリックして [OK] をクリックします。

3 [General] > [Settings] の順にクリックして、説明を入力します。

4 Subscriber をグループのメンバーに含めるには、[Members] タブを選択して次の操作を行います。

4a [Add] をクリックし、Subscriber オブジェクトを参照して選択し（ワークシートの項目 18）、[OK] をクリックします。

4b 一覧から Subscriber を削除するには、Subscriber を選択して [Delete] をクリックします。

4c Subscriber のプロパティを表示するには、Subscriber を選択して [Details] をクリックします。

5 Subscriber Group オブジェクトの設定が終了したら [OK] をクリックします。

6 54 ページの「Distribution および関連 Channel の作成」に進みます。

Distribution および関連 Channel の作成

Distribution の一般的な作成手順については次の節を参照してください。主要な Distribution タイプの詳しい作成手順については、87 ページの「Tiered Electronic Distribution」を参照してください。Distribution ウィザードを使用して File または FTP Distribution を作成する手順については、146 ページの「Distribution ウィザードの使用」を参照してください。

既存の Channel を使用しない場合は、Distribution を作成してから Channel を作成する必要があります。

- 54 ページの「Distribution の作成と設定」
- 55 ページの「Channel の作成と設定」

Distribution の作成と設定

1 ConsoleOne で、Tiered Electronic Distribution オブジェクトがインストールされているコンテナを特定します。

2 Distribution 用のコンテナを右クリックし、[New] > [Object] の順にクリックします。次に、[TED Distribution] をクリックします。

3 Distribution 名を指定します（ワークシートの項目 19）。

Distribution には、内容が識別できるような名前を付けます。

4 この Distribution を所有する Distributor オブジェクトを参照して選択します（ワークシートの項目 19）。

各 Distribution は 1 つの Distributor に関連付けられます。Distribution の構築および送信は、その Distributor によって行なわれます。

5 [Define Additional Properties] チェックボックスをオンにします。

6 [OK] をクリックしてオブジェクトを作成します。

Distribution のプロパティが表示されます。

7 [Type] タブを選択し、[Select Type] ドロップダウンボックスで Distribution タイプを選択します（ワークシートの項目 19）。

8 Distribution を設定します。

Distribution のタイプ別の設定については、112 ページの「Distribution」を参照してください。

上向き矢印と下向き矢印を使用して、配布順序を変更します。

9 [Schedule] タブを選択します。

Distribution のスケジュールによって、Distributor が新しいバージョンの Distribution を構築する頻度が決定します。新しいバージョンは、最後のバージョンが作成されて以降変更が加えられている場合にのみ構築されます。

10 ドロップダウンリストから [Run Immediate] を選択します。

これにより、Distributor が eDirectory から Distribution 情報を読み込むとすぐに Distribution が構築されます。

11 [Distribution Properties] ダイアログボックスの下部にある [OK] をクリックし、すべての変更を保存します。

12 NetWare および Windows サーバで証明書を解決していない場合は、セキュリティ証明書をコピーするかどうかを確認するメッセージが表示されたときに [Yes] をクリックします。

Linux および Solaris サーバでドライブをマッピングしていない場合は、証明書を手動で解決する必要があります。詳細については、317 ページの「証明書の解決」を参照してください。

証明書を作成するには、Distributor を最低一度は実行する必要があります。

Distributor は、Subscriber ごとに証明書を一度だけ解決する必要があります。

セキュリティ証明書を解決するサーバ上で、Subscribe ソフトウェアが実行されている必要はありません。サーバが起動していることのみ必要です。

[Channel] タブで選択された Channel に登録された各 Subscriber サーバに、ConsoleOne からセキュリティ証明書が送信されます。Distributor から Distribution を受信する前に、各 Subscriber にはその Distributor からのセキュリティ証明書が必要になります。

各 Subscriber にセキュリティ証明書をコピーするには、数分かかる場合があります。

重要： 証明書は、各 Distributor/Subscriber 関係で 1 度だけコピーする必要があります。

13 Distributor が証明書を Windows Subscriber にコピーしようとしてエラーが発生した場合は、次のパスを入力します。

¥¥*IP_Address*¥zen$¥pds¥ted¥security

IP_Address は、その Windows Subscriber の IP アドレスです。

14 Distributor が証明書を Linux または Solaris Subscriber にコピーしようとしてエラーが発生した場合、または証明書を解決するためにサーバを参照して選択できない場合は、ドライブをサーバにマッピングして (Samba を使用するなど) から、証明書の解決を続行する必要があります。

15 今回作成するその他の Distribution についても、この手順を繰り返します (ワークシートの項目 19)。

16 55 ページの「Channel の作成と設定」に進みます。

Channel の作成と設定

Channel オブジェクトは、Subscriber と Distribution を関連付けるために使用されます。Subscriber を Channel に登録すると、Subscriber はその Channel に関連付けられている Distribution をすべて受信します。各 Channel にはスケジュールが設定され、そのスケジュールに基づいて関連付けられている Distribution が Subscriber に送信されるタイミングが決定します。

1 ConsoleOne で、Channel オブジェクトを作成するコンテナを特定します (ワークシートの項目 20)。

このコンテナはすでに存在している必要があります。

管理を容易にするために、すべての Channel で同じ OU を使用することをお勧めします。

2 Channel オブジェクトのコンテナを右クリックし、[New] > [Object] の順にクリックします。次に、[Channel] を選択して [OK] をクリックします。

3 Channel の名前を指定し (ワークシートの項目 21)、[OK] をクリックします。

Channel には、関連付ける Distribution に応じた名前を付けます。たとえば、「Channel - Antivirus Update」のような名前を付けます。

4 新しい Channel オブジェクトを右クリックし、[Properties] をクリックします。

5 [Distributions] タブを選択し、[Add] をクリックします。Channel に関連付ける Distribution を参照して選択し (ワークシートの項目 22)、[OK] をクリックします。

これにより、Distribution が Channel に関連付けられます。この Channel に登録された Subscriber は、現在ここに一覧表示されているすべての Distribution を受信します。

6 Channel の送信スケジュールを設定するには、[Schedule] タブを選択し、[Interval] を選択します。1 次間間隔などの間隔を指定して、[OK] をクリックします。

7 計画した Channel ごとに、ステップ 1 からステップ 5 を繰り返します (ワークシートの項目 21)。

8 56 ページの「Distribution への登録」に進みます。

Distribution への登録

- 56 ページの「Subscriber の抽出スケジュールの設定」
- 57 ページの「Channel への登録」

Subscriber の抽出スケジュールの設定

Tiered Electronic Distribution を介して送信された Distribution を Subscriber で使用する前に、Distribution を抽出する必要があります。したがって、Distribution が送信される前に、Subscriber の抽出スケジュールを設定する必要があります。

1 ConsoleOne で、抽出スケジュールを設定するサーバの Subscriber オブジェクトを右クリックし (ワークシートの項目 23)、[Properties] をクリックします。

2 [Schedule] タブを選択し、ドロップダウンボックスの矢印をクリックして [Run Immediately] を選択します。次に、[OK] をクリックします。

これにより、選択した Subscriber では Distribution が受信されるとすぐに抽出されます。

3 必要に応じてステップ 1 およびステップ 2 を繰り返し、すべての Subscriber のスケジュールを設定します。

4 57 ページの「Channel への登録」に進みます。

Channel への登録

Channel に関連付けられた Distribution を受信するには、Subscriber をその Channel に登録する必要があります。次の手順を使用して、作成済みの Channel に Subscriber を登録します。

1 ConsoleOne で、Channel オブジェクトを右クリックし（ワークシートの項目 21）、[Properties] をクリックします。

2 [Subscribers] タブを選択し、[Add] をクリックして、この Channel に登録する各 Subscriber または Subscriber Group オブジェクトを参照します（ワークシートの項目 24）。次に、[Select] をクリックし [OK] をクリックします。

3 [General] タブをクリックし、[Active] チェックボックスが選択されていることを確認します。

4 [OK] をクリックして Channel オブジェクトのプロパティを閉じ、変更内容を保存します。

5 セキュリティ証明書をコピーするかどうかを確認するメッセージが表示されたら、[No] を選択します。

6 Channel ごとに、ステップ 1 からステップ 5 を繰り返します（ワークシートの項目 21）。

7 57 ページの「Distribution の送信」に進みます。

Distribution の送信

Distributor、Subscriber、Channel、および Distribution のインストール、作成、および設定が終了したら、配布プロセスを開始できます。

次の操作を順に実行してください。

1. 57 ページの「Distributor のスケジュール設定と更新」
2. 58 ページの「配布プロセスの成功の確認」

Distributor のスケジュール設定と更新

1 ConsoleOne で、Distributor オブジェクトを右クリックし（ワークシートの項目 2）、[Properties] をクリックします。

2 Distribution オブジェクトの [Build Schedule] タブで、[Send Distribution Immediately After Building] をクリックし、[OK] をクリックしてプロパティを閉じます。

Channel の送信スケジュールに関係なく、Distribution は作成後すぐに送信されます。

3 Distributor オブジェクトを右クリックし、[Refresh Distributor] をクリックします。

これにより、Distributor は eDirectory を読み取って、eDirectory に加えられた変更をすべて取得します。

4 58 ページの「配布プロセスの成功の確認」に進みます。

設定済みの構築スケジュールに基づいて、Distribution の構築がすぐに開始されます。設定済みの送信スケジュールに基づいて、Distribution が 5 分以内に送信されます。

Subscriber が Distribution を受信すると、Subscriber オブジェクトのプロパティで指定した作業ディレクトリに Distribution の内容がすぐに抽出されます。

配布プロセスの成功の確認

配布プロセスが正常に完了したかどうかを確認する方法は多数あります。

- **iManager:** [Tiered Distribution] ビューおよび [Subscriber Distribution] ビューは、この情報を確認する最も簡単な方法です。これらのビューの使用方法については、各ページの iManager のヘルプを参照してください。
- **レポート：** Distribution でレポートを実行しステータスを確認します。Tiered Electronic Distribution のレポートについては、11 章 379 ページの「レポート機能」を参照してください。
- **ログファイル：** 使用しているログレベルに応じて、配布ステータスのログファイルを確認できます。ログファイル (.log) は、Distributor および Subscriber の作業ディレクトリに作成されます。
- **Distribution ファイル：** Distributor のファイルシステム (¥zenworks¥pds¥ted¥dist) と Subscriber のファイルシステム (¥zenworks¥pds¥ted¥sub¥*individual_Distribution's_path*) の Distribution ファイルを比較し、受信されているかどうかを確認します。Distribution ファイルには両方のサーバで同じ名前が使用されます。

配布システムの管理

ここまでの操作で、Policy and Distribution Services システムの設定が完了し使用できる状態になります。配布システムを更新する場合は、46 ページの「配布システムの設定」の必要な節を再度参照します。

配布システムは、ConsoleOne および iManager ツールを使用して管理できます。これらのツールには、それぞれ他方にはない機能がいくつかあります。通常、ConsoleOne はインストールや設定作業に使用し、iManager は管理作業に使用します。詳細については、84 ページの「iManager の ZENworks Server Management の役割と ConsoleOne 機能の比較」を参照してください。

ConsoleOne の使用については、次の章を参照してください。

- 3 章 87 ページの「Tiered Electronic Distribution」
- 4 章 197 ページの「Server Policies（サーバポリシー）」
- 5 章 241 ページの「Server Software Package に関する問題」
- 6 章 283 ページの「Desktop Application Distribution」
- 11 章 379 ページの「レポート機能」

iManager の使用については、69 ページの「Novell iManager」を参照してください。

設定計画ワークシート

配布システムの設定を計画する際、次のワークシートに設定情報を記録してください。一部の項目では、リストを添付する必要があります。

このワークシートは、PDF バージョンの文書から適切に印刷されるように設計されています。

重要： 十分な経験があるユーザでも、この計画ワークシートだけを使用して Policy and Distribution Services を設定しないでください。計画が不要なためこのワークシートに含まれていない設定手順もあります。Policy and Distribution Services を実際に設定する際のガイドとして、46 ページの「配布システムの設定」の各節を参照してください。

設定情報	説明
追加の Distributor、データベース、および Subscriber のインストール	追加の Distributor、データベース、または Subscriber をインストールしない場合は、ワークシートの項目 12 に進みます。
1) Distributor および ZENworks データベースオブジェクト用のツリー：	Server Management オブジェクトをインストールする eDirectory ツリーの名前を指定します。 詳細については、33 ページの「ネットワークトポロジの理解」を参照してください。
2) Distributor サーバ名：	Distributor にする各サーバのサーバ名を指定します。Distributor サーバは、Distribution を構築して所有するサーバです。 詳細については、34 ページの「Distributor プロパティ」を参照してください。
3) Subscriber サーバ名：	Subscriber にする各サーバのサーバ名を指定します。Subscriber サーバは、Distribution を受信して抽出するサーバです。 詳細については、37 ページの「他の Subscriber のインストールの必要性」を参照してください。

設定情報	説明
4) データベースサーバ名：	Server Management データベースをインストールする各サーバのサーバ名を指定します。Server Management データベースは、NetWare および Windows サーバにインストールできます。 Policy and Distribution Services では複数のデータベースを使用できますが、1 つのサーバにインストールできるのは 1 つデータベースのみです。 各データベースを同じ方法で使用する場合は、個々のデータベースの目的を指定するか、Distributor ID を指定します。 詳細については、35 ページの「Distributor サーバで Server Management データベースをホストするかどうか」を参照してください。
5) Distributor ソフトウェアのインストールパス：	Distributor ソフトウェアをインストールするパスを指定します。デフォルトのパスは、NetWare および Windows サーバのいずれも ¥zenworks です。 詳細については、35 ページの「ソフトウェアのインストールパス」を参照してください。
6) Subscriber ソフトウェアのインストールパス：	Subscriber ソフトウェアをインストールするパスを指定します。デフォルトのパスは、NetWare および Windows サーバのいずれも ¥zenworks です。 詳細については、35 ページの「ソフトウェアのインストールパス」を参照してください。

設定情報	説明
7）インストール時のデフォルトと異なる Distributor のプロパティ：	Distributor サーバの次の情報を編集します。 ◆ Distributor オブジェクトの名前（デフォルトは Distributor_*server_name*） ◆ Distributor のコンテキスト ◆ Distributor サーバの作業ディレクトリ 詳細については、34 ページの「Distributor プロパティ」を参照してください。
8）インストール時のデフォルトと異なる Subscriber のプロパティ：	Subscriber サーバの次の情報を編集します。 ◆ Subscriber オブジェクトの名前（デフォルトは Subscriber_*server_name*） ◆ Subscriber のコンテキスト ◆ Subscriber サーバの作業ディレクトリ 詳細については、37 ページの「他の Subscriber のインストールの必要性」を参照してください。

設定情報	説明
9) Server Management データベースソフトウェアのインストールパス：	zfslog.db ファイルを保存するパスを指定します。デフォルトのパスは、¥zenworks¥database です。データベースファイルはサイズが非常に大きくなる可能性があるため、NetWare サーバでは、sys: ボリュームを使用しないことをお勧めします。また、[Database Purge] オプションを使用できるように、データベースソフトウェアと Subscriber ソフトウェアを同じサーバにインストールすることをお勧めします。 詳細については、35 ページの「ソフトウェアのインストールパス」を参照してください。
10) データベースオブジェクト名：	デフォルトの名前を使用するか、データベースの目的を識別しやすい名前を指定します。 詳細については、35 ページの「Distributor サーバで Server Management データベースをホストするかどうか」を参照してください。
11) データベースオブジェクトのコンテナ：	他の Tiered Electronic Distribution オブジェクトと同じコンテナを使用することをお勧めします。 詳細については、35 ページの「Distributor サーバで Server Management データベースをホストするかどうか」を参照してください。
混在 eDirectory 環境での Distributor の設定	混在 eDirectory 環境でない場合は、ワークシートの項目 13 に進みます。
12) eDirectory 8.*x* のサーバの IP アドレス：	eDirectory 8.*x* を使用しているツリー内のサーバの IP アドレスを指定します。Distributor サーバで eDirectory 8.*x* を実行している場合は、Distributor サーバの IP アドレスになる場合があります。 詳細については、36 ページの「Distributor を混在 eDirectory 環境で実行できるかどうか」を参照してください。
サーバ間通信のインストール	サーバ間通信のセットアップが不要な場合は、ワークシートの項目 14 に進みます。

設定情報	説明
13) セキュリティで保護されたネットワーク外の Subscriber サーバ：	Distributor および Subscriber サーバがセキュリティで保護されたネットワーク外のサーバと通信する場合は、サーバ間通信セキュリティが必要になる場合があります。 詳細については、41 ページの「サーバ間通信セキュリティの必要性の判断」を参照してください。
Windows、Linux、または Solaris サーバへの NICI のインストール	これらのサーバに NICI をインストールする必要がない場合は、ワークシートの項目 15 に進みます。
14) Distribution の暗号化に関連する Windows、Linux、または Solaris サーバ (Distributor または Subscriber)：	暗号化された Distribution を構築 (Distributor) または抽出 (Subscriber) する Windows、Linux、または Solaris サーバのリストを作成します。 詳細については、41 ページの「Windows サーバに対する暗号化セキュリティの必要性の判断」を参照してください。

設定情報	説明
Distributor のルーティング階層の設定	
15) 階層化された Subscriber から成る Distributor のルーティング階層：	ネットワーク上での Distribution の配布方法を示す階層化された Subscriber の図を Distributor ごとに作成します。別の Distributor のルーティング階層にある Subscriber を他の Distributor でも使用することができます。ただし、エンドノード Subscriber が特定の Distribution を受信するときに配布パスが 1 つになるように、1 つの Subscriber は 1 つの Distributor の階層で一度だけ使用するようにします。 詳細については、38 ページの「配布フローの決定」を参照してください。
親 Subscriber の設定	
16) Subscriber/ 親 Subscriber の割り当て (親 Subscriber とエンドノード Subscriber の関連付け):	各親 Subscriber が Distribution を配布する Subscriber のリストを作成します。Distributor から直接 Distribution を受信するエンドノード Subscriber を除いて、各エンドノード Subscriber を親 Subscriber に割り当てます。 詳細については、39 ページの「配布ルートに対する Subscriber の選択」を参照してください。

設定情報	説明
Subscriber Group の作成と設定	Subscriber Group を使用しない場合は、ワークシートの項目 19 に進みます。
17) Subscriber Group オブジェクト名：	Subscriber Group の一意な名前を指定します。 詳細については、44 ページの「Subscriber Group」を参照してください。
18) このグループに含める Subscriber:	グループが登録されている Channel からの Distribution を必要とする Subscriber のリストを作成します。
Policy Package Distribution の作成	

設定情報	説明
19) Distribution、Distribution のタイプ、および Distributor:	Distribution のリストを作成します。各 Distribution について、Distribution のタイプ、オブジェクト名、およびその Distribution を必要とするサーバを指定します。Distribution のタイプは次のとおりです。 ◆ 29 ページの「Desktop Application」 ◆ 29 ページの「File」 ◆ 29 ページの「FTP」 ◆ 30 ページの「HTTP」 ◆ 30 ページの「MSI」 ◆ 30 ページの「ポリシーパッケージ」 ◆ 32 ページの「RPM」 ◆ 32 ページの「Software Package」 詳細については、28 ページの「Distribution の選択」を参照してください。
Channel の作成と設定	
20) Tiered Electronic Distribution オブジェクトの eDirectory コンテナ：	Tiered Electronic Distribution オブジェクトを作成および管理するためのコンテナです。 コンテナは、Policy and Distribution Services のインストール時に作成している場合があります。作成していない場合は、Tiered Electronic Distribution オブジェクトの管理専用に作成する必要があります。 詳細については、35 ページの「Distributor サーバで Server Management データベースをホストするかどうか」を参照してください。

設定情報	説明
21) Channel 名：	Distribution に必要な Channel オブジェクトの名前を指定します。Distribution または Distribution のグループごとに一意の Channel 名を使用することをお勧めします。 詳細については、42 ページの「Distribution の Channel の決定」を参照してください。
22) Channel の Distribution:	Channel が所有する Distribution のリストを作成します。 詳細については、42 ページの「Distribution の Channel の決定」を参照してください。

設定情報	説明
Channel への登録	
23) Subscriber の抽出スケジュール：	Subscriber が Distribution を抽出する最適なタイミングに基づいて、Subscriber サーバごとに抽出スケジュールを設定します。 詳細については、43 ページの「Subscriber の登録の決定」を参照してください。
24) Channel と Subscriber/Subscriber Group との関連付け：	Channel に関連付ける Subscriber/Subscriber Group のリストを作成します。Subscriber/Subscriber Group は関連付けられた Channel から Distribution を受信します。

2 Novell iManager

Novell® iManager をまだインストールしていない場合は、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「管理固有のワークステーションの要件」を参照してください。ZENworks® 6.5 SP1 Server Management は、iManager 2.0.2 および 2.5 をサポートしています。ただし、Windows Server 2003 の場合はバージョン 2.5 が必要です。

iManager の ZENworks Server Management の役割を使用すると、Server Policies と Tiered Electronic Distribution のオブジェクト、エージェント、およびプロセスを、Web ブラウザ Internet Explorer 5.5 以上を使用できる任意の場所から管理できます。iManager 用 Server Management プラグインは、このブラウザでのみ機能します。ZENworks 6.5 SP1 では、その他のブラウザはサポートされていません。

ZENworks Server Management の役割で次の操作を実行できます。

- Tiered Electronic Distribution オブジェクト (Distribution、Subscriber、Distributor、Channel、Subscriber Group、および External Subscriber) の作成、修正、および削除。
- ポリシーおよびポリシーパッケージの作成、変更、削除、配布、および適用。
- グラフ形式での配布システムの表示。これにより、Distribution が通過する親 Subscriber の数に関係なく、Distributor からエンドノード Subscriber に送信される Distribution を簡単に追跡できます。
- ブラウザベースのコンソールの表示。このコンソールは Remote Web Console と呼ばれ、システム内の Distributor Agent および Policy/Package Agent ごとに表示されます。Remote Web Console を使用して、エージェントの設定のチェック、エージェントの動作の監視のほか、Distributor または Subscriber サーバでのアクションの強制実行や Distributor または Subscriber のステータスの監視などの多数のエージェント機能の制御が可能です。

次の節では、ZENworks Server Management の役割の主要な機能を使用するために必要な情報を紹介します。

- 70 ページの「iManager の ZENworks Server Management の役割へのアクセス」
- 73 ページの「Tiered Electronic Distribution オブジェクトの管理」
- 76 ページの「配布プロセスの監視」
- 79 ページの「Remote Web Console によるエージェントの管理」
- 84 ページの「iManager の ZENworks Server Management の役割と ConsoleOne 機能の比較」

iManager の ZENworks Server Management の役割へのアクセス

iManager にログインして、iManager での ZENworks の役割を理解するには、次の節を参照してください。

- 70 ページの「iManager へのログイン」
- 71 ページの「インタフェースの理解」
- 72 ページの「役割とタスクの表示」

iManager へのログイン

バージョン 2.0.2 はツリーに依存し、バージョン 2.5 はツリーに依存していないため、iManager にログインする手順は、バージョン 2.0.2 と 2.5 では異なります。

Web ブラウザで iManager にアクセスするには

- 70 ページの「iManager 2.0.2 へのログイン」
- 71 ページの「iManager 2.5 へのログイン」

iManager 2.0.2 へのログイン

1 Tiered Electronic Distribution オブジェクトが存在する Novell eDirectory™ ツリーにログインしていない場合は、ログインします。

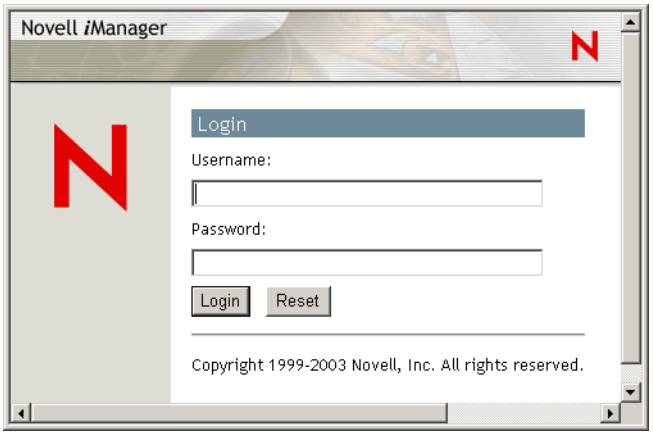
ヒント： Novell Client™ がインストールされていない Windows サーバで iManager を実行する場合は、ツリー名を指定するのではなく、eDirectory ツリーのレプリカが存在するサーバの IP アドレスを指定します。

2 次の URL にアクセスします。

`http://server/nps/iManager.html`

server は、iManager がインストールされている IP アドレスまたは DNS ホスト名です。

次のダイアログが表示されます。



3 iManager ログインページが表示されない場合は、正しいサーバを指定していること、および nps と iManager.html を例のように正確に入力していること（大文字と小文字が区別されます）を確認してください。

ヒント： http ではなく https を使用する場合もあります。

4 ステップ 2 で識別したサーバのユーザ名およびパスワードを指定して、<Enter> キーを押すか [Login] をクリックします。

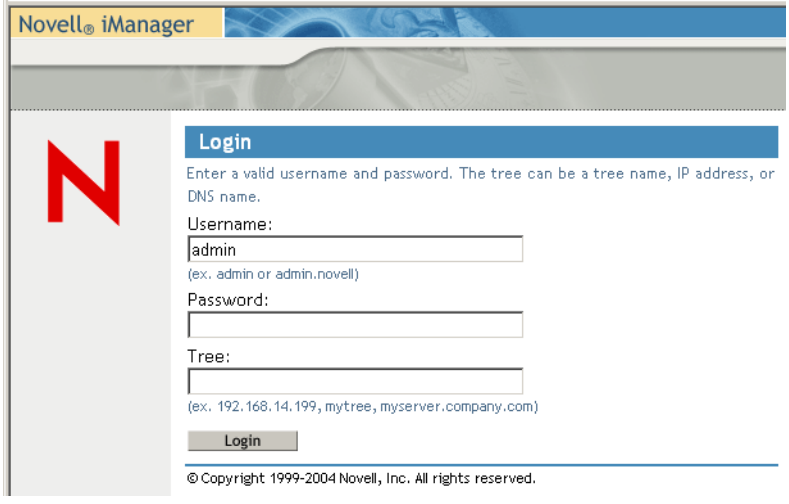
iManager 2.5 へのログイン

1 次の URL にアクセスします。

`http://server/nps/iManager.html`

server は、iManager がインストールされている IP アドレスまたは DNS ホスト名です。

次のダイアログが表示されます。



2 Manager ログインページが表示されない場合は、正しいサーバを指定していること、および nps と iManager.html を例のように正確に入力していること（大文字と小文字が区別されます）を確認してください。

ヒント： http ではなく https を使用する場合もあります。

3 ステップ 1 で識別したサーバのユーザ名およびパスワードを指定します。

4 そのサーバのツリー指定を入力して、<Enter> キーを押すか［Login］をクリックします。

iManager 2.5 はツリーに依存していません。したがって、バージョン 2.0.2 の場合のようにログインする前ではなく、ログイン中にツリーを指定でき、サーバの IP アドレス、ツリー名、サーバの DNS 名のいずれかを使用してツリーを特定できます。

インタフェースの理解

1 ログインが完了すると、iManager のメインページが表示されます。上部のフレームには、各機能を表すアイコンが表示されます。



2 マウスポインタをアイコンの上に移動して、各機能の目的を確認します。

アイコンの列の右側に、ヒントのテキストが表示されます。

デフォルトでは、［Roles and Tasks］アイコンがアクティブになっています。このアイコンには、ZENworks の機能が存在します。

役割とタスクの表示

1 iManager で［Roles and Tasks］アイコンを選択します。

デフォルトでは、左側のペインのツリー構造の一番下に、ZENworks Server Management の役割が表示されます。

2 左側のパネルで［ZENworks Server Management］を展開し、利用可能なタスクの一覧を表示します。



これらのタスクの機能は、次のとおりです。

タスク	機能
TED オブジェクトの作成	Distributor と Subscriber を除く、Tiered Electronic Distribution オブジェクトを作成します。
TED オブジェクトの削除	Tiered Electronic Distribution オブジェクトを削除します。
TED オブジェクトの編集	Tiered Electronic Distribution オブジェクトのプロパティを編集します。
Remote Web Console（リモート Web コンソール）	Tiered Electronic Distribution 情報または Server Policies 情報を表示および管理します。
［Subscriber Distribution］ビュー	選択した Subscriber と、そのすべての Distribution を表示および管理します。
［Tiered Distribution］ビュー	選択した Distribution、または選択した Distributor とそのすべての Distribution を表示および管理します。

3 前記の ZENworks Server Management タスクの一部が表示されず、RBS(Role-Based Services) を設定している場合、表示されないタスクにアクセスする管理者用に、ZENworks Server Management モジュールをアップグレードまたは再インストールする必要があります。

たとえば、iManager 用の ZENworks Server Management プラグインをアップグレードした後に、アップグレードによって新しいタスクが導入された場合、設定された RBS コレクションには新しいタスクは表示されません。

この問題を解決するには、使用している iManager のバージョンに応じた手順に従います。

- 73 ページの「iManager 2.0.2 でのコレクションのアップグレード」
- 73 ページの「iManager 2.5 でのコレクションの再インストール」

4 実行するタスクに進みます。

- 73 ページの「Tiered Electronic Distribution オブジェクトの管理」
- 76 ページの「配布プロセスの監視」
- 79 ページの「Remote Web Console によるエージェントの管理」

iManager 2.0.2 でのコレクションのアップグレード

1 iManager にログインして、[Configure] アイコンをクリックします。

2 [RBS Configuration] の下で [Configure iManager] をクリックします。

3 [Upgrade Collections] を選択し、[Next] をクリックします。

4 アップグレードするコレクションが選択されていることを確認して、[Next] をクリックします。

期限切れまたはまだインストールされていない iManager モジュールを持つコレクションのみが表示されます。

5 ZFSModule が選択されていることを確認し、スコープを選択して、[Start] をクリックします。

6 モジュールが正常にアップグレードされたことを確認し、[Close] をクリックします。

7 [Roles and Tasks] アイコンをクリックします。

[ZENworks Server Management] の下に、表示されていなかった ZENworks Server Management の役割が表示されます。

8 72 ページのステップ 4 に進みます。

iManager 2.5 でのコレクションの再インストール

1 iManager にログインして、[Configure] アイコンをクリックします。

2 [Role Based Services] を展開して、[RBS Configuration] をクリックします。

3 [Name] 列で、編集するコレクションを選択します。

4 [Name] 列で、ZENworks Server Management の役割を選択します。

5 [Reinstall] 列で、表示されている ZFSModule 名のチェックボックスをクリックします。

6 [Reinstall]（列見出し）をクリックします。

7 情報のダイアログボックスで [OK] をクリックし、モジュールの再インストールを開始します。

8 モジュールが正常に再インストールされたことを確認し、[Roles and Tasks] アイコンをクリックします。

[ZENworks Server Management] の下に、表示されていなかった ZENworks Server Management の役割が表示されます。

9 72 ページのステップ 4 に進みます。

Tiered Electronic Distribution オブジェクトの管理

iManager の ZENworks Server Management の役割で、eDirectory の次の Tiered Electronic Distribution オブジェクトのいくつかを作成、編集、または削除できます。

Distributor（作成不可）
Channel
Distribution
Subscriber（作成不可）

Subscriber Group
External Subscriber

これらの Tiered Electronic Distribution オブジェクトに対して、ConsoleOne® で実行できるすべての管理タスクを iManager でも実行できます。

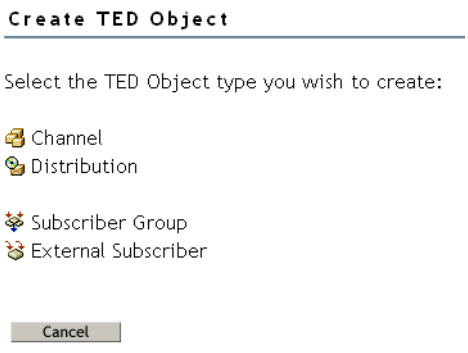
- 74 ページの「iManager での Tiered Electronic Distribution オブジェクトの作成」
- 75 ページの「iManager での Tiered Electronic Distribution オブジェクトプロパティの編集」
- 75 ページの「iManager での Tiered Electronic Distribution オブジェクトの削除」

Policy and Distribution Services の次の管理タスクは、iManager では実行できません。これらのタスクは、ConsoleOne で実行する必要があります。

- Server Management データベースの管理。10 章 365 ページの「ZENworks Database」を参照してください。
- Server Management データベースからのレポートの作成。11 章 379 ページの「レポート機能」を参照してください。

iManager での Tiered Electronic Distribution オブジェクトの作成

1 上部のフレームで［Roles and Tasks］を選択し、左側のフレームで［ZENworks Server Management］を展開して［Create TED Object］をクリックします。



2 作成するオブジェクトのタイプを選択します。

ConsoleOne で作成できる Distribution タイプは、iManager でも作成できます。

3 オブジェクトの一意の名前、オブジェクトを作成するコンテキストなど、作成するオブジェクトのタイプに必要な情報を指定します。

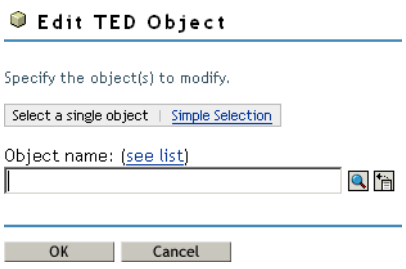
詳細については、［Help］アイコン（疑問符マーク）をクリックします。

4 ［OK］をクリックしてオブジェクトの作成を終了します。

5 75 ページの「iManager での Tiered Electronic Distribution オブジェクトプロパティの編集」に進んで、新しい Tiered Electronic Distribution オブジェクトを設定します。

iManager での Tiered Electronic Distribution オブジェクトプロパティの編集

1 上部のフレームで［Roles and Tasks］を選択し、左側のフレームで［ZENworks Server Management］を展開して［Edit TED Object］をクリックします。



2 プロパティを編集する Tiered Electronic Distribution オブジェクトを参照して選択し、［OK］をクリックします。

ConsoleOne で利用可能なプロパティページとオプションが iManager でも利用できます。

オプション設定の詳細については、各プロパティページで［Help］をクリックします。

3 必要に応じてオブジェクトを設定し、［OK］をクリックして新しいプロパティ設定を保存します。

iManager での Tiered Electronic Distribution オブジェクトの削除

1 上部のフレームで［Roles and Tasks］を選択し、左側のフレームで［ZENworks Server Management］を展開して［Delete TED Object］をクリックします。



2 削除する Tiered Electronic Distribution オブジェクト（複数可）を選択し、［OK］をクリックして［Delete TED Objects］ページにオブジェクトの一覧を表示します。

3 配布システムから特定のタイプのオブジェクトを削除した場合の影響については、［Help］アイコンをクリックします。

4 ［OK］をクリックして一覧のオブジェクトを削除し、再度［OK］をクリックして削除を確認します。

5 オブジェクトの削除によって配布システムに支障が生じないよう、オンラインヘルプの手順に従って残りのオブジェクトを設定し直します。

配布プロセスの監視

[Tiered Distribution] ビューを使用すると、Distributor から送信された Distribution が親 Subscriber を通過してエンドノード Subscriber に受信されるまでを監視することができます。これにより、Distribution を受信した Subscriber、その Distribution の送信元、および受信時間を確認できます。また、配布プロセスで発生する可能性のある問題のトラブルシューティングや解決にも役立ちます。

[Subscriber Distribution] ビューには、監視リストに追加する各 Subscriber のすべての Distribution のステータスビューが表示されます。このビューを使用すると、Subscriber の Distribution をトラブルシューティングできます。

これらの機能は、ConsoleOne では使用できません。

次の節では、これらのビューの使用方法を説明します。

- 76 ページの「[Tiered Distribution] ビューの使用」
- 77 ページの「[Subscriber Distribution] ビューの使用」

[Tiered Distribution] ビューの使用

iManager の [Tiered Distribution] ビューにアクセスするには

1. 上部のフレームで [Roles and Tasks] を選択し、左側のフレームで [ZENworks Server Management] を展開して [Tiered Distribution] ビューをクリックします。
2. 追跡する Distribution を参照して選択し、[Next] をクリックします。
3. Distribution を追跡する Channel を選択し、[Next] をクリックします。

   [Distribution System] ウィンドウに Distribution を受信する Subscriber の一覧が表示されます。
4. [Expand All] をクリックし、Distribution を構築および送信した Distributor とその Distribution を受信するエンドノード Subscriber 間のルーティング階層を表示します。

   または

   個々のサーバを選択して階層の一部を展開します。

   各アイコンは次のような Distribution のステータスを示します。

アイコン	意味
	Distribution は正常に受信および抽出されました。
	Distribution は受信されましたが、まだ抽出されていません。 Subscriber の抽出スケジュールをチェックし、抽出が試行されたかどうかを確認してください。抽出が試行され失敗していた場合は、Subscriber のイベントログで抽出時に発生したエラーを確認します。80 ページの「Distributor Agent の管理」を参照してください。
	Distribution は Subscriber に受信されていません。 Subscriber のイベントログで、問題を記述したエラーメッセージを確認してください。80 ページの「Distributor Agent の管理」を参照してください。

アイコン	意味
	Distribution のステータスについて、Subscriber から Distributor に応答がありません。 Subscriber および Subscriber と Distributor 間にある親 Subscriber のステータスをチェックしてください。80 ページの「Distributor Agent の管理」を参照してください。

5 [Refresh Screen Every __ Seconds] フィールドに時間間隔を入力して、[Start] をクリックすると、その頻度で表示が更新されます。

入力できるのは秒数のみです。

これは、配布プロセスが発生したときにトラブルシューティングを行う場合に便利です。

6 ステータス情報を表示するには、Distributor または Subscriber を選択し、[Remote Web Console] を選択します。

取得できるステータス情報のタイプについては、79 ページの「Remote Web Console によるエージェントの管理」を参照してください。

7 設定情報をチェックするには、Distributor または Subscriber を選択し、[eDirectory Configuration] を選択します。

Distributor または Subscriber オブジェクトのプロパティは、[ZENworks Server Management] の [Edit TED Object] をクリックした場合と同様に編集できます。ConsoleOne で利用可能なプロパティページとオプションが iManager でも利用できます。

[Subscriber Distribution] ビューの使用

iManager の [Subscriber Distribution] ビューにアクセスするには

1 上部のフレームで [Roles and Tasks] を選択し、左側のフレームで [ZENworks Server Management] を展開して [Subscriber Distribution] ビューをクリックします。

2 [Add] をクリックして、追跡する Subscriber を選択します。

追加された各 Subscriber には、最初は Distribution は表示されません。

3 Distribution リストを展開するには、個別の Subscriber を選択します。

または

[Expand All] をクリックすると、表示された各 Subscriber の Distribution が表示されます。

各アイコンは、次のような Subscriber の Distribution のステータスを示します。

アイコン	意味
	Distribution が正常に受信されなかったか、抽出に失敗しました。 Subscriber のイベントログで、問題を記述したエラーメッセージを確認してください。80 ページの「Distributor Agent の管理」を参照してください。

アイコン	意味
	Distributor にアクセスできなかったか、Distributor が Subscriber からステータスを受信していないため、Distribution のステータスは不明です。 Subscriber または Distributor のステータスを確認します。80 ページの「Distributor Agent の管理」を参照してください。
	Distribution は正常に受信されましたが、抽出スケジュールが開始されていないなどの理由で、まだ抽出されていません。 Subscriber の抽出スケジュールをチェックし、抽出が試行されたかどうかを確認してください。
	Distribution は正常に受信および抽出されました。

Subscriber と Distribution はステータス別にソートされた後、ステータス内でアルファベット順に並べ替えられます。重大な Distribution ステータスを先に表示する場合、ステータスの順序は次のようになります。

1. 重大
2. 不明
3. 受信済み
4. 抽出済み

次の項目の隣にいずれかのアイコンが表示される場合：

- **[Subscriber]（ツリー構造のルート項目）：** ステータスは、下位の複数の Distribution に適用されます。したがって、[Subscribers] には、リストのステータスの最も重大なアイコンが表示されます。
- **[Subscriber] アイコン：** ステータスは、Subscriber の複数の Distribution に適用されます。したがって、ステータスアイコンには、Subscriber の Distribution の最も重大なステータスアイコンが表示されます。
- **[Distribution] アイコン：** ステータスは、この Distribution にのみ適用されます。

4 マウスを Distribution の上に移動すると、次の情報が表示されます。

DNS 名
NDS 名
TED バージョン
受信ステータス
受信時刻
抽出可否（Distribution に Subscriber が登録されているかどうかを示すために、True または False が表示されます）
抽出時刻
抽出ステータス
Distributor
親 Subscriber

マウスをステータスアイコンの上に移動すると、関連するオブジェクト（Subscriber または Distribution）の最も重大なステータスを示す短い文が表示されます。

5 [Refresh Screen Every __ Seconds] フィールドに時間間隔を入力して、[Start] をクリックすると、その頻度で表示が更新されます。

入力できるのは秒数のみです。

更新を中断するには、[Stop] をクリックします。

これは、Distribution の修正が機能しているかどうかを判断したり、別の Subscriber にロールアウトするときに配布プロセスをトラブルシューティングする場合に便利です。

6 ステータス情報を表示するには、Subscriber を選択し、[Remote Web Console] を選択します。

このオプションは、Distribution には適用されません。

取得できるステータス情報のタイプについては、79 ページの「Remote Web Console によるエージェントの管理」を参照してください。

7 設定情報を編集するには、Subscriber または Distribution を選択し、[eDirectory Configuration] を選択します。

Subscriber または Distribution オブジェクトのプロパティは、ZENworks Server Management の役割で [Edit TED Object] をクリックした場合と同様に編集できます。ConsoleOne で利用可能なプロパティページとオプションが iManager でも利用できます。

Remote Web Console によるエージェントの管理

NetWare® サーバでは、Distributor Agent および Policy/Package Agent を実行しているサーバコンソールで、これらのエージェントを監視できます。また、iManager の ZENworks Server Management の役割を使用すると、サポートされているプラットフォーム (NetWare、Windows、Linux、または Solaris) 上で実行されているエージェントを Internet Explorer から監視できます。

- 80 ページの「Distributor Agent の管理」
- 82 ページの「Policy/Package Agent の管理」
- 84 ページの「複数の Remote Web Console ウィンドウの表示」

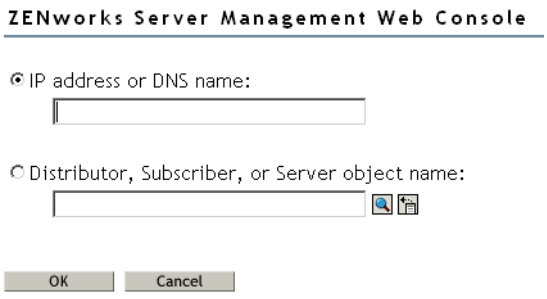
Policy and Distribution Services の次の管理タスクは、iManager では実行できません。これらのタスクは、ConsoleOne で実行する必要があります。

- ポリシーパッケージの作成、編集、および削除。4 章 197 ページの「Server Policies (サーバポリシー)」を参照してください。
- ソフトウェアパッケージの作成、編集、および削除。5 章 241 ページの「Server Software Package に関する問題」を参照してください。

Distributor Agent の管理

iManager で Distributor または Subscriber の Remote Web Console にアクセスするには

1 上部のフレームで［Roles and Tasks］を選択し、左側のフレームで［ZENworks Server Management］を展開して［Remote Web Console］をクリックします。



2 Distributor Agent または Policy/Package Agent が実行されているサーバの IP アドレスまたは DNS ホスト名を指定します。

または

Distributor または Subscriber オブジェクトを参照して選択するか、Distributor Agent が実行されているサーバを示すサーバオブジェクトを参照して選択します。

3 ［OK］をクリックします。

［Display］フィールドに、Tiered Electronic Distribution がデフォルトで表示されます。

Remote Web Console のフレーム上部のタブに、Policy and Distribution Services エージェントに関するさまざまなタイプの情報が表示されます。詳細なオプションは各タブで利用できます。



［Remote Web Console］ページで利用可能な機能について詳細を参照するには、各ページで［Help］をクリックします。

4 実行するタスクに進みます。

- 81 ページの「Tiered Electronic Distribution オブジェクトの管理」
- 81 ページの「Policy and Distribution Services エージェントのステータスの監視」
- 81 ページの「Distribution のステータスの監視」
- 82 ページの「Policy and Distribution Services エージェントの強制実行」
- 82 ページの「セキュリティ証明書の管理」

これらのタスク、各タスクに使用する Remote Web Console のタブとオプション、およびそのタスクが ConsoleOne で実行できるかどうかを次の表にまとめます。

Tiered Electronic Distribution オブジェクトの管理

Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
Distributor および Subscriber オブジェクトの全オブジェクトプロパティを単一リストに表示	[Configuration] > [Configuration]	No
ルーティング階層内にある下位 Subscriber のオブジェクトプロパティをリストに表示	[Configuration] > [Subordinate Configuration]	No
Distribution オブジェクトの全オブジェクトプロパティ（タイプ固有の情報を除く）を単一リストに表示	[Distributions] > [Distribution Information]	No
Channel オブジェクトの全オブジェクトプロパティを単一リストに表示	[Channels] > [Channel Information]	No
Server Management データベースに関する情報を表示	[Configuration] > [Database]	Yes

eDirectory のオブジェクトプロパティが変更された後、Distributor が更新されるまでは、Remote Web Console に表示されるオブジェクトプロパティと ConsoleOne に表示されるオブジェクトプロパティに相違が生じます。Remote Web Console には、Distributor Agent 側からの情報が表示されます。

Policy and Distribution Services エージェントのステータスの監視

Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
現在の Distributor のイベントログを重要度レベルのメッセージ付きで参照および継続的に更新	[Events] > [Distributor Event Log]	No
現在の Subscriber のイベントログを重要度レベルのメッセージ付きで参照および継続的に更新	[Events] > [Subscriber Event Log]	No
Policy and Distribution Services エージェントの機能を実行するために開始されたさまざまな配布スレッドの現在のステータスを表示	[Configuration] > [Threads]	No

Distribution のステータスの監視

Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
Distributor および Subscriber で現在処理されているすべての Distribution とその詳しいステータス情報をリストに表示	[Distributions] > [Active Distributions]	No
Subscriber が受信した Distribution のステータス情報を選択して表示	[Distributions] > [Received Distributions]	No

Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
Distributor または親 Subscriber から下位の Subscriber まで、ルーティング階層内で Distribution が使用するルートを表示	[Configuration] > [Route to Subscriber]	No

Policy and Distribution Services エージェントの強制実行

Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
Distributor をただちに更新し、eDirectory を読み込んで修正されたDistributionをチェック	[Configuration] > [Refresh Distributor]	Yes
Distribution をただちに構築	[Distributions] > [Build Distribution]	スケジュールによる
選択された Channel のすべての Distribution を Subscriber にただちに送信	[Channels] > [Distribute Channel]	一度のクリックでは不可

セキュリティ証明書の管理

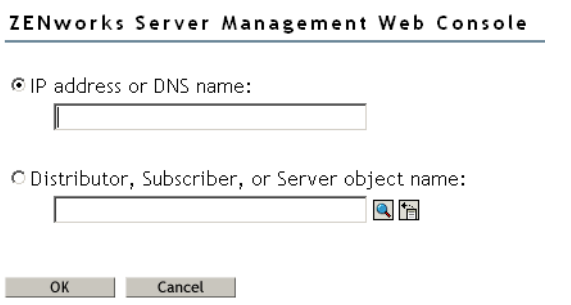
Policy and Distribution Services エージェントの管理タスク	Remote Web Console のタブとオプション	ConsoleOne
Subscriber で利用可能なセキュリティ証明書をリストに表示	[Security] > [Show Certificates]	No
Subscriber からセキュリティ証明書を削除	[Security] > [Show Certificates] > [Remove Certificate]	No
Distributor から送信された暗号化 Distribution が Subscriber で受信されるように、Subscriber の .csr(Certificate Signing Request) ファイルに Distributor から署名	[Security] > [Sign CSR]	Yes

Policy/Package Agent の管理

Policy/Package Agent は、ソフトウェアをインストールし、受信および抽出したポリシーを適用する役割を果たします。Remote Web Console を使用すると、ConsoleOne ではできない Policy/Package Agent の管理を行なうことができます。

iManager で Policy/Package Agent の Remote Web Console にアクセスするには

1 上部のフレームで［Roles and Tasks］を選択し、左側のフレームで［ZENworks Server Management］を展開して［Remote Web Console］をクリックします。



2 Policy/Package Agent が実行されているサーバの IP アドレスまたは DNS ホスト名を指定します。

または

Subscriber オブジェクトを参照して選択するか、Policy/Package Agent が実行されているサーバを示すサーバオブジェクトを参照して選択します。

3 ［OK］をクリックします。

4 ［Display］フィールドで［Policy Package Agent］を選択します（Tiered Electronic Distribution がデフォルトで表示されます）。

Remote Web Console のフレーム上部のタブに、Policy/Package Agent に関するさまざまなタイプの情報が表示されます。



［Remote Web Console］ページで利用可能な機能について詳細を参照するには、各ページで［Help］をクリックします。

5 実行するタスクに進みます。

これらのタスクと各タスクに対する Remote Web Console のタブについて、次の表にまとめます。

Policy/Package Agent の管理タスク	Remote Web Console（リモート Web コンソール）	ConsoleOne
サーバポリシーを適用するために現在ロードされているプラグインをリストに表示	環境設定	No
Policy/Package Agent に値があるすべての変数をリストに表示	環境設定	No
Policy/Package Agent によって Subscriber サーバで適用されるすべてのポリシーをリストに表示	Policies	No
Subscriber サーバ上のポリシー（複数可）をただちに適用	Policies	No
Subscriber サーバからポリシーを個別に削除	Policies	No

Policy/Package Agent の管理タスク	Remote Web Console（リモート Web コンソール）	ConsoleOne
ポリシー（複数可）をただちに更新し Distributor Agent から eDirectory の変更内容を読み込み	Policies	No
Policy/Package Agent によって Subscriber サーバにインストールされたすべてのソフトウェアパッケージをリストに表示	[Software Packages]	No
Subscriber サーバにインストールされたすべてのソフトウェアパッケージの現在のステータスを確認	[Software Packages]	No
Subscriber サーバでプログラムまたはスクリプトを作成し実行（1 回または繰り返し）	[Schedule]	No
Subscriber サーバを停止	アクション	No
Policy/Package Agent を再開	アクション	No

複数の Remote Web Console ウィンドウの表示

Remote Web Console の任意のページで右上隅の［Detach］をクリックすると、現在のページが新しいブラウザウィンドウで開きます。これにより、複数の Remote Web Console 機能に同時にアクセスできます。たとえば、Tiered Electronic Distribution エージェントのウィンドウと Policy/Package Agent のウィンドウを同時に表示できます。また、Remote Web Console のウィンドウを表示したまま、Novell iManager のメインウィンドウで別の ZENworks Server Management タスクを実行することもできます。

iManager の ZENworks Server Management の役割と ConsoleOne 機能の比較

主要な類似点と相違点を次の表にまとめます。

タスク	iManager	ConsoleOne
次の Tiered Electronic Distribution オブジェクトの作成、編集、および削除 Distributor（作成不可） Subscriber（作成不可） Distribution Channel Subscriber Group External Subscriber	Yes	Yes
次の Policy and Distribution Services コンポーネントの作成、編集、および削除 Policy Package Server Software Package Desktop Application	No	Yes

タスク	iManager	ConsoleOne
次の Distribution タイプのセットアップ Desktop Application File FTP HTTP MSI Policy Package RPM Software Package	Yes	Yes
Distributor の即時更新	Yes	Yes
Distribution の即時構築	Yes	一度のクリックでは不可
Channel にリストされたすべての Distribution の Subscriber への即時送信	Yes	一度のクリックでは不可
Policy and Distribution Services エージェントのイベントログとステータスの監視	Yes	No
Subscriber サーバのポリシーの一覧表示と管理	Yes	No
Subscriber サーバにインストールされたソフトウェアパッケージのステータスの一覧表示とチェック	Yes	No
Subscriber サーバでのプログラムおよびスクリプトの実行	Yes	No
Subscriber サーバの停止	Yes	No
セキュリティ証明書の管理 利用可能な証明書の一覧表示 証明書の解決 CSR への署名	 はい いいえ はい	 いいえ はい はい
Policy/Package Agent の管理	Yes	No

3 Tiered Electronic Distribution

Novell® ZENworks® Server Management には、ネットワーク上でのファイル、ポリシー、およびソフトウェアの配布を管理する Tiered Electronic Distribution が用意されています。

Tiered Electronic Distribution は、ConsoleOne® フレームワークのスナップインであるその他の Novell ネットワーク管理アプリケーションと統合され、Novell eDirectory™ の管理およびファイルアクセス制御を利用します。Tiered Electronic Distribution は、Novell iManager で ZENworks Server Management の役割を使用して管理することもできます。

Tiered Electronic Distribution については、次の節を参照してください。

- 87 ページの「一般的な配布タスク」
- 89 ページの「Tiered Electronic Distribution の理解」
- 96 ページの「Distributor」
- 112 ページの「Distribution」
- 147 ページの「Channels」
- 150 ページの「Subscriber」
- 158 ページの「Subscriber Group」
- 160 ページの「External Subscriber」
- 169 ページの「複数の Tiered Electronic Distribution オブジェクトの設定」
- 176 ページの「Distribution の送信」
- 180 ページの「Tiered Electronic Distribution に関するその他の問題」
- 190 ページの「作業ディレクトリ」
- 194 ページの「Tednode.properties ファイルの編集」

一般的な配布タスク

次の表に、よく使用する Tiered Electronic Distribution タスクへのリンクを示します。すべてのリンクは、このガイドの Policy and Distribution Services に関連する節に対応しています。

Tiered Electronic Distribution オブジェクト

タスク	説明
Distributor または Subscriber の作成	『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」
複数の Tiered Electronic Distribution オブジェクトの設定	169 ページの「複数の Tiered Electronic Distribution オブジェクトの設定」
Tiered Electronic Distribution サーバの DNS 名または IP アドレスの変更	188 ページの「Tiered Electronic Distribution サーバの DNS 名または IP アドレスの変更」

Distributor

タスク	説明
Distributor オブジェクトの設定	108 ページの「Distributor の設定」
Distributor のルーティング階層の作成	99 ページの「配布ルーティングの理解」 および 108 ページの「Distributor の設定」
Distributor オブジェクトの削除	112 ページの「Distributor オブジェクトの削除と Distribution への影響」
Distributor の更新	111 ページの「Distributor の更新」
Distributor でのセキュリティ証明書の作成と、関連付けられた Subscriber へのコピー	322 ページの「暗号化されていない Distribution 用のセキュリティ証明書の作成」

Distribution

タスク	説明
Distribution の作成	112 ページの「Distribution」
Distribution の削除	139 ページの「Distribution の削除」
孤立した Distribution の管理 (Distributor オブジェクトが削除された場合)	112 ページの「Distributor オブジェクトの削除と Distribution への影響」
Distribution のスケジュール設定と送信	176 ページの「Distribution の送信」
Distribution の強制送信	178 ページの「単一の Distribution の強制送信」
親 Subscriber による Distribution の送信	178 ページの「親 Subscriber による Distribution の送信」
他のツリーへの Distribution の送信	179 ページの「ツリー間の Distribution の送信」
手動での Distribution のインポートまたはエクスポート	143 ページの「手動による Distribution のインポートとエクスポート」

タスク	説明
ウィザードによる File Distribution の作成および送信	146 ページの「Distribution ウィザードの使用」

Channel

タスク	説明
Channel の作成	148 ページの「Channel の作成と設定」
Channel からの強制送信	150 ページの「Channel からの強制送信」

Subscriber

タスク	説明
Subscriber オブジェクトの設定	153 ページの「Subscriber の設定」
External Subscriber オブジェクトの作成	168 ページの「External Subscriber の作成と設定」
独自の設定機能がない Subscriber サーバでの tednode.properties ファイルの設定	194 ページの「Tednode.properties ファイルの編集」

ネットワークのトラフィック管理

タスク	説明
I/O レートの設定による Distribution トラフィックの帯域幅使用の制御	186 ページの「I/O レートと同時に実行可能な Distribution の制御」
ネットワークメッセージトラフィックの極小化	187 ページの「メッセージトラフィックの極小化」

Tiered Electronic Distribution の理解

Tiered Electronic Distribution を理解するには、次の節を参照してください。

- 90 ページの「Tiered Electronic Distribution による配布管理」
- 90 ページの「基本配布プロセス」
- 91 ページの「Tiered Electronic Distribution の eDirectory オブジェクト」
- 92 ページの「物理ネットワーク接続」
- 92 ページの「配布フローの詳細」
- 91 ページの「Tiered Electronic Distribution オブジェクトの関係」
- 93 ページの「Tiered Electronic Distribution のプロセス」
- 95 ページの「階層配布モデル」
- 96 ページの「Tiered Electronic Distribution の重要なコンポーネント」

Tiered Electronic Distribution による配布管理

Tiered Electronic Distribution には、サーバ間での電子データの配布を通じてサーバを管理する機能が用意されています。配布可能な電子データには、アプリケーションプログラム、複数のデータファイル、ソフトウェアパッチ、サーバポリシーなどがあります。

Policy and Distribution Services をインストールすると、Tiered Electronic Distribution とサーバポリシーオブジェクトが eDirectory ツリーに作成され、ソフトウェアが複数のサーバにコピーされ、インストール時の設定に従って Tiered Electronic Distribution と Server Policies コンポーネントの基本設定がセットアップされます。

Tiered Electronic Distribution ソフトウェアは、NetWare®、Windows NT、Windows 2000、Windows 2003 Server、Linux、および Solaris の各サーバで使用できます。

Tiered Electronic Distribution の階層配布モデルを使用すると、1 つのサーバから間接的に数百または数千のサーバに配布できるようになります。Tiered Electronic Distribution では、ファイルおよびポリシーパッケージを圧縮データファイルに組み込み、適切なサーバへの配布に必要な配布チャネルで圧縮データファイルをホストすることにより、ファイルおよびポリシーパッケージを簡単に配布できます。

Tiered Electronic Distribution を使用すると、オフピーク時を利用した配布プロセスの実行をスケジュールできます。電子メールメッセージの送信、イベントの記録、リアルタイムメッセージの表示、データベースのレポート機能、および SNMP トラップの送信によって、配布ステータスの通知を送信することもできます。

Server Management は、50,000 以上のファイルエントリを含む総容量 4GB のボリュームなど、多数のファイルを含む大容量の Distribution を効率的に処理（送信 / 受信 / 抽出）できます。

基本配布プロセス

Tiered Electronic Distribution の配布プロセスの基礎は、ファイルとポリシーをネットワークサーバに移動するときに使用する Distribution（圧縮されたファイルの集まり）の作成にあります。詳細については、176 ページの「配布プロセスの理解」を参照してください。

次に配布プロセスを簡単に説明します。このプロセスは、Distribution ファイルに含まれる Tiered Electronic Distribution オブジェクトごとに設定されたスケジュールによって制御されます。

1. Distributor は、配布のセキュリティを提供するセキュリティ証明書を作成します。
2. Distribution オブジェクトの設定に従って、Distributor サーバのファイルシステムに Distribution が構築されます。
3. Distribution を Channel に関連付けます。
4. ターゲット Subscriber サーバを Channel に登録します。これにより、Subscriber サーバは、この Channel に含まれるすべての Distribution を受信します。
5. 証明書（手順 1）が Subscriber サーバにコピーされ、Distribution のセキュリティが検証されます。
6. Channel のリスト内の Distribution のうち、セキュリティ証明書が有効と判断されたものが、Distributor から Subscriber サーバに送信されます。

7. Subscriber は、圧縮された Distribution ファイルからファイルまたはポリシーを抽出し、Distribution オブジェクトの設定に従って適用します。

Distribution の送信に必要なスケジュールは、Distributor の更新スケジュール、Distribution の構築スケジュール、および Channel の送信スケジュールです。

Distribution の受信および抽出に必要なスケジュールは、Channel の送信スケジュールと Subscriber の抽出スケジュールです。

Tiered Electronic Distribution の eDirectory オブジェクト

Tiered Electronic Distribution は、eDirectory オブジェクトと関連ソフトウェアを使用して、配布機能を実行します。すべての Tiered Electronic Distribution オブジェクトの識別名 (DN) には、ホストサーバのサーバ名とコンポーネント関数が含まれます。

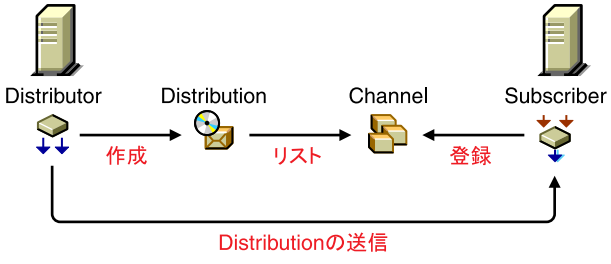
Tiered Electronic Distribution の eDirectory スキーマの拡張は、eDirectory ツリーに作成される eDirectory オブジェクトのクラスを定義します。これには、オブジェクトの作成時に必要な情報、または任意の情報が含まれます。eDirectory ツリーで Tiered Electronic Distribution と関連するすべてのオブジェクトでは、そのツリーのスキーマでクラスが定義されています。

ZENworks 6.5 Server Management をインストールすると、次の eDirectory オブジェクトについてツリーのスキーマが拡張されます。

オブジェクト	基本機能	説明
Distributor	Distribution の構築と送信	96 ページの「Distributor」
Distribution	ファイルとポリシーの格納	112 ページの「Distribution」
Channel	Distribution のリスト作成	147 ページの「Channels」
Subscriber	Distribution の受信と抽出	150 ページの「Subscriber」
Subscriber Group	複数の Subscriber による Channel 登録	158 ページの「Subscriber Group」
External Subscriber	ツリー間配布の有効化	160 ページの「External Subscriber」

Tiered Electronic Distribution オブジェクトの関係

次の図は、主な Tiered Electronic Distribution オブジェクトの関係を示しています。



この図から次のことがわかります。

- Distributor は Distribution を作成します。
- Distribution のリストが Channel に作成されます。
- Subscriber が Channel に登録されます。
- Subscriberは、DistributorからDistributionを受信します(親Subscriberを経由する場合があります)。

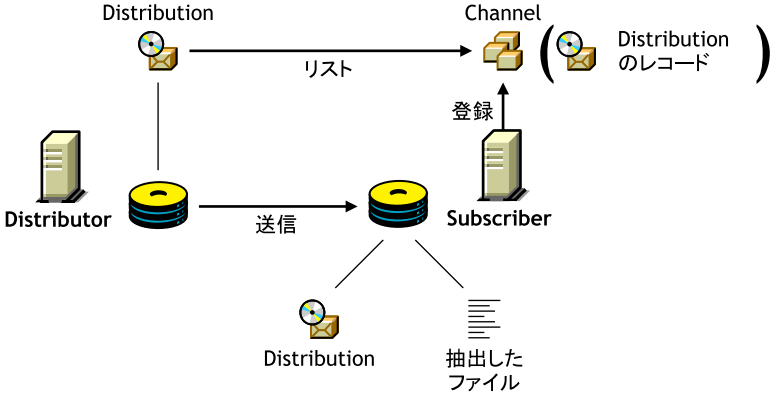
物理ネットワーク接続

Distributor サーバと Subscriber サーバは、たとえば WAN リンク経由で複数のサーバを接続するというように、さまざまな構成でネットワークに物理的に接続できます。Distributor サーバと Subscriber サーバ間で実現可能な物理接続を次に示します。

- Subscriber サーバは、Distributor サーバと地理的に同じ場所に配置できます。
- Subscriber サーバは、Distributor サーバと地理的に異なる場所に配置できます(WAN リンクの使用など)。
- Distributor サーバは、複数の Subscriber サーバに配布できます。
- Subscriber サーバは、複数の Distributor サーバから受信できます。
- Subscriber サーバは、Distributor サーバから直接 Distribution ファイルを受信できます。
- Subscriberサーバは、親Subscriberとして機能する他のSubscriberサーバを介して間接的に Distribution ファイルを受信できます。

配布フローの詳細

次の図は、Tiered Electronic Distribution の Distribution の物理的な流れを示しています。



この図から次のことがわかります。

- Distribution ファイルは Distributor サーバのハードドライブに保存されます。
- ChannelはDistributionのリストを作成します(Distributionのコピーを保持しません)。
- SubscriberはChannelに登録され、リスト内のすべてのDistributionを取得します。

- Subscriber は、圧縮されたファイル形式から Distribution の内容を抽出し、Distribution の設定で指定されたボリュームとディレクトリにその内容を書き込みます。

重要： File または Desktop Application Distribution のバージョンが複数ある場合、Subscriber は、Distribution オブジェクトのプロパティ設定に従って、その各バージョンのコピーを維持します。デフォルトでは、Distribution のタイプごとに 10 バージョンまで保持されます。

Tiered Electronic Distribution のプロセス

次のプロセスを使用して、Tiered Electronic Distribution の機能を実行されます。

- 93 ページの「Distributor Agent」
- 93 ページの「Policy/Package Agent」
- 94 ページの「Subscriberサーバで実行されるTiered Electronic Distributionソフトウェア」
- 94 ページの「配布プロセスの概要」

Distributor Agent

Distributor Agent は、インストール時に［Distributor］オプションを選択した各サーバにインストールされます。

このエージェントには、次の機能があります。

- 更新スケジュールに従って eDirectory を読み取り、Tiered Electronic Distribution のすべての設定情報（Distribution、Channel、および Subscriber の各情報）を取得します。
- Distributor に関連付けられた Distribution オブジェクト内の情報に基づいて Distribution を構築します。
- 構築スケジュールに従って Distribution を構築します。
- 送信スケジュールに従って Distribution を送信します。
- Subscriber のすべての通知とイベントを処理します。
- Subscriber オブジェクトの DS 設定情報を、各 Distribution の一部として各 Subscriber に送信します。
- レポーティング用に Tiered Electronic Distribution 情報を ted.log ファイルに記録します。

Policy/Package Agent

Policy/Package Agent は、インストール時に［Policy and Distribution Server］オプションを選択した各サーバにインストールされます。

このエージェントには、次の Tiered Electronic Distribution 機能があります。

- Policy Package Distributionから抽出されたポリシー情報を読み取って実行します。

  ポリシーの詳細については、4 章 197 ページの「Server Policies（サーバポリシー）」を参照してください。

- Software Package Distribution から抽出された Server Software Package をインストールします。

Software Package の詳細については、5 章 241 ページの「Server Software Package に関する問題」を参照してください。

- レポーティング用にポリシーおよびソフトウェアパッケージ情報を zfs-startup.log ファイルに記録します。

Subscriber サーバで実行される Tiered Electronic Distribution ソフトウェア

Tiered Electronic Distribution ソフトウェアは、インストール時に［Policy and Distribution Server］オプションを選択した各サーバにインストールされます。

このソフトウェアには、次の機能があります。

- Subscriber サーバを Channel に登録して、Distribution を受信します。
- 次のタイプの Distribution を受信して、抽出スケジュールに従ってサーバのファイルシステムに抽出します。

  Desktop Application [1]
  File
  FTP
  HTTP
  MSI
  ポリシーパッケージ
  RPM
  Software Package

  [1] Desktop Application Distribution は、ZENworks Desktop Management がインストールされている場合にのみ利用できます。

- 次の抽出された Distribution をインストールします。

  Desktop Application
  MSI
  RPM

- 親 Subscriber の役割では、Distribution を受信して他の Subscriber サーバに転送します。

配布プロセスの概要

機能	プロセス	説明
Distribution の構築と送信	Distributor Agent	Distributor サーバの CPU およびファイルシステムを使用してすべての Distribution を検出、構築、および送信します。
Distribution の抽出	Subscriber サーバで実行される Tiered Electronic Distribution ソフトウェア	Subscriber サーバの CPU とファイルシステムを使用して Distribution のデータを Subscriber サーバに抽出します。 さらに、適用対象の Server Policies またはインストール対象の Server Software Package があるときに Policy/Package Agent に通知します。
配布されたソフトウェアのインストール	Policy/Package Agent	Subscriber サーバの CPU とファイルシステムを使用して、Server Software Package を Subscriber サーバにインストールします。

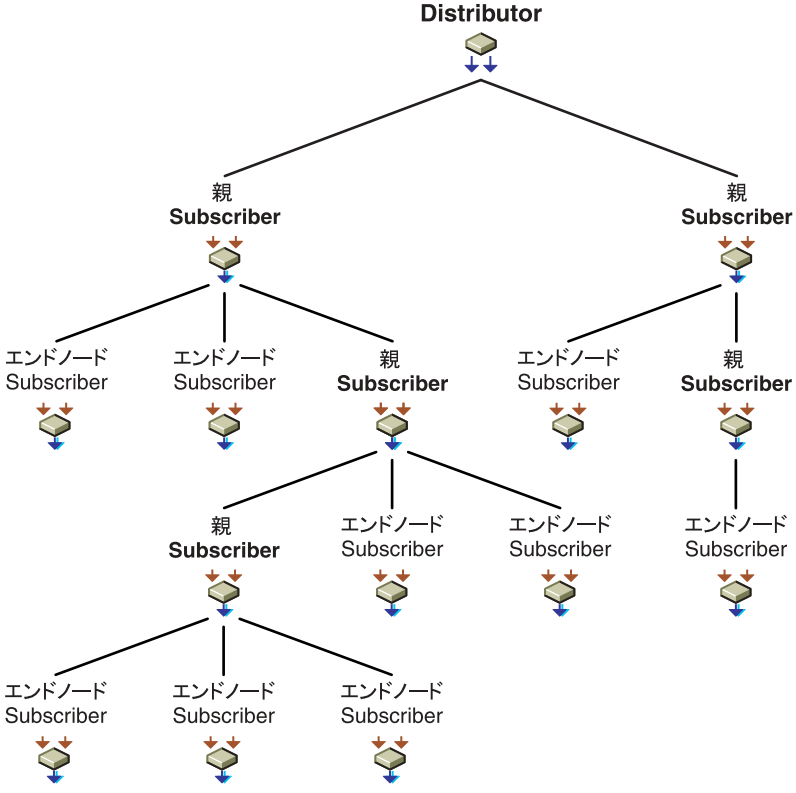
機能	プロセス	説明
インストールしたポリシーの適用	Policy/Package Agent	Subscriber サーバの CPU とファイルシステムを使用して、抽出されたポリシーを読み取り、Subscriber サーバに適用します。

階層配布モデル

階層配布モデルの利点は、Distribution 送信時の負荷を分散できることです。これは、Distributor サーバでは特に重要です。配布処理を親 Subscriber と共有することにより、Distributor は、eDirectory の読み取り、各 Distribution の構築、およびデータベースへの情報の記録に、より多くのリソースを使用できます。

多数の Subscriber を使用する場合は、1 つの Distributor がこれらの Subscriber に直接配布しないようにすることで、階層配布レベルが深くなります。

次の図は、Distributor、複数の親 Subscriber、および多数のエンドノード Subscriber を含む配布ルーティング階層を示しています。



Distributor は、多数の親 Subscriber に直接配布できます。または、第 1 層にある少数の親 Subscriber に配布して、その親 Subscriber に残りの配布作業を実行させることもできます。この図では、Distributor は 2 つの親 Subscriber に Distribution を送信するだけですが、9 のエンドノード Subscriber がこの Distribution を受信します。

この図の親 Subscriber が Distribution の Channel にも登録されている場合は、Distribution の受信後に抽出もできます。この図のすべての親 Subscriber が、エンドノード Subscriber に送信される Distribution を受信するよう登録されている場合、Distributor は Distribution を 2 回送信するだけで合計 14 の Subscriber サーバに配布します。

それぞれの親 Subscriber は、この他にも多数の親 Subscriber やエンドノード Subscriber（Distribution の受信先）に配布できます。親 Subscriber が Distribution を渡すときの負荷は、Distributor が Distribution を構築するときの負荷よりも小さくなります。

図からわかるように、階層配布モデルを使用すると、Distributor サーバの配布負荷を最小限に抑えることができます。

Tiered Electronic Distribution の重要なコンポーネント

Tiered Electronic Distribution の重要なコンポーネントを次に示します。

- eDirectory スキーマの拡張。Distributor、Distribution、Channel、Subscriber、および External Subscriber のオブジェクトを含みます。
- ConsoleOne スナップインと iManager プラグイン。Tiered Electronic Distribution を作成、設定、および管理します。
- Distributor Java プロセス。NetWare、Windows 2000、Windows 2003 Server、Linux、または Solaris サーバでホストされ、Subscriber へのデータパッケージの配布を処理します。
- Subscriber Java プロセス。Distribution の Channel に登録される NetWare、Windows 2000、Windows 2003 Server、Linux、または Solaris サーバでホストされます。
- 各 Distributor のルーティング階層。Distribution を受信し、他の Subscriber に Distribution を渡す Subscriber の階層リストです。
- 親 Subscriber。Distribution を他の Subscriber に渡します。
- External Subscriber オブジェクト。ツリー間の配布、または eDirectory サーバオブジェクトが存在しないサーバへの配布を可能にします。
- Distributor Agent。Distributor の Distribution ファイルを構築する実際のプロセスを制御します。
- Policy/Package Agent。Policy Package Distribution からポリシー情報を抽出して実行します。ソフトウェアパッケージの内容を抽出してインストールします。
- 証明書。配布セキュリティを提供します。

Distributor

次の節では、Distributor オブジェクトの概念と使用方法について説明します。

- 97 ページの「Distributor の理解」
- 99 ページの「配布ルーティングの理解」
- 107 ページの「Distributor の作成」
- 108 ページの「Distributor の設定」
- 111 ページの「Distributor の更新」
- 112 ページの「Distributor オブジェクトの削除と Distribution への影響」

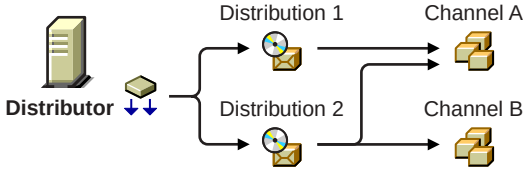
Distributor の理解

Distributor オブジェクト (TED Distributor) は、Distributor のプロパティを定義する eDirectory オブジェクトです。

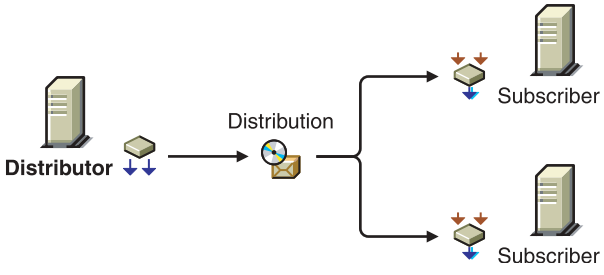
- 97 ページの「他の Tiered Electronic Distribution オブジェクトとの機能的関係」
- 97 ページの「Distributor の説明」
- 98 ページの「スケジュール設定」
- 98 ページの「配布のルーティング」
- 98 ページの「ツリー内の複数の Distributor 」
- 99 ページの「データベースへのログの記録」

他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、Distributor が 1 つの Distribution を複数の Channel のリストに追加できることと、複数の Distribution を 1 つの Channel に追加できることを示しています。



次の図は、Subscriber サーバに Distribution を送信する Distributor を示しています。



Distributor の説明

Distributor サーバの主な Tiered Electronic Distribution 機能は、Distribution の作成と送信です。Distributor にデータベースファイルを割り当てた場合は、情報がデータベースファイルに記録されます。

Distributor Agent は、Distribution オブジェクトの作成および設定時に指定された情報に基づいて、Distributor サーバに Distribution ファイルを構築します。Distributor は複数の Distribution を所有できます。

Distributor は、Distribution を構築するときに、Subscriber が照合に使用する MD5 チェックサムを提供するダイジェストをオプションで作成できます。ダイジェストは、送信中に Distribution が改ざんされていないことを確認するために、Subscriber によって使用されます。ダイジェストの作成は Distributor ごとのオプション機能であるため、このオプションが有効になっている Subscriber でのチェックサムの照合に、ダイジェストを常に使用できるとは限りません。

ダイジェストは、Distribution のパッケージの破損も検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。

Distributor は、Channel に Distribution のリストを作成します。Distributor は Channel を所有しません。ただし、Distribution を所有するのは Distributor だけです。

Distributor は、Distribution を Subscriber に送信します (通常は親 Subscriber が Distribution を転送します)。エンドノード Subscriber が、Distribution を送信する Distributor(または親 Subscriber) に応答しない場合、Distributor は 2 分ごとの再送信を 30 分間継続した後、送信を中止します。Channel の送信スケジュールが再度開始されるまで、Distribution は再送信されません。

スケジュール設定

Distributor の更新スケジュールは、Distributor が eDirectory を読み取って、Distribution とその他の Tiered Electronic Distribution オブジェクトの変更を認識するタイミングを決定します。Distributor は、すべての新しい Distribution を構築し、変更された Distribution を再構築します。新しい Distribution と再構築された Distribution は、Channel の送信スケジュールが開始されると送信されます。

重要： Distributor の更新スケジュールは、Distribution を頻繁に変更して更新が必要になる場合を除き、毎日実行することをお勧めします。ただし、Distributor の更新頻度を 5 分に 1 回よりも多くしないでください。Distribution の構築、eDirectory の複製、およびツリーの検索 (検索ポリシーが定義されていない場合) には、最大で 5 分を要する場合があります。

Distributor は、更新スケジュールが開始されるたびに Distribution を構築します。ただし、Distribution の構築は、サーバのコマンドラインから強制的に実行することもできます。

Distribution を削除した場合は Distributor をすぐに更新して、Distributor が削除を識別し、削除された Distribution を再構築しないようにする必要があります。Distribution の削除については、139 ページの「Distribution の削除」を参照してください。

スケジュール設定については、8 章 331 ページの「スケジュール設定」を参照してください。

配布のルーティング

Distributor に含まれる配布ルートは、Distributor が Subscriber サーバに Distribution を送信するときのルートを示す Subscriber の階層リストです。ルーティング階層については、38 ページの「配布ルートの理解」を参照してください。

ツリー内の複数の Distributor

ツリーには複数の Distributor オブジェクトを配置できます。ただし、各サーバには 1 つの Distributor しかインストールできません。いくつかの要因によって、複数の Distributor が必要になる場合があります。詳細については、34 ページの「追加の Distributor の必要性」を参照してください。

データベースへのログの記録

Distributor は、それぞれ独自のデータベースファイルに情報を記録できます。すべての Distributor が 1 つの共通データベースファイルに情報を記録することもできます。データベースの詳細については、10 章 365 ページの「ZENworks Database」を参照してください。

配布ルーティングの理解

配布ルートは、WAN のセグメントに対する最も効率の良い経路を表します。配布ルートは、Distribution を親 Subscriber またはエンドノード Subscriber に転送する親 Subscriber のリストです。親 Subscriber を使用すると、親 Subscriber が Distribution を他の Subscriber に渡すため、Distributor の負荷を最小限に抑えることができます。

次の節では、Distributor がネットワークのサーバに Distribution を移動する方法について説明します。

- 99 ページの「親 Subscriber の理解」
- 101 ページの「ルーティング階層の理解」
- 103 ページの「他の Distributor との親 Subscriber の共有」
- 105 ページの「WAN リンクを使用した配布」
- 106 ページの「別のツリーへの配布」
- 107 ページの「ルーティング階層設定のガイドライン」

親 Subscriber の理解

親 Subscriber は、Distribution を保存および転送する Distributor のプロキシとして機能するため、Distributor がすべての Subscriber に直接 Distribution を送信する必要はありません。親 Subscriber サーバは、Distribution を一時的に保存して他の Subscriber サーバに渡すので、それ自体が Distribution の受信先である必要はありません。

- 99 ページの「親 Subscriber の使用による Distributor からの Distribution の送信」
- 100 ページの「未登録の Distribution の転送」
- 100 ページの「配布負荷の共有」
- 100 ページの「負荷分散」

親 Subscriber の使用による Distributor からの Distribution の送信

Distribution ファイルは Distributor サーバのファイルシステムに保存されているため、Distributor は各 Distribution を実際に送信する必要があります。

Distributor がネットワーク上の各 Subscriber サーバに Distribution を個別に送信すると、Distributor の負荷が大きくなる場合があります。そのため、Distribution を効率的に送信するには親 Subscriber が使用されます。

適切な配布ルートを設定して、親 Subscriber を選択するには、ネットワークのトポロジをよく理解することが重要です。必要に応じてすべての WAN リンクを示すネットワークの図を作成し、親 Subscriber の使用方法を決定してください。

未登録の Distribution の転送

Subscriber は、Distributor のルーティング階層内にある場合は、その Distributor の Distribution を含む Channel に登録する必要はありません。親 Subscriber 自体は、転送する Distribution の受信先である必要はありません。

親 Subscriber が Channel の Distribution を転送できるようにするために、親 Subscriber を下位の Subscriber と同じ Channel に登録する必要はありません。

配布負荷の共有

101 ページの「ルーティング階層」の図では、各 Subscriber が同じ LAN 上の他の Subscriber に対する親である可能性があります。たとえば、図中のすべての Subscriber が 20 のエンドノード Subscriber の親である場合、Distributor は、物理的に 3 つの Subscriber（第 1 層の親 Subscriber 01、04、および 09）に Distribution を送信するたけで、合計 210 の Subscriber に配布できます。

親 Subscriber 04 は、2 つの親 Subscriber（05 と 06）と直下にある 20 のエンドノード Subscriber に直接送信するだけで、104 の Subscriber に配布しています。

負荷分散

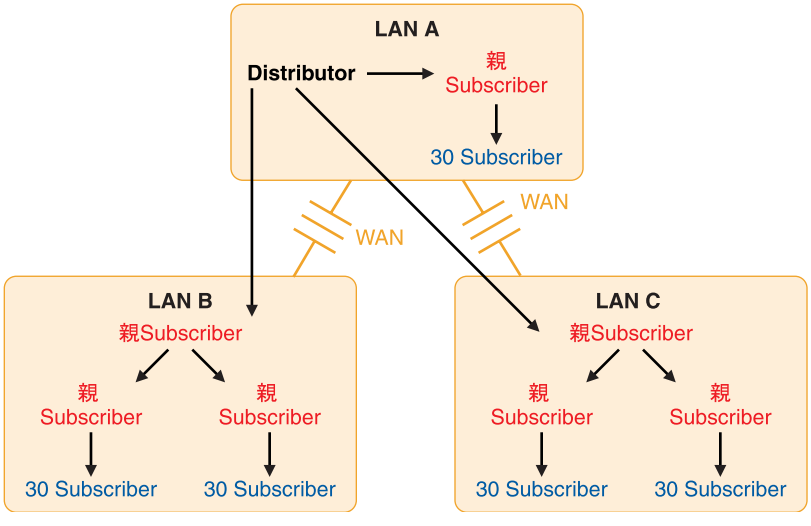
Distributor は、ルーティング階層で親 Subscriber を使用することにより、Distribution のルートを明確に決定できます。これにより、Subscriber への配布に関する負荷を軽減できます。

親 Subscriber は、Distributor のプロキシとして機能し、他の Subscriber に Distribution を渡すことによって、Distributor の負荷も軽減できます。LAN 上に複数の親 Subscriber を配置すると、LAN 上での配布負荷が共有されます。

1 つの Distributor または親 Subscriber が送信する Subscriber または親 Subscriber の数は、およそ 40 と推定されます。この値は、ネットワーク速度、Distribution のサイズなどの要素によって変化します。

親 Subscriber は、Distributor やその他の親 Subscriber の負荷分散に効果的な場所に配置する必要があります。

次の図は、親 Subscriber を含む WAN 環境を示しています。



この図から次のことがわかります。

- Distributor の配布線が指し示す 3 つの親 Subscriber は、Distributor のルーティング階層の第 1 層にある Subscriber です。
- その他の4つの親Subscriber（LAN BおよびLAN C）は、配布階層の第2層にあります。
- LAN A の親 Subscriber が LAN A の 30 の Subscriber に Distribution を送信するため、Distributor が直接送信する必要はありません。
- Distributor は、Distribution を 3 つの親 Subscriber に直接送信するだけですが、合計 157 の Subscriber がそれらの Distribution を受信できます。
- LAN B の 1 つの親 Subscriber（LAN C についても同様）は、Distributor から Distribution を直接受信するためだけに使用され、受信した Distribution を他の親 Subscriber に渡します。これらの親 Subscriber が 60 の Subscriber に Distribution を渡します。大規模システムでは、このしくみによって、WAN リンク先の親 Subscriber が多くのエンドノード Subscriber に Distribution を送信できるため、負荷の増大を回避でき、この親 Subscriber の Distributor に対する有用性が高まります。ネットワークに最適な階層構造を検討してください。

Distributor には、Distribution の変更に関する eDirectory の読み取り、Distribution の構築、Distribution の送信、および Server Management データベースへの書き込み時に負荷がかかります。Distributor が Distribution を直接送信する Subscriber の数を最小限に抑えることにより、Distributor のさまざまな機能に、より多くのリソースを使用できるようになります。

ルーティング階層の理解

Tiered Electronic Distribution には、Distributor サーバから Subscriber サーバに Distribution を自動送信するルーティング階層が用意されています。

- 101 ページの「ルーティング階層」
- 102 ページの「階層を使用した配布」
- 103 ページの「ルーティング階層から孤立した Subscriber 」
- 103 ページの「ルーティング階層の変更に伴うルーティング」

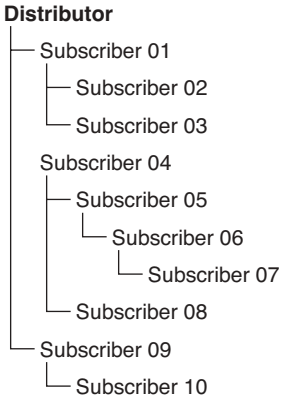
ルーティング階層

Distribution 送信時の Distributor の負荷を軽減するため、各 Distributor では独自のルーティング階層が使用されます。これは、Distribution を Subscriber に送信するときの Distribution のルートを示す Subscriber の階層リストです。ルーティング階層の Subscriber は親 Subscriber です。親 Subscriber は多数の階層にわたってネストできます。

親 Subscriber は、Distribution を受信して抽出することも、受信後に他の Subscriber に送信することもできます。

Distributor オブジェクトのプロパティを編集することにより、いつでも配布ルートを変更できます。

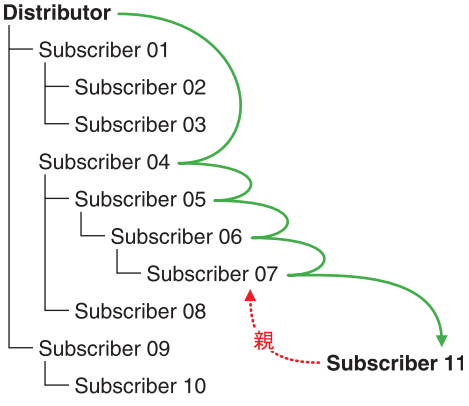
次の図は、Distributor のルーティング階層を示しています。



Distributor のルーティング階層に含める必要のある Subscriber は、他の Subscriber に Distribution を渡すものだけです。Distribution を他の Subscriber に渡さない Subscriber は、エンドノード Subscriber と呼ばれます。

階層を使用した配布

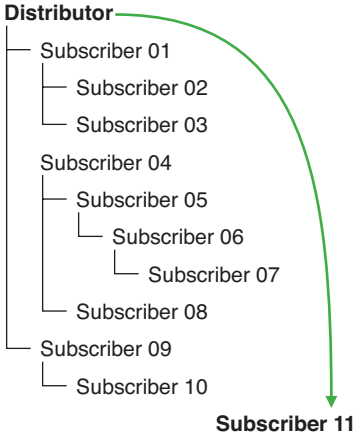
Subscriber 07 は、Subscriber 11（ルーティング階層に含まれない）の親であるとします。Distributor から Subscriber 11 への配布ルートは次の図のようになります。



Distributor は、4 つの親 Subscriber（04、05、06、および 07）を使用して、Subscriber 11 に Distribution を送信しました。

ルーティング階層から孤立した Subscriber

Subscriber 11 に親 Subscriber（Subscriber 07 など）がない場合、Distribution は Distributor から直接送信されます。



ルーティング階層に含める必要のある Subscriber は、他の Subscriber に Distribution を渡すものだけです。エンドノード Subscriber（Distribution を受信するだけで送信しない Subscriber）は、階層に含める必要はありません。エンドノード Subscriber は、eDirectory で親にリンクされています。

ルーティング階層に存在する Subscriber は、通常は親 Subscriber ですが、これは必須ではありません。

重要： 親 Subscriber を利用しない Subscriber によって、Distributor の負荷と、WAN リンクを介したネットワークトラフィックが増加する場合があります。Distributor から Distribution を直接受信する第 1 層の Subscriber を除き、すべての Subscriber は親 Subscriber に属している必要があります。

ルーティング階層の変更に伴うルーティング

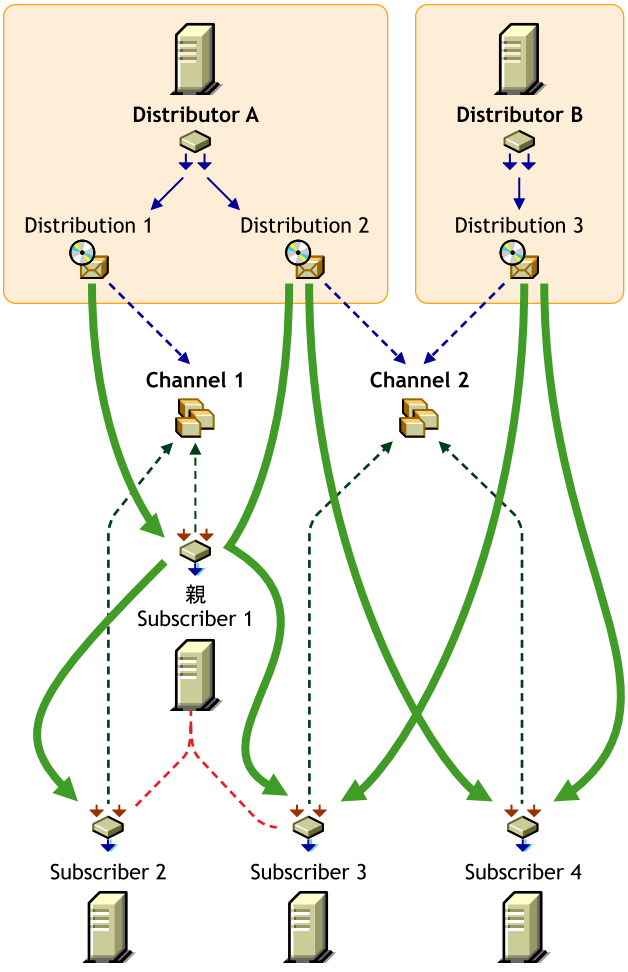
親 Subscriber が変更されるか、またはルーティングリスト（Distributor オブジェクトのプロパティの［Routing Hierarchy］タブ）が変更されると、変更は Channel スケジュールの開始時に毎回解釈されるため、この変更はルーティングスリップ（配布プロセスで使用されるデータファイル）に反映されます。eDirectory を読み取って、新しいルーティング階層を取得するには、Distributor の更新が必要です。

Subscriber サーバがネットワークから排除されていても、Distributor のルーティング階層で使用されている場合は、Distributor オブジェクトのプロパティを編集して、Subscriber の排除についてルーティング階層を適合させる必要があります。次に Distributor を更新すると、Distributor は新しいルーティング階層を認識します。

他の Distributor との親 Subscriber の共有

複数の Distributor を使用する場合は、Distributor 間で配布ルートの一部を共有できます。つまり、Subscriber を複数の Distributor の配布ルーティング階層に配置できます。これは、Subscriber へのルートが Distributor に依存し、Distributor から Subscriber への経路が Distributor ごとに異なるためです。

次の図は、Distribution を送信する複数の Distributor と親 Subscriber を示しています。



矢印と線は、Channel への登録と Distribution の接続（点線）を示し、Distributor から Subscriber への配布経路（実線）を示しています。

この図は、配布ルート階層ではありません。この図は次の要点を示すことを目的としています。

- Subscriber 1 は Distributor A の階層に属しています。
- Subscriber 1 は Subscriber 2 と 3 の親です。
- Subscriber 3 と 4 は Distributor B の階層に属しています。
- Subscriber 4 は Distributor A の階層に属していません。

Distribution を送信する複数の Distributor と親 Subscriber を示す図から、次のことがわかります。

- **Distribution の所有権：** Distributor は、Distribution を所有し、各 Distribution を構築および送信します。
- **複数の Distributor：** 複数の Distributor は、同じ Channel のリストに Distribution を追加できます。つまり、Subscriber は複数の Distributor から Distribution を受信できます。
- **Distributor による Channel の使用：** Distributor はどの Channel のリストにも Distribution を追加できます。複数の Channel に 1 つの Distribution を追加することもできます。

- **Channelごとの複数のDistribution:** Channelは、1つまたは複数のDistributorによる複数の Distribution を保持できます。
- **Channelの登録:** 各Subscriberは、必要なDistributionを含むあらゆるChannelに登録されます。1 つの Subscriber を複数の Channel に登録したり、複数の Subscriber を 1 つの Channel に登録したりできます。
- **親 Subscriber:** 親 Subscriber は Distributor のプロキシとして使用され、他の Subscriber に Distribution を渡します。
- **孤立した Subscriber:** Subscriber が Distributor の配布ルート外にある場合、または階層内の親 Subscriber の子でない場合、Distributor は Subscriber に直接 Distribution を送信します。この場合は、WAN リンクおよびその他のトポロジに問題が発生することがあります。

WAN リンクを使用した配布

ルーティング階層で親 Subscriber を使用すると、Distributor が WAN リンクを介して Distribution を渡す回数が制限されるため、ネットワークトラフィックを最小限に抑えることができます。

Distributor が Distribution を親 Subscriber に送信し、その親 Subscriber が Distribution を他の Subscriber に送信するため、WAN リンクを経由する Distribution の送信は 1 回で済み、WAN リンク先のすべての Subscriber に Distribution が配布されるまで何度も送信する必要はありません。

通常は、すべての LAN に少なくとも 1 つの親 Subscriber を配置して、Distribution が WAN リンク経由で送信される回数を最小限に抑える必要があります。LAN 上に 2 つの Subscriber しかない場合でも、一方を他方の親 Subscriber として使用することで、ネットワークトラフィックを軽減できます。

親 Subscriber の使用は、低速の WAN リンクでは特に有効です。

WAN リンクを介した配布方法を決定する際には、次の点を考慮してください。

- **DistributorのLANセグメント上の親Subscriber:** DistributorのLANセグメントでは、少なくとも 1 つの Subscriber をその他すべての Subscriber の親 Subscriber として指定する必要があります。これにより、Distributor では、WAN リンクを介した Distribution の送信時に、より多くのリソースを使用できます。
- **WANリンクをブリッジするための親Subscriber:** 他のすべてのLANセグメントに少なくとも 1 つの親 Subscriber を指定し、これらの親 Subscriber を Distributor のルーティング階層に含めることにより、Distributor が WAN リンクを介して直接サービスを提供する Subscriber の数を最小限に抑えることができます。

  たとえば、WAN に 4 つの LAN が属しているとします。ある LAN セグメントの Distributor は、3 つの WAN リンクを介して、その他 3 つの LAN セグメントの Subscriber に Distribution を送信する必要があります。その他の LAN ではそれぞれ 160 の Subscriber が Distributor からの Distribution を必要としていると仮定します。Distributor のルーティング階層で親 Subscriber を使用しない場合、Distributor は WAN リンクを介して Distribution を 480 回送信する必要があります。親 Subscriber（LAN の Distribution 負荷を共有する目的で LAN セグメントごとに 4 つ配置）を使用すると、Distributor は Distribution を 9 回送信するだけで済みます。

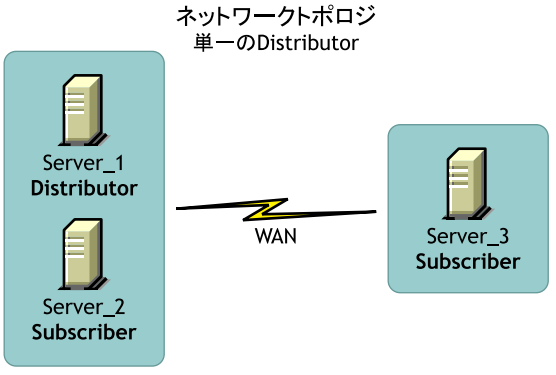
- **LANの主要な親Subscriber:** DistributorからのWANリンク先で親Subscriberを階層状に配置することで、WAN トラフィックを軽減できます。つまり、ルーティング階層に親 Subscriber を 1 つだけ配置し、LAN セグメント上ではその親 Subscriber を他の多数の親 Subscriber に対する親として構成できます。

  先に挙げた例を使用すると、各 LAN セグメントの Subscriber 1 は、Subscriber 2、3、および 4 の親 Subscriber であるとします。親 Subscriber 1、2、3、および 4 は、それぞれに属する Subscriber に配布します。これにより、Distributor は WAN リンクを介して Distribution を Subscriber 1 に 1 回渡すだけで済み、Subscriber 1 がその他 3 つの親 Subscriber に Distribution を渡すため、Distributor は 3 回分の WAN リンク転送を省くことができます。そのため、以前の例と比較すると 9 回の転送が 3 回に減少されます。

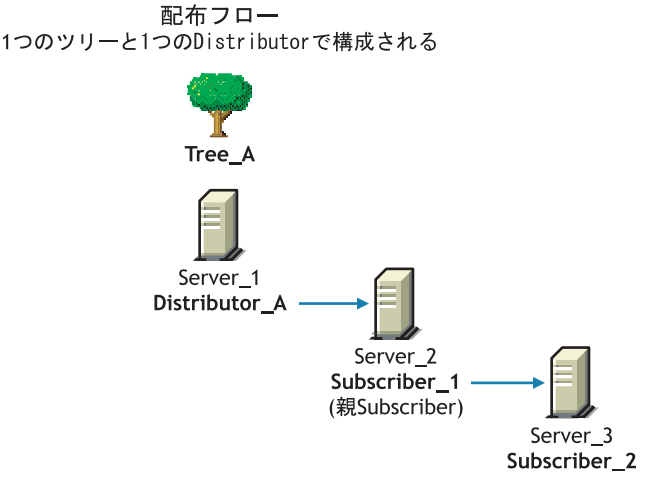
別のツリーへの配布

複数のツリーで Policy and Distribution Services を使用するには、ツリーごとに個別にソフトウェアをインストールする必要があります。ただし、Server Management オブジェクトは、いずれかのツリーにインストールするだけです。

たとえば、次のようなネットワークトポロジの場合を考えます。



Distributor のルーティング階層には、次のような Tiered Electronic Distribution が設定されているとします。



この例では、Subscriber とサーバオブジェクトはすべて Tree_A に存在します。これにより、ネットワークトポロジに関係なく Tiered Electronic Distribution オブジェクトを一元管理できます。

Distributor オブジェクトと Subscriber オブジェクトは 1 つのツリー内にのみ作成できますが、Policy and Distribution Services ソフトウェアはネットワークのどのサーバにもインストールできます。これは、サーバの eDirectory オブジェクトが、Tiered Electronic Distribution オブジェクトが作成されるのと同じツリーにある場合でも、eDirectory サーバオブジェクトがサーバのツリーにない場合（ドメイン内の Windows サーバなど）でも同様です。これにより、複数のツリーを使用し、サーバのオペレーティングシステムが混在する環境（NetWare サーバと Windows サーバなど）で、Tiered Electronic Distribution を一元管理できます。

ツリー間で Distribution を送信する場合の External Subscriber の使用方法については、179 ページの「ツリー間の Distribution の送信」を参照してください。

ルーティング階層設定のガイドライン

ルーティング階層に親 Subscriber を配置するには、次のガイドラインに従う必要があります。

- 各 LAN セグメントに少なくとも 1 つの親 Subscriber を配置して、WAN トラフィックを最小限に抑えます。
- 40 以上の Subscriber がある各 LAN では、複数の親 Subscriber を配置して、親 Subscriber 間で負荷を分散します。
- Distributor の配布ルートに含まれないすべての Subscriber が、LAN の親 Subscriber に割り当てられるようにします。

親 Subscriber は、WAN リンクに必ずしも必要なものではありません。たとえば、高速の WAN リンクで接続された LAN 上に Subscriber が 2 つしか存在しない場合、Distribution を 1 回送信するときと 2 回送信するときのトラフィックの差はごくわずかです。ただし、低速の WAN リンクでの結果は異なります。

Subscriber が Distributor から直接 Distribution を受信するか、親 Subscriber を経由して受信するかは、次の要素によって判断します。

- ネットワーク接続

  たとえば配布時の状況を考慮します。

  - LAN 内のみ
  - 低速 WAN の使用または高速 WAN の使用
  - ファイアウォールの使用
  - NAT の使用
- Distribution の送信頻度
- Distribution のサイズ

Distributor の作成

ネットワークトポロジ、Distribution（数、サイズ、再構築の頻度など）、およびさまざまな Distribution を受信する Subscriber の数を理解することにより、必要な Distributor の数を判断できます。

Distributor は、*ZENworks 6.5 Server Management Program* CD を使用して、ソフトウェアと eDirectory オブジェクトをインストールすると作成されます。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」を参照してください。

複数の Distributor が必要かどうかを判断するには、34 ページの「追加の Distributor の必要性」を参照してください。

Distributor の設定

Distributor オブジェクトは、Distributor のソフトウェアをサーバにインストールすると自動的に作成されます。Distributor オブジェクトのプロパティはいつでも編集できます。

Distributor オブジェクトに関連付けられているプロパティは、すべてが必要になるとは限りません。必要なプロパティを次の手順で示します。それ以外のプロパティはすべてオプションです。

1 ConsoleOne で、Distributor オブジェクトを右クリックし、[Properties] をクリックします。

2 [General] > [Settings] の順にクリックし、次のフィールドに入力します。

[Use Policy]： Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Distributor サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。このオプションを選択すると、残りのフィールドが淡色表示され、このポリシー設定が使用されます。

[Input Rate]： Subscriber に対する Distribution の受信レートです。デフォルト値は、その接続で処理可能な最大値です。このレートは、狭い帯域幅のリンクを使用する Distributor サーバを制御するために使用します。

[Output Rates Based Upon Distribution's Priority]： デフォルトの出力レートを設定して、Tiered Electronic Distribution オブジェクトのネットワークトラフィックを最小限に抑えます。これは、Distributor の送信レートを決定します。デフォルト値は接続で処理できる最大値です。何も指定しない場合、帯域幅はサードパーティのソフトウェアから取得されます。

出力には 3 つの優先度があり、速度を指定できます。

- **[High Priority]：** この Distribution は、[Medium Priority] または [Low Priority] の Distribution よりも前に送信されます。
- **[Medium Priority]：** この Distribution は、[High Priority] の Distribution がすべて送信された後、[Low Priority] の Distribution よりも前に送信されます。
- **[Low Priority]：** この Distribution は、[High Priority] と [Medium Priority] のすべての Distribution が送信された後で送信されます。

詳細については、128 ページの「Distribution の優先度」を参照してください。

[Maximum Concurrent Distributions to Build]： Distribution を構築するために同時に実行できる配布スレッドの最大数を指定します。デフォルト値は 5 です。有効な値は 1 から 10 までです。

この数値によって、Distributor の構築アクティビティの負荷を分散させることができます。

[Maximum Concurrent Distributions to Send]：Distribution を送信するために同時に実行できる配布スレッドの最大数を指定します。デフォルト値は指定されていません（空フィールド）。

この数値によって、Distributor の送信アクティビティの負荷を分散させ、ネットワークトラフィックをスケジュール設定期間全体に分散させることができます。

[Connection Time-out]：Distributor が他のノードに接続する際にタイムアウトになるまでの時間を指定します。デフォルト値は 300 秒（5 分）です。その後、接続は終了し、送信スケジュールが再度開始されるまで接続されません。有効な値は 1 ～ 60,000（秒）です。

この設定を増加または減少することにより、配布プロセス中にエージェント間でメッセージを相互に送信できます。あるノードが他のノードからメッセージを受信しようとする場合、送信元が使用できなくなっていると判断されるまで、適当な時間をおく必要があります。

重要： 遅延が大きくなることが多い低速またはビジー状態のリンクでは、この値を大きくする必要があります。

[Working Directory]：Distribution によって使用されるディレクトリを指定します。このディレクトリには、Distribution、永続ステータス、および一時作業ファイルが格納されます。デフォルトパスは次のとおりです。

- [NetWare]：sys:¥zenworks¥pds¥ted¥dist

  重要： デフォルトボリュームは、NetWare サーバの sys: です。ログファイルは非常に大きくなる可能性があるため、sys: ボリュームを使用しないことをお勧めします。

- [Windows]：c:¥zenworks¥pds¥ted¥dist

- Linux または Solaris：/var/opt/zenworks/zfs/pds/ted/dist

Distributor の作業ディレクトリは、Distribution の作成時にも使用されます。Distribution オブジェクトの DN を使用して、作業ディレクトリの下位にサブディレクトリが作成されます。

作業ディレクトリの詳細については、190 ページの「作業ディレクトリ」を参照してください。

3 [General] > [Messaging] の順にクリックし、次のフィールドに入力します。

[Use Policy]：Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Distributor サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。このオプションを選択すると、残りのフィールドが淡色表示され、メッセージングのポリシー設定が使用されます。

[Server Console]：サーバコンソールで Distributor コンソールに送信する出力メッセージのレベルを指定します。

[SNMP Trap]：SNMP を経由して送信するメッセージのレベルを指定します。

[Log File]：ログファイルに送信するメッセージのレベルを指定します。

[Path and Filename]：この Distributor オブジェクトのカスタムログファイルの名前および場所を指定できます。デフォルトは次のとおりです。

- [NetWare]：sys:¥zenworks¥pds¥ted¥dist¥ted.log

  重要： デフォルトボリュームは、NetWare サーバの sys: です。ログファイルは非常に大きくなる可能性があるため、sys: ボリュームを使用しないことをお勧めします。

- **[Windows]**：c:¥zenworks¥pds¥ted¥dist¥ted.log
- **Linux または Solaris**：/var/opt/zenworks/zfs/pds/ted/dist/ted.log

Tiered Electronic Distribution ポリシーを使用して、すべての Distributor オブジェクトのカスタムログファイルを作成する方法については、235 ページの「ポリシーを使用したカスタムログファイルの作成」を参照してください。

[Delete Log Entries Older Than __ Days]：Distributor のログファイルエントリは、指定した日数が経過すると削除されます。デフォルト値は 6 日です。

[E-Mail]：電子メールで送信されるメッセージのレベルを指定します。

[Users]：通知する電子メールユーザを指定します。

[Address Attribute]：通知する電子メールアドレスを指定します。

eDirectory に保存されているユーザまたはグループを追加できます。eDirectory に含まれないユーザの電子メールアドレスを指定することもできます。デフォルトの属性は、eDirectory ユーザに関連付けられている電子メールアドレス属性です。

重要：通知を受信する方法に電子メールを選択した場合は、ネットワークトラフィックが増加する可能性があることに注意してください。

4 [Schedules] タブを選択します。

Distributor のスケジュールは、eDirectory の Tiered Electronic Distribution オブジェクトに含まれる情報を Distributor が読み取る頻度を決定します。このスケジュールに基づいて、Channel、Distribution、および Distributor オブジェクトが読み取られます。これらのオブジェクトの情報を変更する頻度や、新しいオブジェクトが作成される頻度を考慮してスケジュールを決める必要があります。

Distributor オブジェクトを右クリックし、[Refresh] メニューオプションを選択することによって、Distributor による eDirectory の読み取りを強制的に実行できます。

5 スケジュールを選択して、次のフィールドに入力します。

[Use Policy]：Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Distributor サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。このオプションを選択すると、残りのフィールドが淡色表示され、このポリシー設定が使用されます。

[Schedule Type]：選択される更新スケジュールは、Distributor が次に eDirectory を読み取るタイミングを決定します。

重要：Distributor に対する変更が多く、より頻繁な更新が必要である場合以外は、Distributor の更新スケジュールを 1 日に 1 回に設定することをお勧めします。ただし、Distributor の更新頻度を 5 分に 1 回よりも多くしないでください。Distribution の構築、eDirectory の複製、およびツリーの検索（検索ポリシーが定義されていない場合）には、最大で 5 分を要する場合があります。

利用可能なスケジュールについては、8 章 331 ページの「スケジュール設定」を参照してください。

6 [Routing] タブを選択し、Distributor のルーティング階層を作成します。

[Subscriber Routing Hierarchy]：Distributor が Distribution を Subscriber に送信するときに使用するルートを設定します。この階層はあらかじめ計画しておく必要があります。

次の方法で階層を作成します。

6a Distributor を選択します。

6b [Add] をクリックし、1 つまたは複数の Subscriber を選択した後、[Select] をクリックして [OK] をクリックします。

Distributor の下に複数の Subscriber を直接配置できます。

6c Subscriber を 1 つ選択します。

6d [Add] をクリックし、1 つまたは複数の Subscriber を選択した後、[Select] をクリックして [OK] をクリックします。

各 Subscriber の下に複数の Subscriber を直接配置できます。

6e 希望する階層が完成するまで、Subscriber ごとにステップ 6c とステップ 6d を繰り返します。

7 [Distributions] タブを選択して、この Distributor が配布する Distribution を表示します。

8 Distribution を編集するには、Distribution を選択し、[Details] をクリックして、プロパティを編集します。次に、[OK] をクリックして、Distribution オブジェクトのプロパティを終了します。

9 Distributor と Distribution の設定が終了したら、[OK] をクリックして Distributor オブジェクトのプロパティを終了します。

重要： Tiered Electronic Distribution オブジェクト（Distribution 以外）への変更は、Distributor による eDirectory の読み取り後に有効になります。

Distributor の更新

Distributor に影響を与える変更を eDirectory に加えた場合は、すぐに手動で Distributor を更新して、Distributor がその変更を認識するようにする必要があります。構築スケジュールは、Distributor がすでに認識している既存 Distribution の変更についてのみ Distributor に情報を提供します。

たとえば、Distribution を新規作成した場合、構築スケジュールはその新しい Distribution について Distributor に通知しません。Distributor を手動で更新して、eDirectory での変更が Distributor に検出されるようにする必要があります。

Distributor を更新するには

1 ConsoleOne で、Distributor オブジェクトを右クリックします。

2 [Refresh Distributor] をクリックします。

これにより、Distributor は eDirectory を読み取って、eDirectory に加えられた変更をすべて取得します。次に、Distributor Agent が Distributor に適用された変更に基づいて処理を実行します。

iManager でこのタスクを実行するには、82 ページの「Policy and Distribution Services エージェントの強制実行」を参照してください。

Distribution の構築は、現在の構築スケジュールに従って開始されます。Distribution は、送信スケジュールに従って送信されます。

Subscriber は、Distribution を受信するとすぐに、Subscriber オブジェクトのプロパティで指定された作業ディレクトリに内容を抽出します。

Distributor オブジェクトの削除と Distribution への影響

Distributor オブジェクトは eDirectory から削除できます。ただし、その Distributor の再配置時に再利用できる次の重要な情報が失われます。

- Distributor の配布階層

  これは、Distribution オブジェクトのプロパティの一部で、Distribution を次に渡す Subscriber サーバが示されます。

- Distribution のリスト

  Distributor に属する Distribution は分離され、使用できなくなります。

孤立した Distribution の処理方法については、142 ページの「孤立した Distribution の処理」を参照してください。

Distribution

次の節では、Distribution オブジェクトの概念と使用方法について説明します。

- 112 ページの「Distribution の理解」
- 116 ページの「Distribution に関する問題」
- 119 ページの「Distribution の決定」
- 125 ページの「Distribution の作成」
- 128 ページの「Distribution の優先度」
- 129 ページの「Distribution の前後の処理」
- 135 ページの「他の Distributor への Distribution の再割り当て」
- 139 ページの「Distribution の削除」
- 139 ページの「Distribution オブジェクトの削除 - 一時ファイルの自動削除」
- 142 ページの「孤立した Distribution の処理」
- 143 ページの「手動による Distribution のインポートとエクスポート」
- 146 ページの「Distribution ウィザードの使用」

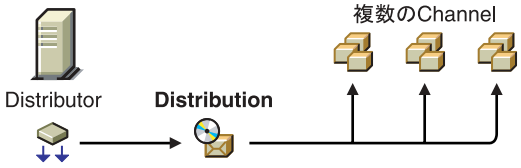
Distribution の理解

Distribution (TED Distribution) オブジェクトには、データパッケージのリストまたはデータグループ情報が含まれます。

- 113 ページの「他のTiered Electronic Distributionオブジェクトとの機能的関係」
- 113 ページの「Distribution の説明」
- 114 ページの「スケジュール設定」
- 114 ページの「既存のDistributionの新しいバージョンを作成および配布する方法」
- 114 ページの「配布セキュリティ」
- 115 ページの「Distribution の削除」
- 115 ページの「一時的な Distribution ファイルのクリーンアップ」

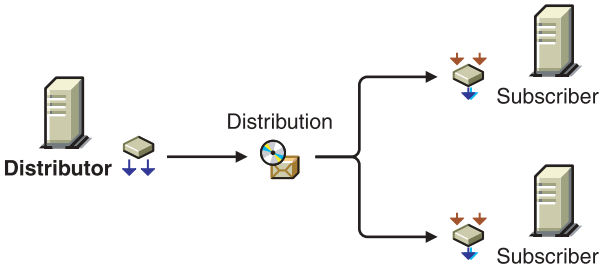
他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、Distribution、Distributor、および Channel の関係を示しています。



Distributor は Distribution を Channel に関連付けます。

次の図は、Subscriber サーバに Distribution を送信する Distributor を示しています。



Distribution の説明

Distribution は、ネットワークのさまざまなサーバで必要なソフトウェアとファイル、またはポリシーパッケージをコンパイルしたものです。

Distribution は、1 つの Distributor によってのみ所有されます。Distribution は、Channel との関連付けに関するリストを保持し、複数の Channel に配置されます。

Distribution は、Distribution のタイプに従って構築されます。Distribution のタイプは 7 つあります。

- Desktop Application [1]
- File
- FTP
- HTTP
- MSI
- ポリシーパッケージ
- RPM
- Software Package

[1] Desktop Application Distribution は、Desktop Management がインストールされている場合にのみ利用できます。

Distribution のタイプについては、119 ページの「Distribution のタイプ」を参照してください。

スケジュール設定

Distribution の構築スケジュールは、どのくらいの頻度で Distribution を構築する必要があるかを Distributor に通知します。Distribution が最後に構築された後に変更されている場合は、新しい Distribution が作成されます。

Distribution は、アクティブまたは非アクティブにして Distribution の構築を制御することもできます。

スケジュール設定については、8 章 331 ページの「スケジュール設定」を参照してください。

既存の Distribution の新しいバージョンを作成および配布する方法

Distribution オブジェクトを設定し、さまざまな配布スケジュールを設定すると、既存の Distribution の新しいバージョンが次のパラメータに従って自動的に作成および配布されます。

- **更新スケジュール：** このスケジュールは、Distributor が eDirectory を読み取って、すべての Distribution の変更を認識するタイミングを決定します。特定の Distribution で変更が検出された場合、Distribution は構築スケジュールに従って再構築されます。

  更新スケジュールの詳細については、335 ページの「Distributor オブジェクトの更新スケジュール」を参照してください。

- **構築スケジュール：** このスケジュールは各 Distribution で個別に設定されます。変更が加えられたと判断された Distribution でこのスケジュールが開始されると、Distributor は Distribution を再構築します。

  構築スケジュールの詳細については、336 ページの「Distribution オブジェクトの構築スケジュール」を参照してください。

- **[Maximum Revisions]：** このフィールド（[General] > [Settings] の順にクリックして表示される Distribution オブジェクトのプロパティ）は、Distributor および Subscriber サーバのファイルシステムで保持される Distribution のバージョン数を決定します。Distribution のいくつかのタイプでは、このフィールドは Distribution の一部を再構築するか（デルタ）、または Distribution 全体を再構築するかを決定します。それ以外の場合、このフィールドは主にディスク容量の使用状況を制御するために使用されます。

  リビジョン数が最大値に近づくと、SMTP 通知が設定されている場合、SMTP 電子メール通知が送信されます。

  [Maximum Revisions] フィールドのスケジュールの詳細については、117 ページの「最大リビジョン数」を参照してください。

これらのパラメータは、Distribution の再構築が必要になるタイミングを決定します。他のスケジュール（送信および抽出）は、再構築された Distribution ファイルが送信および抽出されるタイミングを決定します。

配布セキュリティ

Policy and Distribution Services には、Distribution をセキュリティで保護する複数の方法が用意されています。

- 115 ページの「証明書」
- 115 ページの「暗号化」
- 115 ページの「サーバ間の通信」

証明書

証明書は Policy and Distribution Services によって使用されるセキュリティメカニズムであり、Subscriber が受信した Distribution が、その Distribution を所有する Distributor が実際に送信したものであることを保証します。一致する証明書がない場合、Subscriber は Distributor から Distribution を受信できません。

詳細については、313 ページの「署名付き証明書とダイジェストを使用した配布のセキュリティ」を参照してください。

暗号化

Distribution を安全なネットワークの外側に送信する場合は、暗号化できます。

詳細については、324 ページの「暗号化を使用した Distribution のセキュリティ」を参照してください。

サーバ間の通信

必要に応じてサーバ間通信のセキュリティをインストールすることにより、安全なネットワーク内外の Tiered Electronic Distribution コンポーネント間の通信をセキュリティで保護できます。

詳細については、328 ページの「セキュリティ保護されていない接続でのサーバ間通信のセキュリティ」を参照してください。

Distribution の削除

Distribution が構築された後に、Distribution オブジェクトまたは Distributor サーバのファイルシステムで削除（ファイルやディレクトリの削除など）を実行すると、これらのファイルまたはディレクトリは Distribution の再構築時に Distribution からも削除されます。ただし、同期を有効にすると、ファイルおよびフォルダを Subscriber サーバのファイルシステムからも削除できます。

詳細については、180 ページの「File Distribution のディレクトリ同期の細分性」を参照してください。

一時的な Distribution ファイルのクリーンアップ

一時的な Distribution ファイルによって使用されるディスク容量を減らすために、これらのファイルを自動的にクリーンアップするようになりました。以前は、Subscriber サーバによる Distribution の抽出後に、distfile.ted ファイルが Subscriber サーバの作業ディレクトリに残されていました。

このクリーンアップ機能によって、Distribution の抽出後に、distfile.ted ファイルと一時的なその他の Distribution ファイルが自動的に削除されます。ただし、この Subscriber に Distribution が再送信されないようにするため、Distribution が抽出およびクリーンアップされたことを示すステータスファイルが Subscriber の作業ディレクトリに残されます。

重要： Distribution のクリーンアップ機能は、ZENworks 6.5 Server Management の Distributor および Subscriber によって送受信された Distribution に対してのみ使用できます。以前のバージョンの Server Management ソフトウェアを実行する Distributor または Subscriber によって送受信された Distribution は、クリーンアップできません。

親 Subscriber

Distribution を転送する必要がある親 Subscriber では、このファイルが親 Subscriber のサーバでクリーンアップされないため、親 Subscriber は Distribution の転送を継続できます。

親 Subscriber は、転送しない Distribution がクリーンアップされた後に、転送用に同じ Distribution を受信すると、その Distribution が必要ないことがステータスファイルに示されていても、再度その Distribution を受信します。

Distribution タイプとクリーンアップ

FTP、HTTP、RPM、MSI、Software Package、および Policy Package タイプの Distribution では、常にクリーンアップされます。[Maximum Revisions] フィールドは、これらのタイプの Distribution では使用できません。

File および Desktop Application タイプでは、[Maximum Revisions] フィールドに 1 を設定すると、Distribution の抽出後に一時ファイルをクリーンアップできます。ただし、File Distribution では、[Verify Distributions] チェックボックスが選択されていると、[Maximum Revisions] フィールドに 1 を設定しても Distribution はクリーンアップされません。

iManager でのクリーンアップステータスの再設定

iManager では、ステータスファイルをリセットして、クリーンアップされた Distribution を Subscriber に強制的に受信させることができます。

ロールバックされないクリーンアップ

一時ファイルのクリーンアップでは、抽出済みの Distribution をロールバックすることはできません。クリーンアップは、単に一時ファイルを削除するだけです。

再割り当てされた Distribution のクリーンアップ

古い Distributor から新しい Distributor に再割り当てされた Distribution の作業ディレクトリは、古い Distributor サーバでは自動的にクリーンアップされません。古い Distributor サーバでは、Distribution の一時ファイルを手動でクリーンアップする必要があります。

Distribution に関する問題

Distribution を決定する場合は、次の点を考慮してください。

- ファイルサイズと圧縮の可能性 (.jpg ファイルは、圧縮に関してテキストファイルほど効果が得られない)
- WAN リンクの帯域幅
- ファイルの変更頻度
- ネットワークリソースの制約 (少ないディクス容量、帯域幅増加の可能性など)

このような情報をよく考えて判断することにより、リソースを分散して活用し、リソースの使用を最小限に抑えることができます。

Distribution を構成して、ターゲットと異なるファイルだけをコピーしたり、元の状態のファイルをすべてコピーしたりできます。

次の節では、Distribution のその他の問題について説明します。

- 117 ページの「同時に実行可能な Distribution の最大数」
- 117 ページの「最大リビジョン数」
- 118 ページの「I/O レート（1 秒あたりのバイト数）」
- 118 ページの「Distributor の eDirectory 情報の更新」
- 118 ページの「Distribution パッケージの変更の確認」
- 118 ページの「MSI Distribution の抽出エラー」

同時に実行可能な Distribution の最大数

これは、Distributor および Subscriber オブジェクトの属性です。Distribution の送信時に同時に処理される Subscriber の数を制御するために使用されます。これは、Distributor または親 Subscriber が多数の Subscriber に配布する場合に役立ちます。この設定により、Distributor が Distribution をすべての Subscriber に一度に送信しないようにできます。

たとえば、Distributor または親 Subscriber が 100 の Subscriber に送信するときに、同時に実行される Distribution の数が 10 に設定されている場合、送信元は 10 の接続に対して送信を開始します。接続されている Subscriber が Distribution の受信を終了すると、次に別の 10 の Subscriber に送信されます。これは、100 の Subscriber すべてにサービスが提供されるまで継続されます。

最大リビジョン数

各 Distribution では、Distributor および Subscriber によって作業ディレクトリに保持される Distribution のバージョン数を指定できます。Distribution が ConsoleOne または iManager のいずれで作成されるに関係なく、すべての Distribution タイプではデフォルト値は無制限です。ただし、ConsoleOne で作成される場合、File および Desktop Application タイプの Distribution のデフォルト値は 10 になります。Distribution を作成するときに、[Maximum Revisions] フィールドに値が入力されていることを確認します。リビジョンの最大数を計算するときは、利用可能なディスク容量を考慮してください。

1 を入力すると、[Delete Previous Revision Before Receiving Next] フィールドにアクセスできるようになります。このフィールドにより、Distribution の 1 つのコピーだけをサーバのファイルシステムに保持することで、ディスク容量を制御できます。

File Distribution は、最初の作成時にのみ、Distribution 全体が構築されます。以後に作成されるバージョンはすべて、現在のバージョンと以前のバージョンとの相違点（デルタ）のみを含みます。ただし、File Distribution では、リビジョン数が最大値に達すると、以前のバージョンがすべて削除された後に新しい Distribution（基本）が構築され、リビジョン数は 1 からカウントされます。

FTP、HTTP、および Server Software Package タイプでは、リビジョンの最大数に達すると、エージェントが Distribution の一番古いバージョンを削除し、現在のバージョンをリビジョンに追加します。そのため、Distribution オブジェクトに入力された最大数を超えることはありません。

リビジョン数が最大値に近づくと、SMTP 通知が設定されている場合、SMTP 電子メール通知が送信されます。

I/O レート（1 秒あたりのバイト数）

これは、Distributor および Subscriber オブジェクトの属性です。Distribution の送信時に、Distributor または親 Subscriber が利用する帯域幅の制御に使用されます。デフォルト値は指定されていません。つまり、Distribution の送信にはあらゆる帯域幅を使用できます。

Distributor の eDirectory 情報の更新

Distributor は、eDirectory の Tiered Electronic Distribution オブジェクトに含まれる設定情報で更新される必要があります。

設定の変更には、Distributor オブジェクトの属性、Distributor オブジェクトに属する Distribution オブジェクト、または Distributor オブジェクトが関連付けられている Channel オブジェクトへの変更が含まれます。

Distributor のスケジュールは、Distributor が eDirectory を読み取って、設定情報を認識するタイミングを決定します。このスケジュールは、Tiered Electronic Distribution オブジェクトが eDirectory で変更される頻度と一致するように設定してください。

Distributor オブジェクトを右クリックして［Refresh］メニューオプションを選択するか、または iManager で ZENworks Server Management の役割を使用することにより、eDirectory 情報を強制的に更新することもできます（82 ページの「Policy and Distribution Services エージェントの強制実行」を参照してください）。

Distribution パッケージの変更の確認

Distribution の構築スケジュールは、Distribution の変更を確認する頻度を Distributor に通知します。

たとえば、Distribution のスケジュールに週 1 回の構築を指定できます。Distributor はパッケージを再構築し、以前のバージョンと比較して、変更されているかどうかを確認します。

MSI Distribution の抽出エラー

一部の MSI Distribution は、Windows 2000 サーバでは抽出できませんが（通常はエラー 1603 が表示されます）、Windows Server 2003 サーバでは抽出できます。この違いは、2 つのオペレーティングシステムが MSI パッケージのインストールに必要な権利を処理する方法が異なるために生じます。

これは、Windows 2000 サーバでは、MSI Distribution のプロパティを編集することで解決できます。

1. ConsoleOne で MSI Distribution のプロパティにアクセスします。
2. ［Type］タブで、［Selected Packages］の下に表示される MSI パッケージを選択します。
3. ［Edit Parameter List］をクリックして、［Edit Parameters］ダイアログボックスを開きます。
4. ［Custom Parameters］フィールドに次のように入力します。

   ```
   ALLUSERS=1
   ```

5. ［OK］をクリックして変更内容を保存します。

6 [Selected Packages] の下に表示される MSI パッケージごとに、ステップ 2 からステップ 5 を繰り返します。

7 [OK] をクリックして、更新された MSI Distribution のプロパティを保存します。

Distribution の決定

ファイルシステムに表示されるものはすべて配布できます。これには、サーバアプリケーションやファイルなどがあります。たとえば、アプリケーションやファイルは、次の目的のいずれかを実現できます。

- サーバソフトウェアのインストール（ウイルス対策ソフトウェアなど）
- サーバソフトウェアの更新（NetWare Support Pack など）
- サーバ上のファイルの更新（ウイルスパターンなど）
- サーバファイルまたは設定への標準化の導入（NetWareサーバのautoexec.ncfファイルと更新バージョンとの置換など）

Distribution に名前を付けるときは、わかりやすい名前を使用してください。このような名前は、Distribution に関連付けられた Channel に名前を付けるときにも使用できます。たとえば、次のように入力します。

```
VirusProtect
VProtectPatterns
NW51patch4
NW6patch1
AUTOEXECNCF000326
```

次の節では、複数の Distribution タイプと、Distribution の決定に関する問題について説明します。

- 119 ページの「Distribution のタイプ」
- 124 ページの「Distribution パッケージのサイズと頻度の決定」

Distribution のタイプ

Distribution には複数のタイプがあります。各タイプは、特定のニーズに合わせた独自の機能を備えています。

- 120 ページの「Desktop Application」
- 120 ページの「File」
- 121 ページの「FTP」
- 122 ページの「HTTP」
- 122 ページの「MSI」
- 123 ページの「ポリシーパッケージ」
- 124 ページの「RPM」
- 124 ページの「Software Package」

Distribution の各タイプを設定する方法については、125 ページの「Distribution の作成」（特に 127 ページのステップ 6）を参照してください。

File および FTP タイプの Distribution では、作成プロセスを自動化するために Distribution ウィザードを利用できます。詳細については、146 ページの「Distribution ウィザードの使用」を参照してください。

Desktop Application

eDirectory ツリーとターゲット Subscriber サーバ上の指定の場所に、(Desktop Management で作成された) アプリケーションオブジェクトとアプリケーションの関連ファイルを配布します。この Distribution タイプを使用すると、Novell Application Launcher によって配布されるアプリケーションの地理的、負荷、および冗長性の問題を解決できます。この Distribution タイプを使用しない場合、Novell Application Launcher では、デスクトップ管理での手動設定作業に時間がかかります。詳細については、6 章 283 ページの「Desktop Application Distribution」を参照してください。

Desktop Application Distribution タイプは、Linux および Solaris サーバではサポートされていません。

この Distribution タイプは、eDirectory ツリー内のコンテキスト (Subscriber の作業コンテキスト) にオリジナルのアプリケーションオブジェクトの変更されたコピーを自動的に配布して、ユーザとワークステーションをローカルで処理する Subscriber サーバにアプリケーションのファイルを自動的にコピーします。変更されたアプリケーションオブジェクトの機能を完全に有効にするために、オブジェクトへの適切なフックアップがすべて実行されます。

Desktop Application Distribution では、Distribution オブジェクトでリビジョンの最大数を設定できます。バージョン番号が指定した番号に達すると、Distributor は Distribution 全体を再構築します。デフォルトでは、この数は 10 です。

Desktop Application Distribution は、Distributor サーバと異なるツリーの Subscriber サーバに送信できます。ただし、受信サーバの Subscriber オブジェクトは、Distribution によって作成される変更されたアプリケーションオブジェクトと同じツリーに属している必要があります。他のツリーのサーバに Desktop Application Distribution を送信するには、Distributor のツリーで External Subscriber オブジェクトを使用します。

File

このタイプでは、配布するファイルまたはディレクトリを Distributor サーバから選択し、Subscriber に抽出する場所を選択できます。

File タイプは連続して処理されるため、Distribution の構築と抽出の順序を制御します。これにより、構築と抽出のプロセスが同期せずに実行されることを防ぐことができます。

重要： Linux と Solaris のファイルシステムでは大文字と小文字が区別されるため、大文字と小文字が異なる点以外は同一のパスおよびファイル名を使用できます。だたし、このようなファイルを 2 つ選択すると、File タイプでは大文字と小文字が区別されないため、抽出時に選択された最初のファイルだけが配布されます。したがって、大文字と小文字が異なる点以外は同一のパスおよびファイル名を持つ 2 つのファイルを、File Distribution に配置しないようにしてください。

デフォルトでは、[Cache and Forward] が使用されます。このプロセスでは、親 Subscriber は Distribution を受信し終わる前に、下位の Subscriber に Distribution を送信し始めることができます。これにより、各 Subscriber が Distribution の受信完了後に送信を開始する場合に比べて、Distributor のルーティング階層内にある一連の親 Subscriber を介して Distribution 全体をすばやく送信できます。

File Distribution は、頻繁に変更され、アップデートの配布が必要になる、サイズの大きな Distribution を配布する場合に役立ちます。

Distribution の最初のバージョンでは、Distributor は Distribution 全体を構築します (基本の作成)。File タイプの独自の機能として、以後に作成されるバージョンでは、構築時との相違点が計算され、Distribution のデルタだけが構築されます。

これは、ソースコンピュータ（Distributor または親 Subscriber）の Distribution に含まれるファイルおよびディレクトリのリストを保持することによって実行されます。ソースファイルが変更されると、構築スケジュールが次に開始されるときに新しい Distribution が構築されます。ただし、この新しい Distribution には、以前のバージョンと現在のバージョン間で異なるファイルだけが含まれます。これは、元の Distribution のデルタと呼ばれます。

Distribution ファイルのデルタは Subscriber に配布されますが、Distribution 全体ではありません。

File タイプは、より小さいデルタを構築できるため、頻繁に変更を加える場合にも有効です。

File Distribution 全体を送信するオプションはありません。ただし、リビジョンの最大数に達すると、Distribution は完全に再構築され、デルタと以前のリビジョンはすべて削除されます。したがって、リビジョンの最大数を 1 に設定した場合は、デルタは使用されず、Distribution 全体が毎回構築され、送信されます。

たとえば、最初に構築されるのは基本 Distribution（バージョン 1）、最初のアップデート（デルタ 1）はバージョン番号 2、次のアップデート（デルタ 2）はバージョン番号 3 となり、これは設定したリビジョン数に達するまで続きます。リビジョン数に達すると、新しい基本 Distribution が再構築されます。デフォルトでは、この数は 10 です。

File Distribution では、前後のアクションを設定できます。詳細については、129 ページの「Distribution の前後の処理」を参照してください。

リビジョンの最大数は Distribution オブジェクトで設定できます。

File タイプでは、同期を有効にすると、次のいずれかの方法で Distribution の抽出時に Subscriber サーバのファイルシステムからファイルおよびディレクトリを削除できます。

- **Distribution オブジェクトの編集：** Distribution オブジェクトのファイルおよびディレクトリのリストからファイルを削除します。Distribution の再構築時には、これらのファイルおよびディレクトリは含まれません。
- **Distributor のファイルシステムからのファイルの削除：** Distribution に属していたファイルを Distributor のファイルシステムから削除します。Distributor が更新されると、これらのファイルおよびディレクトリを含まない Distribution が再構築されます。

どちらの場合も、同期が有効になっている場合は、Distribution の抽出時にこれらのファイルおよびディレクトリが Subscriber サーバのファイルシステムから削除されます。同期の詳細については、180 ページの「File Distribution のディレクトリ同期の細分性」を参照してください。

手動で強制的に Distribution を構築するには、iManager を使用します（82 ページの「Policy and Distribution Services エージェントの強制実行」を参照してください）。

FTP

このタイプでは、1 つまたは複数の FTP ソースのファイルで構成される Distribution を作成できます。各ソースには、1 つまたは複数のディレクトリやファイルを含めることができます。

FTP サイトディレクトリのエントリがディレクトリの場合は、そのディレクトリに属するファイルとサブディレクトリがすべて Distribution に構築されます。

Server Management は、シンボリックリンクファイルの取得をサポートするようになりました。この結果、Linux または Solaris 環境で、他の環境では無効になると想定される FTP ファイルを受信できるようになりました。

Distribution の構築スケジュールが開始されると、次のプロセスが実行されます。

- FTP タイプは、新しいバージョンが以前のバージョンと異なる場合にのみ新しい Distribution を作成します。
- Distributor は完全に新しい Distribution を構築します。
- Distributor は、新しいバージョンの Distribution を適切な Subscriber に送信します。

リビジョンの最大数を Distribution オブジェクトで設定すると、ディスク容量を節約できます。デフォルトでは、この数は指定されていません。

HTTP

このタイプでは、1 つまたは複数の HTTP ソースで構成される Distribution を作成できます。各ソースには、1 つまたは複数のターゲットエントリを含むことができます。

Distribution の構築スケジュールが開始されると、次のプロセスが実行されます。

- HTTP タイプは、新しいバージョンが以前のバージョンと異なる場合にのみ新しい Distribution を作成します。
- Distributor は完全に新しい Distribution を構築します。
- Distributor は、新しいバージョンの Distribution を適切な Subscriber に送信します。

リビジョンの最大数を Distribution オブジェクトで設定すると、ディスク容量を節約できます。デフォルトでは、この数は指定されていません。

MSI

MSI (Microsoft Software Installer) パッケージを Windows サーバに配布します。MSI エンジンは、MSI Distribution に含まれる Windows 固有のソフトウェアのインストールに使用されます。ベンダは、Windows 環境でインストールするソフトウェア用の MSI パッケージを作成できます。

.mst ファイルを作成する Installshield* AdminStudio* ZENworks Edition ソフトウェアは、ZENworks 6.5 製品に付属の CD から利用できます。

MSI 3 は、配布可能なバージョンとしてサポートされます。ただし、ZENworks 6.5 では、MSI 3 の新機能を個別にはサポートしていません。

MSI Distribution のコンポーネントは、.msi、.msp、および .mst ファイルで構成されます。

- **.msi ファイル:** MSIエンジンによってインストールされるMicrosoftソフトウェアを含む MSI パッケージです。

  MSI パッケージには、.msi ファイルのみ、または .msi ファイルのフォルダに含まれるファイルすべてとサブフォルダのファイルすべてを含めることができます。
- **.mst ファイル：** MSI パッケージのプロパティを追加、削除、または変更するファイルです。このファイルにより、さまざまなユーザグループに合わせてインストール処理をカスタマイズできます。
- **.msp ファイル：** MSI パッケージにパッチを提供する MSP パッケージです。

  MSI ベースのパッチファイルは、.msp 以外のファイル拡張子を持つ場合があります。

MSI Distribution には、次のものを含めることができます。

- 1 つまたは複数の MSI パッケージ
- 1つまたは複数のMSIパッケージと、各MSIパッケージに適用される1つまたは複数の .mst ファイル
- 1 つまたは複数の MSI パッケージと 1 つまたは複数の MSP パッケージ
- 1 つまたは複数の MSI パッケージ、1 つまたは複数の MSP パッケージ、および各 MSI パッケージに適用される 1 つまたは複数の .mst ファイル
- 1 つまたは複数の MSP パッケージのみ。.msp ファイルには、パッチを適用する MSI パッケージのアプリケーションを特定するのに必要な情報が含まれるため。

  パッチを適用すると、ファイルの更新だけでなく、コンピュータの設定を変更することもできます。

MSI パッケージごとに .mst ファイルのアプリケーション順序を決定したり、Distribution のリストに属する MSI パッケージと MSP パッケージの実行順序を決定したりできます。

MSI Distribution が MSI コンポーネントと MSP コンポーネントの両方を含む場合は、インストール後のアクションが Distributor によって Distribution に追加され、正しい順序で完了できます。

MSP は特定の MSI パッケージを変更するように設計されているため、正しい実行順序が指定されていることを確認する必要があります。

一部の MSI Distribution は、Windows 2000 サーバでは抽出できない場合があります。この問題を解決するには、118 ページの「MSI Distribution の抽出エラー」を参照してください。

ポリシーパッケージ

このタイプは、サーバにポリシーを適用するメカニズムを提供します。以前のバージョンの Policy and Distribution Services では、すべてのポリシーは eDirectory オブジェクトとコンテナの関連付けによって実行されていました。ZENworks 6.5 Server Management では、ポリシーは、Distributed Policy Package を使用して適用するために Subscriber サーバに配布されます。ただし、Distributor のポリシーは、Container Package または Service Location Package を使用して、コンテキストの関連によって引き続き実行されます。

Policy Package Distribution では、ポリシーは Distribution としてサーバに直接送信され、受信側の Subscriber サーバで抽出されます。次に、Distribution に含まれていたポリシーがそのサーバで実行されます。

リビジョンの最大数を Distribution オブジェクトで設定すると、ディスク容量を節約できます。デフォルトでは、この数は指定されていません。

External Subscriber オブジェクトを使用して Policy Package Distribution を Subscriber に送信するには、agentinfo.properties ファイルを編集して、信頼されるツリーでのエラーの発生を防ぐ必要があります。詳細については、165 ページの「Policy Package Distribution 送信時に信頼されるツリーで発生するエラーの回避」を参照してください。

各ポリシーの詳細については、205 ページの「サーバポリシーの説明」を参照してください。

RPM

RPM Distribution を使用すると、Linux および Solaris サーバ向けに作成した Red Hat Package Manager (RPM) パッケージを配布できます。ト

Solaris の場合、デフォルトでは Solaris ソフトウェアのインストール時に RPM がインストールされないため、最初に RPM をサーバにインストールしておく必要があります。Solaris で RPM に相当するのは PKG です。

Distribution の構築スケジュールが開始されると、次のプロセスが実行されます。

- Distributor は完全に新しい Distribution を構築します。
- Distributor は、新しいバージョンの Distribution を適切な Subscriber に送信します。

リビジョンの最大数を Distribution オブジェクトで設定すると、ディスク容量を節約できます。デフォルトでは、この数は指定されていません。

Software Package

Server Software Package は、ConsoleOne の Server Software Package ネームスペースに作成されます。詳細については、5 章 241 ページの「Server Software Package に関する問題」を参照してください。

Software Package は、Distribution タイプの中で最も多くの機能を備えています。インストールの前提条件、インストール前の動作、およびインストール後の動作のほかに、テキストフィールド、SET パラメータ、レジストリ設定、および products.dat ファイルを変更する機能が含まれます。

Software Package Distribution では、配布する .cpk ファイルを選択できます。これにより、受信サーバに自動的にインストールされるソフトウェア製品を Distribution に配置できます。サーバ上の既存のサーバソフトウェアに対するソフトウェアアップデートを含めることもできます。

1 つの Distribution に対して複数の .cpk ファイルを選択できます。個々の .cpk ファイルは、.cpk ファイルの前提条件に一致しているかどうかによって、Subscriber に適用されます。

重要： .cpk ファイルがサーバに適用される順序は保証されていないため、ある順序で開始される Distribution 内の .cpk file が同じ順序で終了されるとは限りません。そのため、.cpk ファイルを特定の順序でインストールする場合は、各 .cpk ファイルを Distribution に個別に配置し、Distribution のスケジュールを設定して順序を決定してください。詳細については、244 ページの「複数の Distribution を使用したソフトウェアパッケージの配布順序の強制的な指定」を参照してください。

Distribution パッケージのサイズと頻度の決定

Distribution が構築および送信されるときのサイズと頻度は、次の条件によって決まります。

- 配布されるファイルのサイズと数。これは、Distributor、Subscriber、および親 Subscriber の各サーバで使用されるディスク容量を決定するときに役立ちます。
- Software Package Distribution (.cpk) では、ソースが変更されるたびに、新しいバージョンの Distribution が常に構築されます。
- HTTP Distribution および FTP Distribution は、ソース変更の有無にかかわらず、新しい Distribution のバージョンを常に構築します。

- パッケージが変更され、更新が必要になる頻度。これは、新しいバージョンのパッケージを作成する頻度を決定するときに役立ちます。サイズの大きな Distribution パッケージを定期的に再構築するサーバには、この作業を実行する処理能力が必要です。パッケージの多数バージョンの作成は、Distributor の作業ディレクトリで使用されるディスク容量にも影響します。
- 保持される Distribution パッケージのバージョン数。これも、Distributor および Subscriber のサーバで使用されるディスク容量に影響します。
- File Distribution では、[Revisions] フィールドの [Maximum Number] で指定した数 (デフォルトは 10) に達するまで、Distribution の新しいバージョンごとにデルタファイルが作成されます。指定した数に達すると、新しい基本 Distribution が作成されます。デルタファイルには、Distribution の以前のバージョンと現在のバージョンとの相違点だけが含まれます。

Distribution の作成

1 ConsoleOne で、Distribution を作成するコンテナを選択し、[File] > [New] > [Object] の順にクリックします。次に、Distribution のタイプを選択し、[OK] をクリックします。

2 Distribution 名を指定します。

重要： Distribution 名にピリオド (.) は使用できません。代わりに、単語の区切り文字としてはダッシュ (-) またはアンダースコア (_) を使用します。Distribution 名にピリオドを使用した場合、Distribution は送信されず、Distributor は終了後も再ロードされません。

3 Distributor に Distribution の所有権を与えるには、Distributor オブジェクトを参照して選択し、[Define Additional Properties] を選択し、[OK] をクリックします。

Distribution オブジェクトのプロパティが表示されます。

各 Distribution は 1 つの Distributor に属し、Distributor によって構築および送信されます。

4 [General] > [Settings] の順にクリックし、次のフィールドに入力します。

[Active] : 必須。Distribution を Subscriber で利用できるようにするには、アクティブにする必要があります。

[Use Digests] : ダイジェストは、送信中に Distribution が改ざんされていないことを確認するために、Distributor と Subscriber によって使用されます。このダイジェストは、Subscriber が照合する MD5 チェックサムを提供します。

サイズの大きい Distribution でダイジェストを作成すると時間がかかります。メガバイトあたりの時間数 (分) は、ダイジェストが作成されるサーバのハードウェア設定によって異なります。

ダイジェストは、Distribution のパッケージの破損も検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。

[Encrypt]：セキュリティで保護されていない接続を介して送信する場合に、Distribution を暗号化できます。暗号化によって、同一ファイアウォール内にない Distributor と Subscriber の間で送信される Distribution のセキュリティが向上します。[Strong] または [Weak] のいずれかの暗号化をクリック選択します。暗号化を実行する各サーバに同じバージョンの NICI 2.6.4 をインストールする必要があります（51 ページの「NICI 2.6.4 のインストール」を参照してください）。ただし、NICI 2.4.6 がインストール済みである場合は、NICI 2.6.4 にアップグレードするかどうかはオプションです。この 2 つのバージョン間では互換性があります。

[Maximum Revisions]：この数値は、Distributor と Subscriber の作業ディレクトリに特定の Distribution のバージョンをいくつまで保存できるかを指定することによって、ディスク容量の使用状況を制御するのに役立ちます。File Distribution では、デフォルト値は 10 です。

データが頻繁に変更され、変更が最小限である（デルタファイルが小さい）場合は、保存するリビジョンを増やします。データが頻繁に変更されない場合や、大部分のデータが変更される（デルタファイルが大きい）場合は、保存するリビジョンを減らします。[1] を選択すると、[Delete Previous Revision] フィールドが利用できます。

[Delete Previous Revision Before Receiving Next]：このオプションは、[Maximum Revisions] フィールドで [1] を選択した場合に、利用できます。Distribution のサイズが大きく、Subscriber サーバ上の利用可能なディスク容量が犠牲になる場合は、このオプションを選択して、以前のバージョンを削除してから次のバージョンを受信することによって、ディスク容量を節約できます。

このチェックボックスをオフにした場合、以前のバージョンが削除される前に、新しいバージョン全体が受信されます。いずれの場合も、Distribution を受信した後、Subscriber の作業ディレクトリに保存できる Distribution のバージョンは 1 つだけです。

[Priority]：Distribution に優先度を指定して、他の Distribution との関係で Distribution をどのように送信するかを指定できます。高優先度の Distribution は、中優先度または低優先度の Distribution よりも前に送信されます。Distribution の優先度については、128 ページの「Distribution の優先度」を参照してください。

Distributor: この Distribution を構築および送信する Distributor オブジェクトの DN です。この属性は変更できません。Distributor は、Distribution オブジェクトの作成時に選択しています。

説明： Distribution に関する役に立つ詳細情報を入力します。たとえば、デスクトップアプリケーションの名前、含まれているファイルやディレクトリ、対象になるユーザグループなどです。

5 [General] > [Restrictions] の順にクリックし、次のプラットフォーム制限を選択します。

[Platform Restrictions]：この Distribution の受信に関する前提条件として、特定のオペレーティングシステムのバージョンを選択する場合は、[No Restrictions] の選択を解除して、希望するオペレーティングシステムのバージョンを選択します。次の中から選択できます。

[No Restrictions]
[NetWare All]
[NetWare 4.*x*]（以前のバージョンの ZfS でサポートされていたプラットフォーム）
[NetWare 5.0]（以前のバージョンの ZfS でサポートされていたプラットフォーム）
[NetWare 5.1]
[NetWare 5.*x*]
[NetWare 6.*x*]
[Windows Server]
[Solaris]
[Linux]

[No Restrictions] チェックボックスをオンにすると、Distribution の送信先のプラットフォームが制限されません。

[NetWare All] を選択した場合、個々の NetWare プラットフォームを選択する必要はありません。

6 [Type] タブを選択し、ドロップダウンボックスを使用して [Select Type] フィールドで Distribution タイプを選択します。

399 ページの「Desktop Application」
400 ページの「File」
402 ページの「FTP」
404 ページの「HTTP」
405 ページの「MSI」
408 ページの「ポリシーパッケージ」
409 ページの「RPM」
410 ページの「Software Package」

一部の Distribution タイプでは、フィールドにディレクトリ名などの情報を入力するときに、必ず (Enter) を押して変更を保存してください。

重要： FTP、HTTP、RPM、Software Package、および Desktop Application の各タイプでは、抽出時にターゲットファイルがロックされている場合、Subscriber はファイルをコピーできなかったことを示す例外処理を実行します。Distributor はこの情報を Subscriber から受信し、エラーをレポーティングデータベースに記録します。

7 [Schedule] タブを選択して、スケジュールを選択します。

構築スケジュールは、Distributor が新しいバージョンの Distribution を構築する頻度を決定します。

次の 2 つのオプションを使用して、Channel の送信スケジュールと Subscriber の抽出スケジュールを指定できます。

- **[Send Distribution Immediately After Building]：** Channel の送信スケジュールより優先され、送信スケジュールの開始を待たずに Distribution をすぐに送信できます。ただし、Distribution を抽出して使用するタイミングは、Subscriber の抽出スケジュールによって決定されます。
- **[Extract Distribution Immediately After Receiving]:** Subscriber の抽出スケジュールより優先され、抽出スケジュールの開始を待たずに、Distribution をすぐに抽出できます。これは、ウイルスパターンを提供する Distribution など、すぐに抽出する必要がある Distribution に役立ちます。

File Distribution の構築スケジュール： このタイプは新しい Distribution を構築し、変更があるかどうかを以前のバージョンと比較します。変更がある場合、File タイプは現在のバージョンと以前のバージョンとの相違点で構成されるファイルを構築します。バージョンの最大数に達すると、このタイプは、相違点だけを含むファイルを構築する代わりに Distribution 全体を構築し、以前のバージョンをすべて削除します。

HTTP、FTP、および Software Package Distribution の構築スケジュール： これらのタイプは、Distribution の変更に関係なく、構築スケジュールが開始されるたびに新しいバージョンの Distribution を構築します。この新しいバージョンは、すべての Subscriber に送信されます。

Distribution の送信時に、送信元は 2 分ごとの再送信を 30 分間継続した後、送信を中止します。Channel のスケジュールが再度開始されるまで、Distribution は再送信されません。

8 [Channels] タブを選択し、次のフィールドに入力します。

[Channels]： Distribution を Subscriber に送信するには、各 Distribution を少なくとも 1 つの Channel に関連付ける必要があります。Distribution は、選択した Channel（複数可）のすべての Subscriber に送信されます。

9 Distribution の前後のアクションを設定する場合は、129 ページの「Distribution の前後の処理」の手順を参照してください。

10 [OK] をクリックし、[Yes] を選択して証明書を解決します。

NetWare サーバや Windows サーバの場合は、これによって、Channel に登録済みの Subscriber に Distributor からセキュリティ証明書がコピーされます。Linux サーバや Solaris サーバの場合（ドライブをマッピングしていない場合）は、証明書を手動で解決する必要があります。

詳細については、317 ページの「証明書の解決」を参照してください。

Distribution の優先度

Distribution の優先順位は次の 2 つの方法で決定できます。

- **[Send Queue]：** Distribution の送信順序に [High]、[Medium]、または [Low] の優先度を指定できます。たとえば、Channel では、優先度が [High] の Distribution が最初にすべて送信され、次に [Medium] の Distribution が送信され、最後に [Low] の Distribution が送信されます。

  優先度が異なる Distribution は同時に送信されないため、Distribution に割り当てた優先度によって送信順序を制御できます。

- **[Output Rate]：** Distribution の出力レートに [High]、[Medium]、または [Low] の優先度を指定できます。これにより、Distribution で使用される帯域幅を制御できます。たとえば、高優先度の Distribution が最大帯域幅を使用するようにするには、出力レートを [High] に設定する必要があります。空白は、サードパーティアプリケーションから帯域幅が割り当てられることを意味します。

同時に実行可能な Distribution の最大数は、優先度によって影響を受けます。この値は、Distributions に設定された優先度に依存します。たとえば、次のように入力します。

- 同時に実行可能な Distribution の数を 10 に設定します。
- 優先度が [High] の Distribution が 3 つあります。

- 優先度が［Medium］の Distribution が 6 つあります。
- 優先度が［Low］の Distribution が 20 あります。
- 最初に、［High］の Distribution が 3 つ同時に送信されます。
- 3 つの Distribution の送信が終了したら、次に［Medium］の Distribution が 6 つ同時に送信されます。
- 6 つの Distribution の送信が終了したら、次に 20 ある［Low］の Distribution うち 10 が同時に送信され、その後も同様に送信が継続されます。

Distribution の前後の処理

前後処理のアクションは、ZENworks 6.5 Server Management の Distribution の新機能です。

- 129 ページの「Distribution で現在利用できる前後処理のアクション」
- 130 ページの「ソフトウェアパッケージと Distribution の前後のアクション」
- 130 ページの「Software Package Distribution の処理を拡張する前後の機能」
- 130 ページの「有効な Distribution タイプが選択されなかった場合のエラーメッセージ」
- 131 ページの「Distribution の前後の処理アクション」

Distribution で現在利用できる前後処理のアクション

Distribution に実行論理を適用するため、前後のアクションは次の Distribution タイプで使用できます。

File
FTP
HTTP
MSI
RPM
Software Package 1

以前は、Server Software Package でのみ、この機能を利用できました。現在では、ソフトウェアパッケージと Software Package Distribution の両方に、前後のアクションを定義できます。

この Distribution のタイプで前後のアクションを実行できるメリットは、これらのアクションを実行するのに Server Software Packages を使用する必要がなくなる点です。

前後処理のアクションは、Distribution の次のタイプでは使用できません。

Desktop Application
ポリシーパッケージ

ソフトウェアパッケージと Distribution の前後のアクション

Server Software Packages では、前後の機能は［Pre-Installation］タブと［Post-Installation］タブで設定します。これらのタブには、さまざまなオプションにアクセスできる［Script］タブと［Load/Unload］タブが含まれています。

この機能を備えた Distribution タイプでは、［Pre/Post Actions］タブが Distribution オブジェクトのプロパティに追加されます（［Pre-Distribution Actions］タブと［Post-Distribution Actions］タブ）。

［Pre/Post Actions］タブでは、次のオプションを利用できます。

Load Java Class
Script
Start Process
Stop Process
Start Windows Service
Stop Windows Service

これらのオプションの詳細については、131 ページの「Distribution の前後の処理アクション」を参照してください。

Software Package Distribution の処理を拡張する前後の機能

前後のアクションのいずれかを Software Package Distribution に定義すると、次の処理が実行されます。

1. Distribution に含まれる .cpk ファイルのリストが、Distribution オブジェクトの［Type］タブに作成されます。
2. 定義した順序に従って、前のアクションがすべて処理されます。
3. .cpk ファイルが連続して処理されます。
4. 定義した順序に従って、後のアクションがすべて処理されます。

複数のソフトウェアパッケージを含む Distribution オブジェクトで前後のアクションを使用すると、Distribution にリストされたソフトウェアパッケージの前と後に、前後のアクションが確実に実行されるようにできます。ただし、前後の処理は、ZENworks for Servers 3.*x* の Subscriber に対する後方互換性がないため、ZENworks 6.5 Server Management の Subscriber での順序のみが保証されます。

有効な Distribution タイプが選択されなかった場合のエラーメッセージ

［Pre/Post Actions］タブにメッセージだけが表示される場合の例を示します。

- Distributionオブジェクトのプロパティで Distributionタイプを選択していない場合、次のメッセージが［Pre/Post Actions］タブに表示されます。

  ```
  You must select a Distribution type before you can configure pre or post actions.
  ```

  ただし、Distribution タイプを選択するときには、［Apply］をクリックして保存する必要があります。保存すると、Distribution がこのページで認識され、前後のアクションが適用できます。

- 選択したDistributionタイプがPolicy PackageまたはDesktop Applicationのとき、これらのタイプは前後のアクションをサポートしていないため、次のメッセージが［Pre/Post Action］タブに表示されます。

  ```
  This Distribution type does not support pre or post distribution actions.
  ```

Distribution の前後の処理アクション

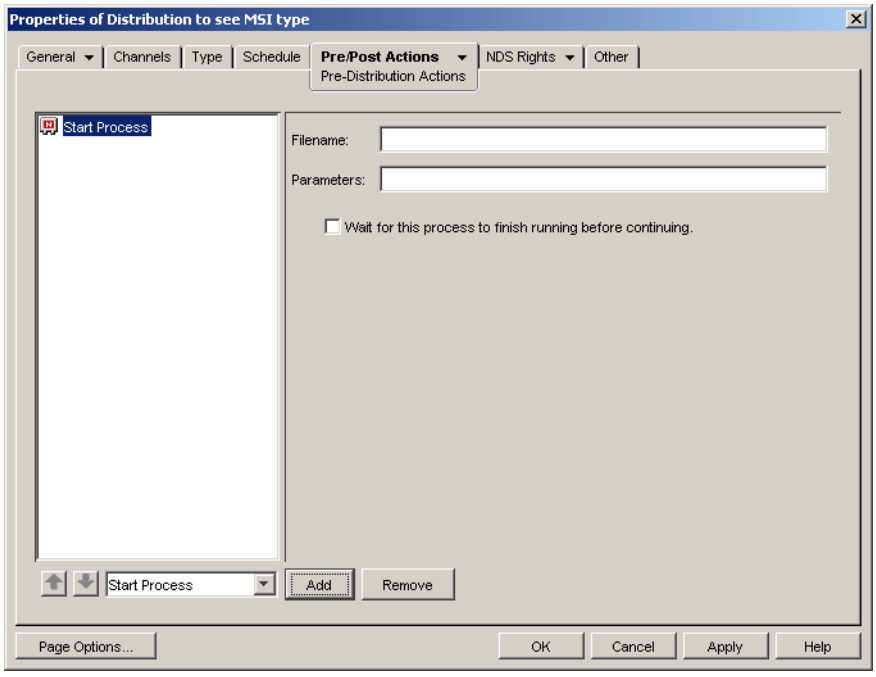
次の各節の説明は、[Pre/Post Actions] タブの [Pre-Distribution Actions] サブタブと [Post-Distribution Actions] サブタブの両方に適用されます。[Pre-Distribution Actions] は Distribution が抽出される前に実行され、[Post-Distribution Actions] はその Distribution の抽出が完了した後に実行されます。

- 131 ページの「プロセス起動アクション」
- 133 ページの「Windows サービス起動 / 停止アクション」
- 134 ページの「スクリプトアクション」
- 135 ページの「Java クラスロードアクション」

プロセス起動アクション

このアクションは、Windows サービス、Java プロセス、および NLM プロセスに使用できます。

プロセス起動アクションは、Server Software Package の NLM/ プロセスロードアクションに類似しています。



プロセス起動アクションを追加するには、ドロップダウンボックスのオプションを選択し、[Add] ボタンをクリックします。次のフィールドに入力します。

- **[Filename]：** これは正確な名前である必要があります。NetWare の場合は、.nlm 拡張子を含めます。

  Linux および Solaris の場合は、フルパスを含める必要があります。

- **[Parameters]：** NLM™ またはプロセスの実行を開始するためのコマンドラインパラメータを含めます。

- **[Wait For This Process To Finish Running Before Continuing]：** NLM やプロセスがそれ自体を終了する場合は、このチェックボックスを選択できます。NLM やプロセスは 10 分以内に終了する必要があります。終了しない場合、ロード処理全体が失敗します。デフォルトでは、このオプションは選択されていません。

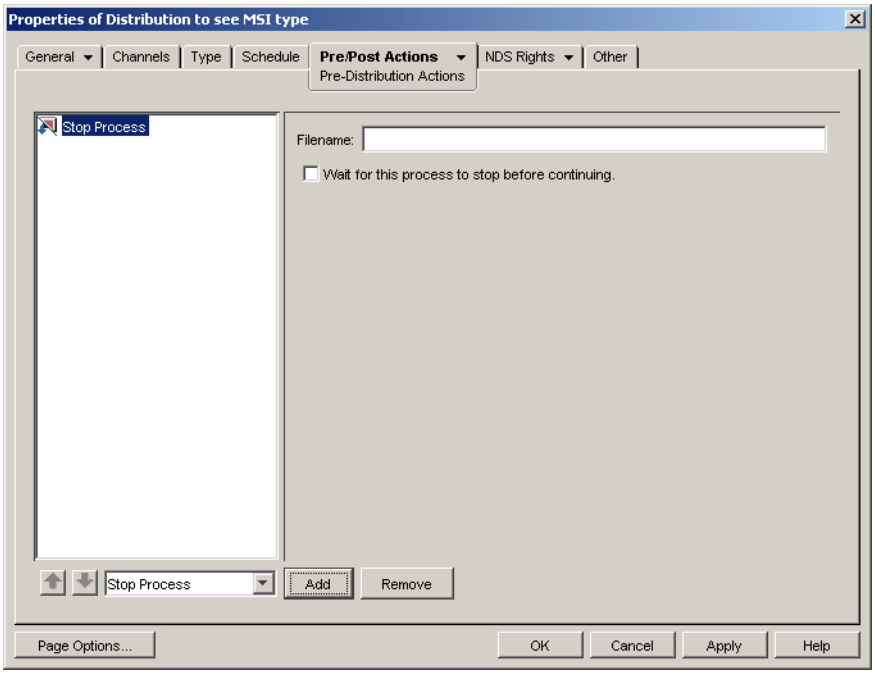
Distribution によって NLM をロードすることを選択し、その NLM がターゲットサーバ上ですでに実行されている場合、パッケージのインストールは失敗し、ロールバックされます（ロールバックが有効になっている場合）。

Distribution に NLM を含めている場合に、NLM がまだロードされていないことを保証するには、[Start Process] オプションを追加する前に、その NLM の [Stop Process] オプションを追加します。ただし、この方法を使用できるのは、その NLM をアンロードするときにユーザによるキーボードからの入力を必要としない場合だけです。

プロセス停止アクション

このアクションは、Windows サービス、Java プロセス、および NLM プロセスに使用できます。

プロセス停止アクションは、Server Software Package の NLM アンロードアクションに類似しています。



プロセス停止アクションを追加するには、ドロップダウンボックスのオプションを選択し、[Add] ボタンをクリックします。次のフィールドに入力します。

- **[Filename]**：これは正確な名前である必要があります（NLM の場合は拡張子までを含む）。多くの NLM ファイルはアンロードするときにユーザの入力を必要とするため、アンロードを自動化することはできません。

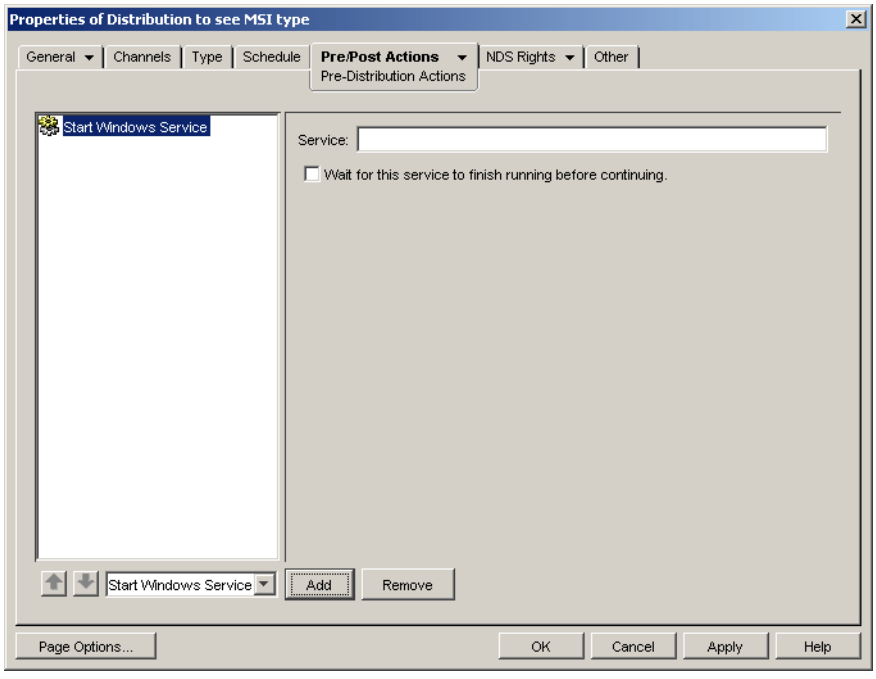
  Linux と Solaris の場合は、プロセスの名前のみを入力します。パス情報は入力しないでください。コンピュータで、その名前で実行されているすべてのプロセスが停止します。

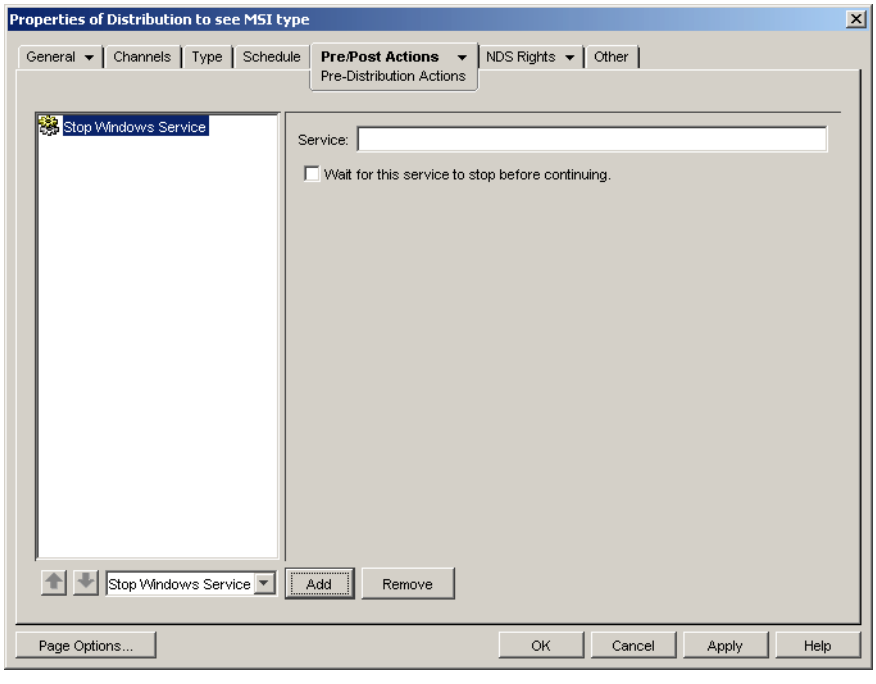
- **[Wait For This Process To Finish Running Before Continuing]**：プロセスがそれ自体を終了する場合は、このオプションを選択できます。デフォルトでは、このオプションは選択されていません。

NLM をアンロードするのにユーザの操作が必要な場合は、Distribution をインストールする前に、手動で NLM をアンロードする必要があります。

Windows サービス起動 / 停止アクション

このアクションは、Windows サービスにのみ使用できます。





サービス起動 / 停止アクションを追加するには、ドロップダウンボックスのオプションを選択し、[Add] ボタンをクリックします。次のフィールドに入力します。

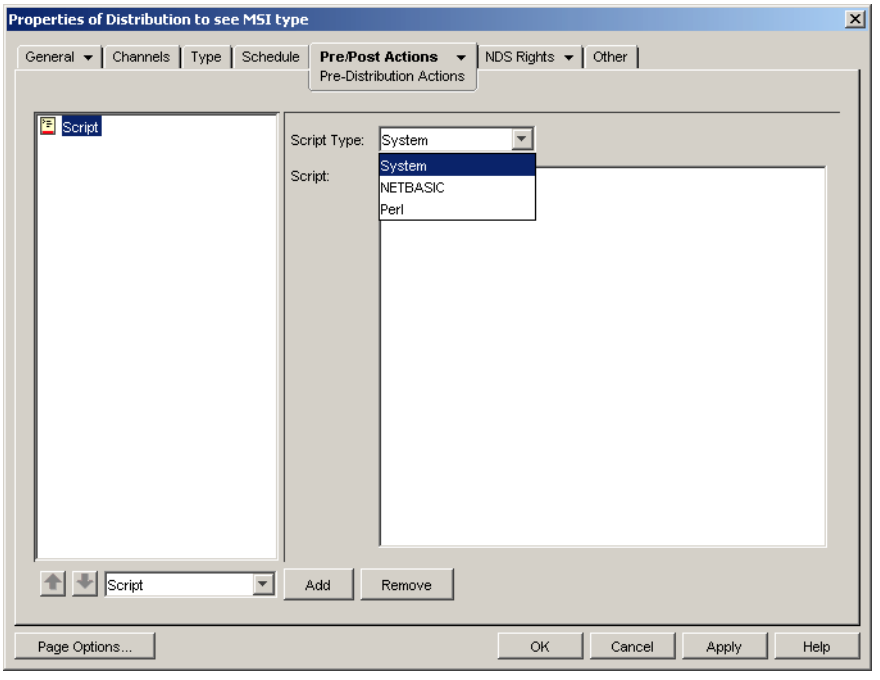
- [Service] : これは正確なサービス名である必要があります。

- **[Wait For This Service To Finish Running Before Continuing]：** サービスがそれ自体を開始または終了する場合は、このオプションを選択できます。デフォルトでは、このオプションは選択されていません。

スクリプトアクション

このアクションは、Windows サービス、Java プロセス、および NLM プロセスに使用できます。

主要な Distribution ファイルをインストールする前にサーバスクリプトを実行できます。矢印ボタンを使用して、スクリプトの実行順序を並べ替えます。



スクリプトアクションを追加するには、ドロップダウンボックスのオプションを選択し、[Add] ボタンをクリックします。デフォルト名は「Script」です。これをフルパスを含むスクリプトファイル名に変更する必要があります。（パスを指定しないと、スクリプトの実行時に認識されません。）

次のフィールドに入力します。

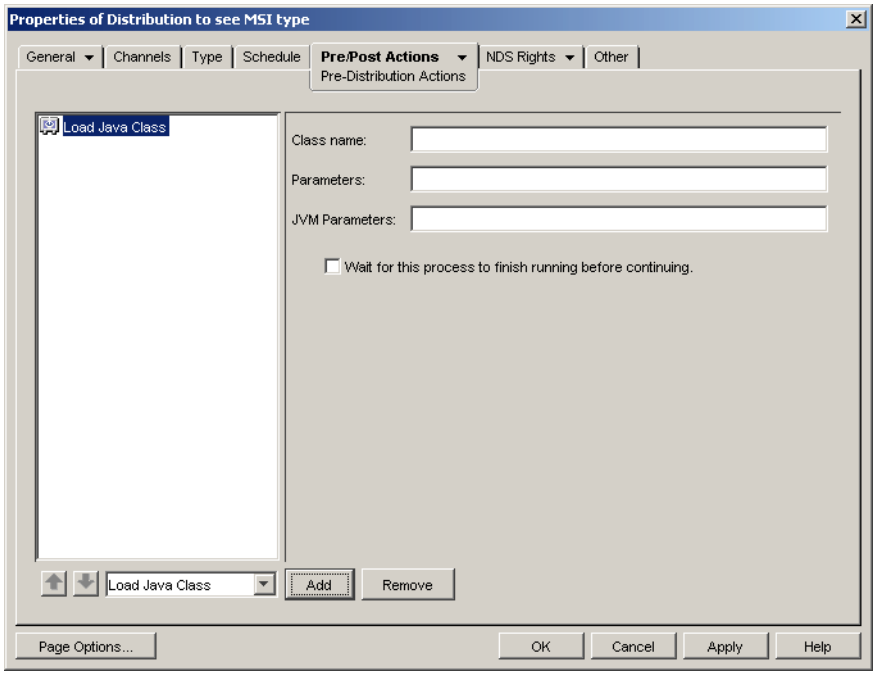
- **[Script Type]：** 使用できるスクリプトの種類は、[System]、[NetBasic]、および [PERL] の 3 つです。[Script] ボックスに入力するテキストは、選択したスクリプトの種類と一致している必要があります。

  重要： NetBasic は NetWare 6.5 サーバではサポートされていません。

- **[Script]：** スクリプトのテキストを入力します。

  警告： Distribution がスクリプトを実行する場合、このスクリプトによる処理はロールバックによって元に戻すことができません。

Java クラスロードアクション



このアクションは、NetWare にのみ使用できます。

Java クラスロードアクションを追加するには、ドロップダウンボックスのオプションを選択し、[Add] ボタンをクリックします。次のフィールドに入力します。

- **[Class Name]**：これは正確な名前である必要があります。拡張子 .class は必要ありません。

  重要：Java クラスをロードするには、Distribution を受信するサーバ上のパスに既存の java.exe または jre.exe が必要です。パスにファイルがない場合は、このフィールドを使用して、ファイルへのフルパスを入力できます。

- **[Parameters]**：Java アプリケーションの実行を開始するためのコマンドラインパラメータを含めます。
- **[JVM Parameters]**：Java 仮想コンピュータのパラメータを含めます。
- **[Wait For This Process To Finish Running Before Continuing]**：Java アプリケーションがそれ自体を終了する場合は、このオプションを選択できます。NLM やプロセスは 10 分以内に終了する必要があります。終了しない場合、ロード処理全体が失敗します。デフォルトでは、このオプションは選択されていません。

他の Distributor への Distribution の再割り当て

単一の Distributor を使って多数の Distribution を処理できます。この結果、Distributor のサーバでパフォーマンスの低下が生じることがあります。バージョン 6.5 では、Distribution を現在の Distributor から別の Distributor に割り当てることで負荷を分散できるため、Distribution を作成し直す必要はありません。

別の Distributor に割り当てるときは、1 つまたは複数の Distribution を選択できます。

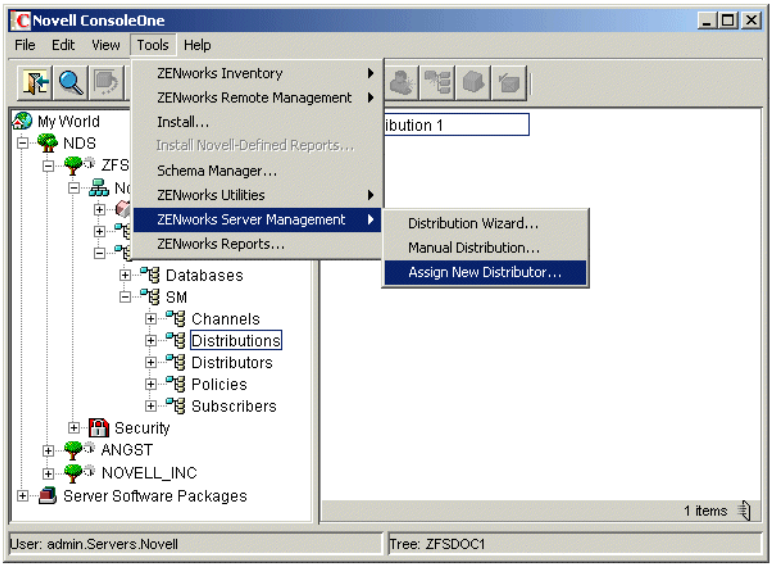
ConsoleOne で Distributor オブジェクトを削除する場合は、その Distributor オブジェクトが処理する Distribution の再割り当てが必要かどうかの確認が求められます。

Distribution を他の Distributor に割り当てるには

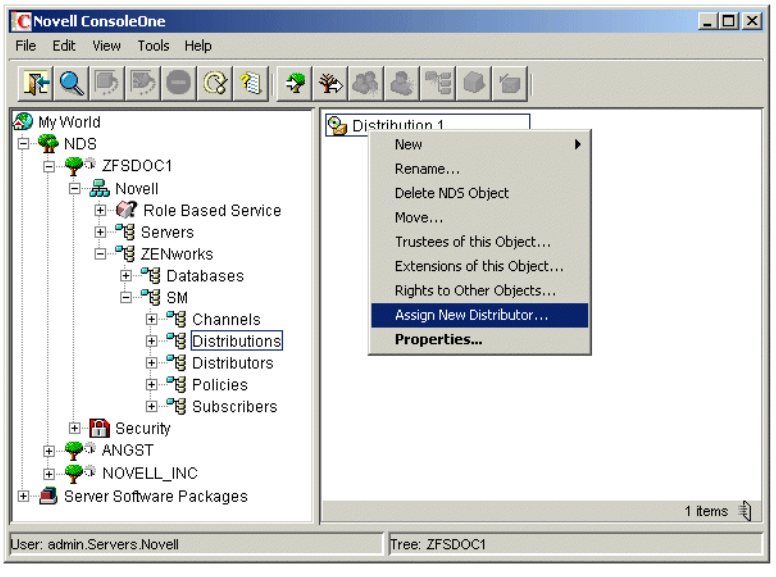
1 他の Distributor に割り当てる Distribution を決定します。

2 ConsoleOne で、次のいずれかの操作を行います。

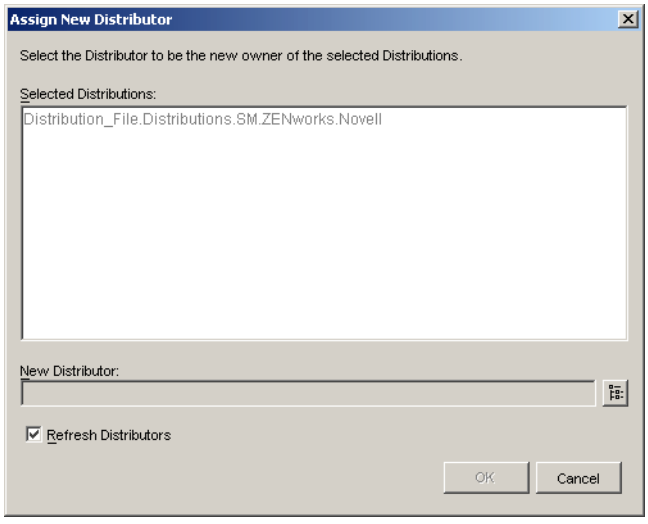
- 1 つまたは複数の Distribution オブジェクトを選択し、[Tools] > [ZENworks Server Management] > [Assign New Distributor] の順にクリックします。



- 1 つまたは複数の Distribution オブジェクトを選択し、選択したオブジェクトを右クリックして、[Assign New Distributor] をクリックします。



この方法のいずれかを実行すると、次のダイアログボックスが表示されます。



選択した Distribution が［Selected Distributions］リストに表示されます。

リストを変更する場合は、［Cancel］をクリックして Distribution オブジェクトを再度選択する必要があります。

3 ［New Distributor］フィールドで、これらの Distribution に割り当てる Distributor オブジェクトを参照します。

重要： この Distribution に属する現在の Distributor サーバ上のファイルは、同一のフルパスを使用して、新しい Distributor サーバのファイルシステムにコピーまたは移動する必要があります。これは、ステップ 7 で説明します。

4 再割り当て後、新しい Distributor による Distribution の構築がすぐに必要な場合は、［Refresh Distributors］チェックボックスを選択します。

新しい Distributor は、このプロセスの終了時（ステップ 5 を参照）に更新されるため、すぐに新しい Distribution を認識します。

重要： File、MSI、および Desktop Application タイプの Distribution などに使用するファイルをコピーする場合は、これらのファイルのコピーまたは移動が完了してから新しい Distributor を更新する必要があります。この作業は、ステップ 7 からステップ 12 で実行されます。

5 ［OK］をクリックして、Distribution オブジェクトを新しい Distributor に割り当てます。

6 Distribution が再割り当てされ、その Distribution の所有権がないことを古い Distributor が認識するようにするには、古い Distributor オブジェクトを右クリックして、［Refresh Distributor］をクリックします。

重要： ConsoleOne の再割り当てツールは、eDirectory オブジェクトのみの再割り当てを実行します。そのため、File Distribution または MSI Distribution では、これらの Distribution に含まれるファイルが古い Distributor のファイルシステムに残されます。これらのファイルは、新しい Distributor が File または MSI タイプの Distribution を構築するときにアクセスできるように、新しい Distributor のファイルシステムに移動する必要があります。これは、ステップ 7 で説明します。

Desktop Application Distribution では、アプリケーションオブジェクトを見直して、古い Distributor のファイルシステムにあるファイルのうち、新しい Distributor のファイルシステムに移動するものを決める必要があります。これは、ステップ 10 で説明します。

7 File または MSI タイプの Distribution の場合は、次の手順に従います。

7a ConsoleOne で、再割り当てが必要な Distribution の Distribution オブジェクトを右クリックし、[Properties] をクリックします。

7b [Type] タブをクリックします。

7c [Files To Be Distributed] リストで、配布されるすべてのファイルまたはディレクトリを、フルパスを含めて書き留めます。

7d Distribution オブジェクトを終了します。

8 ファイルの場所を書き留めたメモとファイル管理ソフトウェア (Windows のエクスプローラなど) を使用して、現在の Distributor サーバのファイルシステムから、Distribution を新しく割り当てた Distributor サーバのファイルシステムに Distribution のファイルをすべてコピーまたは移動します。

フルパスとファイル名は、2 つの Distributor サーバのファイルシステムで一致している必要があります。古い Distributor サーバと新しい Distributor サーバでパスが異なる場合は、新しいパスが一致するように Distribution のプロパティを編集する必要があります。

9 再割り当てが必要な Distribution ごとに、ステップ 7 とステップ 8 を繰り返します。

10 Desktop Application タイプの Distribution の場合は、次の手順に従います。

10a ConsoleOne で、再割り当てが必要な Distribution の Distribution オブジェクトを右クリックし、[Properties] をクリックします。

10b [Type] タブをクリックします。

10c Distribution に含まれるアプリケーションオブジェクトを書き留め、各アプリケーションオブジェクトの .fil ファイルを、フルパスを含めて書き留めます。

10d Distribution オブジェクトを終了します。

11 ファイルの場所を書き留めたメモとファイル管理ソフトウェア (Windows のエクスプローラなど) を使用して、現在の Distributor サーバのファイルシステムから、Distribution を新しく割り当てた Distributor サーバのファイルシステムに Distribution のアプリケーションオブジェクトファイルをすべてコピーまたは移動します。

フルパスとファイル名は、2 つの Distributor サーバのファイルシステムで一致している必要があります。古い Distributor サーバと新しい Distributor サーバでパスが異なる場合は、新しいパスが一致するようにアプリケーションオブジェクトのプロパティを編集する必要があります。

重要： 通常、この Distribution の一時ファイルは自動的にクリーンアップされますが、再割り当てされた Distribution の一時ファイルは、古い Distributor のサーバから手動でクリーンアップする必要があります。

12 再割り当てが必要な Distribution ごとに、ステップ 10 とステップ 11 を繰り返します。

13 再割り当て後の Distributor の更新を選択しなかった場合、新しい Distributor が新しい Distribution をすぐに認識するようにするには、新しい Distributor を右クリックし、[Refresh Distributor] をクリックします。

古い Distributor が、再割り当てされた Distribution を今後構築することはありません。Distribution を現在所有している Distributor が、構築スケジュールと送信スケジュールに従って Distribution を構築および送信します。

Distribution の削除

Distribution オブジェクトを削除したら、その Distribution を所有していた Distributor をすぐに更新する必要があります。更新しない場合は、次の問題が発生します。

- 構築スケジュールが開始されると、Distributor は Distribution が存在していると認識したままなので、Distribution の構築を実行し、エラーの原因となります。
- iManager で、[Distribution Information] オプションを選択して Distribution を削除しようとすると、Distributor は 601 ヌルポインタエラーを受信します。

Distributor をすぐに更新すると、次の理由によって、この 2 つのエラーが発生しないようにできます。

- Distributor は、更新時に eDirectory を読み取り、削除された Distribution を認識しなくなります。
- iManager では、削除された Distribution の [Distribution Information] オプションが使用できなくなります。

Distribution オブジェクトの削除 - 一時ファイルの自動削除

以前は、Distribution オブジェクトまたは Channel オブジェクトを削除したり、Channel から Distribution や Subscriber を削除したり、何らかの方法で 1 つまたは複数の Distribution と 1 つまたは複数の Subscriber の関連付けを解除した場合、Distribution の一時ファイルが Subscriber サーバに残されるため、こうしたファイルを検索して手動で削除し、ディスクの空き容量を増やす必要がありました。

バージョン 6.5 では、Distributor の更新時に、削除済みの Distribution の一時ファイルが Subscriber から自動的に削除され、ディスクの空き容量が増加します。

一時的な Distribution ファイルがクリーンアップされるタイミング

Distribution の一時ファイルは、次のタイミングで Subscriber サーバのファイルシステムから削除されます。

- Distribution オブジェクトが削除されたとき
- Distribution をホストしている Channel オブジェクトが削除されたとき
- Distribution が Channel から削除されたとき
- Subscriber が Channel への登録を解除されたとき

Distributor による処理の内容

Distributor は更新時に、すべてのサーバ (ルーティング階層の親 Subscriber を含む) が Distribution を今後も受信する必要があるかどうかを決定します。Distribution を必要としないサーバがある場合、Distributor は Subscriber(親 Subscriber を含む) に Distribution の一時ファイルをクリーンアップするよう通知します。

Distributor が Subscriber に接続できない場合、または削除の完了に関する応答を受信しなかった場合、Distributor は次回の更新時にその Subscriber に再度通知を送信します。つまり、更新スケジュールは、削除された Distribution の一時ファイルのクリーンアップを Subscriber に通知する頻度を決定します。

Distributor による Subscriber へのクリーンアップの通知は、成功するまで 5 回繰り返されます。成功しなかった場合、Distributor は Subscriber への通知を中止します。これ以降の Subscriber サーバの一時ファイルは、手動でのみクリーンアップできます。

Subscriber による処理の内容

Subscriber は、Distribution の一時ファイルの削除通知を受信すると、最初に、クリーンアップ対象の Distribution が Subscriber サーバによる受信、送信、または抽出の処理中かどうかを判断します。処理中でない場合、Subscriber は保留中の転送イベントまたは抽出イベントを削除し、一時ファイルを含む Distribution のディレクトリを削除します。次に、削除を実行した Subscriber を Distributor が追跡できるように、Subscriber は Distributor に削除を通知します。

Distribution ファイルのクリーンアップでは、親 Subscriber はエンドノード Subscriber と同様に処理されます。

Distributor サーバでの一時的な Distribution ファイルのクリーンアップ

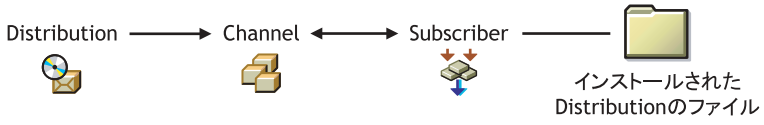
Distribution オブジェクトが eDirectory から削除されていることが Distributor によって判断されると、Distribution のバージョンディレクトリ（Distribution のディレクトリとは異なる）が Distributor の作業ディレクトリから自動的に削除されます。

Distributor は、通知したすべての Subscriber がファイルシステムから Distribution ディレクトリを削除したと判断すると、Distributor のファイルシステムから Distribution のディレクトリを削除します。

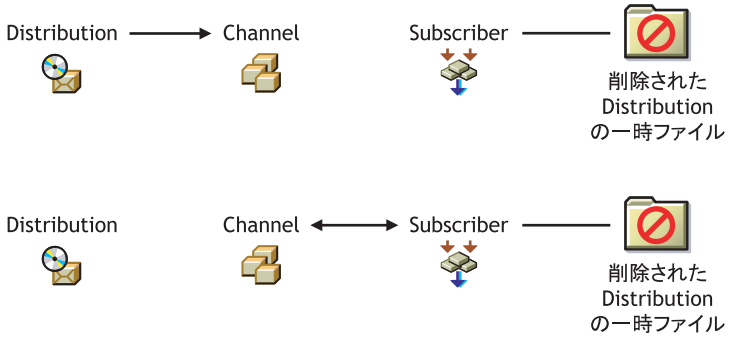
Subscriber が一時的な Distribution ファイルのクリーンアップを待つ必要がある場合

一時的な Distribution ファイルは、Distribution と Subscriber の関連付けがなくなるまで、Subscriber のファイルシステムから削除できません。たとえば、次のように入力します。

- Distribution が Channel のリストに含まれ、Subscriber がその Channel に登録されると、Distribution のファイルは Subscriber サーバで受信および抽出できます。

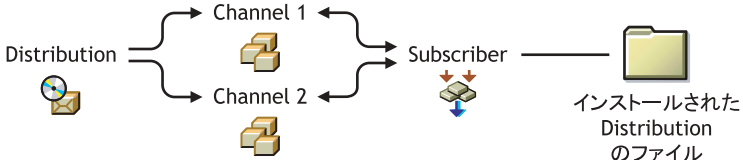


- Subscriber が Channel への登録を解除されるか、Distribution が Channel のリストから削除されると、Distribution の一時ファイルを Subscriber サーバから削除できます。

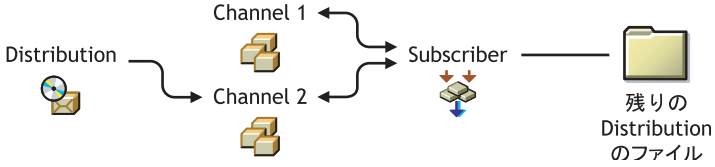


ただし、Distribution と Subscriber が複数の Channel で関連付けられている場合、Distribution の一時ファイルは、すべての Channel による Distribution オブジェクトと Subscriber オブジェクトの関連付けがなくなるまで、Subscriber のファイルシステムから削除されません。たとえば、次のように入力します。

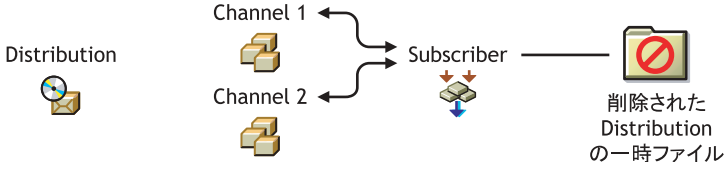
- Distribution が異なる 2 つの Channel のリストに含まれ、Subscriber が両方の Channel に登録されている場合、Distribution のファイルは Subscriber サーバで受信および抽出できます。



- Distribution がいずれかの Channel から削除されても、Distribution のファイルは Subscriber サーバで受信および抽出できます。



- Distribution が両方の Channel から削除されると、Distribution の一時ファイルは Subscriber サーバから削除できます。



親 Subscriber が一時的な Distribution ファイルを削除できる場合

次の場合に、親 Subscriber はサーバに Distribution ファイルを保存できます。

- 同じ Channel に登録された親 Subscriber とエンドノード Subscriber が、Distribution を受信するとき。親 Subscriber は、Distribution の転送と、親 Subscriber での抽出を実行します。
- エンドノード Subscriber が登録された Channel に親 Subscriber が登録されていないとき。親 Subscriber は、その Channel の Distribution を転送するだけです。

どちらの場合も、Distribution ファイルが親 Subscriber のサーバからクリーンアップされるときは、次のルールが適用されます。

- 親 Subscriber が Channel への登録を解除された場合でも、Distribution のファイルは親 Subscriber のサーバから削除されないため、親 Subscriber はこれらの Distribution をエンドノード Subscriber サーバに転送し続けることができます。
- エンドノード Subscriber が Channel への登録を解除された後にのみ、親 Subscriber は Distribution のファイルをサーバからクリーンアップできます。

孤立した Distribution の処理

次の節では、削除された Distributor オブジェクトの Distribution を処理する方法について説明します。

- 142 ページの「孤立した Distribution 」
- 142 ページの「孤立した Distribution のクリーンアップ」
- 142 ページの「削除された Distribution の再作成」

孤立した Distribution

Distribution は、それぞれの Distributor に排他的に属しているため、Distributor オブジェクトを eDirectory から削除すると、これらの Distribution は構築および送信できなくなります。削除された Distributor に関連付けられている Distribution は孤立し、使用することができません。

孤立した Distribution が Distributor オブジェクトの削除前に送信および抽出されていた場合、抽出された Subscriber サーバでは使用できます。ただし、これらのサーバは、孤立した Distribution の更新バージョンを受信できなくなります。

孤立した Distribution オブジェクトは、eDirectory では参照できますが、現在の Distributor オブジェクトまたは今後作成される Distributor オブジェクトに関連付けることはできません。

孤立した Distribution のクリーンアップ

Distribution のタイプに関係なく、Subscriber サーバのファイルシステム上にある孤立したすべての Distribution のディレクトリを削除できます。Distribution を再作成する場合は、Distribution のディレクトリを削除することをお勧めします。

Distribution の多くのタイプでは、孤立した Distribution のディレクトリを削除するだけで、管理やディスク容量の節約を目的としたクリーンアップを実行できます。このような Distribution タイプを次に示します。

Desktop Application
File
FTP
HTTP
RPM

ただし、Policy Package タイプと Software Package タイプでは、Distribution が抽出およびインストールされたときに起動されたプロセスを取り消す必要があります。

たとえば、Policy Package Distribution では、Distribution によってサーバに設定されたポリシーを iManager を使用して削除する必要があります。詳細については、82 ページの「Policy/Package Agent の管理」のステップ 4 を参照してください。

削除された Distribution の再作成

孤立した Distribution の使用を継続する場合は、Distribution ごとに再作成する必要があります。既存の Distributor オブジェクトを使用した再作成も可能ですが、新しい Distributor のインストール後に再作成を実行することもできます。

Distribution を再作成した場合は、孤立した Distribution に関連付けられていたすべての Channel を新しく作成した Distribution に関連付ける必要があります。

Distribution を再作成するときは、孤立した Distribution オブジェクトの設定情報を使用できます。孤立した Distribution オブジェクトは、必要なくなったときに削除できます。削除すると、Channel オブジェクトの［Distributions］タブに表示されなくなります。

手動による Distribution のインポートとエクスポート

エクスポートとインポートは、次の場合に便利です。

- Distributor サーバから低速な WAN リンクで接続された Subscriber サーバに大きな Distribution を送信する。
- 低速な WAN リンクで接続された親 Subscriber サーバに大きな Distribution を送信して、WAN 側の下位の Subscriber に Distribution を渡す。
- Distribution をアーカイブして、必要なときに必要な場所にインポートする。

次の節では、Distribution のエクスポートとインポートについて説明します。

- 143 ページの「エクスポートおよびインポートのプロセスの理解」
- 144 ページの「特別なスケジュールの設定」
- 144 ページの「Distribution のエクスポート」
- 144 ページの「Distribution のインポート」

エクスポートおよびインポートのプロセスの理解

Distributor サーバから Distribution を手動でエクスポートするには、フロッピーディスク、ZIP ディスク、CD、DVD などのメディアソースに書き込み、そのメディアから Subscriber サーバにインポートします。

エクスポートプロセスは、Distribution 情報をハードドライブ、フロッピーディスク、ZIP ディスクなどの UNC パスまたはドライブマッピングにコピーします。ハードドライブ上のコピーから、情報を CD または DVD に焼き付けることができます。

Distribution 情報には、eDirectory オブジェクトからの Channel および Distribution データ、および Distribution のファイルの内容（すべてのデルタを含む）が含まれます。Distribution 情報は、手動配布ウィザードを実行したときに名前を付けた *filename*.ted ファイルにコピーされます。ファイル名には .ted 拡張子を付ける必要があります。また、メディアの内容を確認するときに Distribution を認識できるように、わかりやすいファイル名を使用してください。

エクスポートした .ted ファイルをインポートする場合、eDirectory オブジェクト情報と Distribution の内容を使用して、Subscriber サーバのファイルシステム上に Distribution が作成されます。その後、Distribution のデルタをネットワークで送信できます。これは通常、Distribution のデルタは、エクスポートおよびインポートされたオリジナルの Distribution よりも小さいためです。

Distribution をエクスポートまたはインポートできるのは、関連する Channel がすべての Distributor と Subscriber に認識されている同じツリー内のみです。

特別なスケジュールの設定

インポートされた Distribution をいつ抽出するかによって、Distribution をエクスポートする前に、異なるスケジュールのセットの設定が必要になる場合があります。

たとえば、エクスポートした Distribution を、インポート先の別の Subscriber によって異なるタイミングで抽出する場合、次のようにします。

1 エクスポートされる Distribution の構築スケジュールを［Immediate］に設定します。

2 送信スケジュールを［Never］に設定して、Distribution を Channel に追加します。

これにより、Distribution を手動でインポートしていない Subscriber が、まだ受信されていない Distribution の抽出を開始する Channel の通知を受信するのを防ぐことができます。

3 Distribution がインポートされるすべての Subscriber を、ステップ 2 で使用した Channel に追加します。

4 エクスポートされる Distribution を所有する Distributor を更新します。

5 Distribution が構築されたら、144 ページの「Distribution のエクスポート」に進みます。

特別なスケジュールが不要な場合は、次の 2 つの節の説明に従ってください。これらの節では、既存のスケジュールを使用することを前提とします。

Distribution のエクスポート

1 ConsoleOne で［Tools］をクリックし、［Manual Distribution］をクリックして、手動配布ウィザードを起動します。

2 ［Export］をクリックし、［Next］をクリックします。

3 Channel を選択し、その Channel の Distribution を選択して、［Next］をクリックします。

この Channel の ID は、Distribution をインポートするときに使用するために .ted ファイルに保持されます。

4 Distribution の場合、パス（UNC またはドライブマッピング）とファイル名（メディア上にある Distribution を識別するためにわかりやすい名前）を指定して、［Next］をクリックします。

ファイル名は拡張子として .ted を含める必要があります。

5 この概要で問題がなければ［Finish］をクリックします。

指定したパスに完全な Distribution が、.ted ファイルとして保存されます。

6 パスをハードドライブに指定した場合、.ted ファイルを CD または DVD に焼き付けることができます。

Distribution のインポート

1 ConsoleOne で［Tools］をクリックし、［Manual Distribution］をクリックして、手動配布ウィザードを起動します。

2 ［Import］をクリックして、［Next］をクリックします。

3 .ted ファイルのパスとファイル名を入力して、［Next］をクリックします。

これは、メディアソースにエクスポートした .ted ファイルです。

4 上部のボックスで親 Subscriber を選択し、下部のボックスで個々の Subscriber を選択して、[Next] をクリックします。

ルーティング階層にある親 Subscriber を選択すると、階層内でその下にあるすべての Subscriber に、インポートされた Distribution が渡されます。ただし、これは Subscriber が Distribution の Channel にすでに登録されている場合のみです。

下部のボックスに表示されるのは、現在 Distribution の Channel に登録されている Subscriber です。見出しには、インポートされる Distribution に関連付けられた Channel が表示されます。この情報は、インポートされる .ted ファイルに含まれます。

External Subscriber は、手動では Distribution を受信できないため、下部のボックスには表示されません。

5 この概要で問題がなければ [Finish] をクリックします。

Distribution が指定したメディアソースからコピーされ、選択した Subscriber の作業ディレクトリに配置されます。Channel オブジェクトと Distribution オブジェクトの情報は、eDirectory に書き込まれます。

この時点で、インポートされた Distribution は、[Tiered Distribution] ビューまたは [Subscriber Distribution] ビューではなく、iManager の [Remote Web Console] に表示されます。次の 2 つの手順でこれを処理します。

6 インポートされた Distribution に特別なスケジュールを設定した場合は (144 ページの「特別なスケジュールの設定」を参照)、インポート先の各 Subscriber サーバで Server Management プロセスを再起動します。それ以外の場合は、ステップ 7 に進みます。

Subscriber の個別の抽出スケジュールに基づいて Subscriber サーバで Distribution が抽出されます。抽出後、Distribution の情報を iManager で表示できます。

7 Subscriber が新しい Distribution を手動で受信したことを Distributor に認識させるには

7a iManager の ZENworks Server Management の役割で、[Remote Web Console] をクリックします。

7b 次のフィールドのいずれかに、インポートされた Distribution を所有する Distributor を指定します。

[IP Address or DNS Name]

[Distributor, Subscriber, or Server Object Name]

7c [OK] をクリックします。

7d [Display] フィールドで、[Tiered Electronic Distribution] を選択します。

7e [Channels] タブをクリックして、[Distribute Channel] を選択します。

7f インポートされた Distribution に関連付けられた Channel をクリックして、[OK] をクリックします。

Distributor は、Channel に表示された Distribution の Subscriber への送信を開始しますが、Subscriber はすでに Distribution があるという応答をして、インポートされた Distribution の抽出を開始します。

Subscriber が、インポートされた Distribution を下位の Subscriber に渡す必要がある親 Subscriber の場合、Distribution の Channel が開始したときに渡されます。

Distribution ウィザードの使用

Server Management には、Distribution の作成と送信に関するプロセスの理解に役立つ Distribution ウィザードが用意されています。このウィザードを使用すると、File Distribution または FTP Distribution を作成および送信できます。

Distribution ウィザードを使用するには

1 ConsoleOne で、Distribution オブジェクトを作成するコンテナを選択し、[Tools] をクリックして、[Distribution Wizard] を選択します。

2 [Introduction] ページの情報を確認し、[Next] をクリックします。

3 [Distributor Selection] ページで、File Distribution または FTP Distribution を所有する Distributor を参照して選択し、[Next] をクリックします。

4 [Subscriber Selection] ページで [Add] をクリックし、この Distribution を受信する Subscriber を参照して [Select] をクリックし、[OK] > [Next] の順にクリックします。

5 [File Source] ページで、ファイルソース (Distributor のファイルシステムまたはリモート FTP サイト) を選択し、[Next] をクリックします。

6 [Destination Volume or Drive] ページでオプションを選択し、フィールドに情報を入力して、[Next] をクリックします。

[Use the Same Volume or Drive for All Subscribers]: 各ターゲット Subscriber で同じボリュームまたはドライブを利用できる場合は、このオプションを選択し、ボリュームラベルまたはドライブ文字を指定します。

[Use a Variable for the Volume or Drive] : ターゲット Subscriber が異なるパスを使用している場合 (たとえば、NetWare、Windows、Linux、および Solaris の Subscriber サーバなど)、変数値を指定できます。Distribution を受信するには、この値を各 Subscriber で定義する必要があります。

7 [Additional Destination Directories] ページで、ターゲット Subscriber サーバのパス情報を追加し、[Next] をクリックします。

パス情報は、入力すると [Data Will Be Placed In Path] の見出しの下に表示されます。操作を続行する前に、この情報を参照してパスが有効であることを確認してください。

8 [File Selection From Distributor Server] ページで [Add] をクリックし、Distribution に含めるファイルまたはディレクトリを参照して [Select] をクリックします。次に、[OK] > [Next] の順にクリックします。

ローカルコンピュータのファイルシステムではなく、Distributor のファイルシステムを参照します。

Distribution に含めるすべてのファイルおよびディレクトリを指定するまで、[Add] のクリックを繰り返します。

9 [Distribution Name and Context] ページで、フィールドに情報を入力し、[Next] をクリックします。

[Distribution Name] : Distribution に固有の名前を指定します。

[Context] : Distribution オブジェクトを作成するコンテナを参照して、選択します。

10 [Additional Options] ページで、必要に応じてオプションを選択または選択解除し、[Next] をクリックします。

デフォルトでは、次のオプションはすべて選択されています。

[Copy the Distributor's Security Certificate To All Subscribers] : これは、Subscriber がこの Distribution を受信して抽出する場合に必要です。同じ Distributor と Subscriber で再度ウィザードを実行する場合は、このオプションを選択する必要はありません。

[Verify That All Subscribers Are Up and Running] : ターゲット Subscriber がこの Distribution を受信できることを確認する場合は、このオプションを選択します。

[Notify the Distributor To Read eDirectory For New Information] : Distribution がすぐに構築されます。

11 [Summary] ページで、Distribution ウィザードで実行した手順を確認し、[Finish] をクリックして Distribution を作成します。

Distribution が作成および送信されると、情報が表示されます。

12 ログファイルを確認するには、メッセージに対して [Yes] をクリックします。

[Yes] を選択すると、ログファイルを確認できます。[Close] をクリックして、ログウィンドウと Distribution ウィザードを終了します。

[No] を選択すると、Distribution ウィザードが終了します。

Channels

次の節では、Channel オブジェクトの概念と使用方法について説明します。

- 147 ページの「Channel の理解」
- 148 ページの「Channel の作成と設定」
- 150 ページの「Channel からの強制送信」

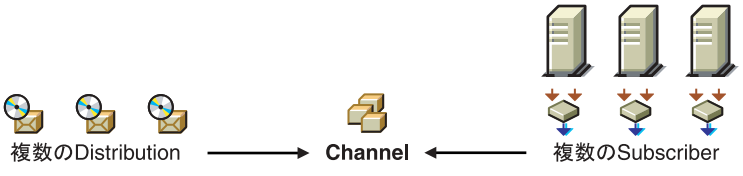
Channel の理解

Channel オブジェクト (TED Channel) には、Channel に関連付けられた Distribution と Channel に登録された Subscriber のリストが含まれます。

- 147 ページの「他のTiered Electronic Distributionオブジェクトとの機能的関係」
- 148 ページの「Channel の説明」
- 148 ページの「スケジュール設定」
- 148 ページの「Channel への登録」

他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、Channel、Distribution、および Subscriber の関係を示しています。



Distribution は Channel のリストに含まれ、Subscriber は Channel に登録されます。

Channel の説明

Distributor は、1 つの Distribution を複数の Channel のリストに含めることができます。複数の Distributor は、同じ Channel のリストに Distribution を含めることができます。

必要な数の Channel を使用できます。Channel には、実際の Distribution は格納されず、Distribution へのリファレンスのみが含まれます。Channel が送信できる Distribution のリファレンス数に制限はありません。実際には、Channel ごとに追跡する Distribution の数によって制限されます。

スケジュール設定

Channel の送信スケジュールは、Distribution が Distributor から Subscriber に送信されるタイミングを決定します。

Channel をアクティブまたは非アクティブにすることで、Distribution が送信されるタイミングを制御できます。

Channel と、関連付けられた Distributor および Subscriber との間のスケジュール設定に影響するタイムゾーンについては、348 ページの「タイムゾーンが異なる Tiered Electronic Distribution オブジェクトのスケジュール設定」を参照してください。

Channel への登録

Channel には、複数の Subscriber を登録できます。

Distribution を受信するには、その Distribution を含む Channel に Subscriber を登録する必要があります。ただし、Subscriber は Channel のリストに含まれる Distribution をすべて受信します。つまり、すべての Distribution が抽出され、Subscriber サーバに適用されます。

Channel の作成と設定

次の節では、ConsoleOne で Tiered Electronic Distribution オブジェクトを作成および設定する手順について説明します。

Distributor ごとに次の順序で実行します。

- 148 ページの「Channel 名の決定」
- 149 ページの「Channel オブジェクトの作成」
- 149 ページの「Channel の設定」

Channel 名の決定

Channel に名前を付けるときは、わかりやすい名前を使用してください。たとえば、次のように入力します。

```
VirusProtect
VProtectPatterns
VirusProtection
NW51patch4
NW6patch1
AUTOEXECNCF000326
```

次のように名前を決めると、Channel をより簡単に管理できます。

- 目的に合った名前を使用する
- Channel と Distribution に類似した名前を使用する

149 ページの「Channel オブジェクトの作成」に進みます。

Channel オブジェクトの作成

Channel を使用して、Distribution をグループ化し、Channel に登録された Subscriber に Distributor の Distribution を渡すスケジュールを作成します。Channel は、多くの Distributor の Distribution を処理できます。1 つの Channel に複数の Subscriber を登録できます。

Channel オブジェクトを作成するには

1. ConsoleOne で、Channel オブジェクトを格納するコンテナオブジェクトを選択し、[File] > [New] > [Object] の順にクリックして、[TED Channel] を選択します。
2. Channel オブジェクトの名前を指定して、[OK] をクリックします。
3. Distribution をタイプ別または送信スケジュール別にグループ化するのに必要な数の Channel オブジェクトを作成します。
4. 149 ページの「Channel の設定」に進みます。

Channel の設定

Channel オブジェクトは、使用前に設定する必要があります。

Channel オブジェクトに関連付けられているプロパティは、すべてが必要になるとは限りません。必要なプロパティを次に説明します。それ以外はすべてオプションです。

Channel オブジェクトを設定するには

1. ConsoleOne で Channel オブジェクトを右クリックし、[Properties] をクリックします。
2. [General] タブを選択し、次のフィールドに入力します。

   [Active]： チェックボックスを選択すると、Channel による Distribution の送信が有効になります。

   [Description]： Channel が関連付けられている Distribution の説明など、わかりやすい説明を入力します。
3. [Distributions] タブを選択し、[Add] をクリックして Distribution を追加します。

   [Distributions]： この Channel に関連付けられている Distribution のリストです。Distribution パッケージの作成については、112 ページの「Distribution」を参照してください。
4. [Subscribers] タブを選択し、[Add] をクリックして Channel に Subscriber を追加します。

   [Subscribers Subscribed to This Channel]： この Channel に登録された Subscriber と External Subscriber のリストです。
5. [Schedule] タブを選択し、Channel の Distribution を配布するスケジュールを選択します。

   利用可能なスケジュールについては、8 章 331 ページの「スケジュール設定」を参照してください。

Channel からの強制送信

Channel の通常の送信スケジュールとは別に、Channel の Distribution をすべて送信する場合は、手動で強制的に配布プロセスを起動できます。

新しい Distribution を構築し、Channel の送信スケジュールがまだ開始されない場合は、次のいずれかの方法で Channel での送信を強制的に実行します。

- iManager で ZENworks Server Management の役割を使用して、[Edit TED Object] をクリックし、Channel を参照して選択します。次に [OK] > [Distribute Channel] の順にクリックします。
- ConsoleOne では、次の手順に従います。

  1. Channel オブジェクトを選択し、[Properties] をクリックして [Schedule] タブを選択します。[Run Immediately] > [OK] の順にクリックし、Distributor オブジェクトを右クリックして、[Refresh Distributor] をクリックします。

  2. Distribution が送信されたら、手順 1 での変更を元に戻します。Channel オブジェクトを選択し、[Properties] をクリックして [Schedule] タブを選択します。最初に設定されていた Channel のスケジュールを選択し、[OK] をクリックします。

Subscriber は Distribution 全体を受信するとすぐに、Subscriber の抽出スケジュールに従って抽出します。

Subscriber

次の節では、Subscriber オブジェクトの概念と使用方法について説明します。

- 150 ページの「Subscriber の理解」
- 152 ページの「Subscriber の作成」
- 153 ページの「Subscriber の設定」
- 156 ページの「Subscriber 設定の更新」
- 157 ページの「Subscriber と Channel の関連付け」
- 158 ページの「Distributor のルーティング階層に属する Subscriber オブジェクトの削除」

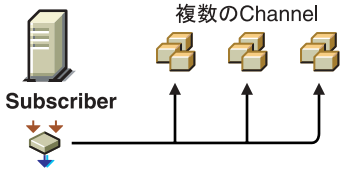
Subscriber の理解

Subscriber オブジェクト (TED Subscriber) は、Subscriber のプロパティを定義する eDirectory オブジェクトです。

- 151 ページの「他のTiered Electronic Distributionオブジェクトとの機能的関係」
- 151 ページの「Subscriber の説明」
- 151 ページの「スケジュール設定」
- 151 ページの「Channel への登録」
- 152 ページの「親 Subscriber 」

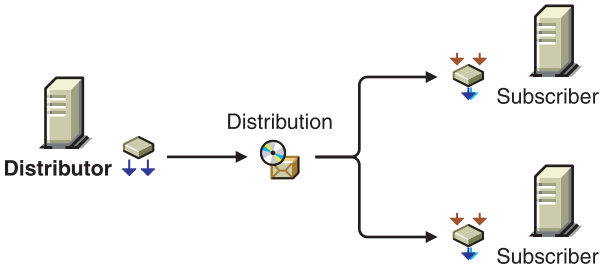
他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、Subscriber と Channel の関係を示しています。



Subscriber は Channel に登録されます。

次の図は、Subscriber、Distributor、および Distribution の関係を示しています。



Subscriber の説明

Subscriber は、Distribution を受信して抽出し、必要なソフトウェア、ファイル、またはポリシーを取得するサービスです。

アプリケーション、ファイル、またはポリシーパッケージを配布するサーバには、Subscriber ソフトウェアをインストールして、eDirectory ツリーに Subscriber オブジェクトを配置する必要があります。Subscriber サーバへの Distribution ファイルの移動には IP アドレスまたは DNS 名が使用されるため、Subscriber オブジェクトはサーバの NCP™ サーバオブジェクトとは異なるツリーにあります。

Distribution は、Subscriber サーバのハードドライブにコピーされます。Subscriber は Distribution を受信して抽出し、ソフトウェア、ファイルまたはポリシーをインストールします。

スケジュール設定

Subscriber の抽出スケジュールは、Subscriber が Distribution を抽出するタイミングを決定します。

スケジュール設定については、8 章 331 ページの「スケジュール設定」を参照してください。

Channel への登録

Subscriber は、Channel に登録すると、Channel のリストに含まれるすべての Distribution を受信できます。Subscriber オブジェクトのプロパティには、Subscriber が登録された Channel が一覧表示されます。

Subscriber は、次の理由によって複数の Distributor から Distribution を受信できます。

- 複数の Distributor は、同じ Channel のリストに Distribution を追加できます。
- Subscriber は、複数の Channel に登録できます。

親 Subscriber

Subscriber は、Distributor のプロキシである親 Subscriber として、他の Subscriber に Distribution を渡すことができます。これにより、Distributor が多くの Subscriber に Distribution を送信する場合に負荷を分散できます。

Subscriber オブジェクトのプロパティには、受信するすべての Distribution に使用される親 Subscriber が一覧表示されます。Subscriber が親 Subscriber を使用せず、Distributor のルーティング階層に表示されない場合、Subscriber は Distributor から直接 Distribution を受信できます。

親 Subscriber を WAN リンクのブリッジに使用すると、WAN リンク経由の Distribution パッケージの送信を最低回数で実現できます。

特殊文字の処理

サポートするプラットフォーム間における構文の違い（特定のプラットフォームでは無効になる文字など）を処理できるようになりました。Distributor サーバのプラットフォームにかかわらず、エージェントは無効な文字について、すべてのファイルを適切に収集します。Subscriber サーバは、Distribution パッケージ内のファイルに無効な文字が含まれているかどうかを検出し、抽出時にこれらのファイルを無視するかスキップします。スキップされたファイルはログに記録されます。これまでは Distribution 全体を抽出することができず、したがってこうした Distribution はインストールできませんでした。

NetWare および Windows では認識されない文字を、Linux および Solaris でファイル名およびディレクトリ名として使用することができます。

Subscriber の作成

Subscriber は、*ZENworks 6.5 Server Management Program* CD を使用して、ソフトウェアと eDirectory オブジェクトをインストールすると作成されます。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」を参照してください。

Subscriber オブジェクトを誤って削除した場合は、ConsoleOne で再作成できます。ただし、新しい Subscriber オブジェクトのリビジョン番号は、ted.cfg ファイル内のリビジョン番号より小さくなります。リビジョン番号が小さいと、設定データが現在のものより古いと見なされるため、Subscriber は設定に対する更新を取得できません。この問題を解決するには、Subscriber サーバの ted.cfg ファイルを削除します。Distribution が次に Subscriber に送信されるときに、新しい設定が取得され、新しい ted.cfg ファイルが作成されます。

Subscriber の設定

Subscriber オブジェクトは、Subscriber ソフトウェアをサーバにインストールすると自動的に作成されます。

Subscriber オブジェクトに関連付けられているプロパティは、すべてが必要になるとは限りません。必要なプロパティを次に説明します。それ以外はすべてオプションです。

Subscriber オブジェクトのプロパティを設定するには

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [General] > [Settings] の順にクリックし、次のフィールドに入力します。

[Use Policy]：Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Subscriber サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。

このオプションを選択すると、残りのフィールドが淡色表示され、このポリシー設定が使用されます。現在のポリシーは括弧内に表示されます。

[Input Rate]：Distribution の受信レートです。デフォルト値は、その接続で処理可能な最大値です。このレートは、狭い帯域幅のリンクを使用する Subscriber サーバを制御するために使用します。

[Output Rates Based Upon Distribution's Priority]：デフォルトの出力レートを設定して、Tiered Electronic Distribution オブジェクトのネットワークトラフィックを最小限に抑えます。これにより、親 Subscriber から下位 Subscriber への送信レートが決まります。デフォルト値は接続で処理できる最大値です。空白は、サードパーティアプリケーションから帯域幅が割り当てられることを意味します。

出力には 3 つの優先度があり、速度を指定できます。

- **[High Priority]**：この Distribution は、[Medium Priority] または [Low Priority] の Distribution よりも前に送信されます。
- **[Medium Priority]**：この Distribution は、[High Priority] の Distribution がすべて送信された後、[Low Priority] の Distribution よりも前に送信されます。
- **[Low Priority]**：この Distribution は、[High Priority] と [Medium Priority] のすべての Distribution が送信された後で送信されます。

詳細については、128 ページの「Distribution の優先度」を参照してください。

[Maximum Concurrent Distributions to Send]：Distribution の送信時に同時に実行できる配布スレッドの最大数を指定します。デフォルト値は指定されていません（空フィールド）。

これは、下位の Subscriber に Distribution を送信する親 Subscriber にのみ適用されます。

[Connection Time-out]：Subscriber が接続を終了する前に Distributor（受信）からまたは Subscriber（送信）からの応答を待つ秒数を指定します。送信または受信中に接続が終了した場合、次に Channel スケジュールが開始されるまで送信は開始されません。送信が開始されると、中断した時点からの処理が継続されます。

デフォルト値は 300 秒（5 分）です。有効な値は 1 ～ 60,000（秒）です。あるノードから他のノードへの応答を待つのに適当な時間を設定する必要があります。

遅延が大きくなることが多い低速またはビジー状態のリンクでは、この値を大きくする必要があります。

[Working Directory]：Distribution によって使用されるディレクトリを指定します。このディレクトリには、Distribution、永続ステータス、および一時作業ファイルが格納されます。デフォルトパスは次のとおりです。

- **[NetWare]**：sys:¥zenworks¥pds¥ted¥sub

  重要：デフォルトボリュームは、NetWare サーバの sys: です。ログファイルは非常に大きくなる可能性があるため、sys: ボリュームを使用しないことをお勧めします。

- **[Windows]**：c:¥zenworks¥pds¥ted¥sub
- **Linux または Solaris:** /var/opt/zenworks/zfs/pds/ted/sub

作業ディレクトリの詳細については、190 ページの「作業ディレクトリ」を参照してください。

[Parent Subscriber（省略可能）]：受信する Distribution の送信元となる親 Subscriber を指定します。

このフィールドでは、Distributor から Subscriber に効率的な配布を実行できます。Distributor オブジェクトのプロパティのルーティング情報は、親 Subscriber（階層配布モデル）のみを考慮します。エンドノード Subscriber（ツリー内のほとんどの Subscriber）は、リスト内には表示されません。

このフィールドを使用すると、Distributor から直接ではなく、特定の親 Subscriber を経由して Distribution を受信するようにエンドノード Subscriber ごとに指定できます。これにより、Distributor サーバの負荷が軽減し、階層配布モデルに Distribution を効率的に送信できます。

このフィールドは、親 Subscriber が別のツリーにある External Subscriber のサーバに Distribution を送信できるようにする場合にも便利です。

[Disk Space Desired To Be Left Free]：Distribution の受信に必要なディスク空き容量を確保するには、この値を使用します。ここで設定したディスク容量が不十分である場合は、Subscriber は Distribution を受信しません。

3 [General] > [Messaging] の順にクリックし、次のフィールドに入力します。

重要：この Subscriber が Distributor と同じサーバにある場合は、これらのフィールドに入力する必要はありません。Distributor のメッセージ設定だけが使用されます。

[Use Policy]：Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Subscriber サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。

このオプションを選択すると、残りのフィールドが淡色表示され、メッセージングのポリシー設定が使用されます。現在のポリシーは括弧内に表示されます。

[Server Console]：サーバコンソールで Subscriber コンソールに送信する出力メッセージのレベルを指定します。

[SNMP Trap]：SNMP を経由して送信するメッセージのレベルを指定します。

[Log File]：ログファイルに送信するメッセージのレベルを指定します。

[Path and Filename]：この Subscriber オブジェクトのカスタムログファイルの名前と場所を指定できます。デフォルトは次のとおりです。

- **[NetWare]**：sys:¥zenworks¥pds¥ted¥dist¥ted.log

重要： デフォルトボリュームは、NetWare サーバの sys: です。ログファイルは非常に大きくなる可能性があるため、sys: ボリュームを使用しないことをお勧めします。

- **[Windows]：** c:¥zenworks¥pds¥ted¥dist¥ted.log
- **Linux または Solaris:** /var/opt/zenworks/zfs/pds/ted/dist/ted.log

これは Distributor が使用するのと同じログファイルです。

[Delete Log Entries Older Than __ Days]：Subscriber のログファイルエントリは、指定した日数が経過すると削除されます。デフォルト値は 6 日です。

[E-Mail]： 電子メールで送信されるメッセージのレベルを指定します。

[Users]： 通知する電子メールユーザを指定します。

[Address Attribute]： 通知する電子メールアドレスを指定します。

eDirectory に保存されているユーザまたはグループを追加できます。eDirectory に含まれないユーザの電子メールアドレスを指定することもできます。デフォルトの属性は、eDirectory ユーザに関連付けられている電子メールアドレス属性です。

重要： 通知を受信する方法に電子メールを選択した場合は、ネットワークトラフィックが増加する可能性があることに注意してください。

4 [General] > [Working Context] の順にクリックして、作業コンテキストを参照します。

これは、Subscriber が受信する Desktop Application Distribution に関連したオブジェクトを作成する eDirectory コンテキストです。

5 [Schedules] タブを選択してスケジュールを選択し、次のフィールドに情報を入力します。

[Use Policy]： Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Subscriber サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。このオプションを選択すると、残りのフィールドが淡色表示され、スケジュール設定のポリシー設定が使用されます。

[Schedule Type]： このスケジュールは、Subscriber が Distribution を抽出するタイミングを決定します。

利用可能なスケジュールについては、8 章 331 ページの「スケジュール設定」を参照してください。

6 [Channels] タブを選択し、次のフィールドに入力します。

- **[Channels This Subscriber Is Subscribed To]**

  Subscriber が登録された Channel が表示されます。

  [Active]： この Subscriber サーバが Channel の Distribution を受信できるように Channel を有効にするには、Channel をクリックして、チェックボックスを選択します。Subscriber が Channel の Distribution を受信しないように Channel を無効にするには、チェックボックスの選択を解除します。

  [Channel]： Channel を作成するには、[Add] をクリックします。Channel を編集するには、[Details] をクリックします。

- **[Channels Subscribed to Through Subscriber Group Memberships]**

  Subscriber が属する Subscriber Group と、Subscriber Group のメンバーシップによって Subscriber が登録された Channel が表示されます。

これらの列は表示専用です。[Details]、[Add]、および [Delete] ボタンは使用できません。

[Active]： 登録された Channel が有効になっているかどうかが表示されます。

[Channel]： グループのメンバーシップによって登録された Channel が表示されます。

[Subscriber Groups]： Subscriber が属するグループが表示されます。列見出しをクリックすると、ソートできます。

7 [Variables] タブを選択し、次のフィールドに入力します。

[Include Policy]： Tiered Electronic Distribution ポリシーで設定した値を使用する場合は、このフィールドを選択して有効なポリシーを使用します。このフィールドは、Tiered Electronic Distribution ポリシーの作成後に、Subscriber サーバへの配布、Policy/Package Agent による抽出を経て、サーバで実行されている場合に表示されます。

このオプションを選択すると、Tiered Electronic Distribution ポリシーで指定した変数が変数リストに追加されます。ただし、変数が重複する場合は Subscriber の変数が優先されます。

[Variable]： 変数の名前です。変数の使用方法を示す名前にしてください。たとえば、WORKINGVOL などです。

値： この変数が指定されている場合に、Subscriber が使用する値です。たとえば、data: と指定します。

抽出が確実に行われるようにするには、Subscriber への絶対パスを指定します。たとえば、パスが data: ボリュームだけである場合でも、コロン (:) が含まれていることを確認します。コロンがフルパスに必要な部分であるからです。

[Description]： 変数の使用方法の説明です。たとえば、次のように入力します。

```
Volume for the working directory.
```

変数については、363 ページの「変数を使用したファイルの抽出の制御」を参照してください。

8 この Subscriber をグループに含めるには、[Group Membership] > [Add] の順にクリックし、Subscriber Group オブジェクトを参照して、[Select] > [OK] の順にクリックします。

9 Subscriber オブジェクトの設定が終了したら、[OK] をクリックして、Subscriber オブジェクトのプロパティを終了します。

Subscriber 設定の更新

Subscriber が、作業ディレクトリの場所などの Tiered Electronic Distribution 設定を認識していない場合は、サーバで Subscriber ソフトウェアを実行できません。そのため、インストール処理中に、インストールする各 Subscriber で Tiered Electronic Distribution の基本設定を決定します。

インストールプログラムは、この入力を使用して、Tiered Electronic Distribution 初期設定を含む tednode.properties ファイルを各 Subscriber サーバに作成します。サーバが最初の Distribution を受信するまでは、この tednode.properties ファイルが Tiered Electronic Distribution 設定情報をサーバに提供するため、このファイルは Subscriber として機能します。

Subscriber サーバは、このサーバの Subscriber オブジェクトと同じツリーに属する Distributor オブジェクトの Distributor サーバからのみ設定情報を受信できます。これは信頼されるツリーと呼ばれ、インストール処理中に構築されます。信頼されるツリーが必要な場合については、163 ページの「Subscriber ソフトウェアの設定と信頼されるツリー」を参照してください。

Distributor サーバが Subscriber サーバに Distribution を送信するとき、Distributor は、Subscriber サーバが現在の Tiered Electronic Distribution 設定を tcpip.nlm 形式で所有しているかどうかを最初に確認します。Subscriber が最初に Distribution を受信した場合は、このファイルを所有していません。次に、Distributor が tcpip.nlm ファイルを Subscriber に送信すると、tednode.properties ファイルは Subscriber では使用されなくなります。Distributor は、Subscriber サーバが現在の tcpip.nlm ファイルを所有しているかどうかを再度確認します。Subscriber からの確認が得られると、Distribution が送信されます。つまり、Distributor は、設定情報が最新ではない Subscriber サーバには Distribution を送信しません。

Subscriber オブジェクトのプロパティで設定を変更したときはいつでも tcpip.nlm ファイルを更新できます。ただし、Subscriber は eDirectory を読み取らないため、Subscriber に変更を加えたときは、Distributor がこれらの変更を検出し、新しい設定情報を Subscriber サーバに送信して tcpip.nlm ファイルを更新する必要があります。

eDirectory ツリーで、Microsoft ドメインサーバなど、Subscriber オブジェクトを含まないサーバに Subscriber ソフトウェアをインストールする必要がある場合は、Distributor サーバによって更新される Tiered Electronic Distribution 設定を使用する代わりに、tednode.properties ファイルがこのようなサーバで使用されます。この場合は、設定の変更時にサーバの tednode.properties ファイルを編集する必要があります。詳細については、165 ページの「Tednode.properties ファイルの要件」および 194 ページの「Tednode.properties ファイルの編集」を参照してください。

Subscriber と Channel の関連付け

Subscriber が Distribution を受信できるようにするには、Distribution を保持する Channel に Subscriber を関連付ける必要があります。この操作は、Subscriber オブジェクトまたは Channel オブジェクトのプロパティから実行できます。

- 157 ページの「Channel と複数の Subscriber の関連付け」
- 158 ページの「Subscriber と複数の Channel との関連付け」

Channel と複数の Subscriber の関連付け

特定の Distribution を多数の Subscriber サーバに送信するには

1. ConsoleOne で、Distribution をリストに含む Channel オブジェクトを右クリックし、[Properties] をクリックします。
2. [Subscribers] タブを選択し、[Add] をクリックして、必要な Subscriber を追加します。
3. [Schedule] タブを選択して、スケジュールを選択します。

   スケジュールは、受信した Distribution の抽出またはインストールのタイミングを決定します。

   利用可能なスケジュールについては、8 章 331 ページの「スケジュール設定」を参照してください。
4. [OK] をクリックして変更内容を保存します。

Subscriber と複数の Channel との関連付け

Subscriber サーバを複数の Channel に登録して、異なる Distribution を受信するようにするには

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [Channels] タブを選択し、[Add] をクリックして、必要な Channel を追加します。

3 [Schedule] タブを選択して、スケジュールを選択します。

スケジュールは、受信した Distribution の抽出またはインストールのタイミングを決定します。

利用可能なスケジュールについては、8 章 331 ページの「スケジュール設定」を参照してください。

4 [Variables] タブを選択して次のフィールドに入力し、[OK] をクリックします。

[Variable Name]： ファイルを抽出するディレクトリの場所を指定します。% 記号の間に、使用する変数名を正確に入力します。

[Value]： 変数の値です。もう 1 つの変数名として使用されます。

[Description]： 変数の説明を入力するテキストフィールドです。

変数については、363 ページの「変数を使用したファイルの抽出の制御」を参照してください。

5 [OK] をクリックして変更内容を保存します。

Distributor のルーティング階層に属する Subscriber オブジェクトの削除

Subscriber オブジェクトが eDirectory から削除されるか、または Subscriber サーバがネットワークから削除（eDirectory からの Subscriber オブジェクトの削除とは無関係）され、その Subscriber が Distributor のルーティング階層に属している場合は、Distributor オブジェクトのプロパティを編集して、ルーティング階層が適合するように調整する必要があります。この調整を行わないと、親 Subscriber を介して送信される Distribution が、指定された Subscriber サーバまで配布されません。

Subscriber Group

次の節では、Subscriber Group オブジェクトの概念と使用方法について説明します。

- 158 ページの「Subscriber Group の理解」
- 159 ページの「Subscriber Group の作成と設定」

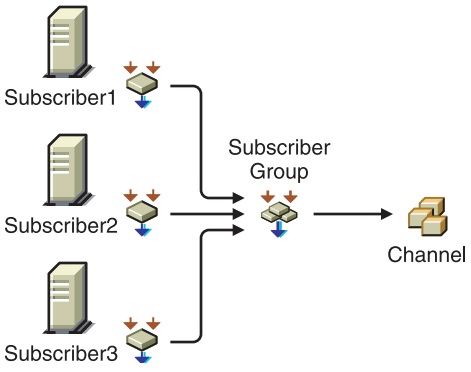
Subscriber Group の理解

Subscriber Group は、Subscriber オブジェクトのグループ化に使用される eDirectory オブジェクト（TED Subscriber Group）です。

- 159 ページの「他のTiered Electronic Distributionオブジェクトとの機能的関係」
- 159 ページの「Subscriber Group の説明」
- 159 ページの「スケジュール設定」

他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、Subscriber Group、Subscriber、および Channel の関係を示しています。



Subscriber Group の説明

Subscriber Group は、同じ Distribution を必要とする Subscriber のグループ化に使用されます。

Subscriber Group は、異なる複数の Distribution を同じ Subscriber のグループに送信する場合に役立ちます。Subscriber が 1 つの Channel にだけ関連付けられている場合は、Subscriber Group を作成する必要はありません。

たとえば、Channel A は Distribution A を含み、Channel B は Distribution B を含むという構成の複数の Channel があるとします。この場合、Subscriber Group を使用しないと、各 Subscriber を Channel A に登録し、さらに Channel B にも登録するというように、長いプロセスが必要になります。Subscriber Group を使用すると、グループを作成して複数の Subscriber を追加し、そのグループを各 Channel に登録するだけで済みます。

Subscriber Group の別の使用法として、グループが複数の Channel に関連付けられている場合は、グループのメンバーシップを編集すると、より簡単に複数の Channel に同じ変更を加えることができます。たとえば、Subscriber Group から Subscriber を削除するには、グループのプロパティを編集するだけです。複数の Channel から同じ Subscriber を削除するには、各 Channel のプロパティを編集する必要があります。

スケジュール設定

Subscriber Group にはスケジュールを設定できません。

Subscriber Group の作成と設定

1 ConsoleOne で、Subscriber Group オブジェクトを格納するコンテナを選択し、[File] > [New] > [Object] の順にクリックして、[TED Subscriber Group] を選択します。

2 [New TED Subscriber Group] ダイアログボックスで、Subscribe グループ名を指定し（ワークシートの項目 17）、[Define Additional Properties] を選択して [OK] をクリックします。

3 [General] > [Settings] の順にクリックして、説明を入力します。

4 Subscriber をグループのメンバーに含めるには、[Members] タブを選択して次の操作を行います。

4a [Add] をクリックし、Subscriber オブジェクトを参照して選択し (ワークシートの項目 18)、[OK] をクリックします。

4b 一覧から Subscriber を削除するには、Subscriber を選択して [Delete] をクリックします。

4c Subscriber のプロパティを表示するには、Subscriber を選択して [Details] をクリックします。

5 Subscriber Group オブジェクトの設定が終了したら [OK] をクリックします。

External Subscriber

次の節では、External Subscriber オブジェクトの概念と使用方法について説明します。

- 160 ページの「External Subscriber の理解」
- 166 ページの「External Subscriber による別のツリーへの配布」
- 168 ページの「External Subscriber の作成と設定」

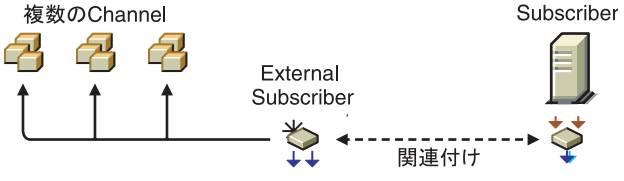
External Subscriber の理解

External Subscriber は、別のツリーに Subscriber オブジェクトを表示する eDirectory オブジェクト (TED External Subscriber) です。

- 160 ページの「他のTiered Electronic Distributionオブジェクトとの機能的関係」
- 160 ページの「External Subscriber の説明」
- 163 ページの「Subscriber ソフトウェアの設定と信頼されるツリー」
- 166 ページの「スケジュール設定」

他の Tiered Electronic Distribution オブジェクトとの機能的関係

次の図は、External Subscriber と Channel の関係を示しています。



External Subscriber は Channel に登録されます。

External Subscriber の説明

Distributor は、Subscriber オブジェクトが Distributor オブジェクトと異なるツリーに属する Subscriber サーバや、Subscriber オブジェクトを含まないサーバには Distribution を送信できません。別のツリーに配布するには、External Subscriber オブジェクトが必要です。

External Subscriber オブジェクトについては、次の節を参照してください。

- 161 ページの「External Subscriber の目的」
- 161 ページの「保持されない Distribution 情報」
- 161 ページの「重複する Distribution の管理」
- 162 ページの「External Subscriber の特徴」
- 162 ページの「External Subscriber に関する要件」
- 162 ページの「External Subscriber オブジェクトのプロパティ」

External Subscriber の目的

すべての Tiered Electronic Distribution オブジェクトを 1 つのツリーにインストールした場合は、同じツリー内の Distributor オブジェクトと Subscriber オブジェクトを使用して Distribution を送信できるため、External Subscriber オブジェクトは必要ありません。

External Subscriber オブジェクトは、次の条件のいずれかに該当する場合、別のツリーに Distribution を送信するときに役立ちます。

- **ターゲットサーバのツリーに Subscriber オブジェクトがない：** Microsoft ドメインの Windows サーバなどのターゲットサーバには、Subscriber ソフトウェアのみがインストールされています。
- **ターゲットサーバのSubscriberオブジェクトが別のツリーにある：** ターゲットサーバには Subscriber ソフトウェアがインストールされていますが、その Subscriber オブジェクトは、Distribution を送信する Distributor オブジェクトとは別のツリーに属しています。

eDirectory ツリーのオブジェクトである External Subscriber は、実際には Distribution ファイルを処理せず、Distribution ファイルを受信するサーバを識別するだけです。

保持されない Distribution 情報

External Subscriber を通じて Distribution を送信する場合、信頼されるツリーの権限は保持されません。

External Subscriber を通じて Desktop Application タイプの Distribution を送信する場合、アプリケーションオブジェクトの関連付けは保持できません。ただし、グループの関連付けを作成するため、このグループの関連付けを送信できます。

重複する Distribution の管理

External Subscriber オブジェクトを使用すると、別のツリーに Distribution の配布タスクを複製する必要がなくなります。

たとえば、リモートサイトのツリーに属する Subscriber は、Distributor のツリーに属する External Subscriber を経由してすべての Distribution を受信できます。これにより、リモートサイトに Distributor サーバを配置して、Distribution 設定や管理タスクを重複して実行する必要がなくなります。

External Subscriber の特徴

External Subscriber に関連付けられるのは、Subscriber ソフトウェアを実行し、Subscriber オブジェクトがどのツリーにも含まれないサーバか、または Subscriber オブジェクトが Distribution の送信元の Distributor と同じ eDirectory ツリーに含まれないサーバです。

External Subscriber オブジェクトは、サーバの IP アドレスまたは DNS 名によって Subscriber サーバに関連付けられます。

Distribution は、Microsoft ドメインの Windows サーバなど、eDirectory の外側にも送信できます。このタイプの Distribution の詳細については、163 ページの「Subscriber ソフトウェアの設定と信頼されるツリー」と 165 ページの「Tednode.properties ファイルの要件」を参照してください。

External Subscriber オブジェクトは親 Subscriber として使用できません。External Subscriber に親 Subscriber がある場合は、External Subscriber のオブジェクトと親 Subscriber のオブジェクトが同じツリーに属している必要があります。

External Subscriber に関する要件

ターゲットサーバの Subscriber オブジェクトが、Distribution を送信するサーバの Distributor オブジェクトとは異なるツリーに属している場合、このターゲットサーバは Distributor のツリーの External Subscriber オブジェクトとして表示される必要があります。

Tiered Electronic Distribution は、IP アドレスまたは DNS 名を使用してサーバの場所を特定するため、Subscriber オブジェクトはサーバの NCP オブジェクトと異なるツリーに配置できます。

External Subscriber は、関連付けられた Subscriber に必要な Distribution を含む Channel に登録する必要があります。

External Subscriber を介して Distribution を受信するサーバは、Distribution を受信および抽出できるように、Subscriber ソフトウェアをインストールする必要があります。ドメイン内に Windows サーバがある場合などは、ツリーに Subscriber オブジェクトを含める必要はありません（163 ページの「Subscriber ソフトウェアの設定と信頼されるツリー」と 165 ページの「Tednode.properties ファイルの要件」を参照）。

External Subscriber オブジェクトのプロパティ

External Subscriber オブジェクトのプロパティを次に示します。

- 異なるツリー内またはドメイン内のSubscriberサーバのIPアドレスまたはDNS名（必須）

  これは、あるツリー（External Subscriber オブジェクトが属するツリー）の Distributor から Distribution を受信する、別のツリーの Subscriber サーバの ID です。

- 登録する Channel（必須）

  これは、別のツリーの Subscriber サーバに送信する必要のある Distribution を特定します。

- Subscriber Group のメンバーシップ（省略可能）

  グループが登録される Channel に External Subscriber を登録します。

- External Subscriber のツリー内の親 Subscriber のコンテキスト（省略可能）

親 Subscriber は、通常、Distributor の配布階層に属しています。

これを使用すると、親 Subscriber は Distribution ファイルを他のツリーのサーバに送信する物理タスクを実行します。使用しない場合、Distributor サーバは、他のツリーの Subscriber サーバに直接 Distribution を送信します。

Subscriber ソフトウェアの設定と信頼されるツリー

Subscriber は Distributor によって設定できますが、External Subscriber は設定できません。External Subscriber は、サーバの認識のみを行うオブジェクトです。ただし、External Subscriber オブジェクトによって認識された Subscriber サーバが External Subscriber オブジェクトを介して Distribution を受信するには、Tiered Electronic Distribution を設定する必要があります。

External Subscriber オブジェクトを使用するには、次の節を参照して信頼されるツリーを理解する必要があります。

- 163 ページの「信頼されるツリーを使用する理由」
- 164 ページの「信頼されるツリーの決定」
- 165 ページの「Tednode.properties ファイルの要件」
- 165 ページの「Policy Package Distribution送信時に信頼されるツリーで発生するエラーの回避」

信頼されるツリーを使用する理由

NetWare または Windows サーバでは、eDirectory ツリーに NCP サーバオブジェクトがあるかどうか、または Microsoft ドメインにサーバオブジェクトがあるかどうかによって、次の処理が適用されます。

- インストール時に、サーバには Subscriber オブジェクトが作成され、Subscriber ソフトウェアがインストールされます。
- インストール時に、サーバでは Subscriber ソフトウェアのインストールだけが実行されます (Subscriber オブジェクトは作成されません)。
- インストール時に、Subscriber オブジェクトが作成されなかったサーバの信頼されるツリーを特定する必要があります。

信頼されるツリーの特定には 2 つの目的があります。

- Subscriber の Tiered Electronic Distribution 設定情報を更新できる Distributor を特定します。
- ポリシーを受け入れるツリーを指定すること

Subscriber サーバの Tiered Electronic Distribution 設定情報は、Subscriber オブジェクトの eDirectory(Distributor によって読み取られる)、および Subscriber サーバのファイルシステムの tcpip.nlm ファイル (Subscriber によって読み取られる) に保存されます。設定情報を送信する Distributor サーバの Distributor オブジェクトは、設定される Subscriber オブジェクトと同じツリー内にある必要があります。

Subscriber サーバは、信頼されるツリー内の Distributor からのみ Subscriber ソフトウェア設定を受信できます。信頼されるツリーとは、サーバの Subscriber オブジェクトと Distributor オブジェクトの両方が含まれるツリーです。これは、関連付けられた External Subscriber オブジェクトが属するツリーではありません。サーバの NCP オブジェクトが属するツリーと同じかどうかは問題ではありません。

Subscriber サーバのツリーに Subscriber オブジェクトがない場合（Microsoft ドメインの Windows サーバなど）は、Tiered Electronic Distribution 設定情報の tednode.properties ファイルを使用する必要があります。このファイルは、Subscriber ソフトウェアのインストール時にサーバに作成されます。次に、Distributor から（External Subscriber オブジェクトを介して）別のツリーに送信された Distribution を受信および抽出します。抽出プロセスでは、信頼されるツリーの要件が満たされていることが必要です。詳細については、165 ページの「Tednode.properties ファイルの要件」を参照してください。

信頼されるツリーの決定

次の 2 つの状況によって、Subscriber オブジェクトが Subscriber サーバにインストールされるかどうかが決まります。

- **eDirectory サーバ：** Subscriber ソフトウェアをサーバにインストールし、そのサーバの NCP サーバオブジェクトが別のツリーにあるときは、次のいずれかのオプションを選択します。
  - DistributorのツリーがSubscriberのNCPサーバオブジェクトを含まない場合でも、このツリーに Subscriber オブジェクトを作成できます（サーバの Subscriber オブジェクトと NCP オブジェクトは同じツリー内にある必要はありません）。この場合は、Subscriber オブジェクトがツリー内にあるため、Subscriber への Distribution の送信に External Subscriber オブジェクトを使用する必要はありません。

    Subscriber サーバの信頼されるツリーは、Distributor オブジェクトを含むツリーです。したがって、Subscriber は、信頼されるツリーの Distributor から送信される Tiered Electronic Distribution 設定更新を受信します。
  - サーバに Subscriber オブジェクトを作成しないようにもできます。この場合は、tednode.properties ファイルを使用して Subscriber サーバを設定する必要があります。External Subscriber オブジェクトを使用して Subscriber サーバに Distribution を送信する必要もあります。

    この Subscriber でポリシーを実行するには、Policy Package Distribution の送信元である、信頼されるツリーを特定する必要があります。
- **eDirectory 以外のサーバ：** Subscriber ソフトウェアを Microsoft ドメイン内のサーバにインストールし、サーバの eDirectory ツリーに NCP サーバオブジェクトがないときは、サーバに Subscriber オブジェクトを作成できますが、必須ではありません。Subscriber オブジェクトがない場合は、tednode.properties ファイルを使用してその Subscriber サーバを設定する必要があります。External Subscriber オブジェクトを使用して Subscriber サーバに Distribution を送信する必要もあります。

  この Subscriber でポリシーを実行するには、Policy Package Distribution の送信元である、信頼されるツリーを特定する必要があります。

インストールプログラムの［File Installation Paths and Options］ページには、［Trusted Tree］フィールドが表示されます。ただし、このフィールドは［Installation Options］ページの［Create eDirectory Objects］チェックボックスの選択を解除した場合にのみ表示されます。これにより、インストールプログラムは、選択されたサーバにソフトウェアのみをインストールします。

Subscriber ソフトウェアをインストールする各サーバでは信頼されるツリーを選択する必要があります。選択しないと、ポリシーはツリー内のオブジェクトを指しているため、Policy Package Distribution が Subscriber サーバで抽出されない場合があります。

[Trusted Tree] フィールドに関するインストールの説明については、次の該当する節の手順を参照してください。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」を参照してください。

Tednode.properties ファイルの要件

次の Subscriber サーバに設定情報を提供するには、tednode.properties ファイルを使用する必要があります。

- Subscriber オブジェクトを含み、最初の Distribution をまだ受信していない Subscriber サーバ。最初の Distribution を受信すると、信頼されるツリー内でその Distribution を送信した Distributor から提供された tcpip.nlm ファイルを使用します。

  Subscriber は、Subscriber オブジェクトと同じツリーに属する Distributor オブジェクトの Distributor サーバによってのみ設定できます。

- ツリーに Subscriber オブジェクトを含まない Subscriber サーバ。

  これは、Subscriber オブジェクトを作成せずに Subscriber ソフトウェアのみをインストールした Microsoft ドメイン内の Windows サーバなどです。

  Subscriber オブジェクトを作成せずに Subscriber ソフトウェアをインストールした場合は (ZENworks Server Management インストールプログラムを使用)、tednode.properties ファイルが自動的に作成および設定されます。

  詳細については、194 ページの「Tednode.properties ファイルの編集」を参照してください。

Policy Package Distribution 送信時に信頼されるツリーで発生するエラーの回避

External Subscriber オブジェクトを使用して Policy Package Distribution を Subscriber に送信するときに、信頼されるツリーで発生するエラーを防ぐには、agentinfo.properties ファイルを編集する必要があります。

1. External Subscriber オブジェクトを使用して Policy Package Distribution を受信するサーバで、¥zenworks¥pds¥ted ディレクトリの agentinfo.properties ファイルの場所に移動します。
2. agentinfo.properties ファイルをテキストエディタで開きます。
3. ファイルに次の行を追加します。

   TRUSTED_TREE=*source_tree_name*
   TRUSTED_TDN=*External_Subscriber_DN*

   source_tree_name は、Policy Package Distribution を送信する Distributor オブジェクトが属するツリーです。*External_Subscriber_DN* は、Distribution を受信する External Subscriber オブジェクトの完全識別名です。
4. agentinfo.properties ファイルを保存して、テキストエディタを終了します。
5. 準備ができたら、Policy Package Distribution を External Subscriber に送信します。

スケジュール設定

External Subscriber オブジェクトにはスケジュールを設定できません。

External Subscriber による別のツリーへの配布

External Subscriber を使用して別のツリーに配布する方法については、次の節を参照してください。

- 166 ページの「External Subscriber、単一の Distributor、および単一のツリー」
- 167 ページの「External Subscriber、複数の Distributor、および複数のツリー」

External Subscriber、単一の Distributor、および単一のツリー

Policy and Distribution Services ソフトウェアをサーバにインストールしてから、External Subscriber オブジェクトを使用すると、ツリーに Subscriber オブジェクトを含まないサーバに Distribution を送信できます。

External Subscriber を経由して Distribution を送信するときの Distributor のルーティングに、次のような Tiered Electronic Distribution 設定が存在するとします。



この例では、Server_2 のツリーに Subscriber オブジェクトがありません。Subscriber ソフトウェアだけがインストールされており、Server_2 は Distribution を受信および抽出できます。このようなサーバには、ツリーに NCP サーバオブジェクトを含む NetWare サーバや、Microsoft ドメインの Windows サーバがあります。

Distribution を Distributor_A から Server_2 に送信するには、Tree_A に External Subscriber オブジェクトを作成し、External Subscriber オブジェクトのプロパティに Server_2 の IP アドレスまたは DNS 名を指定します。

eDirectory での Distribution の表示

eDirectory の観点から見ると、Distribution は Distributor オブジェクトから External Subscriber オブジェクトに送信され、この External Subscriber オブジェクトによって Server_2 に送信されます。Distributor が Server_2 に直接 Distribution を送信しないようにするには、Tree_A の親 Subscriber(非表示)を使用します。

実際の配布プロセス

トポロジの観点から見ると、Distribution ファイルは、External Subscriber オブジェクトのプロパティで指定した Server_2 の IP アドレスまたは DNS 名を使用して、Server_1 から Server_2 に送信されます。

Subscriber サーバの設定

Server_2 は、Subscriber ソフトウェアのインストール時にサーバにインストールされた tednode.properties ファイルから Tiered Electronic Distribution 設定情報を受信します。設定する Subscriber オブジェクトがないため、設定を変更するには、Server_2 の tednode.properties ファイルを編集する必要があります。tednode.properties ファイルの編集については、194 ページの「Tednode.properties ファイルの編集」を参照してください。

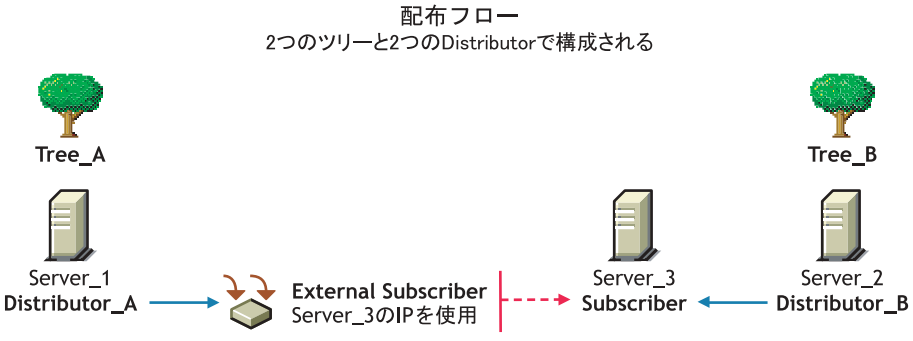
Subscriber サーバの信頼されるツリー

Server_2 でポリシーを実行するには、Subscriber ソフトウェアをサーバにインストールするときに、Tree_A を信頼されるツリーとして構築する必要があります。インストールの手順については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」を参照してください。

External Subscriber、複数の Distributor、および複数のツリー

複数のツリー内のサーバに Policy and Distribution Services ソフトウェアをインストールしてから、External Subscriber オブジェクトを使用すると、ツリー間で Distribution を送信できます。

External Subscriber を経由して Distribution を送信するときの Distributor のルーティングに、次のような Tiered Electronic Distribution 設定が存在するとします。



この例では、Tree_B の Server_3 に Subscriber オブジェクトがあります。

Distribution を Distributor_A から Server_3 に送信するには、Tree_A に External Subscriber オブジェクトを作成し、External Subscriber オブジェクトのプロパティに Server_3 の IP アドレスまたは DNS 名を指定します。

eDirectory での Distribution の表示

eDirectory の観点から見ると、Distribution は Distributor_A から External Subscriber オブジェクトに送信され、この External Subscriber オブジェクトによって Server_3 に送信されます。Distributor_A が Server_3 に直接 Distribution を送信しないようにするには、Tree_A の親 Subscriber（非表示）を使用します。

実際の配布プロセス

トポロジの観点から見ると、Distribution ファイルは、External Subscriber オブジェクトのプロパティで指定した Server_3 の IP アドレスまたは DNS 名を使用して、Server_1 から Server_3 に送信されます。

Subscriber Server_3 の信頼されるツリーと Tiered Electronic Distribution 設定

各ツリーの Distributor は、ツリー内の Subscriber サーバの設定情報を提供します。

Tree_B は、インストールプログラムによる Subscriber の構築時に、Server_3 の信頼されるツリーとして設定されているため、Server_3 は Distributor_B から Tiered Electronic Distribution 設定情報を受信します。ただし、Server_3 は Distributor_B によって設定されるまで Distributor_A からの Distribution を抽出できません。抽出は、Subscriber が Distributor_B から Distribution を最初に受信したときに実行されます。

External Subscriber の作成と設定

Subscriber オブジェクトが別のツリーにある Subscriber サーバや、ツリーに Subscriber オブジェクトがない Subscriber サーバに Distribution を送信するには、External Subscriber オブジェクトを作成します。

次の節では、External Subscriber を作成および設定する手順について説明します。

- 168 ページの「External Subscriber オブジェクトの作成」
- 168 ページの「External Subscriber オブジェクトの設定」

External Subscriber オブジェクトの作成

1 ConsoleOne で、External Subscriber オブジェクトを格納するコンテナを選択し、[File] > [New] > [Object] の順にクリックして、[TED External Subscriber] を選択します。

2 External Subscriber オブジェクトの名前を指定します。

他のツリーからサーバを識別できるように固有の名前を付けます。

3 サーバの TCP/IP アドレスまたは DNS 名を指定して、[OK] をクリックします。

有効な TCP/IP アドレスまたは完全識別 DNS 名を指定する必要があります。

4 168 ページの「External Subscriber オブジェクトの設定」に進みます。

External Subscriber オブジェクトの設定

1 ConsoleOne で、External Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [General] > [Settings] の順にクリックし、次の設定フィールドに入力します。

[Use Policy]： External Subscriber のサーバで実行する Tiered Electronic Distribution ポリシーに設定された値を使用する場合は、このチェックボックスを選択します。

このオプションを選択すると、[Parent Subscriber] フィールドが淡色表示され、このポリシー設定が使用されます。

[Parent Subscriber]： 受信するすべての Distribution の送信元となる親 Subscriber を指定します。

Distributor オブジェクトのプロパティで作成されたルーティング階層には、親 Subscriber のみが含まれるため、このフィールドによってエンドノード Subscriber をルーティング階層に結び付けることができます。これらのエンドノード Subscriber（この場合は External Subscriber）は、他の Subscriber に Distribution を渡すことができません。

3 [Network Address] タブを選択して、External Subscriber のサーバの IP アドレスを確認します。

[IP Address]：この IP アドレスは、オブジェクトの作成時に指定しています。IP アドレスが正しいことを確認します。

4 [Channels] タブを選択し、次のフィールドに入力します。

- [Channels This Subscriber Is Subscribed To]

  External Subscriber が登録された Channel が表示されます。

  [Active]：この External Subscriber が Channel の Distribution を受信できるように Channel を有効にするには、Channel を選択して、チェックボックスを選択します。External Subscriber が Channel の Distribution を受信しないように Channel を無効にするには、チェックボックスの選択を解除します。

  [Channel]：Channel を作成するには、[Add] をクリックします。Channel を編集するには、[Details] をクリックします。

- [Channels Subscribed to Through Subscriber Group Memberships]

  External Subscriber が属する Subscriber Group と、Subscriber Group のメンバーシップによって External Subscriber が登録された Channel が表示されます。

  これらの列は表示専用です。[Details]、[Add]、および [Delete] ボタンは使用できません。

  [Active]：登録された Channel が有効になっているかどうかが表示されます。

  [Channel]：グループのメンバーシップによって登録された Channel が表示されます。

  [Subscriber Groups]：External Subscriber が属するグループが表示されます。列見出しをクリックすると、ソートできます。

5 この External Subscriber をグループに含めるには、[Group Membership] > [Add] の順にクリックし、Subscriber Group オブジェクトを参照して、[Select] > [OK] の順にクリックします。

6 External Subscriber オブジェクトの設定が終了したら、[OK] をクリックして、オブジェクトのプロパティを終了します。

複数の Tiered Electronic Distribution オブジェクトの設定

複数の Tiered Electronic Distribution オブジェクトの設定に同じ変更を加えるときは、複数のオブジェクトのプロパティを変更することで時間を節約できます。

複数のオブジェクトの変更は、次の Tiered Electronic Distribution オブジェクトで実行できます。

Distributor
Distribution
Channel
Subscriber
External Subscriber
Subscriber Group
ポリシーパッケージ

詳細については、次の節を参照してください。

- 170 ページの「複数の Tiered Electronic Distribution オブジェクトプロパティの変更に関する問題」
- 171 ページの「複数の Tiered Electronic Distribution オブジェクトのプロパティの変更」
- 172 ページの「複数のオブジェクトの変更に使用するプロパティタブ」

複数の Tiered Electronic Distribution オブジェクトプロパティの変更に関する問題

- **使用可能なプロパティ：** この方法は、複数のオブジェクトに同じ変更を加えられるようにすることが目的ですが、Tiered Electronic Distribution オブジェクトのすべてのプロパティがこの方法で変更できるとは限りません。

  複数の Tiered Electronic Distribution オブジェクトを選択してプロパティを編集する場合は、[Schedule] および [Other] プロパティタブが使用できません。Distribution オブジェクトでは、[Type] タブも使用できません。これらのプロパティタブについて変更するには、各 Tiered Electronic Distribution オブジェクトを個別に編集する必要があります。

- **変更されるフィールド：** [Properties of Multiple Objects] ダイアログボックスで変更するフィールドは、選択したオブジェクトについて変更が必要なフィールドだけです。つまり、フィールドを空白にした（変更しない）場合は、選択したすべてのオブジェクトについてそのフィールドは変更されません。各オブジェクトの元のフィールドエントリが残されます。

  フィールドの情報が複数のオブジェクトで異なる場合、[Properties of Multiple Objects] ダイアログボックスのフィールドは空白になります。

- **情報の削除：** いくつかのフィールドでは、スペースを入力できます。選択したすべてのオブジェクトについてフィールドを空白にする場合は、選択した各 Tiered Electronic Distribution オブジェクトの異なる複数のエントリを削除する方法として使用できます。

- **ポリシーのデフォルト：** Tiered Electronic Distribution ポリシーが有効になっている場合、[Use Policy] チェックボックスは各 Tiered Electronic Distribution オブジェクトのプロパティに表示されますが、ポリシーを適用する個々の Tiered Electronic Distribution オブジェクトのチェックボックスが選択されているだけです（これらのプロパティは未編集か、またはチェックボックスが選択されているため）。

  複数のオブジェクトプロパティでは、[Use Policy] チェックボックスが表示され、選択されている場合、ポリシーの内容は適切なフィールドに淡色表示されます。これらの属性は、Tiered Electronic Distribution オブジェクトのプロパティのうち、選択された [Use Policy] チェックボックスを含む個々のプロパティにのみ適用されます。

  ポリシーを使用している Tiered Electronic Distribution オブジェクトを選択し、複数のプロパティを編集して、これらのオブジェクトの Tiered Electronic Distribution ポリシーを無効にするには、[Use Policy] チェックボックスの選択を解除します。変更は、選択した Tiered Electronic Distribution オブジェクトにすべて複製され、Tiered Electronic Distribution ポリシーはこれらのオブジェクトでは無効となります。

重要： あるオブジェクトの［Working Directory］フィールドが Tiered Electronic Distribution ポリシーによって指定され、複数のプロパティの編集時に［Use Policy］チェックボックスの選択が解除された場合、そのオブジェクトの［Working Directory］フィールドは空白になります。そのため、次にそのオブジェクトのプロパティにアクセスしたときは、作業ディレクトリの場所を指定する必要があります。

複数の Tiered Electronic Distribution オブジェクトのプロパティの変更

複数の Tiered Electronic Distribution オブジェクトのプロパティを変更するには

1 ConsoleOne で、複数の Tiered Electronic Distribution オブジェクトを選択します。

すべて Distributor オブジェクトを選択するというように、同じ種類のオブジェクトを選択する必要があります。異なる種類のオブジェクトを選択した場合は、［Properties of Multiple Objects］メニューオプションが表示されません。

(Shift) キーや (Ctrl) キーを使用して、複数のオブジェクトを選択します。

2 選択したオブジェクトを右クリックし、［Properties of Multiple Objects］をクリックします。

選択した各オブジェクトは、［Properties of Multiple Objects］ダイアログボックスの［Objects to Modify］タブに表示されます。変更を加えると、これらのオブジェクトのプロパティが変更されます。

3 リストに表示されるオブジェクトを変更するには、［Add］または［Remove］をクリックします。

［Add］ボタンをクリックすると、他の Tiered Electronic Distribution オブジェクトを参照できます。すでに選択したタイプのオブジェクトのみが表示され、リストに追加できます。

［Remove］ボタンを選択する前に、リストから 1 つまたは複数のオブジェクトを選択する必要があります。この操作によってオブジェクトがリストから削除されますが、eDirectory からは削除されません。

4 変更するプロパティを含むタブを選択します。

さまざまな Tiered Electronic Distribution オブジェクトで利用可能なプロパティタブについては、172 ページの「複数のオブジェクトの変更に使用するプロパティタブ」を参照してください。

5 プロパティを編集します。

［Objects to Modify］タブに表示されたすべてのオブジェクトが変更されます。

各プロパティフィールドの詳細については、次の節の手順内の説明を参照してください。

- 108 ページの「Distributor の設定」
- 125 ページの「Distribution の作成」
- 148 ページの「Channel の作成と設定」
- 153 ページの「Subscriber の設定」
- 159 ページの「Subscriber Group の作成と設定」
- 168 ページの「External Subscriber の作成と設定」

6 選択したオブジェクトのプロパティの変更が終了するまで、ステップ 4 とステップ 5 を繰り返します。

7 プロパティの変更が終了したら、[OK] をクリックして [Properties of Multiple Objects] ダイアログボックスを閉じます。

すべての変更が、選択したすべてのオブジェクトに反映されます。

複数のオブジェクトの変更に使用するプロパティタブ

次の表に、各 Tiered Electronic Distribution オブジェクトの複数オブジェクト編集モードで使用できるプロパティタブを示します。

重要： 通常は、情報を変更すると、選択したすべてのオブジェクトのプロパティが変更されます。例外については、各説明中に示します。

- 172 ページの「Distributor オブジェクト」
- 173 ページの「Distribution オブジェクト」
- 173 ページの「Channel オブジェクト」
- 174 ページの「Subscriber オブジェクト」
- 175 ページの「External Subscriber オブジェクト」
- 175 ページの「Subscriber Group オブジェクト」
- 176 ページの「ポリシーパッケージオブジェクト」

Distributor オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから Distributor オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings] サブタブおよび [Messaging] サブタブが表示されます。 [Settings] サブタブでは、選択した Subscriber オブジェクト間でフィールドの情報が同じ場合でも、フィールドには情報が表示されません。ただし、選択した Tiered Electronic Distribution オブジェクトで Tiered Electronic Distribution ポリシーが有効になっているフィールドには、テキストが淡色表示されます。 [Settings] サブタブでは、選択したすべての Subscriber オブジェクトに適用する新しい情報のみを追加できます。[Messaging] サブタブでは、既存のエントリを編集できます。
Routing	選択した Distributor オブジェクト間でルーティング階層が異なる場合、このタブには何も表示されません。複数の Distributor オブジェクトのルーティング階層が同じ場合にのみ編集できます。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

Distribution オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから Distribution オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings] サブタブおよび [Restrictions] サブタブが表示されます。 [Settings] サブタブでは、選択した Subscriber オブジェクト間でフィールドの情報が同じ場合でも、フィールドには情報が表示されません。ただし、選択した Tiered Electronic Distribution オブジェクトで Tiered Electronic Distribution ポリシーが有効になっているフィールドには、テキストが淡色表示されます。 [Settings] サブタブでは、選択したすべての Subscriber オブジェクトに適用する新しい情報のみを追加できます。[Restrictions] サブタブでは、既存のエントリを編集できます。
Channels	Channel は、このタブには自動的に表示されません。選択した各 Distribution オブジェクトに Channel を追加する場合や、Channel に関連付けられている各 Distribution オブジェクトから Channel を削除する場合にのみ、Channel を参照できます。 このタブのリストに Channel を追加または削除しても、eDirectory に Channel オブジェクトが追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

Channel オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから Channel オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings] サブタブ ([Active] チェックボックスと [Description] フィールドを含む) が表示されます。 [Settings] サブタブでは、選択した Subscriber オブジェクト間でフィールドの情報が同じ場合でも、フィールドには情報が表示されません。ただし、選択した Tiered Electronic Distribution オブジェクトで Tiered Electronic Distribution ポリシーが有効になっているフィールドには、テキストが淡色表示されます。 [Settings] サブタブでは、選択したすべての Subscriber オブジェクトに適用する新しい情報のみを追加できます。
Distribution	Distribution は、このタブには自動的に表示されません。選択した各 Channel オブジェクトに Distribution を追加する場合や、Distribution に関連付けられている各 Channel オブジェクトから Distribution を削除する場合にのみ、Distribution を参照できます。 このタブのリストに Distribution を追加または削除しても、eDirectory に Distribution が追加または削除されることはありません。

使用可能なプロパティタブ	説明
Subscriber	Subscriber は、このタブには自動的に表示されません。選択した各 Channel オブジェクトに Subscriber を追加する場合や、Subscriber に関連付けられている各 Channel オブジェクトから Subscriber を削除する場合にのみ、Subscriber を参照できます。 このタブのリストに Subscriber を追加または削除しても、eDirectory に Subscriber が追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

Subscriber オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから Subscriber オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings]、[Messaging]、および [Working Context] サブタブが表示されます。 [Settings] サブタブでは、選択した Subscriber オブジェクト間でフィールドの情報が同じ場合でも、フィールドには情報が表示されません。ただし、選択した Tiered Electronic Distribution オブジェクトで Tiered Electronic Distribution ポリシーが有効になっているフィールドには、テキストが淡色表示されます。 [Settings] サブタブでは、選択したすべての Subscriber オブジェクトに適用する新しい情報のみを追加できます。[Messaging] サブタブでは、既存のエントリを編集できます。
Channels	Channel は、このタブには自動的に表示されません。選択した各 Subscriber オブジェクトに Channel を追加する場合や、Channel に関連付けられている各 Subscriber オブジェクトから Channel を削除する場合にのみ、Channel を参照できます。 このタブのリストに Channel を追加または削除しても、eDirectory に Channel オブジェクトが追加または削除されることはありません。
変数	選択したすべてのオブジェクトに新しい変数を追加するときのみ使用できます。選択したすべてのオブジェクトに共通する変数は表示されず、編集できません。既存の変数を変更するには、各 Subscriber オブジェクトを個別に変更する必要があります。
Group Membership	Group Membership は、このタブには自動的に表示されません。選択した各 Subscriber オブジェクトにグループメンバーシップを追加する場合や、グループメンバーシップに関連付けられている各 Subscriber オブジェクトからグループメンバーシップを削除する場合にのみ、グループメンバーシップを参照できます。 このタブのリストにグループメンバーシップを追加または削除しても、eDirectory にグループメンバーシップが追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

External Subscriber オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから External Subscriber オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings] サブタブが表示されます。 [Settings] サブタブには、[Parent Subscriber] フィールドだけが含まれます。このフィールドに入力すると、選択した External Subscriber がすべて同じ親 Subscriber に関連付けられます。
Channels	Channel は、このタブには自動的に表示されません。選択した各 External Subscriber オブジェクトに Channel を追加する場合や、Channel に関連付けられている各 External Subscriber オブジェクトから Channel を削除する場合にのみ、Channel を参照できます。 このタブのリストに Channel を追加または削除しても、eDirectory に Channel オブジェクトが追加または削除されることはありません。
Group Membership	Group Membership は、このタブには自動的に表示されません。選択した各 Subscriber オブジェクトにグループメンバーシップを追加する場合や、グループメンバーシップに関連付けられている各 Subscriber オブジェクトからグループメンバーシップを削除する場合にのみ、グループメンバーシップを参照できます。 このタブのリストにグループメンバーシップを追加または削除しても、eDirectory にグループメンバーシップが追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

Subscriber Group オブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストから Subscriber Group オブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
一般	[Settings] サブタブおよび [Messaging] サブタブが表示されます。
Channels	Channel は、このタブには自動的に表示されません。選択した各 Subscriber Group オブジェクトに Channel を追加する場合や、Channel に関連付けられている各 Subscriber Group オブジェクトから Channel を削除する場合にのみ、Channel を参照できます。 このタブのリストに Channel を追加または削除しても、eDirectory に Channel オブジェクトが追加または削除されることはありません。

使用可能なプロパティタブ	説明
グループメンバー (Group Members)	Group Members は、このタブには自動的に表示されません。選択した各 Subscriber オブジェクトにグループメンバーを追加する場合や、グループメンバーシップに関連付けられている各 Subscriber オブジェクトからグループメンバーを削除する場合にのみ、グループメンバーを参照できます。 このタブのリストにグループメンバーシップを追加または削除しても、eDirectory にグループメンバーシップが追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

ポリシーパッケージオブジェクト

使用可能なプロパティタブ	説明
Objects to Modify	変更するオブジェクトのリストからポリシーパッケージオブジェクトを追加または削除できます。この操作により、eDirectory にオブジェクトが追加または削除されることはありません。
Policies	サポートされるさまざまなプラットフォームのサブタブが表示されます。これらのプラットフォームで使用できるポリシーの詳細については、205 ページの「サーバポリシーの説明」を参照してください。
Distribution	Distribution は、このタブには自動的に表示されません。選択した各ポリシーパッケージオブジェクトに Distribution を追加する場合や、Distribution に関連付けられている各ポリシーパッケージオブジェクトから Distribution を削除する場合にのみ、Distribution を参照できます。 このタブのリストに Distribution を追加または削除しても、eDirectory に Distribution が追加または削除されることはありません。
NDS Rights	このタブには、[New Trustees] サブタブと [Inherited Filter Rights] サブタブが含まれます。

Distribution の送信

Distribution の送信については、次の節を参照してください。

- 176 ページの「配布プロセスの理解」
- 178 ページの「単一の Distribution の強制送信」
- 178 ページの「親 Subscriber による Distribution の送信」
- 179 ページの「ツリー間の Distribution の送信」

配布プロセスの理解

Distribution の作成および送信プロセスを次に示します。通常はこの順序で実行されます。

1. **Distributor を設定し、スケジュールを決定します。**Distributor を作成するには、*ZENworks 6.5 Server Management Program* CD のインストールプログラムを使用する必要があります。

Distributor については、96 ページの「Distributor」および 335 ページの「Distributor オブジェクトの更新スケジュール」を参照してください。

2. **Subscriber を設定し、スケジュールを決定します。**Subscriber を作成するには、*ZENworks 6.5 Server Management Program* CD のインストールプログラムを使用する必要があります。

   Subscriber の重要な設定には、必要な Distribution を保持する Channel への Subscriber の関連付けがあります。詳細については、157 ページの「Subscriber と Channel の関連付け」を参照してください。

   Subscriber については、150 ページの「Subscriber」および 338 ページの「Subscriber オブジェクトの抽出スケジュール」を参照してください。

3. **必要なポリシーを設定します。**ポリシーパッケージを配布する前に、必要なポリシーを含むポリシーパッケージを ConsoleOne または iManager で作成する必要があります。

   ポリシーの詳細については、210 ページの「サーバポリシーの設定」を参照してください。

4. **Distribution の作成、設定、およびスケジュール設定を行います。**Distribution オブジェクトの作成には、ConsoleOne または iManager のどちらも使用できます。

   設定する Distribution の複雑さにもよりますが、この作業は、プロセス全体の中で最も時間がかかる場合があります。Distributor と Subscriber をセットアップし、Distribution オブジェクトを作成した後は、Distributor のルーティング階層を使用して、ファイルとポリシーを Subscriber サーバに配布するだけです。

   Distribution オブジェクトのスケジュールは、Distribution を個別に送信しない場合に役立ちます。

   Distribution については、112 ページの「Distribution」および 336 ページの「Distribution オブジェクトの構築スケジュール」を参照してください。

5. **Channel の作成、設定、およびスケジュール設定を行います。**Channel オブジェクトの作成には、ConsoleOne または iManager のどちらも使用できます。

   通常は、Distribution ごとに新しい Channel を作成します。一般に、配布される Distribution と Channel が対応していることで、配布システムはより管理しやすくなります。ただし、複数の Distribution が相互に関連し、Channel に登録されたすべての Subscriber がこれらの Distribution をすべて必要としている場合などは、複数の Distribution を 1 つの Channel に含めることができます。たとえば、1 つの Channel が複数の Distribution を保持し、各 Distribution に異なるウイルスパターン更新が含まれる場合などです。

   Channel オブジェクトは、通常、Distribution の送信を制御するのに最適なオブジェクトです。スケジュールに [Never] を設定すると、Channel のリストに含まれるすべての Distribution の配布プロセスが停止します。

   Channel については、147 ページの「Channels」および 337 ページの「Channel オブジェクトの送信スケジュール」を参照してください。

各 Tiered Electronic Distribution オブジェクトで設定したスケジュールに従って、Distribution が構築、送信、および抽出されます。

配布プロセスについては、90 ページの「基本配布プロセス」を参照してください。

これらのプロセスのいくつかは、Server Management のインストール時やシステムの初期設定時に完了している場合があります (1 章 25 ページの「インストール後の設定」を参照)。

単一の Distribution の強制送信

通常の更新、構築および送信スケジュールとは別に単一の Distribution を送信する場合、Channel の送信スケジュールがまだ開始されないときは、iManager で ZENworks Server Management の役割のみを使用し、この配布プロセスを手動で強制的に実行できます。

単一の Distribution を強制的に送信するには、次のいずれかの操作を実行します。

- Distribution のプロパティで［Send Distribution Immediately After Building］オプションが選択されている場合は、iManager に移動して［Distribution］をクリックし、［Build Distribution］をクリックします。

  この Distribution を含む Channel にその他の Distribution がある場合でも、この Distribution だけが送信されます。

- Distribution のプロパティで［Send Distribution Immediately After Building］オプションが選択されていない場合は、iManager に移動して、［Distribution］>［Build Distribution］>［Channel］の順にクリックし、［Distribute Channel］をクリックします。

  Channel 内のその他の Distribution も Subscriber に必要な場合は、すべて送信されます。

Subscriber は Distribution 全体を受信するとすぐに、Subscriber の抽出スケジュールに従って抽出します。

親 Subscriber による Distribution の送信

Subscriber は、Distribution を受信して抽出できますが、Distribution を他の Subscriber に転送することもできます。Distribution を転送する Subscriber は、親 Subscriber と呼ばれます。

親 Subscriber は、転送する Distribution について登録を必要としません。Distribution を受信して、下位の Subscriber に転送するだけです。下位の Subscriber では、次の設定が実行されています。

- Distribution をリストに含む Channel への登録
- 下位 Subscriber のオブジェクトプロパティでの親 Subscriber の指定

Distribution を転送する親 Subscriber をセットアップするには

1. Subscriber（以後、子 Subscriber と呼ぶ）が Distributor のルーティング階層（Distribution を所有する Distributor）に属さないため、この Distribution を受信できない子 Subscriber オブジェクトを特定します。
2. その Subscriber オブジェクトのプロパティで、［General］>［Settings］の順にクリックし、［Parent Subscriber］フィールドで、Distributor のルーティング階層内の Subscriber オブジェクトを参照し、選択して、［OK］をクリックします。

   これにより、選択した Subscriber が親 Subscriber として設定されます。この設定は、親 Subscriber のオブジェクトプロパティでは保持されず、子 Subscriber のプロパティでのみ保持されます。
3. 子 Subscriber だけが関連付けられた Channel オブジェクトを作成します。
4. Distribution を作成し、子 Subscriber の Channel に関連付けます。
5. この Distribution を送信します。

この Distribution は、子 Subscriber が登録された Channel にのみ関連付けられているため、親 Subscriber はこの Distribution を抽出せず、子 Subscriber にそのまま転送します。

親 Subscriber は、Distributor のルーティング階層内にあるため、Distribution にアクセスして転送します。ただし、子 Subscriber はこの Distributor にアクセスできないため、Distribution へのアクセスは親 Subscriber によって実行される必要があります。

子 Subscriber に対して親 Subscriber を指定しても、子 Subscriber は、親 Subscriber が登録された Channel に登録されたままにできます。子 Subscriber は特定の Distributor のルーティング階層にアクセスできるため、親 Subscriber が子 Subscriber に転送しなくても、2 つの Subscriber は Channel の Distribution を受信して抽出できます。重要な点は、必要な Distribution を所有する Distributor が、親 Subscriber を使用せずに子 Subscriber に Distribution を送信できるかどうかです。

ツリー間の Distribution の送信

External Subscriber を使用すると、あるツリーから別のツリーへ Distribution を送信できます。別のツリーへ送信するには、次の手順に従ってください。

1 Tiered Electronic Distribution が両方のツリーにインストールされていることを確認します。

次の手順では、TREE1 は Distribution が作成されるツリーを表し、TREE2 はその Distribution を送信する他のツリーを表します。

TREE1 から Distribution を受信する TREE2 のサーバには、Subscriber ソフトウェアをインストールする必要があります (TREE2 の Subscriber)。

Tiered Electronic Distribution のインストールについては、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「NetWare および Windows へのインストール」を参照してください。

2 TREE1 で External Subscriber オブジェクトを作成します。

このオブジェクトに指定した IP アドレスまたは DNS 名が、Distribution を送信する TREE2 の Subscriber サーバと一致していることを確認します。

External Subscriber の作成手順については、168 ページの「External Subscriber の作成と設定」を参照してください。

3 TREE1 で Distribution の Channel を作成します。

Channel の作成手順については、148 ページの「Channel の作成と設定」を参照してください。

4 ステップ 2 で作成した External Subscriber オブジェクトとステップ 3 で作成した Channel を関連付けます。

TREE1 のその他の Subscriber を、この Channel に関連付けることができます。

Subscriber と Channel の関連付けの手順については、157 ページの「Subscriber と Channel の関連付け」を参照してください。

5 TREE1 で Distribution を作成します。

Distribution の作成手順については、112 ページの「Distribution」を参照してください。

6 この Distribution をステップ 3 で作成した Channel と関連付けます。

7 TREE2 の External Subscriber サーバが Distribution を受信したことを確認します。

Tiered Electronic Distribution に関するその他の問題

- 180 ページの「File Distribution のディレクトリ同期の細分性」
- 185 ページの「Tiered Electronic Distribution の依存関係の理解」
- 185 ページの「システムリソースとサーバの動作」
- 186 ページの「I/O レートと同時に実行可能な Distribution の制御」
- 187 ページの「メッセージトラフィックの極小化」
- 188 ページの「Tiered Electronic DistributionサーバのDNS名またはIPアドレスの変更」
- 189 ページの「Tiered Electronic Distribution プロセスのエラー」

File Distribution のディレクトリ同期の細分性

File Distribution のディレクトリ同期の細分性が向上しました。

- 180 ページの「ディレクトリ同期とその細分性の理解」
- 180 ページの「ディレクトリ同期とその細分性のプロセスのしくみ」
- 183 ページの「File Distribution のディレクトリの同期」

ディレクトリ同期とその細分性の理解

File Distribution は、同期が有効か無効かにかかわらず、Subscriber サーバのファイルおよびディレクトリを追加または更新します。ただし、同期が有効の場合は、ファイルおよびディレクトリが削除されます。そのため、Subscriber サーバでのファイルおよびディレクトリの削除が、同期の主な機能です。

ディレクトリ同期の細分性により、Distribution のディレクトリレベルに同期を指定して、指定ディレクトリ以下の同期を実行できます。

ディレクトリ同期とその細分性のプロセスのしくみ

次の例は、Distribution で同期が有効になっている場合、同期された File Distribution が Subscriber サーバのファイルシステムに及ぼす結果について説明しています。

Distributor サーバに配置され、File Distribution に含まれるファイルおよびディレクトリ	Distribution の受信および抽出前の Subscriber サーバのディレクトリ
data:¥zenworks¥viruspatterns	data:¥zenworks¥viruspatterns
data:¥zenworks¥nw65sp¥nw65sp1.exe	data:¥zenworks¥nw65sp
data:¥zenworks¥nw65sp¥nw65sp2	
上記のパスの末端の項目はそれぞれ、この Distribution で同期されます。	Subscriber の ¥viruspatterns ディレクトリでファイルの 1 つがなくなると、¥nw65sp2 ディレクトリからもそれがなくなります。

File Distribution の抽出時に、Subscriber サーバのファイルシステムでは次の処理が実行されます。

1. なくなったウィルスパターンファイルが、¥viruspatterns ディレクトリに復元されます。

   ...¥viruspatterns ディレクトリに対しては、Distribution に含まれるファイルとサブディレクトリと正確に一致するように、Distribution に含まれない Subscriber のファイルまたはサブディレクトリの削除も行われます。

2. ¥nw65sp ディレクトリの nw65sp1.exe ファイルが更新されます。¥nw65sp ディレクトリ自体に対して同期が有効になっていないため、そのディレクトリのほかのファイルは同期されません。

3. ¥nw65sp2 ディレクトリとそのファイルおよびサブディレクトリが、Subscriber の ¥nw65sp ディレクトリの下にある Distribution から復元されます。

ディレクトリ同期の細分性を利用すると、一部のディレクトリを同期する一方で、他のディレクトリを同期しないままにすることもできます。たとえば、data:¥zenworks¥viruspatterns ディレクトリと data:¥zenworks¥nw65sp¥nw65sp2 ディレクトリを同期し、data:¥zenworks¥nw65sp ディレクトリを同期しないように選択できます。

ただし、親ディレクトリの data:¥zenworks ディレクトリを同期すると、同期は特定のディレクトリ以下で実行されるため、すべてのサブディレクトリが同期されます。そのため、同期するディレクトリを選択するときは、同期する親ディレクトリを選択した後で、同期しない子ディレクトリを選択することができません。

親ディレクトリが同期されるとすべての子ディレクトリも自動的に同期され、子ディレクトリのいずれかの同期が無効になると、親ディレクトリの同期も自動的に解除されます。

例：

誤	正
同期するディレクトリ： data:¥zenworks	同期するディレクトリ： data:¥zenworks¥viruspatterns data:¥zenworks¥nw65sp¥nw65sp1.exe data:¥zenworks¥nw65sp¥nw65sp2
同期しないディレクトリ： data:¥zenworks¥nw65sp	同期しないディレクトリ： data:¥zenworks data:¥zenworks¥nw65sp
¥zenworks ディレクトリを同期と、¥nw65sp ディレクトリも同期する必要があるため、これは機能しません。	同期しないディレクトリが、同期するディレクトリよりもパスの上位にあるため、これは機能します。

次の節では、同期のしくみについて説明します。

- 182 ページの「Distribution のターゲットディレクトリ以下のすべてのディレクトリの同期」
- 182 ページの「ディレクトリ同期の細分性によるさまざまなレベルのディレクトリの同期」
- 182 ページの「Distributor サーバファイルを含む Subscriber サーバディレクトリの同期」

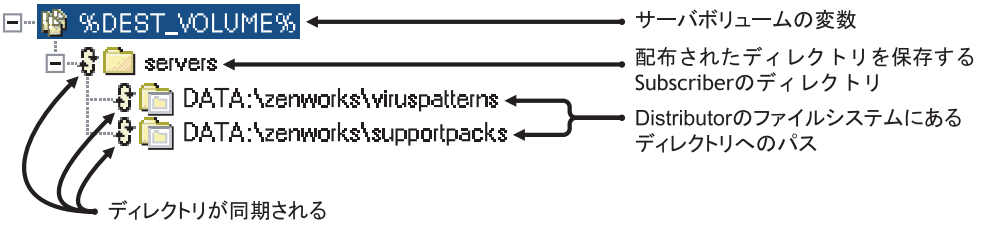
Distribution のターゲットディレクトリ以下のすべてのディレクトリの同期

ソース側で、同期する Distributor サーバのファイルシステムのディレクトリを選択します。配布先では、同期するディレクトリが Subscriber サーバのファイルシステムにすでに存在している場合としていない場合があります。

ファイルが存在する場合は、Distribution が送信されると、その内容が Distributor サーバのファイルシステム上にある対応ディレクトリの内容と一致するように更新されます。ファイルが存在しない場合は、Subscriber サーバのファイルシステムにファイルが追加されます。

これらのディレクトリが Subscriber サーバのファイルシステムに配置される場所を決めます。つまり、親ディレクトリの下に同期されたディレクトリを配置するのか、または Subscriber のファイルシステムのルートに同期されたディレクトリを配置するのかを決定します。Distribution が抽出される Subscriber サーバのファイルシステムでターゲットを指定するときは、変数を使用できます。

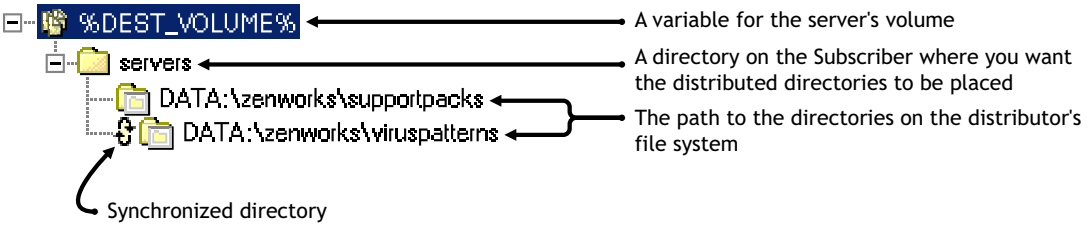
次の図では、Distributor サーバの ¥viruspatterns および ¥supportpacks ディレクトリが、Subscriber サーバの vol1:¥servers ディレクトリの下に作成され、同期されています。



ディレクトリ同期の細分性によるさまざまなレベルのディレクトリの同期

ターゲットレベル (%DEST_VOLUME%) で同期できます。前出の例では、vol1:¥servers を指定して同期を定義しました。この場合、そのディレクトリ以下のサブディレクトリは、viruspatterns と supportpacks だけです。その他の既存のサブディレクトリはすべて削除されます。

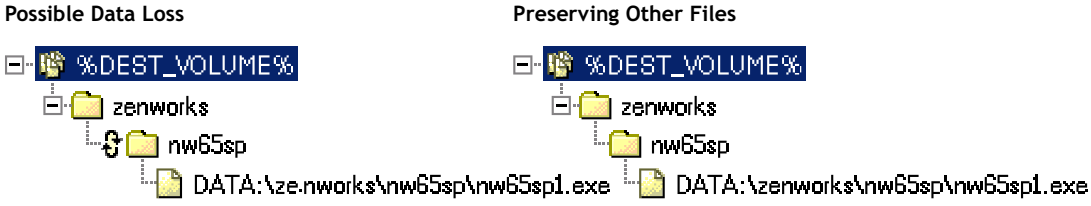
vol1:¥servers 以下のその他のディレクトリを保持するには、ターゲットレベル (%DEST_VOLUME%) での同期を無効にします。代わりに、下位ディレクトリごとに同期します。たとえば、次の図では ¥viruspatterns ディレクトリだけが同期されます。¥supportpacks など、vol1:¥servers 以下のその他のディレクトリは同期されません。



Distributor サーバファイルを含む Subscriber サーバディレクトリの同期

File Distribution に含まれる Distributor サーバのファイルが、Distribution のディレクトリと関連付けられている場合、通常は、Distribution のディレクトリを同期しません。同期すると、Subscriber サーバのディレクトリ内の大切なデータを消してしまう場合があります。

例：

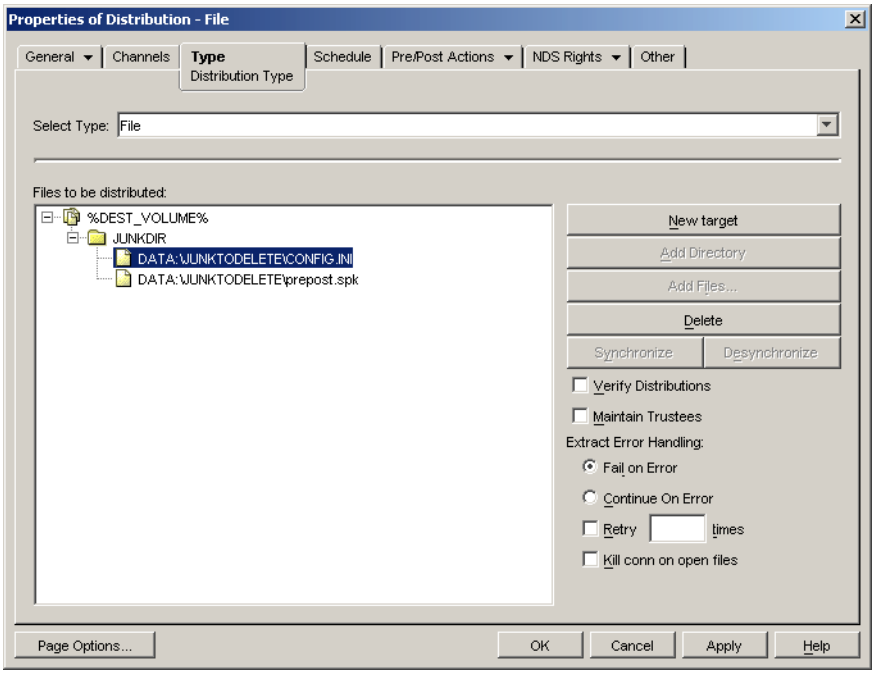


データが失われる場合、nw65sp1.exe ファイルを除く、¥nw65sp ディレクトリおよびサブディレクトリのすべてのファイルが Subscriber サーバから削除されます。その他のファイルが維持される場合は、¥nw65sp ディレクトリの nw65sp1.exe ファイルが更新され、Subscriber サーバのその他のファイルとサブディレクトリはすべて残されます。

File Distribution のディレクトリの同期

1 ConsoleOne® で、Distribution オブジェクトを右クリックし、[Properties] をクリックします。

2 [Type] タブを選択し、Distribution の File タイプを選択します。



3 [New Target] をクリックし、デフォルト変数の %DEST_VOLUME% に各 Subscriber サーバのターゲットパスを指定します。

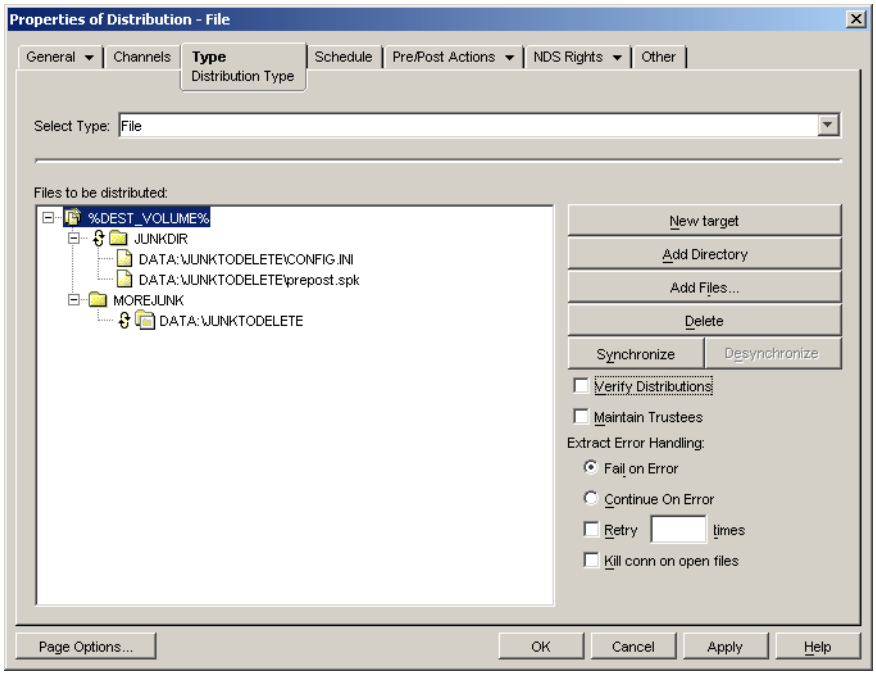
警告： ターゲットレベルで同期する場合は、この変数に、Subscriber サーバのファイルシステムのルートが含まれていないことを確認してください。

4 [Add Directory] ボタンと [Add Files] ボタンを選択して、[Files To Be Distributed] ボックスでディレクトリ構造を作成します。

[Add Directory] ボタンは、Subscriber サーバのターゲットパスとディレクトリを追加する場合に使用し、[Add Files] ボタンは、Distributor のファイルシステムを参照して Distribution に追加するディレクトリとファイルを選択する場合に使用します。

5 必要に応じてプラス記号をクリックし、ディレクトリ構造を展開します。

リストに表示されるディレクトリは、デフォルトでは、同期するものとして選択されていません。



6 同期するディレクトリを指定するには、[Files To Be Distributed] ボックスのディレクトリを選択して、[Synchronize] ボタンをクリックします。

ディレクトリ名の前に同期アイコン (🔄) が表示されます。

ディレクトリ名ではなくファイル名を選択すると、[Synchronize] ボタンと [Desynchronize] ボタンが淡色表示されます。同期を指定できるのは、ディレクトリだけです。

ディレクトリの同期は、選択したディレクトリとすべてのサブディレクトリ（指定ディレクトリ以下）で指定されるため、選択したディレクトリ以下のディレクトリを選択して同期を指定する必要はありません。

ディレクトリに同期を指定した後にそのディレクトリを展開すると、各ディレクトリ名の前に同期アイコンが表示されます。

7 同期するディレクトリの指定を解除するには、同期アイコンが表示されたディレクトリ名を選択し、[Desynchronize] ボタンをクリックします。

ディレクトリに非同期を指定すると、その親ディレクトリに同期が指定されている場合は、親ディレクトリも自動的に非同期となります。同様の処理は、すでに同期が指定されたパスを持つすべてのディレクトリ（親ディレクトリの上位を含む）について実行されます。つまり、あるディレクトリに同期を指定してから、下位のディレクトリに非同期を指定すると、親ディレクトリも必ず非同期になります。

8 同期するディレクトリごとに、ステップ 6 を繰り返します。

9 Distribution の設定を続行します。

Distribution の設定については、54 ページの「Distribution の作成と設定」を参照してください。

10 Distribution の設定を終了するには、[OK] をクリックします。

この Distribution では、同期アイコン (🔄) が表示されたディレクトリ (すべてのサブディレクトリを含む) のみが同期されます。

Tiered Electronic Distribution の依存関係の理解

Policy and Distribution Services のエージェント (Policy/Package Agent および Distributor Agent) は、eDirectory で相互に依存しています。Policy and Distribution Services を使用してネットワークを管理するには、次の依存関係を理解する必要があります。

- 185 ページの「eDirectoryのTiered Electronic Distributionオブジェクトの同期」
- 185 ページの「親 Subscriber のアップロード」

eDirectory の Tiered Electronic Distribution オブジェクトの同期

Server Management では、Tiered Electronic Distribution および Server Policies コンポーネントに必要な情報のリポジトリとして、eDirectory が使用されます。eDirectory は分散型データベースであり、ネットワーク全体でパーティションとレプリカを使用できるため、Server Management オブジェクトが作成または変更されるたびにすべてのレプリカを同期するには時間がかかります。

親 Subscriber のアップロード

親 Subscriber を変更するには、Subscriber オブジェクトの親 Subscriber 属性を変更する必要があります。Distribution が次に送信されるときに、Subscriber への配布ルートが新しい親 Subscriber に反映されます。

親 Subscriber の Java プロセスがアンロード (終了) された場合は、親 Subscriber の下位 Subscriber が他の親 Subscriber と再度通信することはありません。下位 Subscriber は、親 Subscriber が再度ロードされ、使用が続行されるまで待機します。これは、親 Subscriber が、Distributor(WAN 経由で接続) と 20 の Subscriber との間にある唯一のサーバである場合、親 Subscriber が使用できなくなったときに、すべての Subscriber が WAN 経由で Distribution を受信しないようにするためです。

システムリソースとサーバの動作

Policy and Distribution Services を使用すると、システムの動作に影響する場合があります。

- Tiered Electronic Distribution を使用すると、Distribution の送信時に発生するトラフィックによって、システムが影響を受ける場合があります。
- 一部のサーバポリシーは、サーバの停止方法など、サーバの動作を制御するものとして設計されています。
- 一部のサーバポリシーは、SET パラメータ、autoexec.ncf ファイルの内容など、NetWare サーバ設定に使用するものとして設計されています。

Tiered Electronic Distribution をインストールして使用すると、次のものが影響を受ける場合があります。

- CPU 使用率
- ディスク容量リソース

- ネットワークトラフィック
- その他の I/O アクティビティ

Tiered Electronic Distribution のインストールを最適化するには、Distributor および Subscriber サーバを選択するときに、次の点を考慮する必要があります。

- Distributor にかかる大きな負荷に対応可能なサーバはどれか

  Distribution の構築と送信に必要な CPU 速度や、Distributor のすべての Distribution を保存するのに必要なディスク容量を考慮します。

  このサーバでは、Server Management 以外のその他のネットワーク機能の実行、その他の Server Management ソフトウェアまたは Server Management 以外のソフトウェアの起動、または Distributor 機能だけの使用が可能です。

- サーバポリシーを使用して管理するサーバはどれか

  ポリシーで管理する各サーバと、ソフトウェアパッケージを配布する各サーバへの Subscriber ソフトウェアのインストールを考慮します。ポリシーエンジンが Subscriber ソフトウェアと共にインストールされ、Subscriber ソフトウェアはソフトウェアパッケージの抽出とインストールにも使用されます。

- 親 Subscriber の使用によって増加する負荷に対応可能なサーバはどれか (親 Subscriber は、Distribution を保存および転送する Distributor のプロキシとして機能するため、Distributor が Distribution をすべての Subscriber に直接送信する必要はありません。)

  Distribution 送信に必要な CPU 速度と、親 Subscriber が転送する Distribution の保存に必要な空きディスク容量を考慮します。

- 各 LAN セグメントに、親 Subscriber が使用可能なサーバがあるかどうか

  親 Subscriber の場所を決めるときは、WAN トラフィックを考慮します。

- LAN または WAN リンクに、帯域幅を使用するその他のプロセスがあるかどうか

  Distribution の優先度と、送受信レートの設定を考慮して、Distribution が WAN リンクの帯域幅に与える影響を最小限に抑えます。

I/O レートと同時に実行可能な Distribution の制御

Distribution トラフィックの帯域幅の使用を制御するには、I/O レートを設定し、同時に実行可能な Distributor および Subscriber の最大数を設定します。

Distributor オブジェクトと Subscriber オブジェクトの属性によって、次の制御を実現できます。

- **[Input Rate]**: Distribution の送受信時に使用される 1 秒あたりの最大バイト数を設定できます。Distribution は、Distributor Agent から送信され、Policy/Package Agent で受信および抽出されます。この設定により、これらのエージェントで使用される帯域幅を制御できます。デフォルト値は、その接続で処理可能な最大値です。ただし、FTP、HTTP、および RPM Distribution が Distributor で構築されるときのレートは制御できません。
- **[Output Rates Based Upon Distribution's Priority]** : デフォルトの出力レートを設定して、Tiered Electronic Distribution オブジェクトのネットワークトラフィックを最小限に抑えます。これによって、Distributor と親 Subscriber の送信速度を指定します。デフォルト値は接続で処理できる最大値です。空白は、サードパーティアプリケーションから帯域幅が割り当てられることを意味します。

出力には 3 つの優先度があり、速度を指定できます。

- **[High Priority]**： この Distribution は、[Medium Priority] または [Low Priority] の Distribution よりも前に送信されます。
- **[Medium Priority]**： この Distribution は、[High Priority] の Distribution がすべて送信された後、[Low Priority] の Distribution よりも前に送信されます。
- **[Low Priority]**： この Distribution は、[High Priority] と [Medium Priority] のすべての Distribution が送信された後で送信されます。

詳細については、128 ページの「Distribution の優先度」を参照してください。

- **[Maximum Number of Concurrent Distributions]**： Distributor Agent が同時に送信できる Distribution の数を決定します。デフォルト値は指定されていません（空フィールド）。Subscriber は、送信された数の Distribution を常に受信しますが、ここで指定した数だけしか同時に送信できません。

Subscriber が 1 つしかない場合、Distributor は選択されたレートで Distribution を送信します。Subscriber が 2 つある場合、Distribution は半分のレートで送信されます。つまり、最低速の配布レートを判断するには、Distributor の出力レートを、同時に実行可能な Distribution の最大数で割ります。

Subscriber は常に、同時に実行された別の Distribution を受信するため、受信接続の数を制限できない場合でもレートは適用されます。

メッセージトラフィックの極小化

Tiered Electronic Distribution のメッセージ通知機能を使用すると、管理者や選択したエンドユーザに情報を知らせることができます。通知は次の方法で送信されます。

- ログファイルに書き込まれる情報
- 電子メールメッセージで送信される通知
- ローカルコンソールとリモートコンソールで使用および表示される SNMP トラップ

次の節では、通知の使用方法について説明します。

- 187 ページの「メッセージ通知レベル」
- 188 ページの「LAN および WAN の使用による通知の送信」

メッセージ通知レベル

メッセージレベルには、メッセージを送信しないものから、開発者用トレースオプションまで、7 つのレベルがあります。メッセージの送信先に関係なく、リソースは、選択されたレベルから直接影響を受けます。メッセージレベルの設定については、次の手順を参照してください。

- **Distributor オブジェクト**： 109 ページのステップ 3
- **Subscriber オブジェクト**： 154 ページのステップ 3

ログファイルレベルは、ログファイルサイズの増加速度に影響します。ログファイルにはサイズの制限がないため、*x* 日数後にエントリを削除するように指定して、ログファイルのサイズを制御できます。メッセージレベルの設定については、次の手順を参照してください。

- **Distributor オブジェクト**： 108 ページのステップ 2
- **Subscriber オブジェクト**： 153 ページのステップ 2

SNMP トラップおよびリモートコンソールのレベルは、ネットワークトラフィックに最大の影響を与えます。

SNMP トラップ、電子メールメッセージ、およびサーバのコンソールのメッセージレベルの設定については、次の手順を参照してください。

- **Distributor オブジェクト：** 109 ページのステップ 3
- **Subscriber オブジェクト：** 154 ページのステップ 3

SNMP トラップ

SNMP ポリシーが受信サーバで有効になっている場合は、選択したメッセージレベルに関係なく、SNMP メッセージだけが送信されます。SNMP トラフィックは、選択したレベルと、サーバのポリシー内の SNMP 設定の両方から影響を受けます。SNMP トラップターゲットポリシーでは、送信先へのメッセージごとに 1 つの SNMP パケットが使用されます。IPX™ アドレスは、トラップターゲットではサポートされていません。

E-Mail Messages

電子メールメッセージもネットワークトラフィックに影響を与える場合があります。SNMP と同様に、電子メールは定義された電子メールユーザに対してメッセージごとに電子メールが 1 通だけ送信されます。電子メールはサーバポリシーによっても定義されます。電子メールメッセージを送信するには、送信サーバでポリシーを定義し、有効にする必要があります。

Tiered Electronic Distribution サーバの DNS 名または IP アドレスの変更

Distributor サーバまたは Subscriber サーバのいずれかの ID に変更を加えた場合は、これらのサーバの配布プロセスがこれまでどおりに実行されるように、特定のタスクを実行する必要があります。

配布プロセスでは、Tiered Electronic Distribution サーバは DNS 名または IP アドレスによって互いを認識します。次の節では、これらのサーバの ID を変更したことで発生する状況について説明します。

DNS 名を使用してサーバを識別している場合

- Distributor サーバの DNS 名を変更すると、Subscriber サーバは、Distribution の受信に有効なソースとして Distributor を識別できなくなります。
- Subscriber サーバの DNS 名を変更すると、Distributor は、Distribution の送信先として Subscriber サーバの場所を特定できなくなります。これは、Distributor が、Subscriber サーバのアドレスを eDirectory オブジェクトから取得しているためです。

Distributor または Subscriber サーバの Server Management に対する識別に DNS 名を使用している場合、これらのサーバの IP アドレスを変更しても、配布プロセスには何も影響しません。

IP アドレスを使用してサーバを識別している場合

- Distributor サーバの IP アドレスを変更すると、Subscriber サーバは、Distribution の受信に有効なソースとして Distributor を識別できなくなります。

- Subscriber サーバの IP アドレスを変更すると、Distributor は、Distribution の送信先として Subscriber サーバの場所を特定できなくなります。これは、Distributor が、Subscriber サーバのアドレスを eDirectory オブジェクトから取得しているためです。

有効な証明書の復元は、サーバ ID の解決と関連しているため、詳細については、318 ページの「無効な証明書の処理」を参照してください。

Tiered Electronic Distribution プロセスのエラー

コンピュータに関連する多くの一般的な理由により、Tiered Electronic Distribution プロセスにエラーが発生する場合があります。次に例を示します。

- **Distribution が中断される場合があります。**この場合は、送信を再度開始すると、中断した時点からの処理が継続されます。

  Distribution パッケージは、配布前は Distributor に保存されています。配布後も Distribution パッケージは Distributor に保存され、そのコピーが Subscriber に保存されます。中断によってコピーが中止されたのは、配布プロセスの途中です。Distributor がその Distribution を再度送信するとき（Channel スケジュールの次回の開始時）は、中断した時点からの処理が継続され、Distribution 全体が再送信されることはありません。

  Distribution の再送信が中断されると、送信元は 2 分ごとの再送信を 30 分間継続します。ターゲットサーバとの接続が再確立できない場合は、再送信を停止します。Channel のスケジュールが次に開始されると、Distribution の送信が最初に中断された時点からの処理が継続されます。

- **抽出が中断される場合があります。**この場合、抽出は中断した時点からは継続されません。

  Distribution は、サーバ間でネットワークを使用して送信されますが、抽出は Distribution がすでに送信されたサーバで実行されます。そのため、抽出が中断されると、そのままエラーとなります。Distribution がソフトウェアパッケージ（.cpk ファイル）でない限り、エラーになった抽出を Subscriber がロールバックする（元に戻す）ことはありません。次に Subscriber の抽出スケジュールが開始されると、抽出が再度開始されます。

  ファイルは、Distribution パッケージの作成時に指定されたボリュームおよびディレクトリに抽出されます。ファイルのグループとソフトウェアパッケージを使用すると、パッケージが抽出されるボリュームとディレクトリを指定できます。つまり、抽出の途中で中断されると、オペレーティングシステムでファイルをコピーするときと同様にエラーとなります。

- **File タイプでは次のオプションを使用できます。**
  - *X*回再試行する
  - 開いているファイルへの接続を中止する
  - エラー処理（エラー時中止、エラー時のルーチンの実行）

  すべてのオプションが抽出とその処理方法に対応しています。

作業ディレクトリ

Distributor および Subscriber は、作業ディレクトリを使用して、Distribution、パッチ、ステータスファイル、および一時作業ファイルをサーバ上に保存します。作業ディレクトリのサイズは、Distribution のサイズと数によって決定されます。

デフォルトの作業ディレクトリは、NetWare サーバでは sys: ボリューム、Windows サーバでは C: ドライブです。NetWare サーバのディスク容量を考慮して、data: ボリュームなど、サーバ上の異なる場所を選択することをお勧めします。

NetWare および Windows サーバでのデフォルトの作業ディレクトリ名は、Distributor の場合は *path*¥zenworks¥pds¥ted¥dist、Subscriber の場合は *path*¥zenworks¥pds¥ted¥sub です。Linux および Solaris サーバのパスは、/var/opt/novell/zenworks/zfs/pds/ted/working/dist および /var/opt/novell/zenworks/zfs/pds/ted/working/sub です。作業ディレクトリ名は、Tiered Electronic Distribution オブジェクトのプロパティで変更できます。

次の節では、Tiered Electronic Distribution ディレクトリ構造について説明しています。

- 190 ページの「NetWare Distributor のディレクトリ」
- 191 ページの「NetWare Subscriber のディレクトリ」
- 192 ページの「Windows Distributor のディレクトリ」
- 193 ページの「Windows Subscriber のディレクトリ」
- 193 ページの「Linux Distributor または Solaris Distributor のディレクトリ」
- 193 ページの「Linux Subscriber または Solaris Subscriber のディレクトリ」

NetWare Distributor のディレクトリ

NetWare Distributor では次のディレクトリが使用されます。

volume:¥*installation_path*¥zenworks¥pds¥ted

Distributor の Tiered Electronic Distribution ソフトウェアが保存されます。

volume:¥*installation_path*¥zenworks¥pds¥ted¥security¥private

Distributor のプライベートキーが保存されます。

volume:¥*working_directory*

Distributor に属する Distribution ごとに 1 つのディレクトリが含まれます。作業ディレクトリ名は、Distributor オブジェクトでユーザによって定義されます。

volume:¥*working_directory*¥*distribution_directory*

Distribution ごとに専用のディレクトリが作業ディレクトリの下に作成されます。Distribution ディレクトリの名前には、構文 *Tree_DN_of_Distribution* が使用されます。たとえば、TestTree_Files.Distributions.ZENworks.Novell のようになります。

volume:¥working_directory¥distribution_directory¥time_stamp_directory

各 Distribution ディレクトリには、複数のタイムスタンプディレクトリが含まれます。これらのディレクトリは Distribution が構築された日時に従って名前が付けられます。

Distribution の構築時に、Distributor は、Distribution の前回の構築後に変更されたかどうかを毎回確認します。変更されている場合は、新しいタイムスタンプディレクトリが作成されます。

タイムスタンプディレクトリの数は、Distribution オブジェクトのプロパティの [Maximum Number of Revisions to Keep] フィールドで決定されます。Distributor は使用中のタイムスタンプディレクトリを削除しないため、タイムスタンプディレクトリの数が、指定した最大数を超える場合があります。Distributor は一番古いタイムスタンプディレクトリを最初に削除します。

タイムスタンプディレクトリの名前に、_temp が追加される場合があります。Distributor は、Distribution の構築時に、変更があるかどうかを判断する前に ¥*_temp ディレクトリを作成します。変更が検出されると ¥_temp が削除され、ディレクトリは新しい構築用に使用されます。

Distributor のタイムスタンプディレクトリには、次のファイルが格納されます。

ファイル名	Description
distfile.ted	構築された Distribution。Distribution のファイル名はすべて同じです。Distribution は、タイムスタンプディレクトリの名前とパスで区別されます。
digest_file	このファイルは、Distributor Agent によって作成された場合にのみ存在します（省略可能）。 ダイジェストは、送信中に Distribution が改ざんされていないことを確認するために、Distributor と Subscriber によって使用されます。このダイジェストは、Subscriber が照合する MD5 チェックサムを提供します。 ダイジェストは、Distribution のパッケージの破損も検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。 ダイジェストファイル名の作成時には、次の構文が使用されます。 %AGENT%AgentDigest.ted 例： FTPAgentDigest.ted HTTPAgentDigest.ted FileAgentDigest.ted CPKAgentDigest.ted

NetWare Subscriber のディレクトリ

NetWare Subscriber では次のディレクトリが使用されます。

volume:¥installation_path¥zenworks¥pds¥ted

Subscriber および Distributor の Tiered Electronic Distribution ソフトウェアが保存されます。

volume:¥*installation_path*¥zenworks¥pds¥ted¥security

Distributor から受信した証明書が保存されます。

volume:¥*working_directory*

Subscriber が Distributor から受信する Distribution ごとに 1 つのディレクトリが含まれます。作業ディレクトリ名は、Subscriber オブジェクトでユーザによって定義されます。

volume:¥*working_directory*¥*distribution_directory*

Distribution ごとに専用のディレクトリが作業ディレクトリの下に作成されます。Distribution ディレクトリの名前には、構文 *Tree_DN_of_Distribution* が使用されます。たとえば、TestTree_Files.Distributions.ZENworks.Novell のようになります。

volume:¥*working_directory*¥*distribution_directory*¥*time_stamp_directory*

各 Distribution ディレクトリには、複数のタイムスタンプディレクトリが含まれます。これらのディレクトリは Distribution が構築された日時に従って名前が付けられます。

タイムスタンプディレクトリの数は、Distribution オブジェクトのプロパティの [Maximum Number of Revisions to Keep] フィールドで決定されます。

しきい値に達すると、Subscriber は最大リビジョン情報を受信して、一番古いタイムスタンプディレクトリを最初に削除します。

Subscriber のタイムスタンプディレクトリには、次のファイルが格納されます。

ファイル名	Description
distfile.ted	構築された Distribution。Distribution のファイル名はすべて同じです。Distribution は、タイムスタンプディレクトリの名前とパスで区別されます。
diststatus.ted	Distribution の受信に成功すると、このファイルが作成されます。
digest_file	このファイルは、Distributor Agent によって作成された場合にのみ存在します（省略可能）。 ダイジェストは、送信中に Distribution が改ざんされていないことを確認するために、Distributor と Subscriber によって使用されます。このダイジェストは、Subscriber が照合する MD5 チェックサムを提供します。 ダイジェストは、Distribution のパッケージの破損も検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。

Windows Distributor のディレクトリ

Windows Distributor では次のディレクトリが使用されます。

installation_path¥zenworks¥pds¥ted

Distributor の Tiered Electronic Distribution ソフトウェアが保存されます。

installation_path¥zenworks¥pds¥ted¥security¥private

Distributor のプライベートキーが保存されます。

Windows Subscriber のディレクトリ

Windows Subscriber では次のディレクトリが使用されます。

installation_path¥zenworks¥pds

Subscriber の Tiered Electronic Distribution ソフトウェアが保存されます。

installation_path¥zenworks¥pds¥ted¥security¥private

Distributor から受信した証明書が保存されます。

local_drive:¥*working_directory*¥*distribution_directory*¥*time_stamp_directory*

各 Distribution ディレクトリには、複数のタイムスタンプディレクトリが含まれます。これらのディレクトリは Distribution が構築された日時に従って名前が付けられます。

Linux Distributor または Solaris Distributor のディレクトリ

Linux Distributor または Solaris Distributor では次のディレクトリが使用されます。

/var/opt/novell/zenworks/zfs/pds/ted/working/dist

Distributor の Tiered Electronic Distribution ソフトウェアが保存されます。

/var/opt/novell/zenworks/zfs/pds/ted/security/private

Distributor のプライベートキーが保存されます。

各 Distribution ディレクトリには、複数のタイムスタンプディレクトリが含まれます。これらのディレクトリは Distribution が構築された日時に従って名前が付けられます。

Linux Subscriber または Solaris Subscriber のディレクトリ

Linux Subscriber または Solaris Subscriber では次のディレクトリが使用されます。

/var/opt/novell/zenworks/zfs/pds/ted/working/sub

Subscriber の Tiered Electronic Distribution ソフトウェアが保存されます。

/var/opt/novell/zenworks/zfs/pds/ted/security/private

Distributor から受信した証明書が保存されます。

各 Distribution ディレクトリには、複数のタイムスタンプディレクトリが含まれます。これらのディレクトリは Distribution が構築された日時に従って名前が付けられます。

Tednode.properties ファイルの編集

Microsoft ドメインの Windows サーバなど、eDirectory ツリーに Subscriber オブジェクトがないサーバに Subscriber ソフトウェアをインストールする場合、このようなサーバでは設定情報に tednode.properties ファイルが使用されます。Subscriber の設定を変更したときは、この節の情報を使用してサーバの tednode.properties ファイルを編集する必要があります。

tednode.properties ファイルは、サーバの zenworks¥pds¥ted ディレクトリに格納されています。

必要なファイル形式と、エントリに関するコメントを次に示します。= 記号の右側に示された情報は一例であり、その行に必要な値ではありません。ただし、この例では、値に使用される正確な構文が示されています。

行の内容	コメント
workingdir = d:¥ted¥tran	Subscriber の作業ディレクトリ
io.input = 100	受信レート (1 秒あたりのバイト数)
io.output = 1	送信レート (1 秒あたりのバイト数)
variable1 = vol=sys:	変数 vol に値 sys: を定義する
variable1.description = Destination Volume	変数の機能の説明
console.level = 6	サーバのコンソールのメッセージレベル
log.level = 1	ログファイルのメッセージレベル
log.days = 1	ログファイルのエントリを保存する日数
log.path = d:¥¥ted¥¥tran¥¥log.txt	ログファイルのパスとログファイル名
workorder.timeout = 0	接続を中止するまで Distributor からの応答を待つ秒数。0 = 制限なし
workorder.concurrent = 0	同時に実行可能な Distribution
email.level = 0	電子メールのメッセージレベル
smtp.host = email.novell.com	SMTP ホストの場所
snmp.level = 0	SNMP トラップのメッセージレベル
email.target1 = johndoe@novell.com	メッセージの送信先の電子メールアドレス

tednode.properties ファイルの残りのエントリでは、行から # (コメント) 記号を削除して、その行を有効にします。# 記号を削除すると、その行の下に記述されているスケジュールタイプが有効になります。ただし、スケジュールタイプの最初の行は、スケジュールタイプの説明であるため、この行から # 記号を削除しないでください。記載されているデフォルト値は変更できます。

次の例では、適切な # 記号が削除され、毎日実行されるスケジュールが有効になっています。

行の内容
Yearly schedule and associated keys (with default values specified) #schedule.type=yearly #schedule.month=1 #schedule.day=1 #schedule.begin.hour=8 #schedule.begin.minute=0 #schedule.end.hour=17 #schedule.end.minute=0 #schedule.random=false
Monthly schedule and associated keys (with default values specified) #schedule.type=monthly #schedule.day=1 #schedule.begin.hour=8 #schedule.begin.minutes=0 #schedule.end.hour=17 #schedule.end.minute=0 #schedule.random=false

# Daily schedule and associated keys (with default values specified) 	
schedule.type=daily
schedule.days=Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday
schedule.begin.hour=8
schedule.begin.minutes=0
schedule.end.hour=17
schedule.end.minute=0
schedule.repeat.days=0
schedule.repeat.hours=0
schedule.repeat.minutes=0
schedule.random=false

Immediate schedule and associated keys (with default values specified) #schedule.type=immediately #schedule.repeat.days=0 #schedule.repeat.hours=0 #schedule.repeat.minutes=0
Interval schedule and associated keys (with default values specified) #schedule.type=interval #schedule.repeat.hours=0 #schedule.repeat.minutes=0
Never schedule and associated keys (with default values specified) #schedule.type=never
Time schedule and associated keys (with default values specified) #schedule.type=time #schedule.date.year=2001 #schedule.date.month=1 #schedule.date.day=1 #schedule.begin.hour=8 #schedule.begin.minutes=0

4 Server Policies（サーバポリシー）

Novell® ZENworks® Server Management には、サーバの設定、処理、および動作を管理するためのサーバポリシーが用意されています。

次の節では、ポリシーの理解、設定、および設定に役立つ情報を示します。

- 197 ページの「サーバポリシーについて」
- 208 ページの「ポリシーパッケージの作成」
- 210 ページの「サーバポリシーの設定」
- 236 ページの「ポリシーの有効化」
- 236 ページの「ポリシーの配布」
- 237 ページの「ポリシーの関連付け」
- 238 ページの「ポリシーのスケジュール設定」
- 238 ページの「有効なポリシーの表示」
- 238 ページの「ポリシー適用の変更」

サーバポリシーについて

ZENworks 6.5 Server Management では、多くのポリシーはポリシーパッケージの配布によって適用されます。ただし、Distributor で使用される一部のポリシーは、Novell eDirectory™ コンテナに関連付けられることによって適用されます。

ZENworks 6.5 Server Management のポリシーを理解するには、次の節を参照してください。

- 198 ページの「サーバポリシーによる設定および動作の管理」
- 198 ページの「サーバポリシーとポリシーパッケージ」
- 199 ページの「ポリシーの特性」
- 200 ページの「サーバポリシーのアーキテクチャ」
- 203 ページの「ポリシーの適用」
- 205 ページの「サーバポリシーの説明」

サーバポリシーによる設定および動作の管理

Server Policies コンポーネントによって、サーバの設定および動作を管理できます。ポリシーのスケジュール設定および該当するサーバへのポリシーの配布を容易にするために、サーバポリシーは 3 つのパッケージに分かれています。

- **Container Package:** Policy and Distribution Servicesによってポリシーに関連付けられたオブジェクトを eDirectory 内で検索する方法を指定する検索ポリシーを保持します。
- **Service Location Package:** Policy and Distribution Services の実行に固有のポリシーを保持します。
- **Distributed Server Package:** すべてのサーバに適用できる一般的なポリシーのセット、および特定のプラットフォームのサーバ用のポリシーパッケージのセットが含まれます。このパッケージは、適用のために配布されるポリシーを提供します。

環境設定ポリシーは、選択した SET パラメータの適用など、サーバ上でタイプが類似している設定を作成する eDirectory 内の情報を保持します。動作ポリシーは、サーバの停止など、特定の状況で従うルールのセットを保持します。

サーバポリシーによってサーバの管理を自動化でき、ConsoleOne® および Novell iManager での ZENworks Server Management の役割によって 1 台のワークステーションからポリシーを設定し、サーバを管理できます。

サーバポリシーとポリシーパッケージ

サーバポリシーによって、特定のサーバのセットの環境設定パラメータを設定、標準化、および自動化できます。サーバの停止など、特定の状況でのサーバの動作を制御できます。

次の節を参照してください。

- 198 ページの「ポリシーの作成」
- 198 ページの「ポリシーのスケジュール設定」
- 199 ページの「有効にしたすべてのポリシーが適用される」
- 199 ページの「個々のポリシーの変更はポリシーパッケージとは連動していない」

ポリシーの作成

サーバポリシーを使用するには、ConsoleOne で適切なポリシーパッケージオブジェクトを作成し、サーバで必要なポリシーを設定して有効化し、パッケージのポリシーが適用される Subscriber サーバにパッケージを配布します。

ポリシーのスケジュール設定

サーバポリシーを設定する場合、毎日、毎週、毎月、毎年、イベントごとに、特定の日時に、日時から相対的に、時間間隔によって、またはすぐに実行するようにポリシーのスケジュールを設定できます。個々のポリシーのデフォルトのスケジュールは、ポリシーパッケージのスケジュールです。したがって、パッケージのデフォルトのスケジュールを変更した場合、パッケージ内のスケジュールが指定されていないポリシーでは、パッケージの新しいスケジュールが使用されます。

有効にしたすべてのポリシーが適用される

ポリシーパッケージに含まれる Policy and Distribution Services のポリシーの一部またはすべてを実装（有効化）することができます。必要な環境設定のセットごとにポリシーパッケージオブジェクトを作成することもできます。たとえば、一部のサーバを異なる方法で停止する場合に、異なるポリシーパッケージを使用します。

パッケージ内で有効になっているすべてのポリシーは、Policy Package Distribution が受信および抽出されたすべてのサーバに適用されます。つまり、パッケージ内の特定のポリシーを選択的に適用することはできません。パッケージ内で有効になっているすべてのポリシーがサーバに適用されます。

個々のポリシーの変更はポリシーパッケージとは連動していない

ポリシーパッケージ内の各ポリシーは eDirectory にそれぞれの（隠し）オブジェクトを持つので、（[OK] をクリックするか、または [Apply]、[Close] の順にクリックして）ポリシーのダイアログボックスを終了したときに保存されるポリシーに対する変更は、ポリシーパッケージのダイアログボックスで [Cancel] をクリックしても元に戻りません。

ポリシーパッケージのプロパティページで [Cancel] をクリックした場合、パッケージに対して行った変更だけがキャンセルされます。たとえば、ポリシーの有効化や無効化、ポリシーの追加や追加したポリシーの削除などです。

ポリシーを無効にしても、以前にそのポリシーで行った設定は元に戻りません。ポリシーの設定の変更はそのまま残りますが、ポリシーを無効にしたので使用されません。

ポリシーの特性

ポリシーには、その使用方法を決定する 2 つの側面があります。

- 199 ページの「複数ポリシーと累積ポリシー」
- 200 ページの「環境設定ポリシーと動作ポリシー」

複数ポリシーと累積ポリシー

ポリシーパッケージには、複数ポリシーと累積ポリシーの両方が含まれる場合があります。複数ポリシーはすべて累積ポリシーですが、累積ポリシーは必ずしも複数ポリシーというわけではありません。詳細については、次の節を参照してください。

- 199 ページの「複数ポリシー」
- 200 ページの「累積ポリシー」

複数ポリシー

複数ポリシーは、ポリシーパッケージごと、プラットフォームごとに複数のポリシーが含まれる可能性があるポリシーです。

たとえば、1 つのポリシーパッケージに、Scheduled Down ポリシーを追加および設定して、「Scheduled Down for Time A」という名前を付けます。次に、別の Scheduled Down ポリシーを追加および設定し、「Scheduled Down for Time B」という名前を付けることができます。

ポリシーが複数ポリシーであるかどうかを確認するには、[Policies] タブを表示し、[Add] をクリックします。複数ポリシーはすべて [Add] ダイアログボックスに表示されます。

累積ポリシー

累積ポリシーは、複数のポリシーパッケージをサーバに配布したときに、同じポリシーを複数有効にすることができるポリシーです。たとえば、サーバ A に配布された Text File Changes ポリシーに、サーバ A に配布された設定の異なる Text File Changes ポリシーが累積される場合があります。両方のポリシーによるテキストファイルの変更内容はすべて、サーバ A で有効になります。

環境設定ポリシーと動作ポリシー

1 つの環境設定ポリシーを、1 台のサーバまたは複数のサーバの環境設定に反映させることができます。たとえば、ポリシーが定期的に実行されるようにスケジュールを設定し、常にサーバの設定が正しく設定されるようにすることができます。

動作ポリシーには、特定の状況で従う必要があるルールのセットが含まれています。ポリシーエンジンは、これらのルールを、そのサポートモジュールと共に実行します。

たとえば、サーバダウンプロセスポリシーでは、サーバを停止する前に満たしていなければならない次のような条件を定義します。

- サーバを停止するどれくらい前にユーザに通知するか
- ポリシーを適用するときに誰に通知するか
- サーバが稼動状態に復帰しない場合にどのピアサーバがSNMPアラートを送信するか

動作ポリシーは、サーバのインテリジェント機能を向上させ、管理者が気付かないような状況を処理し、管理者のわずらわしさを緩和することを目的として設計されています。

環境設定ポリシーと動作ポリシーの利点をまとめると次のようになります。

- 通常管理者が実行するタスクの自動化
- 指定したユーザにサーバの停止を電子メールで通知
- 特定の状況でのサーバダウンプロセスの中断が可能

サーバポリシーのアーキテクチャ

サーバポリシーを使用してサーバを管理する方法を理解するには、サーバポリシーの eDirectory オブジェクトとそのエージェントについて理解する必要があります。

- 200 ページの「サーバポリシー用の eDirectory スキーマ拡張」
- 203 ページの「Policy/Package Agent」

サーバポリシー用の eDirectory スキーマ拡張

Server Policies コンポーネントに含まれる eDirectory スキーマ拡張は、オブジェクトの作成時に必須および省略可能な情報など、eDirectory ツリーに作成される eDirectory オブジェクトのクラスを定義します。eDirectory ツリー内の Server Policies コンポーネントに関連付けられた各オブジェクトには、ツリーのスキーマ内でそのオブジェクト用に定義されたクラスがあります。

eDirectory スキーマの Server Management オブジェクトは次のとおりです。

Container Package
Server Package
Service Location Package
Distributed Server Package
ZENworks Database

ポリシーの適用については、次の点に注意してください。

- Distributed Server Package 内のどのポリシーも、適用するには配布する必要があります。
- Container Package、Server Package、および Service Location Package 内のどのポリシーも、適用するには関連付ける必要があります。

Server Management 属性の追加によって変更される既存の eDirectory クラスは次のとおりです。

Country
Group
Locality
Organization
Organizational Unit
Server

次の節では、Server Policies コンポーネントによって提供されるスキーマ拡張から eDirectory に追加される主な eDirectory オブジェクトの概要を示します。

- 201 ページの「コンテナパッケージオブジェクト」
- 201 ページの「サーバパッケージオブジェクト」
- 202 ページの「SLP オブジェクト」
- 202 ページの「配布されたサーバパッケージ (Distributed Server Package)」
- 202 ページの「ZENworks データベースオブジェクト」

eDirectory ツリー内のオブジェクトのタイプに関する基本的な情報については、Novell Documentation Web サイト (http://www.novell.com/documentation/lg/nw5/docui/index.html) で、「Procedures」>「Planning」>「Directory Services」>「eDirectory Planning」の順に選択してください。

コンテナパッケージオブジェクト

コンテナパッケージオブジェクトは、検索ポリシーオブジェクトを管理する eDirectory オブジェクトです。このポリシーは、Server Management のすべてのバージョンの Distributor および Subscriber オブジェクトによって使用され、適用するには関連付ける必要があります。

サーバパッケージオブジェクト

サーバパッケージオブジェクトは、ZENworks Server Inventory の次のポリシーオブジェクトを管理する eDirectory オブジェクトです。

Rollup Policy
zeninvDictionaryUpdatePolicy
ZENworks Database

このパッケージ内のどのポリシーも、適用するには関連付ける必要があります。

Policy and Distribution Services では、このパッケージは使用されません。

SLP オブジェクト

SLP オブジェクトは、次のポリシーオブジェクトを管理する eDirectory コンテナオブジェクトです。

- SMTP Host
- SNMP Trap Targets
- Tiered Electronic Distribution
- ZENworks Database

Service Location Package ポリシーは、Policy and Distribution Services の一般的な環境設定と場所の情報を提供します。

このパッケージ内のどのポリシーも、適用するには関連付ける必要があります。

すべてのポリシーは、ZENworks 6.5 Server Management Distributor および Subscriber によって使用されます。

配布されたサーバパッケージ (Distributed Server Package)

Distributed Server Package オブジェクトは、次のポリシーオブジェクトを管理する eDirectory オブジェクトです (ZENworks 6.5 Server Management のみ)。

- Copy Files
- NetWare Set Parameters
- Prohibited File
- Scheduled Down
- Scheduled Load/Unload
- Server Down Process
- Server Scripts
- SMTP Host
- SNMP Community Strings
- SNMP Trap Targets
- Text File Changes
- ZENworks Database
- ZENworks Server Management

Distributed Server Package ポリシーは、サーバの環境設定、サーバの動作の制御、および Server Management の一般的な環境設定と場所情報の提供のために使用されます。

このパッケージ内のどのポリシーも、適用するには配布する必要があります。

ZENworks データベースオブジェクト

レポーティング情報のログを記録するための zfslog.db ファイルの場所を提供します。データベースファイルは、NetWare® サーバおよび Windows サーバにのみインストールできます。

ZENworks データベースオブジェクトは、ツリー内に複数存在し、それぞれにデータベースファイルが関連付けられている場合がありますが、サーバごとにインストールできるデータベースファイルは 1 つだけです。

Server Policies コンポーネントは、ポリシー情報を Server Management データベースファイル (zfslog.db) に書き込みます。ネットワーク内の各サーバで Policy/Package Agent を実行できるので、それぞれが、WAN リンク経由でもデータベースに書き込むことができます。すべてのサーバを対象にした統合サーバポリシーレポートが不要な場合は、各 WAN セグメントにデータベースをインストールできます。

統合サーバポリシーレポートが必要な場合は、Policy/Package Agent を実行するすべてのサーバが情報を記録できる zfslog.db ファイルを 1 つだけ使用できます。Policy/Package Agent がデータベースに書き込むデータ量では、サーバの数と WAN リンクの速度によって、過剰な WAN トラフィックが発生しない場合があります。

Server Management データベースは複数のサーバにインストールできるので、WAN トラフィックを最小限に抑えるために、WAN セグメント上のコンテナでのポリシーパッケージオブジェクトと ZENworks データベースオブジェクトの配置を調整する必要があります。

Policy/Package Agent

Policy and Distribution Services によって、Policy/Package Agent を使用してネットワークサーバを管理できます。このエージェントは、[Subscriber/Policies] インストールオプションを選択した各サーバにインストールされます。

Policy/Package Agent は次の処理を行います。

- ソフトウェアパッケージの内容を抽出 (インストール) します。
- Policy Package Distribution からポリシー情報を抽出します。
- 抽出されたポリシー情報から適用スケジュールに基づいて有効なポリシーを適用します。

サーバの環境設定および動作を管理するためのサーバポリシーは数多く存在します。ポリシーを使って管理する各サーバや、ソフトウェアパッケージを抽出してインストールする各サーバでは、Policy/Package Agent が実行されている必要があります。

ネットワーク内の各サーバに Policy/Package Agent をインストールする必要があります。例外は、ソフトウェアパッケージを配布する必要がないサーバや、ポリシーを使用した管理しないサーバです。

ポリシーの適用

ZENworks 6.5 Server Management の多くのポリシーは、ポリシーパッケージを作成し、ポリシーを有効にして設定し、パッケージのスケジュールを設定し、パッケージを配布し、サーバ上でポリシーを抽出することによって適用されます。

ZENworks 6.5 Server Management の一部のポリシーは、ポリシーパッケージを作成し、ポリシーを有効にして設定し、パッケージのスケジュールを設定し、Distributor または Subscriber オブジェクトが存在するコンテナにパッケージを関連付けることによって適用されます。

詳細については、次の節を参照してください。

- 204 ページの「ポリシーのスケジュール設定」
- 204 ページの「ポリシーの配布」
- 204 ページの「ポリシーの関連付け」

ポリシーのスケジュール設定

一部のサーバポリシーは、適用するためにスケジュールを設定する必要があります。

次のようなスケジュールを利用できます。

- デフォルトパッケージスケジュール(いずれかのスケジュールに設定できる)によってアクティブにする
- 指定したイベントでアクティブにする (システムの起動またはシャットダウン時に実行するなど)
- 特定の期間に 1 回アクティブにする
- 指定した日時にアクティブにする
- 年に 1 回指定した時刻にアクティブにする
- 月に 1 回指定した時刻にアクティブにする
- 週の 1 つ以上の曜日の指定した時刻にアクティブにする
- 週の 1 つ以上の曜日に、指定した時間間隔で繰り返しアクティブにする
- 指定した時間間隔で継続的に繰り返す
- すぐに実行する
- すぐに実行し、指定した時間間隔で繰り返す

重要： ポリシーを有効にしても、スケジュール設定していない場合、デフォルトパッケージスケジュールで現在指定されているスケジュールに従ってアクティブになります。

デフォルトパッケージスケジュールは、ポリシーパッケージでスケジュール設定されていないポリシーのデフォルトになります。デフォルトのスケジュールは、[Run At System Startup event] です。

ポリシーの配布

Distributed Server Package に含まれるポリシーを有効にして設定した後、有効にしたポリシーが実行される Subscriber サーバにそのポリシーパッケージを配布する必要があります。つまり、ポリシーを設定して有効にしても、ポリシーがセットアップされるだけです。Policy and Distribution Services を実行している対象のサーバに配布して抽出することによって、ポリシーが適用されます。

ポリシーの関連付け

Service Location Package に含まれるポリシーを有効にして設定した後、有効にしたポリシーが実行されるようにするには、Distributor または Subscriber オブジェクトが存在するコンテナに、ポリシーパッケージを関連付ける必要があります。この関連付けは、Distributor または Subscriber オブジェクトが存在するコンテナに対して直接行うことも、これらのオブジェクトを保持するコンテナよりもツリー内で上位にあるコンテナに対して行うこともできます。

ポリシーを設定して有効にしてもポリシーがセットアップされるだけなので、ポリシーは Policy and Distribution Services を実行している該当するサーバに関連付けることによって適用されます。

サーバポリシーの説明

次の表は、ポリシーパッケージごとのサーバポリシーの一覧です。2 番目の列には、ポリシーが環境設定ポリシーまたは動作ポリシーのいずれであるか、および累積、複数、または両方のいずれであるかが示されます。

- 205 ページの「Container Package」
- 205 ページの「Service Location Package」
- 206 ページの「Server Package」
- 207 ページの「配布されたサーバパッケージ (Distributed Server Package)」

Container Package

ポリシー名	ポリシータイプキー	ポリシーの機能
Search	動作	検索ポリシーを設定しない場合、デフォルトでは、1 時間ごとに親コンテナからルートまでが検索されます。ただし、これでは不要な検索トラフィックが発生します。そのため、効率的に検索ポリシーを使用することをお勧めます。 この検索ポリシーは ConsoleOne でのみ管理できます。NetWare Administrator for ZENworks で作成した検索ポリシーは、Server Management では認識されません。

Server Management では、大半のポリシーが割り当てではなく配布を通じて適用されますが、配布元には配布が渡されません。そのため、Server Management では配布元エージェントが検索ポリシーを使用して SLP のプロパティパッケージ内のポリシーを検索して使用できるようになっています。たとえば、Distributor Agent は、このパッケージの ZENworks データベースポリシーを使用して、レポーティング情報を ZENworks Server Management データベースファイルに書き込みます。

Distributor は、Subscriber 用の Service Location Package ポリシーを読み込みます。つまり、Subscriber は関連付けによって Service Location Package ポリシーを受信します。

Service Location Package

ポリシー名	ポリシータイプキー	ポリシーの機能
SMTP Host	環境設定	外部に発信されるインターネット電子メールを処理するリレーホストの TCP/IP アドレスを設定します。他のポリシーでメッセージを通知したり、記録するために電子メールオプションを選択した場合は、このポリシーを有効にしなければなりません。

ポリシー名	ポリシータイプキー	ポリシーの機能
SNMP Trap Targets	環境設定	関連する eDirectory オブジェクトの SNMP トラップターゲットを設定します。 ZENworks 6.5 Server Management では、このポリシーのスケジュールを、更新したい時期に設定できます。 SNMP トラップターゲットでは、IPX™ アドレスはサポートされていません。IP アドレスと DNS 名のみ使用できます。
Tiered Electronic Distribution	環境設定	Distributor オブジェクトと Subscriber オブジェクトの次のようなデフォルト値を設定します。 I/O レート 最大同時 Distribution 数 分単位の接続タイムアウト 作業ディレクトリ 親 Subscriber サーバのコンソール、SNMP トラップ、ログファイル、および電子メール通知のメッセージレベル 抽出スケジュール 更新スケジュール 変数 ここで設定したすべてのデフォルト値は、Tiered Electronic Distribution オブジェクトの変更されていないデフォルト値よりも優先されます。ただし、Tiered Electronic Distribution オブジェクトのプロパティが変更されている場合は、変更された値は、Tiered Electronic Distribution ポリシーで設定されているデフォルト値よりも優先されます。
ZENworks Database	環境設定	ZENworks データベースオブジェクトとデータベースファイルの場所を特定するための DN を設定します。データベースは、レポートの作成時に使用される成否のログを記録するために使用されます。 このポリシーを作成すると、Policy and Distribution Services のインストール時に設定されたデータベース設定を変更できます。 Policy/Package Agent と Distributor Agent はどちらも zfslog.db に書き込みます。これらのエージェントが異なるデータベースファイルに書き込むようにする方法については、367 ページの「データベースの共有」を参照してください。

Server Package

ZENworks 6.5 Server Management では、Server Package は Server Inventory で使用するためにのみ存在しています。このパッケージに含まれる ZENworks データベースポリシーは、Server Inventory をインストールするときにインストールプログラムによって自動的に作成され、インベントリデータを記録するためのデータベースの自動検索が有効になります。

Policy and Distribution Services では、このパッケージは使用されません。

このパッケージには他のポリシーも存在しますが、次の表には ZENworks データベースポリシーだけが示されています。

ポリシー名	ポリシータイプキー	ポリシーの機能
ZENworks Database	環境設定	ZENworks データベースオブジェクトの場所を特定するための DN を設定します。Server Inventory でインベントリデータを記録するためのデータベースを検索するには、このポリシーが有効になっている必要があります。

配布されたサーバパッケージ (Distributed Server Package)

このパッケージには、Server Management サーバ上でポリシーを適用するために Server Management サーバに配布する必要があるポリシーが含まれています。

ポリシー名	ポリシータイプキー	ポリシーの機能
Copy Files	複数 累積 環境設定	ポリシー設定を使用して、サーバ上のファイルを特定の場所から別の場所にコピーできるようにします。
NetWare Set Parameters	複数 累積 環境設定	サーバまたはサーバのグループに対して、選択されている設定パラメータを指定および最適化します。 このポリシーは、NetWare プラットフォームでのみ使用できます。
Prohibited File	複数 累積 環境設定	指定したボリューム / ドライブまたはディレクトリ / フォルダからの許可されていないファイルの削除や移動を監視および強制します。
Scheduled Down	複数 累積 環境設定 動作	サーバを停止するタイミングをスケジュールしたり、停止したサーバを自動的に再起動するかどうかを指定します。このポリシーには、サーバを停止するために使用するコマンド (RESET、RESTART、または DOWN) も指定されます。
Scheduled Load/ Unload	複数 累積 環境設定	選択したサーバの NLM™ および Java Class プロセスのロードとアンロードを自動化し、Windows サービスを開始および停止します。アンロードするためにユーザ入力を必要とする NLM ファイルを自動化することはできません。
Server Down Process	動作	サーバを停止する前に従うプロセスや満たす必要がある条件を制御します。
Server Scripts	複数 累積 環境設定	サーバ上でのスクリプトの使用を自動化します。
SMTP Host	環境設定	外部に発信されるインターネット電子メールを処理するリレーホストの TCP/IP アドレスを設定します。他のポリシーでメッセージを通知したり、記録するために電子メールオプションを選択した場合は、このポリシーを有効にしなければなりません。
SNMP Community Strings	環境設定	SNMP 要求を受信し、応答できるようにします。

ポリシー名	ポリシータイプキー	ポリシーの機能
SNMP Trap Targets	環境設定	関連する eDirectory オブジェクトの SNMP トラップターゲットを設定します。 このポリシーのスケジュールは更新したい時期に設定できます。 SNMP トラップターゲットでは、IPX アドレスはサポートされていません。IP アドレスと DNS 名のみ使用できます。
Text File Changes	複数 累積 環境設定	テキストファイルに対する変更を自動化します。
ZENworks Database	環境設定	ZENworks データベースオブジェクトとデータベースファイルの場所を特定するための DN を設定します。データベースは、レポートの作成時に使用される成否のログを記録するために使用されます。 このポリシーを作成すると、Policy and Distribution Services のインストール時に設定されたデータベース設定を変更できます。 Policy/Package Agent と Distributor Agent はどちらも zfslog.db に書き込みます。これらのエージェントが異なるデータベースファイルに書き込むようにする方法については、367 ページの「データベースの共存」を参照してください。
ZENworks Server Management	環境設定	ステータスログの記録、Policy/Package Agent のサーバコンソールプロンプトの定義、作業パスの設定、データベースのパージ範囲の設定など、Policy and Distribution Services の基本的な環境設定パラメータが含まれています。 このポリシーは、サーバポリシーを適用する各サーバ上で有効にすることができます。ただし、このポリシーを有効にしない場合、Policy and Distribution Services はあらかじめプログラムされたデフォルト値を使用して動作します。

ポリシーパッケージの作成

Policy and Distribution Services では、サーバポリシーを 3 つのポリシーパッケージオブジェクトにグループ化しています。

- Container Package
- Service Location Package
- Distributed Server Package (ZENworks 6.5 Server Management のみ)

ポリシーパッケージは、ツリー内の任意の場所に配置できます。管理を容易にするために、ポリシーパッケージをグループ化するための OU コンテナを作成することをお勧めします。たとえば、Policies などです。

ただし、ツリーに ZENworks Desktop Management をインストールしている場合は、Server_Policies と Desktop_Policies のように、Server Management と Desktop Management のポリシーを別のコンテナに保存しておくことができます。

重要： WAN を介してアクセスされるパーティションがある場合は、Policy/Package Agent がロードされるように、ポリシーパッケージオブジェクトをサーバオブジェクトと同じパーティションに配置してください。また、検索ポリシーで、サーバオブジェクトが存在するパーティション以外のパーティションを検索する必要がないようにしてください。

どのようなポリシーパッケージオブジェクトを作成するかを決定するには、必要なポリシーを決定します。

Policy Package オブジェクトを作成するには、次の節の手順を参照してください。

- 209 ページの「ポリシーコンテナの作成」
- 209 ページの「ポリシーパッケージオブジェクトの作成」

ポリシーコンテナの作成

ポリシーパッケージオブジェクトを保持するための OU コンテナオブジェクトを作成するには

1 ConsoleOne で、ポリシーコンテナを配置するコンテナを右クリックします。

重要： OU を作成する場所、および OU の名前に使用する文字数は、複数ポリシーの名前に使用できる文字数に直接影響します。eDirectory では、ポリシーのフルネームおよびツリー内のパスに 64 文字の制限があります。

ポリシーパッケージ内で 1 つの複数ポリシーの複数のバージョンを保持できるので、ポリシーにわかりやすい名前を付けたい場合があります。したがって、ツリー内のできるだけ上位にこの OU を配置し、短い名前を付けて、ポリシー名にできるだけ多くの文字数を使用できるようにします。

2 [New] > [Object] の順にクリックし、[Organizational Unit] を選択します。

3 OU の名前を入力し、[OK] をクリックします。

ポリシーパッケージオブジェクトの作成

ポリシーパッケージオブジェクトを作成するには

1 ConsoleOne で、ポリシーパッケージオブジェクト用に作成したコンテナを右クリックし、[New] をクリックし、[Policy Package] を選択します。

Policy Package ウィザードが表示されます。

2 [Policy Packages] の下で、ポリシーパッケージを選択し、[Next] をクリックします。

利用できるパッケージには、Container、Server、Service Location、および Distributed Server があります。

3 パッケージの名前を入力し、[Next] をクリックします。

同じタイプのパッケージを複数使用できるので、各パッケージについて、一意でわかりやすい名前を使用します。

重要： eDirectory にはパス / 名前に 64 文字の制限があり、ここで指定するパッケージ名は後で作成できる複数ポリシーの名前の一部になるので、簡潔であるが一意のポリシーパッケージオブジェクト名を指定して、できるだけ多くの文字を使用してわかりやすい複数ポリシー名を付けることができるようにします。

4 作成する各パッケージについて、手順 2 およびステップ 3 を繰り返します。

保存してステップ 1 を繰り返すには、[Create Another Policy Package] チェックボックスをオンにします。

サーバポリシーの設定

コンテナ、サーバ、およびサービスロケーションのサーバポリシーを設定できます。これらのポリシーによって、NetWare の機能の使用を自動化できます。詳細については、NetWare のマニュアルを参照してください。

サーバポリシーを設定する方法については、次の節の手順を参照してください。

- 210 ページの「Zentrap.mib のコンパイル」
- 210 ページの「Container Package ポリシーの設定」
- 212 ページの「Service Location Package ポリシーの設定」
- 219 ページの「Distributed Server Package ポリシーの設定」
- 235 ページの「ポリシーを使用したカスタムログファイルの作成」

サーバポリシーのスケジュール設定については、238 ページの「ポリシーのスケジュール設定」を参照してください。

Zentrap.mib のコンパイル

SNMP Community Strings および SNMP Trap Targets ポリシーでは SNMP を利用します。Zentrap.mib は、*Program* CD の ¥zfs¥tedpol¥sfiles¥mibs にあります。

SNMP 管理コンソールで SNMP トラップを受信するには、zentrap.mib ファイルを *ZENworks 6.5 Server Management Program* CD から、管理コンソールで MIB を管理するために使用する場所にコピーし、コンパイルする必要があります。これによって、SNMP 管理コンソールで、Server Management から SNMP トラップを受信して解釈できます。

Container Package ポリシーの設定

検索ポリシーは、Distributor が更新されたときに eDirectory ツリーを読み込む方法に関する情報として Distributor によって使用されます。

重要： 検索ポリシーを使用しない場合、Server Management は、1 時間ごとに［Root］まで検索して、オブジェクトを読み込みます。不要な検索トラフィックを制限するために、検索ポリシーを設定して有効にしてください。

検索ポリシーを作成するには

1 ConsoleOne で、Container Package を右クリックし、［Properties］をクリックします。

2 ［Policies］タブを選択し、［Search Policy］チェックボックスをオンにして、［Properties］をクリックし、［Search Level］タブを選択します。

検索ポリシーの［Enabled］列のボックスがオンになっていない場合は、オンにしてから［Properties］をクリックします。［Properties］ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 検索ポリシーの上限を指定するには、次のいずれかを選択します。

検索する場所	Description
Object Container	サーバオブジェクトの親コンテナまで検索します。
Partition	パーティションのルートまで検索します。

検索する場所	Description
Selected Container	選択したコンテナまで検索します。
Root	ツリーのルートまで検索します。

[Selected Container] を選択した場合は、コンテナを参照して選択します。

検索を選択した項目のいずれかの方向に制限するには、数値を入力します。たとえば、次のように入力します。

#	Description
0	[Search For Policies Up To] フィールドに設定されている現在のレベルに検索範囲が限定されます。
1	[Search For Policies Up To] フィールドに設定されている現在のレベルから、その 1 つ上のレベルまでに検索範囲が限定されます。 たとえば、[Selected Container] フィールドにサーバの親コンテナを指定した場合、+1 に設定すると、親コンテナの 1 つ上のレベルまでが検索範囲になります。
ミ1	[Search For Policies Up To] フィールドに設定されている現在のレベルから、その 1 つ下のレベルまでに検索範囲が限定されます。 たとえば、[Search For Policies Up To] フィールドに [Root] を選択した場合、-1 に設定すると、[Root] の 1 つ下のレベルまでが検索範囲になります。

4 検索順序を指定するには、[Search Order] タブを選択します。

Type	Description
オブジェクト	サーバ
グループ	サーバグループ
Container	サーバのコンテナ

矢印キーを使用して順序を変更します。[Add] または [Remove] をクリックして、使用するオブジェクトタイプを変更することもできます。

5 （省略可能）ポリシーは Subscriber で受信されたときに更新されるので、更新の頻度を指定します。

デフォルトは 1 時間ごとです。

日数と時間の両方をゼロのままにしておくと、[Policy Manager Will Refresh Policies From eDirectory] が選択されていても、eDirectory のポリシーは更新されません。

有効になっているポリシーに加えた変更は、指定された間隔で更新が実行されるまでは適用されません。ただし、サーバコンソールで POLICY REFRESH コマンドを使用して、すべてのポリシーを手動で更新きます。サーバコンソールには、更新間隔は秒単位で示されます (1 時間 =3,600 秒)。

6 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、どのタブで行った検索ポリシーの変更も保存されません。

7 検索ポリシーが Distributor 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

8 Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

[Cancel] をクリックすると、関連付けは保存されません。

Service Location Package ポリシーの設定

Distributor は Distribution を受信しないので、Distributor のポリシーは、そのオブジェクトが存在するコンテナに関連付ける必要があります。Service Location Package には、Distributor によって使用されるポリシーが含まれています。

Service Location Package ポリシーを設定する方法については、次の節を参照してください。

- 212 ページの「SMTP Host」
- 212 ページの「SNMP Trap Targets」
- 213 ページの「Tiered Electronic Distribution」
- 219 ページの「ZENworks Database」

SMTP Host

外部に発信されるインターネット電子メールを処理する SMTP リレーホストの TCP/IP アドレスを設定します。Distributor のメッセージを通知したり、記録するために電子メールオプションを選択した場合は、このポリシーを有効にしなければなりません。

SMTP Host ポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 SMTP Host ポリシーのチェックボックスをオンにして、[Properties] をクリックします。

SMTP Host ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 リレーホストサーバの TCP/IP アドレスまたは DNS 名を入力し、[OK] をクリックします。

4 SMTP Host ポリシーが Distributor 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

5 Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

[Cancel] をクリックすると、関連付けは保存されません。

SNMP Trap Targets

Distributor から SNMP トラップを送信するターゲット（または場所）を指定するには、このプロパティページを使用します。各ターゲットは、有効な TCP/IP アドレスまたは DNS 名でなければなりません。

SNMP Trap Targets ポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 SNMP Trap Targets ポリシーを選択し、[Properties] をクリックします。

SNMP Trap Targets ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 [SNMP Trap Policy] タブの [SNMP Trap Targets] の一覧にアイテムを追加するには、[Add] をクリックします。

4 [SNMP Target] ダイアログボックスで、有効な TCP/IP アドレスまたは DNS 名を入力し、[OK] をクリックします。

5 追加するトラップターゲットごとに、ステップ 3 およびステップ 4 を繰り返します。

6 ポリシーのスケジュールを設定するには、[Schedule] タブを選択し、[Schedule Type] フィールドでタイプを選択して、スケジュールを設定します。

412 ページの「曜日」
412 ページの「イベント」
413 ページの「間隔 (Interval)」
413 ページの「月」
413 ページの「Never」
413 ページの「パッケージスケジュール」
414 ページの「相対 (Relative)」
414 ページの「すぐに実行 (Run Immediately)」
414 ページの「Time」
415 ページの「週」
415 ページの「年」

7 作業が終了したら、[OK] をクリックします。

8 SNMP Trap Targets ポリシーが Distributor 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

9 Distributor オブジェクトが存在しているコンテナ (またはその上位のコンテナ) を参照して選択し、[OK] をクリックします。

[Cancel] をクリックすると、関連付けは保存されません。

Tiered Electronic Distribution

このポリシーによって、Distributor および Subscriber の属性のデフォルト値を設定できます。

- 214 ページの「ポリシーの仕組み」
- 214 ページの「累積ポリシー」
- 214 ページの「プロパティ値の置換、追加、または消失」
- 215 ページの「プラットフォーム環境設定用の複数のポリシー」
- 215 ページの「Tiered Electronic Distribution ポリシーの設定」

ポリシーの仕組み

Tiered Electronic Distribution ポリシーで設定されたデフォルト値は、このポリシーを含む Service Location Package を Distributor および Subscriber オブジェクトが存在する場所よりも上位のコンテナ、または Subscriber オブジェクトが存在するコンテナに関連付けると有効になります。

Tiered Electronic Distribution ポリシーの属性の値は、Distributor および Subscriber オブジェクトの同じような値を自動的に置換しますが、これはそれらの属性のデフォルト値がオブジェクトのプロパティで変更されていない場合だけです。

Distributor および Subscriber オブジェクトで属性の値を変更した後で、Tiered Electronic Distribution ポリシーの値を使用する場合は、Distributor または Subscriber オブジェクトのプロパティを編集し、オブジェクトのプロパティの各タブの上部にある［Use Policy］チェックボックスをオンにします。これで、Tiered Electronic Distribution ポリシーの値が、Distributor または Subscriber オブジェクトの属性に表示されます。

累積ポリシー

Tiered Electronic Distribution ポリシーは累積ポリシーではありません。これは次のことを意味します。

- **一度に1つ：** 複数のService Location Package（Tiered Electronic Distributionポリシーを含む）を同じコンテナに関連付けることはできません。
- **最も近いものが優先：** Subscriberのコンテナが Tiered Electronic Distributionポリシー（Service Location Package 内）に関連付けられており、親コンテナにも Tiered Electronic Distribution ポリシー（Service Location Package 内）が関連付けられている場合、最も近いコンテナ（Subscriber 自体のコンテナ）の Tiered Electronic Distribution ポリシーが優先されます。

プロパティ値の置換、追加、または消失

次の情報は、Tiered Electronic Distribution ポリシーが有効な場合にのみ適用されます。

- Tiered Electronic Distribution ポリシーで定義された変数を Distributor または Subscriber の変数の一覧に追加できます。Distributor または Subscriber オブジェクトで定義済みの変数は置換されません。
- Distributor や Subscriber のプロパティの値に該当するその他のすべてのポリシーフィールドは、Tiered Electronic Distribution ポリシーによって補完ではなく、置換されるので、プロパティ値が空のフィールドに置換される可能性があります。したがって、Tiered Electronic Distribution ポリシーを作成する場合は、影響を受ける Distributor または Subscriber に適用するポリシーの各タブですべてのフィールドに入力していることを確認します。

  たとえば、Subscriber のオブジェクトのプロパティで作業ディレクトリが入力されている場合に、Tiered Electronic Distribution ポリシーで作業ディレクトリを指定しなかった場合、後で Subscriber のプロパティで［Use Policy］チェックボックスをオンにしてこのポリシーを適用すると、Subscriber では作業ディレクトリを利用できなくなります。

プラットフォーム環境設定用の複数のポリシー

Subscriber オブジェクト用の Tiered Electronic Distribution ポリシーの複数のインスタンスを作成し、サーバプラットフォームごとに異なるポリシー設定を定義できます。そのためには、Subscriber オブジェクトを、それぞれのオペレーティングシステムを表す異なるコンテナ内に作成する必要があります。

オペレーティングシステム固有の値を必要とする可能性がある Subscriber の属性は、次のとおりです。

作業ディレクトリ
メッセージングの設定
変数の定義

Tiered Electronic Distribution ポリシーの設定

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 Tiered Electronic Distribution ポリシーを選択し、[Properties] をクリックします。

Tiered Electronic Distribution ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 [General] > [Settings] の順にクリックし、次のフィールドに入力します。

[Input Rate]：Tiered Electronic Distribution オブジェクトのネットワークトラフィックを最小限に抑えるためのデフォルトの入力速度を設定します。これによって、Subscriber と Distributor の受信速度を指定します。デフォルト値は接続で処理できる最大値です。この速度を使用して、帯域幅の狭いリンクの使用を制御できます。

[Output Rate]：デフォルトの出力レートを設定して、Tiered Electronic Distribution オブジェクトのネットワークトラフィックを最小限に抑えます。これによって、Distributor と親 Subscriber の送信速度を指定します。デフォルト値は接続で処理できる最大値です。空白は、サードパーティアプリケーションから帯域幅が割り当てられることを意味します。

出力には 3 つの優先度があり、速度を指定できます。

- **[High Priority]**：この Distribution は、[Medium Priority] または [Low Priority] の Distribution よりも前に送信されます。
- **[Medium Priority]**：この Distribution は、[High Priority] の Distribution がすべて送信された後、[Low Priority] の Distribution よりも前に送信されます。
- **[Low Priority]**：この Distribution は、[High Priority] と [Medium Priority] のすべての Distribution が送信された後で送信されます。

詳細については、128 ページの「Distribution の優先度」を参照してください。

[Maximum Concurrent Distributions to Build]：Distribution を構築するために同時に実行できる配布スレッドの最大数を指定します。デフォルト値は 5 です。有効な値は 1 から 10 までです。

この数値によって、Distributor の構築アクティビティの負荷を分散させることができます。

[Maximum Concurrent Distributions to Send]：Distribution を送信するために同時に実行できる配布スレッドの最大数を指定します。デフォルト値は指定されていません（空フィールド）。

この数値によって、Distributor の送信アクティビティの負荷を分散させ、ネットワークトラフィックをスケジュール設定期間全体に分散させることができます。

[Connection Time-out]：Distributor が別のノードに接続するときにタイムアウトになるまでのデフォルトの秒数を指定します。または、Subscriber が接続を終了する前に、Distributor（受信）または Subscriber（送信）からの応答を待機する秒数を指定します。

この時間が経過すると、Distributor は接続を終了し、Channel の送信スケジュールが再び開始されるまで再試行しません。送信または受信中に接続が終了した場合、Subscriber は次に Channel の送信スケジュールが開始されるまで再開しません。

デフォルト値は 300 秒（5 分）です。秒単位で指定できる範囲は 1 から 60,000 までです。あるノードから別のノードまでの応答を待機するのに適切な時間を選択します。

重要：遅延が大きくなることが多い低速またはビジー状態のリンクでは、この値を大きくする必要があります。

[Working Directory]：Tiered Electronic Distribution で、Distribution、永続ステータス、およびサーバ上の一時ファイルを保存するためのデフォルトのディレクトリを指定します。このディレクトリは、Distribution を処理するために十分な空き容量がある場所に配置されている必要があります。

[Working Directory] フィールドでは、変数を使用してボリューム / ドライブおよびディレクトリ名を指定できます。ただし、変数は Subscriber についてのみ機能します。

重要：Distributor では変数を解決できず、[Working Directory] フィールドで指定されているディレクトリがそのまま使用されます。たとえば、値が %VOL%ted1¥working である場合、Distributor では %VOL% を解決できないので、sys: ボリュームに sys:¥%VOL%¥ted¥working という名前の作業ディレクトリが作成されます。

詳細については、190 ページの「作業ディレクトリ」を参照してください。

[Parent Subscriber]：Subscriber は、通常、Distributor から直接 Distribution を受信するわけではありません。ネットワーク全体のデフォルトの親 Subscriber になる Subscriber を参照できます。この親 Subscriber は、Subscriber オブジェクトのプロパティで親 Subscriber が定義されていない場合に Distribution の受け渡しをします。

[Disk Space Desired To Be Left Free]：Subscriber オブジェクトのプロパティで定義されていない場合に、この値をデフォルト値として使用して Distribution を受信するのに十分な空きディスク容量を確保します。ここで設定したディスク容量が不十分である場合は、Subscriber は Distribution を受信しません。

4 [General] > [Messaging] の順にクリックし、次のフィールドに入力します。

[Server Console]：サーバコンソールにメッセージを表示する場合に従う手順です。デフォルトは [Level 4 (Information & Level 3 Messages)] です。

[SNMP Trap]：SNMP トラップを送信する場合に従う手順です。デフォルトは [Level 0 (No Messages)] です。

[Log File]：ログファイルに情報を記録する場合に従う手順です。デフォルトは [Level 5 (Trace Information & Level 4 Messages)] です。

[Filename]：デフォルトでは、このフィールドは空白になります。ログのファイル名をどのように選択しても、このポリシーが適用されるサーバの名前は ted.log に置き換えられます。

ログファイルを作成するには、ログファイルの名前を次の形式で指定します。

installation_path¥*directory_path*¥*filename*.*filename_extension*

installation_path は ZENworks でログファイルの検索に必須ではありませんが、パスを含めておくと検索が容易になります。

重要： ログファイルはサイズが非常に大きくなる可能性があるため、NetWare サーバでは、sys: ボリュームを使用しないことをお勧めします。

.log や .txt などのファイル名拡張子を使用します。

[Delete Log Entries Older Than __ Days]：ディスク容量の使用状況を制御します。ログファイルの場合、メッセージレベルを最小限の詳細度に設定し、6 日（デフォルト）よりも古いエントリをパージすることが重要です。

[E-Mail]：電子メールメッセージを送信する場合に従う手順です。不要な電子メールのトラフィックを最小限に抑えるには、[None] または [Errors Only] を選択することをお勧めします。デフォルトは [Level 0 (No Messages)] です。

[Users]：ユーザ、グループ、電子メールアドレスを追加します。

[Address Attribute]：関連付けられたユーザまたはグループの属性を表示します。ドロップダウンリストから属性を変更できます。このドロップダウンリストには 30 以上のオプションが表示されます。

これらのオプションの一部を次に示します。

CN	Given Name	Postal Code
Description	Initials	Postal Office Box
EMail Address	Internet EMail Address	Surname
Full Name	Mailbox ID	Telephone Number
Employee ID	NSCP:mailHost	Title
Entrust:User	OU	uniqueID
Generational Qualifier	Physical Delivery Office Name	

5 Subscriber によって使用される変数にデフォルト値を割り当てるには、[Variables] タブを選択し、[Add] をクリックして、次のフィールドに入力します。

[Variable]：変数の名前です。変数の使用方法を示す名前にしてください。たとえば、WORKINGVOL などです。

変数名は定義済みの変数やユーザ定義の変数から付けることもできます。

値： この変数が指定されている場合に、Subscriber が使用する値です。たとえば、data: と指定します。

値に別の変数名を使用できます。この方法を使用して変数をネストできます。

抽出が確実に行われるようにするには、Subscriber への絶対パスを指定します。たとえば、パスが data: ボリュームだけである場合でも、コロン (:) が含まれていることを確認します。コロンがフルパスに必要な部分であるからです。

[Description]：変数の使用方法の説明です。たとえば、次のように入力します。

```
Volume for the working directory.
```

ここで定義した変数が Subscriber の変数リストに存在しない場合は、自動的に追加されます。ただし、変数が Subscriber の変数リストに存在する場合は、Subscriber での定義が使用されます。

6 すべての Distributor のデフォルトの更新スケジュールを割り当てるには、[Schedule] タブを選択し、[Distributor Refresh Schedule] をクリックし、[Schedule Type] フィールドでスケジュールを選択して、スケジュールを設定します。

412 ページの「曜日」
413 ページの「間隔 (Interval)」
413 ページの「月」
413 ページの「Never」
414 ページの「Time」
415 ページの「年」

更新スケジュールについては、98 ページの「スケジュール設定」を参照してください。

重要： Distributor に対する変更が多く、より頻繁な更新が必要である場合以外は、Distributor の更新スケジュールを 1 日に 1 回に設定することをお勧めします。ただし、Distributor の更新頻度を 5 分に 1 回よりも多くしないでください。Distribution の構築、eDirectory の複製、およびツリーの検索（検索ポリシーが定義されていない場合）には、最大で 5 分を要する場合があります。

7 すべての Subscriber のデフォルトの抽出スケジュールを割り当てるには、[Schedule] タブを選択し、[Subscriber Extract Schedule] をクリックし、[Schedule Type] フィールドでスケジュールを選択して、スケジュールを設定します。

412 ページの「曜日」
413 ページの「間隔 (Interval)」
413 ページの「月」
413 ページの「Never」
414 ページの「すぐに実行 (Run Immediately)」
414 ページの「Time」
415 ページの「年」

抽出スケジュールについては、151 ページの「スケジュール設定」を参照してください。

8 [OK] をクリックしてポリシーを閉じます。

9 Tiered Electronic Distribution ポリシーが Distributor 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

10 Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

[Cancel] をクリックすると、関連付けは保存されません。

11 Tiered Electronic Distribution ポリシーが Subscriber 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

12 Subscriber オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

このコンテナは、Tiered Electronic Distribution ポリシーのデフォルトの情報を利用できるようにする Subscriber にします。

特定のオペレーティングシステム用にこのポリシーを作成している場合は、適切なプラットフォーム固有のコンテナを選択し、そのコンテナの下にある Subscriber にのみポリシーが適用されるようにします。

[Cancel] をクリックすると、関連付けは保存されません。

13 このポリシーを使用する Subscriber が存在している各コンテナについて、ステップ 12 を繰り返します。

ZENworks Database

ZENworks データベースオブジェクトの場所を特定するための DN を設定します。Policy and Distribution Services をインストールするときにこの情報を設定しなかった場合、このポリシーを作成して、Server Management でレポートの作成時に使用する成否のログを記録するデータベースファイルを検索できます。このポリシーを作成して、インストール時に設定された情報を変更することもできます。

現在の ZENworks データベースポリシーに関連付けるデータベースオブジェクトを選択するには、このプロパティページを使用します。このポリシーは、ポリシーを Subscriber に配布するか、ポリシーを Distributor に関連付けるまで有効になりません。

Server Management データベースは、Distributions and Server Policies のレポーティング情報を格納するために使用されます。

ZENworks データベースポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 ZENworks データベースポリシーを選択し、[Properties] をクリックします。

ZENworks データベースポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 [Policy/Distribution Management] タブを選択します。

4 [Database DN] フィールドで、このポリシー用のデータベースを表す ZENworks データベースオブジェクトを参照し、[OK] をクリックします。

5 ZENworks データベースポリシーが Distributor 上で適用されるようにポリシーパッケージを関連付けるには、[Associations] タブを選択し、[Add] をクリックします。

6 Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

[Cancel] をクリックすると、関連付けは保存されません。

Distributed Server Package ポリシーの設定

Distributed Server Package ポリシーを設定することによって、さまざまなサーバの動作や処理の制御を自動化したり、SMTP ホストの TCP/IP アドレス、SNMP トラップターゲット、および ZENworks データベースオブジェクトの DN の制御を自動化したりできます。

[Policies] タブには、サポートされている各オペレーティングシステムについて 1 つずつ、サーバポリシー用のオプションがいくつかあります。[General] タブのポリシーはすべてのプラットフォームのサーバに適用されます。特定のプラットフォームのタブにあるポリシーは、そのプラットフォームのサーバにのみ適用されます。

[NetWare] タブにあるポリシーなど、プラットフォーム固有のポリシーは、特定のポリシーパッケージの [General] タブにある同じようなポリシーよりも常に優先されます。

すべてのポリシーは、NetWare ポリシーに含まれています。したがって、ここでは NetWare ポリシーについてのみ説明します。説明の内容はすべてのプラットフォームに当てはまります。

Distributed Server Package ポリシーを設定する方法については、次の節を参照してください。

- 220 ページの「Copy Files」
- 222 ページの「NetWare SET Parameters」
- 223 ページの「Prohibited File」
- 225 ページの「Scheduled Down」
- 226 ページの「Scheduled Load/Unload」
- 227 ページの「Server Down Process」
- 229 ページの「Server Scripts」
- 230 ページの「SMTP Host」
- 230 ページの「SNMP Community Strings」
- 231 ページの「SNMP Trap Targets」
- 232 ページの「Text File Changes」
- 233 ページの「ZENworks Database」
- 234 ページの「ZENworks Server Management」

Copy Files

Copy Files ポリシーによって、ポリシーの設定を使用してサーバ上のファイルをある場所から別の場所にコピーできます。ファイルをコピーすることも、移動することもできます。

Copy Files ポリシーを設定するには

1. ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。
2. [Policies] タブを選択し、次の中からプラットフォームを選択します。

   一般
   Windows:
   NetWare
   Linux
   Solaris
3. [Add]、[Copy Files] の順にクリックし、ポリシー名を入力して、[OK] をクリックします。

4 [Properties] をクリックします。

[Copy Files] タブが表示されます。

5 [Add] をクリックします。

デフォルトは Local File Copy #1 です。この名前は編集できます。

6 次のフィールドに情報を入力します。

[Source Path]：コピーするファイルが保存されている場所のフルパスを指定します。

パスにはワイルドカードを使用できます。

＊ = 任意の数の文字
? = その位置にある任意の 1 文字
??? = それらの位置にある任意の文字

[Target Path]：コピーするファイルの保存先のフルパスを指定します。

このパスにはワイルドカードを使用できます。このパスにはソースパスを反映させる必要はありません。ただし、既存のターゲットパスを反映させることができます。

[Include Subdirectories]：パスの最後にあるディレクトリから始めて、すべてのサブディレクトリとその中にあるファイルを含めます。このオプションを選択しない場合は、パスの最後にあるディレクトリ内のファイルだけがコピーされます。

[Maintain Attributes]：ソースのファイルシステムに存在するファイル属性をターゲットのファイルシステムでも保持します。

[Overwrite Destination Files]：ファイルの日付に関係なく、コピー先のディレクトリで同じ名前のファイルを上書きします。このオプションを選択しない場合、同じ名前のファイルは置き換えられません。

[Maintain Trustees]：ファイルのトラスティ属性を保持します。

[When a File Is Locked]：次のいずれかまたは両方を選択します。

- **[Retry __ Times]**：指定した回数だけロックされたファイルの上書きを再試行した後、ファイルの置換に失敗したことにします。このチェックボックスをオフのままにすると、ターゲットファイルシステム上のロックされたファイルは置換されません。
- **[Kill Connection of Open Files]**:（NetWare のみ）ロックされたファイルに上書きできるように、ロックされたファイルへの接続を強制終了しようとします。このオプションは、ファイルを抽出している場合にのみ適用され、Distribution を構築するためにファイルにアクセスしている場合には適用されません。Distribution を構築しているときに、Distribution に属するファイルがロックされている場合、構築は失敗します。サーバと NLM の接続は強制終了できません。

[Error Processing]：デフォルトでは、[Fail On Error] が選択されています。これによって、コピー中にエラーが発生した場合、ファイルのコピー処理は中止されます。エラーが発生してもファイルのコピーを続行するには、[Continue On Error] を選択します。

[Operation]：[Source Path] で指定されたファイルをコピーするか、移動するかを設定します。

7 [Schedule] タブを選択し、ポリシーのスケジュールを設定します 238 ページの「ポリシーのスケジュール設定」を参照してください。

8 [OK] をクリックしてポリシーを閉じます。

NetWare SET Parameters

サーバによる SET パラメータの使用を自動化できます。

NetWare SET パラメータを設定するには

1. ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。
2. [Policies] > [NetWare] (または [General]) の順にクリックします。
3. [Add] をクリックし、[NetWare Set Parameters] を選択します。
4. この SET パラメータポリシーの名前を入力し、[OK] をクリックします。

   このダイアログボックスから選択したポリシーは複数ポリシーなので、[Policies] タブに複数の SET パラメータポリシーを表示できます。したがって、このポリシーの一意の名前を指定します。

   SET パラメータポリシーに名前を付けて [OK] をクリックすると、[Policies] タブでそのポリシーが選択されます。
5. [Properties] をクリックします。

   [Set Commands] タブが表示されます。
6. [Add] をクリックします。

   NetWare Server SET Command ウィザードが表示されます。
7. SET パラメータが保存されているサーバを選択し、[Next] をクリックします。

   重要： Policy/Package Agent が実行されている必要があります。
8. このポリシーで設定するコマンドをすべて選択します。

   カテゴリのチェックボックスをオンにしてカテゴリ全体を選択することも、プラス記号をクリックして SET コマンドカテゴリを展開し、含める個々のコマンドのチェックボックスをオンにすることもできます。

   警告： SET コマンド Set Developer Option を選択し、Off を On に変更しないでください。このパラメータは、開発者がサーバの異常終了をデバッグできるようにするためのものです。特定の異常終了の発生を防止するために用意されているオペレーティングシステムの一部のチェック機能を無効にします。また、Set Developer Option が On になっている場合、キーボード入力を要求する NCP™ スクリプトを実行するとサーバが異常終了する可能性があります。
9. コマンドの選択が完了したら、[Finish] をクリックします。

   選択したコマンドが、ポリシーの [Set Commands] タブに表示されます。
10. SET コマンドを編集するには、プラス記号をクリックしてその属性を展開します。
11. 属性を編集するには、属性を選択して、[Edit] をクリックします。

    属性を変更できるダイアログボックスが表示されます。
12. 特定の SET コマンドの編集する各属性について、前の手順を繰り返します。
13. 別の SET コマンドの属性を編集するには、手順 10 からステップ 12 までを繰り返します。
14. ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。
15. [OK] をクリックしてポリシーを閉じます。

    [Cancel] をクリックすると、スケジュールの変更も SET パラメータの変更も保存されません。

Prohibited File

このポリシーによって、指定したボリューム / ドライブまたはディレクトリ / フォルダからの許可されていないファイルの削除や移動を監視および強制できます。たとえば、サーバからの .jpg、.mp3、および .avi ファイルの削除を自動化できます。

[General] タブの使用も含め、すべてのプラットフォーム (NetWare®、Windows、Linux、および Solaris) がサポートされています。

このポリシーを使用して、次の作業を行うことができます。

- 監視するボリューム / ドライブまたはディレクトリを指定します。すべてのサブディレクトリを含めるオプションもあります。
- ワイルドカードの組み合わせを使用して監視するファイルタイプを指定します。
- 検出されたすべてのファイルについて次のようなアクションを指定します。
  - 削除
  - 指定した場所への移動
- ポリシーを適用するスケジュールを指定します。

禁止するファイルを管理するためのポリシーを設定するには

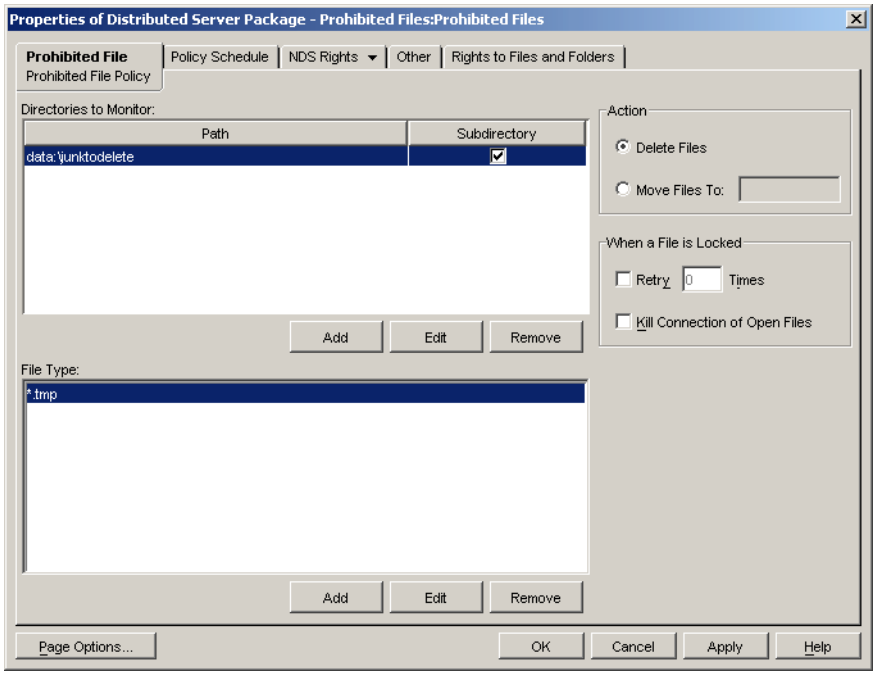
1 ConsoleOne で、Distributed Server Package を右クリックし、[Properties] をクリックします。

2 [Policies] > [NetWare] (またはその他のプラットフォーム) の順にクリックします。

3 [Add] をクリックし、[Prohibited File] を選択します。

4 ポリシーの一意の名前を入力し、[OK] をクリックします。

次のプロパティページが表示されます。



5 次のフィールドに情報を入力します。

[Directories to Monitor]：ポリシーのこのインスタンスについて、監視するパスを指定できます。

- [Path]：ボリューム、ドライブ、またはディレクトリ名を指定できます。ディレクトリを指定する場合は、フルパスを指定する必要があります。

  複数のパスを追加できます。入力した各パスについて、[File Type] フィールドで定義したファイルタイプ一致するファイルが、選択した [Action] ボタンに従って、削除または移動されます。

  パスには変数を使用できます。

- [Subdirectory]：すべてのサブディレクトリを含めることを指定するには、チェックボックスをオンにします。

  特定のサブディレクトリだけを含める場合は、そのサブディレクトリ用に別のポリシーを作成し、[Path] フィールドにそのフルパスを入力します。ただし、監視対象のディレクトリまたはそのサブディレクトリにファイルを移動することはできません。

- [Add]：パスを選択できるダイアログボックスを表示します。このフィールドは参照できないので、移動または削除するファイルのフルパスがわかっている必要があります。
- [Edit]：選択したパスを編集できるようにします。
- [Remove]：選択したパスのエントリを一覧から削除します。

[Files to Manage]：監視するファイルのタイプを指定できます。

- [Add]：ファイルタイプを指定できるダイアログボックスを表示します。パスにはワイルドカードを使用できます。

  * = 任意の数の文字
  ? = その位置にある任意の 1 文字
  ??? = それらの位置にある複数の任意の文字

  このフィールドは参照できないので、移動または削除するファイルを特定するための正しい情報を指定する必要があります。

  重要：? ワイルドカードは、ZENworks と DOS では機能が異なります。たとえば、検索文字列 *.htm? は、.html で終わるファイルのみを検索しますが、DOS は、.htm と .html の両方で終わるファイルを検索します。つまり、ZENworks で ? ワイルドカードを使用すると、文字の位置にファイル名を指定できます。

- [Edit]：選択したファイルタイプを編集できるようにします。
- [Remove]：選択したファイルタイプを一覧から削除します。

[Action]：[Directories to Monitor] および [Files to Manage] ボックスで指定したファイルの処理方法として 2 つのオプションがあります。

- [Delete Files]：指定したファイルを指定した場所から削除するには、このオプションを選択します。
- [Move Files To]：指定したファイルを、このフィールドで指定したパスに移動するには、このオプションを選択します。このフィールドは参照できないので、ファイルの移動先のフルパスがわかっている必要があります。

ファイルを移動する場合、

- ファイルのフルパスは維持されます。ターゲットにパスが存在しない場合は作成されます。
- 同じパスにファイルが存在する場合、ファイルは上書きされます。
- ファイルやディレクトリの属性およびトラスティは転送されません。
- ファイルの所有権は維持されます。

重要： ディレクトリが監視対象になっている場合は、そのディレクトリまたはそのサブディレクトリにファイルを移動することはできません。

[When a File Is Locked]： 削除または移動しようとしたファイルを開くことができない場合があります。このようなファイルについて、次のいずれかの解決方法を指定できます。

- **[Retry ___ Times]：** チェックボックスをオンにして、次のファイルに進む前に、ファイルの削除や移動を再試行する回数を入力します。有効なエントリは 1 から 10 までです。値を大きくするたびに増加する時間は、システムを構成するさまざまなハードウェアやソフトウェアの処理速度によって異なります。

  このフィールドを使用して、一時的に開かれているファイルを閉じるのに十分な時間を指定します。たとえば、アプリケーションが編集用のコピーを取得したり、ファイルの新しいコピーを書き込んだりする間だけ開かれているファイルなどです。

- **[Kill Connection of Open Files]:** (NetWare のみ）ファイルを開いたままにしている接続を強制終了し、ユーザが開いている場合でも、ファイルを削除または移動できるようにします。

  重要： 強制終了できるのは、ワークステーション上のファイルへの接続だけです。サーバのファイルは、そのファイルを開いているプロセスからの接続を解除することはできません。

6 [OK] をクリックしてポリシーを閉じます。

Scheduled Down

サーバを停止する時期および方法を自動化し、サーバを自動的に再起動するかどうかを指定できます。

スケジュールされたサーバの停止を設定するには

1 ConsoleOne で、Distributed Server Package を右クリックし、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 [Add] をクリックし、[Scheduled Down] を選択します。

4 ポリシーの一意の名前を入力し、[OK] をクリックします。

このダイアログボックスから選択したポリシーは複数ポリシーなので、[Policies] タブに複数の Scheduled Down ポリシーを表示できます。したがって、このポリシーの一意の名前を指定します。

Scheduled Down ポリシーに名前を付けて [OK] をクリックすると、[Policies] タブでそのポリシーが選択されます。

5 [Properties] をクリックします。

[Up Procedure] タブが表示されます。

6 停止方法を選択します。

停止オプション	Description
Reset Server	サーバを停止し、ウォームブートを実行します。
Restart Server	サーバを停止し、再起動します。
Down Server	サーバを停止し、再起動しません。

7 ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

8 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、新しくスケジュールを設定した Scheduled Down ポリシーは保存されません。

Scheduled Load/Unload

NLM ファイルや Java Class プロセス、および Linux や Solaris の実行可能ファイルのスケジュールされたロードやアンロードを自動化できます。

スケジュールを設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 [Add] をクリックし、[Scheduled Load/Unload] を選択します。

4 この Load/Unload ポリシーの名前を入力し、[OK] をクリックします。

このダイアログボックスから選択したポリシーは複数ポリシーなので、[Policies] タブに複数の Load/Unload ポリシーを表示できます。したがって、このポリシーの一意の名前を指定します。

Load/Unload ポリシーに名前を付けて [OK] をクリックすると、[Policies] タブでそのポリシーが選択されます。

5 [Properties] をクリックします。

[Scheduled Load/Unload] タブが表示されます。

6 [Add] をクリックします。

7 次のオプションのいずれかを選択します。

421 ページの「Load NLM/Process」
422 ページの「Load Java Class」
422 ページの「Unload Process」
422 ページの「Start Service」
422 ページの「Stop Service」

項目の設定方法の詳細については、各項目をクリックしてください。

8 パッケージに含める各 NLM またはプロセスについて、手順 6 とステップ 7 を繰り返します。

9 順序を変更するには、矢印キーを使用します。

10 ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

11 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、新しくスケジュールを設定した Scheduled Load/Unload ポリシーは保存されません。

Server Down Process

サーバを停止するときにサーバが使用する手順を自動化できます。

サーバの停止プロセスを設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 サーバダウンプロセスポリシーを選択し、[Properties] をクリックします。

サーバダウンプロセスポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

4 停止の手順を設定するには、[Down Procedure] タブ、[Down Procedures] の順に選択します。

5 ポリシーのオプションを有効にするには、[Follow This Procedure When a Down Server Is Triggered] チェックボックスを選択し、サーバを停止するまでの待機する分数を入力します。

6 停止する前にログインを無効にするには、チェックボックスをオンにして、ログインを無効にしてから停止までの分数を入力します。

7 停止する前に接続を解除するには、チェックボックスをオンにして、接続を解除してからサーバを停止するまでの分数を入力します。

8 アンロードの順序を設定するには、Down Procedure タブを選択し、[Ordered Unload] をクリックします。

8a NLM ファイルとプロセスを含めるには、[Unload These NLMs and Kill These Processes in This Order Before Downing] チェックボックスをオンにします。

8b [Add] をクリックします。

8c [NLM] または [Process] のいずれかを選択し、名前を入力して、[OK] をクリックします。

8d 順序を変更するには、矢印キーを使用します。

9 レポーティングを設定するには、[Notification] タブ、[Reporting] の順に選択します。

9a 指定した時間が経過した後、サーバが稼動していない場合に別のサーバが SNMP アラートを送信するようにするには、[Send SNMP Alert] チェックボックスをオンにして、分数を入力します。

管理コンソールでの SNMP トラップの表示については、210 ページの「Zentrap.mib のコンパイル」を参照してください。

9b 障害が発生した場合に再起動を監視し、アラートを送信できるサーバを指定するには、[Add] をクリックして、候補となるサーバの順序付きのリストを表示します。

Policy and Distribution Services は、リストの先頭から順に、最初のサーバと通信し、そのサーバをアラートの通知に使用します。Policy and Distribution Services は、サーバと通信できない場合は、リストの次のサーバに対して通信を試行します。使用できる最初のサーバが、アラート送信のスケジュールが設定されるサーバになります。

9c サーバを参照して選択します。

9d 必要な各サーバについて、ステップ 9a からステップ 9c までを繰り返します。

9e 順序を変更するには、矢印キーを使用します。

10 ブロードキャストメッセージを設定するには、[Notification] タブを選択し、[Broadcast Messages]、[Send Messages To Connected Users] の順にクリックします。

10a メッセージを送信する回数を入力します。

10b カスタムテキストをブロードキャストするには、ボックスにテキストを入力します。

10c ブロードキャストの最終行として時間を含む定義済みのメッセージを含めるには、チェックボックスをオンにします。

x 分は、ステップ 10a で指定した回数で、サーバが停止するまでの残りの分数を割り、その値（分単位）を引いた値を各ブロードキャストに表示します。たとえば、残りの分数が 10 分で、ステップ 10a で 5 を選択した場合、メッセージは 2 分ごとにブロードキャストされます。各ブロードキャストの後の残りの分数は、最後のブロードキャストの時点よりも 2 分少なくなります。

11 ターゲットのメッセージを設定するには、[Notification] タブ、[Targeted Messages]の順に選択し、[Send E-mail To Selected Users When Server Is Going Down] をクリックします。

11a ターゲットメッセージを受信するユーザ、グループ、または電子メールアドレスを指定するには、[Add] をクリックします。

11b [User]、[Group]、または [E-Mail Address] のいずれかを選択します。

11c ユーザまたはグループを参照して選択するか、電子メールアドレスを入力します。

11d 他のユーザ、グループ、または電子メールアドレスについて、ステップ 11a からステップ 11c までを繰り返します。

12 サーバを停止する条件を設定するには、[Conditions] タブを選択し、[Use Conditions] をクリックします。

12a 条件を指定するには、[Add] をクリックします。

12b サーバを停止しない場合を指定するには、次の条件から選択します。

これらの条件の中には、有効な名前を入力しなければならないものがあります。その他については、[Select Object] ダイアログボックスを使用して参照できます。

[File Open]：指定したファイルが開いている場合です。たとえば、.exe などです。

[NLM Loaded]：指定した NLM ファイルが実行されている場合です。

[Server Connected]：指定したサーバが接続されている場合です。

[User Connected]：指定したユーザが接続されている場合です。

[Number of User Connections]：接続されているユーザ数が指定した数を超えた場合です。つまり、影響を受けるユーザが多すぎる場合にはサーバを停止しません。

[Workstation Connected]：指定したワークステーションが接続されている場合です。

12c リストに追加する各条件について、ステップ 12a およびステップ 12b を繰り返します。

12d 順序を変更するには、矢印キーを使用します。

13 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、どのタブで行ったサーバダウンプロセスポリシーの変更も保存されません。

Server Scripts

NetWare サーバによるスクリプトの使用を自動化できます。

サーバスクリプトを設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 [Add] をクリックし、[Server Scripts] を選択します。

4 ポリシーの一意の名前を指定します。

このダイアログボックスから選択したポリシーは複数ポリシーなので、[Policies] タブに複数の Script ポリシーを表示できます。したがって、このポリシーの一意の名前を指定します。

Script ポリシーに名前を付けて [OK] をクリックすると、[Policies] タブでそのポリシーが選択されます。

5 [Properties] をクリックします。

[Script] タブが表示されます。

6 [Add] をクリックし、[Server Scripts] を選択します。

7 スクリプト名を入力します。

Script #1 が表示されます。

8 スクリプトの種類（NCF、NetBasic*、PERL）を選択します。

重要： NetBasic は NetWare 6.5 サーバではサポートされていません。

9 スクリプトのテキストを入力します。

10 追加する各スクリプトについて、手順 6 からステップ 9 までを繰り返します。

11 方向キーを使用して、スクリプトを実行する順序を指定します。

12 ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

13 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、スケジュールも入力したスクリプトも保存されません。

SMTP Host

外部に発信されるインターネット電子メールを処理するリレーホストの TCP/IP アドレスを設定できます。

SMTP Host ポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 SMTP Host ポリシーを選択し、[Properties] をクリックします。

SMTP Host ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

[SMTP Host] ダブがデフォルトで表示されます。

3 TCP/IP アドレスまたは DNS 名 (mail.novell.com など) を入力し、[OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、TCP/IP アドレスは保存されません。

SNMP Community Strings

このポリシーによって、SNMP コミュニティ文字列を設定し、スケジュールを設定できます。

SNMP Community Strings ポリシーを設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare] (またはその他のプラットフォーム) の順にクリックします。

3 SNMP Community Strings ポリシーを選択し、[Properties] をクリックします。

SNMP Community Strings ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

[SNMP Community Policy] タブが表示されます。

4 [Community Strings] の各フィールドに情報を入力します。

Monitor
コントロール
Trap

コミュニティ文字列では、大文字と小文字が区別されます。必要に応じて、各フィールドに文字列を入力します。

5 [Schedule] タブを選択し、ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

6 [OK] をクリックしてポリシーを閉じます。

SNMP Trap Targets

Policy/Package Agent について SNMP トラップのターゲットを設定できます。

管理コンソールでの SNMP トラップの表示については、210 ページの「Zentrap.mib のコンパイル」を参照してください。

Windows Trap Target Policy Enforcer の動作の仕組みについて

この節では、次の Windows レジストリの場所を表すために次の略語を使用します。

- **AGENT_KEY:** HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥SNMP¥Parameters
- **ZFS_KEY:** HKEY_LOCAL_MACHINE¥SOFTWARE¥Novell¥Zenworks¥ZfS

Windows SNMP Trap Target Policy Enforcer は、次の順序で実行されます。

1. Policy Enforcer は、まず SNMP エージェントのインストールを確認します。これは、AGENT_KEY が存在するかどうかを調べることによって確認されます。このキーが存在する場合、Enforcer は SNMP エージェントがインストールされていると見なし、次の手順に進みます。このキーが存在場合は、エラーが返され、処理は停止します。
2. Enforcer は、トラップターゲットを ZFS_KEY に配置することによって、ZENworks Server Management によって追加されたすべてのトラップターゲットを把握します。トラップターゲットは、TrapConfiguration のサブキーを使用して、AGENT_KEY 内のトラップターゲットと同様に分類されます。TrapConfiguration サブキーには、レジストリのサブキーとして表されるコミュニティ文字列が含まれています。これらのコミュニティ文字列には、各コミュニティ文字列に関連付けられたトラップターゲットが含まれています。
3. ZENworks Server Management ポリシーの各トラップターゲットが存在しない場合、そのトラップターゲットは AGENT_KEY に配置されます。Policy Enforcer は、Server Management の各トラップターゲットを検出し、各コミュニティ文字列に追加されるようにします。AGENT_KEY にコミュニティ文字列が存在しない場合、「public」という名前のコミュニティ文字列が作成されます。
4. ZFS_KEY で見つかった以前に追加されたトラップターゲットが、ZENworks Server Management ポリシーから削除された場合、そのトラップターゲットは AGENT_KEY から削除されます。Server Management で追加されたものではないトラップターゲットは削除されません。
5. Microsoft の SNMP エージェントがインストールされている場合、エージェントのトラップターゲットは自動的に更新され、レジストリも変更されます。

SNMP Trap Target ポリシーの設定

SNMP Trap Targets ポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 SNMP Trap Targets ポリシーを選択し、[Properties] をクリックします。

SNMP Trap Targets ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 [Add] をクリックします。

4 新しいターゲットを指定して、[OK] をクリックします。

ヒント： ターゲットサーバの TCP/IP アドレスまたは DNS 名を指定します。IPX アドレスはサポートされていません。

5 新しい各トラップターゲットについて、手順 3 からステップ 4 までを繰り返します。

6 [Schedule] タブを選択し、ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

7 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、指定したどのターゲットも保存されません。

Text File Changes

サーバ上のテキストファイルに対する変更を自動化できます。

テキストファイルの変更を設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 [Add] をクリックし、[Text File Changes] を選択します。

4 ポリシーの一意の名前を指定します。

このダイアログボックスから選択したポリシーは複数ポリシーなので、[Policies] タブに複数のテキストファイルポリシーを表示できます。したがって、このポリシーの一意の名前を指定します。

テキストファイルポリシーに名前を付けて [OK] をクリックすると、[Policies] タブでそのポリシーが選択されます。

5 [Properties] をクリックします。

[Text Files] タブがデフォルトで表示されます。

6 [Add] をクリックします。

1 つのテキストファイルを追加した後、別のテキストファイルを追加するか、または選択したテキストファイルの変更する項目を追加するかを選択できます。

テキストファイルを追加するには、[Text File] を選択します。左側のペインでどのテキストファイルまたは変更項目が選択されていてもかまいません。テキストファイルは最も左のレベルに追加されます。

テキストファイルに別の変更を追加するには、左側のペインで変更するテキストファイルを選択し、[Add] をクリックして、[Change] を選択します。選択したテキストファイルの下に変更項目が追加されます。

7 テキストファイルを追加している場合は、テキストファイルの名前を指定します。

8 デフォルトの名前（Change #1 など）を受け入れるか、デフォルトの名前を変更します。テキストファイルを追加している場合は、[OK] をクリックします。

9 [Change Mode] フィールドの下向きの矢印をクリックし、ドロップダウンリストから変更モードを選択します。

10 [Search Type] フィールドの下向きの矢印をクリックし、ドロップダウンリストから検索の種類を選択します。

11 検索文字列を正確に入力します。

12 大文字と小文字を区別して文字列を検索する場合は、チェックボックスをオンにします。

13 検索文字列のすべての出現箇所を検索するには、チェックボックスをオンにします。このチェックボックスをオフにすると、最初の出現箇所だけが検索されます。

14 [Result Action] フィールドの下向きの矢印をクリックし、ドロップダウンリストから、文字列が一致する場合のアクションを選択します。

15 文字列を置き換えたり、新しい文字列を入力する場合は、[New String] テキストボックスにテキストを入力します。

16 追加する各テキストファイルまたは各変更について、手順 6 からステップ 15 までを繰り返します。

17 テキストファイルや変更項目の順序を変更するには、方向キーを使用します。

18 ポリシーのスケジュールを設定します。238 ページの「ポリシーのスケジュール設定」を参照してください。

19 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、スケジュールも入力したテキストファイルも保存されません。

ZENworks Database

インストール時に Server Management データベースをインストールしたが、データベースファイルを Database オブジェクトに関連付けてはいない場合、そのオブジェクトの DN を設定して、このポリシーが関連付けられるサーバが情報を記録するためのデータベースファイルを検出できるようにすることができます。

ZENworks データベースポリシーを設定するには

1 ConsoleOne で、SLP のプロパティパッケージを右クリックし、[Properties] をクリックします。

2 ZENworks データベースポリシーを選択し、[Properties] をクリックします。

ZENworks データベースポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

3 [Policy/Distribution Management] タブを選択します。

[Inventory Management] タブがデフォルトで表示されます。適切なタブを使用していることを確認します。

4 ZENworks データベースオブジェクトの DN を指定するか、DN を参照して選択し、[OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、DN は保存されません。

このポリシーは、Policy and Distribution Services の基本的な設定パラメータを提供します。

ZENworks Server Management ポリシーを設定するには

1 ConsoleOne で、Distributed Server Package のコンテナを選択し、Distributed Server Package を右クリックして、[Properties] をクリックします。

2 [Policies] > [NetWare]（またはその他のプラットフォーム）の順にクリックします。

3 ZENworks Server Management ポリシーを選択し、[Properties] をクリックします。

ZENworks Server Management ポリシーの [Enabled] 列のボックスがオンになっていない場合は、オンにしてから [Properties] をクリックします。[Properties] ボタンをアクティブにするには、ポリシーが有効になっている必要があります。

[General ミ Status] タブが表示されます。

4 ポリシーの一般的なステータスを指定するには

4a サーバコンソールにメッセージを表示する場合に従う手順を選択します。

4b SNMP トラップを送信する場合に従う手順を選択します。

管理コンソールでの SNMP トラップの表示については、210 ページの「Zentrap.mib のコンパイル」を参照してください。

4c ログファイルに情報を記録する場合に従う手順を選択します。

ログを記録する手順	Description
Log File	このオプションを選択して有効にし、ログファイルのファイル名を入力します。フルパスを指定します。デフォルトでは、ここでファイル名を入力しない限り、Policy and Distribution Services は ¥zenworks¥zfs-startup.log を使用します。次に、このポリシーが適用されるサーバについて、zfs-startup.log の代わりにここで指定したログファイルが使用されます。 次に例を示します。 sys:¥zenworks¥polpack.log sys:¥zenworks¥polpack.txt data:¥zenworks¥policies.log
Delete Log Entries Older Than__Days	このオプションを使用して、ディスク容量の使用状況を制御します。
E-Mail Messages	電子メールメッセージを送信するかどうかを選択します。[None] または [Errors Only] オプションをお勧めします。
◆ Users	ユーザ、グループ、または電子メールアドレスを追加できます。
◆ Address Attribute	ユーザまたはグループを選択すると、関連付けられたユーザまたはグループの属性がこのフィールドに表示されます。ドロップダウンリストから属性を変更できます。

重要： [E-Mail Messages] オプションを [None] または [Errors Only] のいずれかに設定します。このオプションをより詳しいレベルに設定すると、電子メールメッセージが過剰に作成されるためパフォーマンスが低下します。

5 ポリシーの設定を指定するには、[ZENworks Server Management] タブを選択し、[Configuration] をクリックします。

5a コンソールプロンプトを指定します。

プレーンテキストおよび変数を使用してプロンプトをカスタマイズできます。デフォルトは次のとおりです。

```
%SERVER_DN% - ZENworks Server Management >
```

定義済みの変数やユーザ定義の変数を使用できます。詳細については、359 ページの「変数の種類」を参照してください。

5b 作業パスを指定します。

これは、Policy and Distribution Services の一時ファイルおよびバックアップファイル用です。デフォルトのディレクトリは ¥zenworks¥pds¥smanager¥working です。

5c データベースの情報がどの程度古くなったらパージするかを指定するには、日数を入力します。

入力した日数よりも古いポリシー関連のすべての情報は、zfslog.db が保存されている同じサーバで Server Management を起動したときにパージされます。

重要： データベースをパージできるのは、Server Management が、zfslog.db が保存されているサーバと同じサーバで実行されている場合だけです。

Tiered Electronic Distribution の情報は、手動でデータベースからパージします。詳細については、375 ページの「データベースのパージ」を参照してください。

6 ZENworks Web Server のポート番号を設定するには、[Port Configuration] タブを選択し、ポート番号を選択または入力します。

7 [OK] をクリックしてポリシーを閉じます。

[Cancel] をクリックすると、どのタブで行ったポリシーの変更も保存されません。

ポリシーを使用したカスタムログファイルの作成

カスタムログファイルを作成する場合は、次の Tiered Electronic Distribution ポリシー (Service Location Package) または ZENworks Server Management ポリシー (Distributed Server Package) を使用できます。

- **Tiered Electronic Distribution ポリシー：** このポリシーを使用して Service Location Package を eDirectory コンテナに関連付けます。eDirectory コンテナにあるすべての Distributor および Subscriber オブジェクトがこのポリシーを使用できます。各オブジェクトのプロパティで表示される [Use Policy] チェックボックスを使用すると、Distributor または Subscriber がポリシーを使用するかどうかを個別に選択できます。このチェックボックスはデフォルトでは無効に設定されています。

  このポリシーを使用して、Distribution Agent が選択した Distributor および Subscriber に関する Tiered Electronic Distribution 情報をカスタムログファイルに記録します。

- **ZENworks Server Management ポリシー:** このポリシーを使用してポリシーを適用するサーバに Distributed Server Package を配布できます。

  このポリシーを使用して、サーバの Policy/Package Agent がポリシーとソフトウェアパッケージの情報をカスタムログファイルに記録します。

これらのポリシーのいずれかを作成および環境設定する場合、ログファイルの［Path and Filename］フィールドはデフォルトでは空白になります。

これらのポリシーの作成方法と環境設定方法については、次を参照してください。

- 213 ページの「Tiered Electronic Distribution」
- 234 ページの「ZENworks Server Management」

ポリシーの有効化

ポリシーがポリシーパッケージで効力を持つには、ポリシーを有効にする必要があります。パッケージからポリシーを削除せずに、ポリシーを無効にすることができます。

ポリシーを有効にするには

1. ConsoleOne で、有効にするポリシーが含まれているポリシーパッケージオブジェクトを右クリックし、［Properties］をクリックします。
2. ポリシーを有効にするには、［Enabled］列の下のチェックボックスをオンにします。

   ポリシーを有効にする場合は、ポリシーが正しく設定されていることを確認します。
3. 有効にしたポリシーを適用するには、ポリシーパッケージを配布します。

   詳細については、236 ページの「ポリシーの配布」を参照してください。

ポリシーの配布

ポリシーが効力を持つようにするには、Distributed Server Package を配布する必要があります。パッケージを配布する場合、有効にしたポリシーは、Subscriber が Distribution を抽出した後、パッケージが配布されたサーバにのみ適用されます。

サーバにポリシーを配布するには

1. Policy Package タイプである Distribution を作成します。
2. ポリシーパッケージでポリシーを設定します。
3. Policy Package Distribution の Channel を選択します。
4. Subscriber で、選択した Channel を購読します。
5. Distribution を送信します。

受信側のサーバの Policy/Package Agent が有効なポリシーを抽出し、サーバ上でポリシーを適用します。

Policy Package Distribution の作成の詳細については、54 ページの「Distribution の作成と設定」を参照してください。

ポリシーの関連付け

Distributor は Distribution によってポリシーを受信しないので、Distributor オブジェクトにコンテナパッケージオブジェクトを関連付けて、Distributor が更新されたときに eDirectory ツリーを読み込む方法として検索ポリシーを使用できます。

Distributor オブジェクトは、Service Location Package にも関連付けられている必要があります。このパッケージには ZENworks データベースポリシーが含まれており、Distributor Agent はレポート情報を書き込むためのデータベースファイルを見つけることができます。Distributor が使用するその他のポリシーも含まれています。212 ページの「Service Location Package ポリシーの設定」を参照してください。

ポリシーパッケージを Distributor オブジェクトのコンテナに関連付けるには

- 237 ページの「Distributor オブジェクトへのポリシーパッケージの関連付け」
- 237 ページの「ポリシーパッケージへの Distributor オブジェクトの関連付け」

Distributor オブジェクトへのポリシーパッケージの関連付け

ポリシーパッケージを Distributor オブジェクトのコンテナに関連付けるには

1. ConsoleOne で、ポリシーパッケージを右クリックし、[Properties] をクリックします。
2. [Associations] タブを選択し、[Add] をクリックします。
3. Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を参照して選択し、[OK] をクリックします。

   [Cancel] をクリックすると、関連付けは保存されません。

ポリシーパッケージへの Distributor オブジェクトの関連付け

Distributor オブジェクトのコンテナをポリシーパッケージに関連付けるには

1. ConsoleOne で、Distributor オブジェクトが存在しているコンテナ（またはその上位のコンテナ）を右クリックし、[Properties] をクリックします。
2. [ZENworks] タブ、[Associated Policy Packages] の順に選択し、[Add] をクリックします。
3. ポリシーパッケージを参照して選択し、[OK] をクリックします。

   [Cancel] をクリックすると、関連付けは保存されません。
4. Distributor オブジェクトのコンテナに関連付ける他のポリシーパッケージについて、ステップ 2 およびステップ 3 を繰り返します。

ポリシーのスケジュール設定

詳細については、353 ページの「スケジュール設定とサーバポリシー」を参照してください。

有効なポリシーの表示

現在のサーバオブジェクトで有効な ZENworks 6.5 Server Management ポリシーを表示するには

1 サーバ上の ZENworks Server Management プロンプトで、「Policy List」と入力します。

サーバで現在有効になっているポリシーが表示されます。

ポリシー適用の変更

特定のサーバまたはサーバのグループについて、ポリシーの適用を変更または停止しなければならない場合があります。

ポリシーの適用はいくつかの方法で変更できます。

- 238 ページの「適用されるポリシーの変更」
- 239 ページの「特定のポリシーの適用の停止」
- 239 ページの「特定の Subscriber に関するポリシー適用の削除」
- 240 ページの「Policy Package Distribution の適用の停止」

適用されるポリシーの変更

適用されているポリシーを変更するには

1 ConsoleOne で、変更するポリシーが含まれている Distributed Server Package オブジェクトを右クリックし、[Properties] をクリックします。

2 必要に応じてポリシーを変更し、[OK] をクリックしてポリシーパッケージのプロパティを終了します。

次回、このポリシーパッケージを含む Distribution を構築するときに、次の処理が行われます。

1. Distribution が変更されたので、新しいバージョンの Distribution が作成されます。
2. Channel の送信スケジュールに従って、Policy/Package Distribution が送信されます。
3. Channel を購読している各 Subscriber が、Policy/Package Distribution を受信し、抽出スケジュールに従って抽出します。
4. 変更されたポリシーは、Policy Package Distribution が抽出された Subscriber 上で適用されます。

特定のポリシーの適用の停止

特定のポリシーの適用を停止するには

1 ConsoleOne で、停止するポリシーが含まれている Distributed Server Package オブジェクトを右クリックし、[Properties] をクリックします。

2 停止するポリシーを選択し、次のいずれかの操作を行います。

2a [Enabled] 列にあるチェックボックスを選択して、ポリシーを無効にします。

2b [Remove] をクリックして複数ポリシーを削除します。

複数ポリシーは以前に [Add] ボタンを使用して追加したので、ポリシーパッケージから削除できます。

3 [OK] をクリックして変更内容を保存し、ポリシーパッケージのプロパティを終了します。

次回、このポリシーパッケージを含む Distribution を構築するときに、次の処理が行われます。

1. Distribution が変更されたので、新しいバージョンの Distribution が作成されます。
2. Channel の送信スケジュールに従って、Policy Package Distribution が送信されます。
3. Channel を購読している各 Subscriber が、Policy Package Distribution を受信し、抽出スケジュールに従って抽出します。
4. 無効化 / 削除されたポリシーは、Policy Package Distribution が抽出された Subscriber 上で適用されなくなります。

特定の Subscriber に関するポリシー適用の削除

配布されたポリシーが、その Distribution を受信しているすべての Subscriber ではなく、特定の Subscriber サーバで適用されないようにするには、次の操作を行います。

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [Channels] タブを選択し、適用から削除するポリシーを含む Channel を選択し、[Remove]、[OK] の順にクリックします。

3 [OK] をクリックして、Subscriber オブジェクトのプロパティを閉じます。

4 Subscriber サーバのファイルシステムで、次のファイルを削除します。

- ポリシーの Distribution ファイルを含む Distribution ディレクトリ
- …¥smanager¥policy ディレクトリ (Policy Package Distribution の抽出時に作成される) の関連するポリシーファイル (.pol)

5 Subscriber サーバをリセットし、ポリシーの設定を更新します。

Subscriber は、このポリシーを含む Policy Package Distribution を受信しなくなり、以前に Subscriber に配布されたポリシーも適用されなくなります。

Policy Package Distribution の適用の停止

Policy Package Distribution の適用を、この Distribution が配布されたすべての Subscriber で停止する必要がある場合は、特定の手順に従う必要があります。ポリシーパッケージは配布済みなので、ポリシーパッケージオブジェクトを削除しただけでは、Distribution を受信した各 Subscriber でそのポリシーを適用できます。

適用を停止するには、次の操作を行います。

1 ConsoleOne で、Policy Package タイプの Distribution オブジェクトを削除します。

重要： ポリシーパッケージに、停止したくない他のポリシーも含まれている場合は、パッケージを削除しないでください。その代わりに、停止するポリシーだけを無効にします。

2 Subscriber サーバのファイルシステムで、Policy Package Distribution によって作成された .pol ファイルを削除します。

この .pol ファイルは、¥zenworks¥pds¥smanager¥policies ディレクトリにあります。

3 各 Subscriber でポリシーを更新します。

この処理は、各 Subscriber サーバのコンソールで Policy Refresh コマンドを使用して行うことも、iManager から［Refresh］オプションを使用して行うこともできます。

Subscriber サーバのポリシーを更新した後、Policy Package Distribution に含まれるポリシーは、Subscriber 上で適用されなくなります。更新プロセスによって、すべてのポリシーのメモリがクリアされ、ファイルシステムに存在している Policy Package Distribution から再ロードされます。

5 Server Software Package に関する問題

Novell® ZENworks® Server Management には、ネットワーク上のファイルおよびアプリケーションを管理するための Server Software Packages コンポーネントが用意されています。ソフトウェアパッケージを使用して、サーバ上のソフトウェアのインストールおよびアップグレードを自動化できます。

ソフトウェアパッケージを使用することの最大の価値は、パッケージのインストールの前後にサーバ上で実行する処理をセットアップできることです。

次の節では、Server Software Packages コンポーネントを使用することにより、どのような恩恵を受けることができるのかを説明します。

- 241 ページの「Server Software Packages によるソフトウェアの管理」
- 242 ページの「Server Software Packages の理解」
- 255 ページの「Server Software Packages のプランニング」
- 257 ページの「Server Software Package の設定」
- 275 ページの「古いバージョンの Server Software Package の ZENworks 6.5 Server Management への変換」
- 277 ページの「Server Software Packages によるサーバ上のディレクトリの削除」

Server Software Packages によるソフトウェアの管理

ソフトウェアの管理は、Server Software Packages を作成し、Tiered Electronic Distribution を使用してソフトウェアパッケージを配布することによって行います。サーバにパッケージをインストールする前に、サーバが特定の最低限の条件を満たしていなければならないように Server Software Packages を設定できます。ソフトウェアパッケージは、複数のソフトウェアパッケージコンポーネントで構成される場合があります。

各ソフトウェアパッケージコンポーネントも、そのコンポーネントをサーバにインストールする前に、最低限の条件が満たされていなければならないように設定できます。

以前の .spk および .cpk ファイルから ZENworks 6.5 Server Management への変換については、275 ページの「古いバージョンの Server Software Package の ZENworks 6.5 Server Management への変換」を参照してください。

Server Software Packages の理解

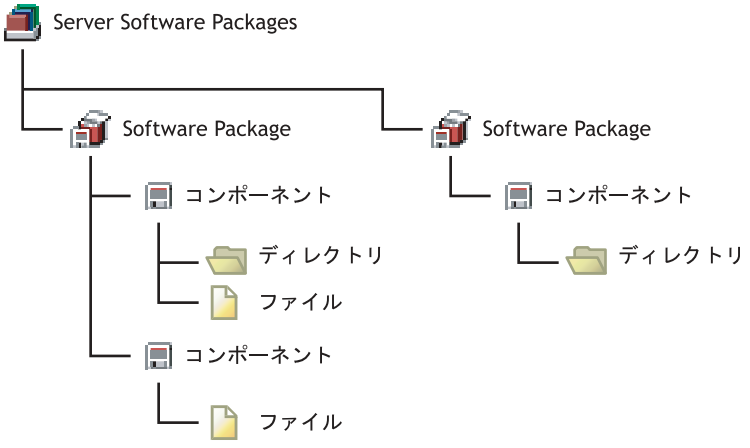
Policy and Distribution Services には、サーバファイルおよびアプリケーションの配布やインストールを自動化および標準化するための手段が用意されています。これには、NLM™ のバージョン、環境設定ファイル、データベースなどを標準化する機能も含まれます。次の節を参照してください。

- 242 ページの「Server Software Packages およびコンポーネントの理解」
- 243 ページの「ソフトウェアパッケージとコンポーネントの環境設定の理解」
- 244 ページの「ソフトウェアパッケージをインストールする順序の決定」
- 245 ページの「抽出したファイルの実行」
- 245 ページの「ソフトウェアパッケージのコンパイル」
- 246 ページの「ソフトウェアパッケージへのアクセス」
- 247 ページの「ソフトウェアパッケージの配布」
- 248 ページの「Server Software Package の管理」
- 247 ページの「クラスタへのソフトウェアパッケージの配布」
- 254 ページの「ソフトウェアパッケージのインストールのロールバック」

Server Software Packages およびコンポーネントの理解

サーバにインストールするためにサーバファイルおよびアプリケーションを配布するには、ソフトウェアパッケージにソフトウェアを含める必要があります。ソフトウェアパッケージは、ConsoleOne® の Server Software Packages ネームスペースに作成します。ソフトウェアパッケージの作成は、ソフトウェアのインストール実行可能ファイルの構築に似ています。

次の図は、ソフトウェアパッケージとパッケージコンポーネントの関係を示しています。



次の点に注意してください。

- ソフトウェアパッケージオブジェクトはServer Software Packagesネームスペースに表示されます。
- ソフトウェアパッケージオブジェクトには複数のコンポーネントオブジェクトが含まれる場合があります。

- コンポーネントオブジェクトにはファイルやディレクトリが含まれる場合があります。
- 各ソフトウェアパッケージには1つまたは複数のアプリケーションのすべてのファイルが含まれる場合があります。
- Software Package 環境設定ファイル (.spk および .cpk) はサーバまたはワークステーションのファイルシステムに格納されます。

ソフトウェアパッケージとコンポーネントの環境設定の理解

ソフトウェアパッケージとそのコンポーネントには、環境設定情報とインストールの要件が含まれます。各コンポーネントオブジェクトはそれぞれの環境設定パラメータによって制御されるので、インストール前のアクション、インストールのアクション、インストール後のアクションなど、1 つのソフトウェアパッケージについて複数のコンポーネントを使用できます。

サーバファイルおよびアプリケーションの配布やインストールに関する次のような項目を設定できます。

- 特定のオペレーティングシステムの要求
- ターゲットサーバで必要な RAM 容量の指定
- ターゲットサーバで必要なディスク容量の指定
- ターゲットサーバ上での特定の SET コマンドの要求
- ターゲットサーバのレジストリの変更
- ターゲットサーバ上でのファイルの置換
- products.dat の特定のエントリの要求

ソフトウェアパッケージのインストールの前提条件の要求

ソフトウェアパッケージでインストールの前提条件を指定できるだけでなく、パッケージの各コンポーネントでもインストールの前提条件を指定できます。前提条件は次の順序で確認され、インストールできるかどうかが判断されます。

- パッケージの前提条件が満たされていない場合は、どのコンポーネントもインストールされません。
- パッケージの前提条件が満たされている場合は、コンポーネントをインストールできます。
- コンポーネントの前提条件が満たされていない場合は、そのコンポーネントはインストールされません。

一部のコンポーネントがインストールされ、他のコンポーネントがインストールされない場合があるので、ソフトウェアパッケージが部分的にインストールされる可能性があります。

重要： 前提条件を指定する場合は、すべてのコンポーネントに等しく適用される前提条件はソフトウェアパッケージレベルで作成し、特定のコンポーネントに固有の前提条件はコンポーネントレベルで作成します。

ソフトウェアパッケージの命名

ソフトウェアパッケージを作成する場合、最初は .spk という拡張子を付けます。これは、まだコンパイルされていないソフトウェアパッケージを表します。このファイルには、ソフトウェアパッケージとそのすべてのコンポーネントのインストールの要件がすべて含まれています。

警告： ソフトウェアパッケージ名に 2 バイト文字を使用しないでください。このソフトウェアパッケージについてレポートを実行したときにエラーの原因になります。

ソフトウェアパッケージをインストールする順序の決定

Distribution 内の Server Software Packages の順序の指定に関して注意事項が 2 つあります。

- 244 ページの「複数の Distribution を使用したソフトウェアパッケージの配布順序の強制的な指定」
- 244 ページの「依存関係を使用したソフトウェアパッケージの配布順序の強制的な指定」
- 245 ページの「ソフトウェアパッケージの順序によるロールバックへの影響」

複数の Distribution を使用したソフトウェアパッケージの配布順序の強制的な指定

1 つの Distribution に複数のソフトウェアパッケージを含める場合は、次の点に注意してください。

- Distribution を構築するときに、複数のソフトウェアパッケージは特定の順序で Distribution にまとめられるわけではありません。
- Distribution を抽出してインストールするときに、複数のソフトウェアパッケージは保証された順序でサーバに適用されるわけではありません。
- 1 つの Distribution に含まれ、特定の順序でインストールが開始された複数のソフトウェアパッケージは、同じ順序でインストールが終了するわけではありません。

ソフトウェアパッケージを特定の順序でインストールするには

1. 各ソフトウェアパッケージをそれ自体の Distribution に (Distribution ごとにソフトウェアパッケージを 1 つ) 配置します。
2. Distribution を送信して抽出する順序をスケジュールすることによって、ソフトウェアパッケージをインストールする順序を制御します。

依存関係を使用したソフトウェアパッケージの配布順序の強制的な指定

ソフトウェアパッケージを特定の順序でインストールする別の方法としては、複数の Software Package Distribution 間に依存関係を使用します。たとえば、前のソフトウェアパッケージと後続のソフトウェアパッケージの間に依存関係を確立します。

例：

1. Software Package Distribution 1 を作成します。
2. Software Package Distribution 1 からインストールされる内容と何らかの依存関係を持たせて Software Package Distribution 2 を作成します。
3. 両方の Distribution を送信します。
4. Subscriber が Software Package Distribution 2 を最初に抽出しようとすると、抽出は失敗します。

5. Subscriber が Software Package Distribution 1 を抽出すると、Software Package Distribution 2 を抽出するのに必要な依存関係が Subscriber に提供されます。
6. これにより、Subscriber は正常に Software Package Distribution 2 を抽出できます。

依存関係を使用すると、スケジュールを使用してインストール順序を制御する必要がありません。

ソフトウェアパッケージの順序によるロールバックへの影響

1 つの Distribution に複数のソフトウェアパッケージが含まれている場合、開始した順序で抽出が終了するとは限らないので、ロールバックもこの影響を受けます。

Distribution に含まれるソフトウェアパッケージの処理の順序を指定することはできますが、この順序は保証されません。これは、ソフトウェアパッケージの処理を終了するまでにかかる時間が各パッケージによって異なり、ロールバックの順序を決定するのがソフトウェアパッケージの処理の終了時刻であるからです。

つまり、最後に正常に処理されたソフトウェアパッケージをロールバックした後、処理が終了した順序とは逆の順序でのみ、その他のソフトウェアパッケージをロールバックできます。

[Package List] コマンドを使用して、ソフトウェアパッケージの処理が終了した順序を表示できます。アスタリスクは、次にロールバックが可能なパッケージを示します。

ロールバックの詳細については、254 ページの「ソフトウェアパッケージのインストールのロールバック」を参照してください。

抽出したファイルの実行

Software Package Distribution では、ソフトウェアパッケージからサーバにコピーされるファイルの中に、パッケージの抽出時に実行する実行可能ファイルが含まれている場合があります。

ソフトウェアパッケージを通じて配布される実行可能ファイルを実行するには、ソフトウェアパッケージのファイルに対して、実行前後のアクション（実行順序など）を設定します。前後のアクションは、Server Software Package の作成時と Software Package Distribution の作成時に使用できます。

詳細については、129 ページの「Distribution の前後の処理」および 263 ページの「ソフトウェアパッケージコンポーネントの環境設定」を参照してください。

ソフトウェアパッケージのコンパイル

コンポーネントの環境設定など、ソフトウェアパッケージを定義した後、ソフトウェアパッケージをコンパイルする必要があります。この処理では、ファイルやアプリケーションとその環境設定を配布用の 1 つのファイルに圧縮します。

コンパイルされたソフトウェアパッケージのデフォルトの拡張子は .cpk です。コンパイル済みのバージョンには、ソフトウェアパッケージが表すファイルやアプリケーションをインストールするために必要なすべてのファイルが含まれています。

重要： コンパイル済みファイル名の指定を求められたときに .spk ファイルのパスとファイル名を指定すると、その .spk ファイルは上書きされ、編集できなくなります。コンパイル済みバージョンの名前を指定するときには、.cpk という拡張子を使用してください。

ソフトウェアパッケージにはコピーされる多くのファイルが含まれる場合があるので、.cpk ファイルのサイズは非常に大きく（数百メガバイト）になる可能性があります。したがって、通常、.cpk ファイルは十分な空きディスク容量があるサーバに保存してください。

ただし、ソフトウェアパッケージによって単純な機能を実行することもでき、この場合 .cpk ファイルのサイズは比較的小さくなるため、ワークステーションに保存することもできます。たとえば、ファイルサーバ上のディレクトリを削除するだけのためにソフトウェアパッケージを設定することもできます。277 ページの「Server Software Packages によるサーバ上のディレクトリの削除」を参照してください。

ロールバックに対応したソフトウェアパッケージが正常にインストールされると、サーバ上にロールバックパッケージが作成されます。このロールバックパッケージを処理すると、サーバはパッケージがインストールされる前の元の状態に戻ります。詳細については、254 ページの「ソフトウェアパッケージのインストールのロールバック」を参照してください。

ソフトウェアパッケージへのアクセス

ソフトウェアパッケージを保存する場所（ワークステーションまたはサーバ）は、ソフトウェアパッケージの管理方法によって異なります。

Server Software Packages コンポーネントは ConsoleOne のネームスペースを使用するので、ConsoleOne を実行している任意のワークステーションまたはサーバからソフトウェアパッケージにアクセスできます。

ただし、次の点に注意する必要があります。

- 246 ページの「ワークステーションからの ConsoleOne の実行」
- 246 ページの「サーバからの ConsoleOne の実行」

複数のワークステーションからのソフトウェアパッケージの管理については、248 ページの「Server Software Package の管理」を参照してください。

ワークステーションからの ConsoleOne の実行

ワークステーションから ConsoleOne を実行し、ソフトウェアパッケージをそのワークステーションに保存する場合、ConsoleOne 内のそのパッケージは、ConsoleOne を実行する他のワークステーションやサーバで利用できません。

サーバからの ConsoleOne の実行

異なるワークステーションでサーバ上の ConsoleOne を実行する場合は、各ワークステーションのサーバへのドライブマッピングが同じである必要があります。ドライブマッピングが異なる場合、そのサーバに保存したソフトウェアパッケージを別のワークステーションで読み込むことができません。

たとえば、次のような場合にはパッケージを見つけることができます。

1. ワークステーション A から ConsoleOne を実行してサーバ A にアクセスします。
2. サーバ A はワークステーション A の S: ドライブとしてマッピングされています。
3. pkg_a.spk をサーバ A に保存します。
4. ワークステーション B から ConsoleOne を実行してサーバ A にアクセスします。
5. サーバ A はワークステーション B でも S: ドライブとしてマッピングされています。
6. 両方のワークステーションが S: ドライブにマッピングされているので、pkg_a.spk を見つけることができます。

次のような場合にはパッケージを見つけることができません。

1. ワークステーション A から ConsoleOne を実行してサーバ A にアクセスします。
2. サーバ A はワークステーション A の S: ドライブとしてマッピングされています。
3. pkg_a.spk をサーバ A に保存します。
4. ワークステーション B から ConsoleOne を実行してサーバ A にアクセスします。
5. サーバ A はワークステーション B では T: ドライブとしてマッピングされています。
6. pkg_a.spk は S: ドライブに保存されており、T: ドライブでパッケージを検索しているので、パッケージを見つけることはできません。

この 2 つの例の違いは、各ワークステーションでのサーバ A に対するドライブ名だけです。

ソフトウェアパッケージの配布

Distribution には、インストールされるソフトウェアパッケージまたは抽出されるファイルのグループを含めることができます。

Policy/Package Agent は、Subscriber サーバに Software Package Distribution を抽出またはインストールします。

ソフトウェアパッケージを作成するときに、ターゲット Subscriber サーバにパッケージをインストールするために満たしていなければならないシステムの要件をパッケージに含めることができます。Subscriber が要件を満たしている場合、パッケージが実際にインストールされる時期は購読スケジュールによって決まります。

クラスタへのソフトウェアパッケージの配布

ソフトウェアパッケージを含む Distribution をクラスタに送信して各ノードの sys: ボリュームを更新する場合、クラスタ内で現在 Subscriber ソフトウェアを実行しているノードだけがパッケージを受信します。

クラスタ内のノードを構成するコンピュータが Subscriber ソフトウェアを実行するので、ある時点で Subscriber ソフトウェアをアクティブに実行しているノードは 1 つだけです。

したがって、Software Package Distribution を使用してクラスタ内の各ノードの sys: ボリューム上のファイルを更新する場合は、手動でこの作業を行う必要があります。まず、1 つのノードを更新し、そのノードを停止することによって、フェールオーバーシーケンス内の次のノードが前のノードでエラーが発生したことを確認し、Subscriber ソフトウェアの実行が開始されるようにします。次に、そのコンピュータを更新して停止するという作業を、クラスタ内のすべてのコンピュータが更新されるまで続けます。次に、停止したすべてのサーバを再起動すると、プライマリノードのコンピュータが再び処理を引き継ぎます。

Software Package Distribution を使用して、Tiered Electronic Distribution の .ncf ファイルなど、クラスタコンピュータ自体に保存されているファイルを更新できます。これは、Subscriber ソフトウェアがクラスタコンピュータの共有ハードディスクドライブに保存されているからです。

Server Software Package の管理

次の節では、Server Software Package のファイルの保存場所および管理方法について説明します。

- 248 ページの「Server Software Package のファイルの理解」
- 249 ページの「ソフトウェアパッケージ管理オプションの理解」
- 249 ページの「1 台のワークステーションによる .spk ファイルの保存と管理」
- 249 ページの「.spk ファイルのネットワークサーバへの保存と複数のワークステーションからの管理」
- 252 ページの「例：マスタ snapinprefs.ser ファイルの使用」

Server Software Package のファイルの理解

ソフトウェアパッケージに関連するファイルには 3 つの種類があります。

- **環境設定ファイル (.spk)：** Server Software Package を作成する場合、最初にパッケージの環境設定ファイル (.spk) を作成します。このファイルの環境設定は、ConsoleOne の Server Software Packages ネームスペース内のソフトウェアパッケージオブジェクトのプロパティで作成します。

  .spk ファイルは一般的にサイズの小さい (約 100KB) ファイルです。したがって、このファイルは一般的に、ソフトウェアパッケージの作成や管理に使用する ConsoleOne のインスタンスを実行しているワークステーションに保存できます。

- **コンパイル済みファイル (.cpk)：** ソフトウェアパッケージをコンパイルするときに、.spk ファイルの環境設定情報から .cpk ファイルが作成されます。このファイルは、ファイルや機能などのソフトウェアパッケージの内容を提供します。.cpk ファイルはソフトウェアパッケージの内容をサーバにインストールするために使用されます。

  コンパイル済みのソフトウェアパッケージには多数のファイルが含まれる場合があるので、一般的に、.cpk ファイルは十分な空きディスク容量があるサーバに保存します。ただし、機能だけを含む小さな .cpk ファイルはワークステーションに保存することもできます。

- **初期設定ファイル (.ser)：** 初期設定ファイル (snapinprefs.ser) は、ソフトウェアパッケージの作成に使用したワークステーション上に自動的に作成されます。このファイルには、ソフトウェアパッケージの .spk ファイルへのポインタが含まれています。

  この初期設定ファイルによって、ソフトウェアパッケージが ConsoleOne のネームスペースにあることを確認できます。つまり、ソフトウェアパッケージが ConsoleOne のインスタンスの Server Software Packages ネームスペースに表示されるのは、.spk ファイルのパスが ConsoleOne のインスタンスを実行するワークステーション上にある初期設定ファイルにリストされている場合だけです。

新しいソフトウェアパッケージを作成する場合は、.spk ファイルのローカルパスを指定します。ソフトウェアパッケージをコンパイルする場合は、サーバの .cpk ファイルのパスを指定します。ConsoleOne を終了した後、ソフトウェアパッケージを作成、削除、またはコンパイルするたびに、.spk ファイルのパスが snapinprefs.ser ファイルに記録されます。

.cpk ファイルへのパスも snapinprefs.ser ファイルに記録されます。次回ソフトウェアパッケージをコンパイルするときには、ウィザードによって .cpk ファイルの以前の保存場所が表示されるので、パッケージをコンパイルするたびにファイルの場所を覚えておく必要はありません。ただし、Tiered Electronic Distribution を使用して .cpk ファイルを配布する場合は、.cpk ファイルを保存した場所をメモしておく必要があります。.cpk ファイルの場所はソフトウェアパッケージのプロパティには保存されないからです。

ソフトウェアパッケージ管理オプションの理解

特定のワークステーションを 1 台だけ使用して、すべてのソフトウェアパッケージファイルを表示、作成、および管理している場合は、.spk ファイルをそのワークステーションに保存できます。

複数のワークステーションからソフトウェアパッケージを管理することもできます。この場合は、.spk ファイルの保存場所をネットワークサーバに一元化する必要があります。また、この方法では、マスタ snapinprefs.ser ファイルを使用して、任意のワークステーションからすべてのソフトウェアパッケージを表示できるようにする必要があります。

次の 2 つの節では、これらの管理オプションについて説明します。

1 台のワークステーションによる .spk ファイルの保存と管理

ワークステーションを 1 台だけ使用してソフトウェアパッケージを表示、作成、および管理する場合は、.spk ファイルをワークステーションに、.cpk ファイルをサーバに保存できます。

ConsoleOne がインストールされているワークステーションから ConsoleOne を実行している場合でも、ネットワークサーバ上にインストールされている ConsoleOne を使用するワークステーションから ConsoleOne を実行している場合でも、ConsoleOne を実行するために使用されているワークステーション上の snapinprefs.ser ファイルが更新されます。

.spk ファイルのネットワークサーバへの保存と複数のワークステーションからの管理

複数のワークステーションを使用して同一セットのソフトウェアパッケージを表示、作成、および管理する場合は、すべての .spk ファイルをネットワークサーバに保存して、各ワークステーションからアクセスできるようにする必要があります。

異なるワークステーションを使用して、異なるソフトウェアパッケージのセットを管理することもできます。任意のワークステーションを使用して .spk ファイルを作成すると、それ自体のソフトウェアパッケージ初期設定ファイルが、ソフトウェアパッケージの管理に使用するワークステーションに作成されます。

snapinprefs.ser ファイルのマスタコピーを使用する場合は、複数のワークステーションからすべてのソフトウェアパッケージを管理できます。

- 250 ページの「ソフトウェアパッケージ初期設定ファイルの理解」
- 251 ページの「複数のワークステーションからのソフトウェアパッケージの管理」
- 251 ページの「複数のワークステーションからのソフトウェアパッケージの管理に関する一般的な規則」
- 252 ページの「複数のワークステーションによるソフトウェアパッケージの管理の最適なシナリオ」

ソフトウェアパッケージ初期設定ファイルの理解

ConsoleOne で Server Software Package オブジェクトを作成すると、ソフトウェアパッケージ初期設定ファイル (snapinprefs.ser) が、ConsoleOne を実行しているワークステーションの次の場所に作成されます。

c:¥documents and settings¥user_ID¥.consoleone (Windows 2000)

user_ID は、ログインしたときの権限 (管理者など) に関連するユーザディレクトリです。

ソフトウェアパッケージのフルパスおよびファイル名はドライブに依存します。snapinprefs.ser ファイルには、ワークステーションによって作成された各 .spk ファイルのドライブ名、パス、およびパッケージ名が記述されます。

snapinprefs.ser ファイルは各ワークステーションに固有です。ワークステーションを使用して .spk ファイルを追加または削除するたびに更新されるのは初期設定ファイルです。したがって、3 台の異なるワークステーションを使用して .spk ファイルを作成した場合、各ワークステーションに 1 つずつ、3 つの異なる snapinprefs.ser ファイルが作成されます。

ConsoleOne を起動すると、そのワークステーションで実行されている ConsoleOne のインスタンスによって、そのワークステーション用の snapinprefs.ser ファイルが作成されているかどうかが確認されます。また、ConsoleOne がそのワークステーションにインストールされているか、またはサーバにインストールされているインスタンスをそのワークステーションで実行しているかが確認されます。snapinprefs.ser ファイルが存在しない場合は、ConsoleOne を終了するときに snapinprefs.ser ファイルが作成されます。snapinprefs.ser ファイルが存在する場合は、snapinprefs.ser ファイルが更新され、新しい .spk ファイルへのフルパスが保存されます。

snapinprefs.ser ファイルを、あるワークステーションから別のワークステーションにコピーできます。ただし、snapinprefs.ser ファイルを別のワークステーションからのコピーと置換した後、変更を有効にするには、ConsoleOne を再起動する必要があります。

パッケージを作成した後でドライブマッピングを変更すると、パッケージに対する snapinprefs.ser ファイルの場所が変わるので、ソフトウェアパッケージが使用できなくなる場合があります。ただし、UNC パスを使用している場合は、ワークステーションがその UNC パスにアクセスできる限り、この問題は発生しません。

ワークステーション上の snapinprefs.ser ファイルを置き換える場合は、新しくコピーした snapinprefs.ser ファイルに不足しているソフトウェアパッケージを手動で挿入する必要があります。この作業を行わない場合、置換された snapinprefs.ser ファイルにリストされていたソフトウェアパッケージは、ワークステーション上でアクセスできなくなります。

ワークステーションをソフトウェアパッケージの作成に一度も使用したことがない場合でも、別のワークステーションから適切な場所 (c:¥....¥.consoleone) に snapinprefs.ser ファイルをコピーできます。コピーした後、ConsoleOne を起動すると、コピーした snapinprefs.ser ファイルにリストされていたすべてのソフトウェアパッケージが表示されます。

詳細については、252 ページの「例：マスタ snapinprefs.ser ファイルの使用」を参照してください。

複数のワークステーションからのソフトウェアパッケージの管理

複数のワークステーションを使用して同一セットのソフトウェアパッケージを作成、削除、およびコンパイルする場合は、次のようにしてください。

1. .spk ファイルをネットワークサーバ（通常、対応する .cpk ファイルを保存しているサーバ）に保存し、すべてのソフトウェアパッケージが任意のワークステーションからアクセスできるようにします。
2. .spk および .cpk ファイルが保存されているサーバにワークステーションをマッピングする場合は、すべてのワークステーションで同じドライブ名を使用します。
3. すべてのワークステーションでソフトウェアパッケージの追加、削除、およびコンパイルの情報を最新情報に更新するために使用されるマスタ snapinprefs.ser ファイルを作成します。257 ページの「マスタ snapinprefs.ser ファイルの設定」を参照してください。
4. ワークステーション上で ConsoleOne を起動および停止するバッチファイルを作成します。258 ページの「ConsoleOne のバッチファイルの作成と使用」を参照してください。このバッチファイルで次の 2 つの処理を実行します。
   - ワークステーションで ConsoleOne が起動されるたびに、ストレージサーバからワークステーションに最新の snapinprefs.ser ファイルを自動的にアップロードします。

     これによって、ConsoleOne を起動したワークステーションですべてのソフトウェアパッケージを表示できます。
   - ワークステーションで ConsoleOne を終了するときに、変更された snapinprefs.ser ファイルをワークステーションからストレージサーバに自動的にダウンロードします。

     これによって、ワークステーションの最新のソフトウェアパッケージの追加が記述された .ser ファイルの新しいマスタコピーが作成されます。
5. ソフトウェアパッケージを管理するワークステーションからバッチファイルを実行します。261 ページの「ConsoleOne バッチファイルの使用」を参照してください。

複数のワークステーションからのソフトウェアパッケージの管理に関する一般的な規則

snapinprefs.ser ファイルのマスタコピーの使用に意味があるのは、あるワークステーションで ConsoleOne を終了し、別のワークステーションで ConsoleOne を起動する場合だけです。この連続的な方法は、ConsoleOne の複数のインスタンスを同時に実行し、各インスタンスがローカルの snapinprefs.ser ファイルを更新する場合には機能しません。最後に終了した ConsoleOne のインスタンスが、そのローカルの .ser ファイルをマスタコピーに上書きします。

重要： snapinprefs.ser ファイルにログが記録される処理は、ConsoleOne でのソフトウェアパッケージの作成、削除、またはコンパイルだけです。したがって、バッチファイルから ConsoleOne を起動しなくても、ConsoleOne を使用して、プロパティの表示や編集など、ソフトウェアパッケージを管理することができます。バッチファイルを使って ConsoleOne を起動しない場合は、ConsoleOne で .spk ファイルを追加、削除、またはコンパイルしないでください。

このマスタコピー / 単一のサーバ / 複数のワークステーションを使用する方法でソフトウェアパッケージを管理するには、以下の一般的な規則に従ってください。

- ソフトウェアパッケージ（.spk ファイル）を新規作成するか、新しいパッケージ（.cpk ファイル）をコンパイルした後、常に ConsoleOne を終了します。これによって、マスタ snapinprefs.ser ファイルに最新のソフトウェアパッケージのリンクが含まれます。

- 複数のワークステーションでソフトウェアパッケージを同時に管理しないでください。これらのワークステーションでバッチファイルを使用して ConsoleOne を起動すると、新規作成したソフトウェアパッケージへのパスが失われる場合があります。
- ソフトウェアパッケージを管理する場合以外は、バッチファイルを使用して ConsoleOne を起動しないでください。バッチファイルを使用せずに、ConsoleOne を起動してください。

  この操作が必要になるのは、バッチファイルは ConsoleOne を終了するときに、常にソフトウェアパッケージストレージサーバ上のマスタコピーを上書きするからです（バッチファイルを使用して ConsoleOne を起動した場合）。誤ってマスタ snapinprefs.ser ファイルが上書きされ、新規作成したソフトウェアパッケージへのリンクが失われる場合があります。

  たとえば、ワークステーション A でバッチファイルを使用して ConsoleOne を起動し、ソフトウェアパッケージ以外の管理作業を行い、何らかの理由でワークステーション B を使ってソフトウェアパッケージを新規作成する（再度バッチファイルを使用する）ことにして、ワークステーション B で ConsoleOne を終了した後、ワークステーション A で ConsoleOne を終了したとします。ワークステーション B で新規作成したソフトウェアパッケージは、マスタ snapinprefs.ser ファイル内でのリンクが失われます。

複数のワークステーションによるソフトウェアパッケージの管理の最適なシナリオ

最適なシナリオは、1 人の管理者が複数のワークステーションを使用してソフトウェアパッケージを管理できるようにすることです。複数の管理者がいる場合は、マスタ snapinprefs.ser ファイルでソフトウェアパッケージの追加や削除に関する最新情報を互いにを上書きしないように調整する必要があります。

詳細については、252 ページの「例：マスタ snapinprefs.ser ファイルの使用」を参照してください。

例：マスタ snapinprefs.ser ファイルの使用

サーバ上のマスタコピーが常に正しく更新されるようにすることは、タイミングの問題です。たとえば、次のシナリオでは、まずワークステーション A で最初の snapinprefs.ser ファイルが作成され、マスタ snapinprefs.ser ファイルとしてネットワークサーバにコピーされました。両方のワークステーションで Windows 2000 を使用しています。

ConsoleOne の使用前後のイベントを制御するために、バッチファイルを使用して ConsoleOne を起動しています。たとえば、次のように入力します。

1. 管理者 A がワークステーション A 上でバッチファイルを使用して ConsoleOne を起動します。
2. ワークステーション A で実行されているバッチファイルが、M: ドライブとしてマッピングされているストレージサーバを識別します（またはバッチファイルが M: ドライブをそのサーバにマッピングします）。
3. このバッチファイルは、M: ドライブにマップされているサーバからマスタ snapinprefs.ser ファイルを、ワークステーション A 上の c:¥documents and settings¥*user_ID*¥.consoleone ディレクトリにコピーします。
4. 管理者 A がソフトウェアパッケージを新規作成し、ssp1.spk という名前を付けます。
5. 管理者 B がワークステーション B 上でバッチファイルを使用して ConsoleOne を起動します。

6. ワークステーション B で実行されているバッチファイルが、M: ドライブとしてマッピングされているストレージサーバを識別します (またはバッチファイルが M: ドライブをそのサーバにマッピングします)。
7. このバッチファイルは、M: ドライブにマップされているサーバからマスタ snapinprefs.ser ファイルを、ワークステーション B 上の c:¥documents and settings¥*user_ID*¥.consoleone ディレクトリにコピーします。

   これは、管理者 A がワークステーション A にコピーした snapinprefs.ser と同じものですが、管理者 A が追加した ssp1.spk の情報は更新されていません。
8. 管理者 B がソフトウェアパッケージを新規作成し、ssp2.spk という名前を付けます。
9. 管理者 B が ConsoleOne を終了し、ワークステーション B 上の snapinprefs.ser で ssp2.spk のパスを更新します。
10. ワークステーション B で実行されているバッチファイルは、ワークステーション B から更新された snapinprefs.ser ファイルを使用して、M: ドライブにマッピングされているネットワークサーバ上のマスタ snapinprefs.ser ファイルを更新します。

    この更新されたマスタ snapinprefs.ser ファイルには、ssp2.spk の場所が保存されています。
11. 管理者 A が ConsoleOne を終了し、ワークステーション A 上の snapinprefs.ser で ssp1.spk のパスを更新します。
12. ワークステーション A で実行されているバッチファイルは、ワークステーション A から更新された snapinprefs.ser ファイルを使用して、M: ドライブにマッピングされているネットワークサーバ上のマスタ snapinprefs.ser ファイルを更新します。

    この更新されたマスタ snapinprefs.ser ファイルには、ssp1.spk の場所が保存されています。ただし、ssp2.spk の場所は失われます。これは、ワークステーション B によって更新されたマスタ snapinprefs.ser ファイルが、後で行われたワークステーション A からの更新によって上書きされるからです。

このシナリオでは、マスタ snapinprefs.ser ファイルに ssp2.spk の場所の情報が含まれていないので、管理者 B は ssp2.spk にアクセスできなくなります。マスタ snapinprefs.ser ファイルは、ssp1.spk の場所だけが含まれている管理者 A の snapinprefs.ser ファイルに置き換えられています。ただし、[Insert Software Package] オプションを使用して手動で ssp2.spk を ConsoleOne に挿入し、ssp1.spk ファイルと共に snapinprefs.ser ファイルにリストすることができます。

この複数のワークステーションによる管理が機能するには、ネットワークサーバに保存しているマスタ snapinprefs.ser ファイルが、.spk ファイルを作成、削除、またはコンパイルするために、一度に 1 台のワークステーションでのみ使用されるようにする必要があります。ただし、複数のワークステーションを使用して、同時に Server Software Package オブジェクトのプロパティを表示または編集できます。これは、表示および編集機能によって snapinprefs.ser ファイルが更新されることはないからです。

警告： snapinprefs.ser ファイルに影響を与えずに Server Software Package オブジェクトのプロパティに対する編集を実行できます。ただし、Server Software Package オブジェクトは eDirectory™ 内ではなく、ネームスペース内にのみ存在するので、サーバのオペレーティングシステムがファイルロックによる保護機能を提供していない限り、.spk ファイルがファイルロックによって保護されない場合があります。したがって、複数のワークステーションを使用してソフトウェアパッケージを管理する場合は、.spk ファイルの上書きを防止するための管理コントロールを考案する必要があります。

ソフトウェアパッケージのインストールの失敗

サーバがソフトウェアパッケージの要件のいずれかを満たしていない場合、ソフトウェアパッケージはインストールされません。

- 254 ページの「インストール中のエラー」
- 254 ページの「コンポーネントのエラー」

インストール中のエラー

ソフトウェアパッケージのインストールによるすべての変更はシステムによってトラッキングされます。254 ページの「ソフトウェアパッケージのインストールのロールバック」で説明されている例外を除いて、サーバが要件を満たしており、インストールが開始された後、エラーによってインストールが途中で停止した場合は、インストールプログラムは、自動的に、その時点までに行った変更を元に戻し、サーバの状態をインストールが開始される前の状態に戻します。

コンポーネントのエラー

サーバがソフトウェアパッケージの要件を満たしている場合に、インストールの要件を満たしているコンポーネントと満たしていないコンポーネントがある場合、要件が満たされていないコンポーネントを除いて、インストールが終了します。この場合、パッケージは部分的にインストールされています。

このような場合に、接続されていないかまたは不完全なファイルやアプリケーションがターゲットコンピュータに残らないように、ソフトウェアパッケージとそのコンポーネントを構成する必要があります。

ソフトウェアパッケージのインストールのロールバック

ソフトウェアパッケージのロールバックはデフォルトで有効になっています。インストールを元に戻す必要がないことが明確である場合以外は、ロールバックを無効にしないでください。

- 254 ページの「ロールバックの方法」
- 255 ページの「以前のインストールのロールバック」
- 255 ページの「ロールバックの例外」

ロールバックの方法

ソフトウェアパッケージのインストールをロールバックするには、2 つの方法があります。

- ロールバックするパッケージが保存されているサーバ上で、サーバの ZENworks Server Management コンソールのプロンプトで **package rollback** と入力します。
- Web ブラウザを使用して、ZENworks Server Management の役割にアクセスし、ロールバックオプションを選択します。詳細については、69 ページの「Novell iManager」を参照してください。

ソフトウェアパッケージはアンインストールされ、サーバはパッケージがインストールされていなかった状態に戻ります。ただし、インストールしたアプリケーションを使用してサーバに対して行った変更内容は除きます。

正常なパッケージのインストールの途中で、一部のコンポーネントがインストールされなかった場合でも、インストールプログラムはソフトウェアパッケージによってインストールされなかった対象をトラッキングしているので、ロールバックは機能します。

以前のインストールのロールバック

ソフトウェアパッケージのインストールをロールバックする場合、そのサーバに最後にインストールされたソフトウェアパッケージがロールバックされます。最後にインストールされたソフトウェアパッケージ以外のソフトウェアパッケージをロールバックする必要がある場合は、最新のインストールから順に、対象となるパッケージまで、各インストールをロールバックする必要があります。

たとえば、1 台のサーバに 3 つのパッケージ (パッケージ 1、パッケージ 2、パッケージ 3) をインストールしたとします。パッケージ 1 を最初にインストールし、パッケージ 3 を最後にインストールしました。パッケージ 2 をロールバックする場合、まずパッケージ 3 をロールバックする必要があります。そのためには、サーバの ZENworks Server Management コンソールのプロンプトで、パッケージ 3 について **package rollback** コマンドを実行した後、パッケージ 2 についてもう一度このコマンドを実行します。

ロールバックの例外

通常、正常にインストールされたソフトウェアパッケージを、ロールバックによって元に戻すことができます。ただし、インストールされたソフトウェアパッケージが、サーバを変更する NetBasic スクリプト、Java Class、または NLM などのプログラムを実行する場合、このソフトウェアパッケージを正しくロールバックできません。これは、これらのプログラムやサービスがサーバ上で変更を行う別のプログラムを起動している可能性があり、このようなプログラムをトラッキングしてロールバックすることができないからです。

Server Software Packages のプランニング

以下の各節を参照して、指示に従ってメモを作成します。この情報は、ソフトウェアパッケージとそのコンポーネントを設定するのに役立ちます。

- 255 ページの「どのファイルまたはアプリケーションを配布する必要があるか」
- 256 ページの「どのようなソフトウェアパッケージコンポーネントが必要であるか」
- 256 ページの「必要な最小限の要件は何か」

ソフトウェアパッケージのプランニングが終了したら、257 ページの「Server Software Package の設定」に進みます。

どのファイルまたはアプリケーションを配布する必要があるか

サーバ用のファイルやアプリケーションを含むソフトウェアパッケージを配布できるだけでなく、ZENworks Desktop Management でさらにワークステーションに配布されるエンドユーザ向けのアプリケーションを含むソフトウェアパッケージも配布できます。Desktop Application Distribution の設定については、Novell Documentation Web サイト (http://www.novell.com/documentation/lg/zdfs/index.html) で「Administration」の下にある「Application Management」を参照してください。

ZENworks 6.5 Desktop Management をインストールしている場合は、デスクトップアプリケーションをソフトウェアパッケージに含める代わりに、Tiered Electronic Distribution を使用して配布することもできます。詳細については、6 章 283 ページの「Desktop Application Distribution」を参照してください。

ファイルやアプリケーションを複数のソフトウェアパッケージに含めることができます。たとえば、ワードプロセッサアプリケーションを秘書グループ向けのソフトウェアパッケージと財務グループ向けのソフトウェアパッケージに含めることができます。

可能であれば、ソフトウェアパッケージに含めるために、ファイルやアプリケーションを論理的なグループに分類します。

261 ページの「Server Software Package の作成」および 262 ページの「ソフトウェアパッケージコンポーネントの作成」の手順に従って、ソフトウェアパッケージとそのコンポーネントを作成するために必要な情報をメモしておきます。

どのようなソフトウェアパッケージコンポーネントが必要であるか

ソフトウェアパッケージには複数のコンポーネントを含めることができます。たとえば、ウイルス対策ソフトウェアをインストールするためのソフトウェアパッケージを作成する場合、オリジナルのウイルス対策プログラムを 1 つのコンポーネントにして、最新のウイルスパターン更新ファイルを別のコンポーネントにすることができます。

ソフトウェアパッケージ内のコンポーネントは、それぞれのインストールの要件が同じである場合と異なる場合があります。コンポーネントの要件が異なる場合は、すべてのコンポーネントがいっしょにインストールされない場合があります。すべてのコンポーネントの要件を同じにしておくことによって、時間を節約し、エラーを最小限に抑えることができます。

重要： 1 つのコンポーネントには、互いに独立したファイルやアプリケーションを含めます。これによって、重要なコンポーネントがインストールされなかった場合に、ファイルやアプリケーションの実行に関する問題を防止することができます。アプリケーションのファイルを複数のコンポーネントに分割する必要がある場合は、各コンポーネントの要件が同じになるようにして、すべてのコンポーネントがインストールされるか、どのコンポーネントもインストールされないかのいずれかになるようにします。

263 ページの「ソフトウェアパッケージコンポーネントの環境設定」の手順に従って、パッケージコンポーネントの環境設定に必要な情報をメモしておきます。

必要な最小限の要件は何か

最小限の要件によって、ソフトウェアパッケージをターゲットコンピュータにインストールできるかどうかが決まります。これらの要件がすべて満たされている場合は、そのサーバにソフトウェアパッケージをインストールできます。

ただし、ソフトウェアパッケージの全体的な要件を設定すると共に、各パッケージコンポーネントの要件を設定することもできます。したがって、パッケージの要件がすべて満たされていても、一部のコンポーネントの要件が満たされていない場合は、パッケージの一部だけがインストールされます。

262 ページの「Server Software Package の環境設定」の手順に従って、ソフトウェアパッケージの環境設定に必要な情報をメモしておきます。

Server Software Package の設定

配布用のソフトウェアパッケージを設定するには、次の作業を順に実行します。

1. 257 ページの「複数のワークステーションによる Server Software Package の管理の設定」
2. 261 ページの「Server Software Package の作成」
3. 262 ページの「Server Software Package の環境設定」
4. 262 ページの「ソフトウェアパッケージコンポーネントの作成」
5. 263 ページの「ソフトウェアパッケージコンポーネントの環境設定」
6. 274 ページの「ソフトウェアパッケージのコンパイル」
7. 275 ページの「ソフトウェアパッケージの配布」

複数のワークステーションによる Server Software Package の管理の設定

ソフトウェアパッケージを複数のワークステーションから管理する場合は、snapinprefs.ser ファイルのマスタコピーを複数のワークステーションに複製する処理を管理できるようにするために、次の作業を行います。それ以外の場合は、261 ページの「Server Software Package の作成」に進みます。

1. 257 ページの「マスタ snapinprefs.ser ファイルの設定」
2. 258 ページの「ConsoleOne のバッチファイルの作成と使用」

マスタ snapinprefs.ser ファイルの設定

以下の手順を実行するには、ソフトウェアパッケージの管理に使用するワークステーションを選択します。ワークステーションを使用してすでにソフトウェアパッケージを作成した場合は、ワークステーションの snapinprefs.ser ファイルに保存されているソフトウェアパッケージの情報が失われないように、そのワークステーションを選択します。

1 .spk ファイルと関連する .cpk ファイルを保存するサーバにドライブをマッピングします。

このドライブ名は、ソフトウェアパッケージの管理に使用する他のすべてのワークステーションで使用できるドライブ名にする必要があります。このドライブ名は、リストされる各 .spk ファイルのパス情報の一部として snapinprefs.ser ファイルに書き込まれるので、すべてのワークステーションで使用できる固定ドライブ名にしてください。

このドライブ名は ConsoleOne を起動するために使用するバッチファイルでも使用され、各ワークステーションから同じ .spk ファイルの保存場所にアクセスできるようになります。

2 このワークステーションですでに Server Software Package オブジェクトを作成した場合は、ステップ 5 に進みます。

または

このワークステーションでまだ Server Software Package オブジェクトを作成していない場合は、ConsoleOne を起動します。

このバージョンの ConsoleOne には、Policy and Distribution Services スナップインがインストールされている必要があります。

3 Server Software Package ネームスペースに、Server Software Package オブジェクトを作成します。

ここでは、Server Software Package オブジェクトの環境設定をすべて行う必要はありません。パッケージ名を指定し、.spk ファイルの保存場所とファイル名を指定します。ステップ 1 で使用したドライブマッピングを使用していることを確認します。

ソフトウェアパッケージの作成については、257 ページの「Server Software Package の設定」を参照してください。

4 ConsoleOne を終了します。

この手順は、このワークステーション用の snapinprefs.ser ファイルを作成するために必要です。

5 snapinprefs.ser ファイルのマスタコピーを保存するために使用するネットワークサーバで、ドライブのルートに ¥C1 という名前のディレクトリを作成します。

マスタ snapinprefs.ser ファイルの保存場所には、サーバ上の任意の安全な場所を選択できます。

後に示すバッチファイルのサンプルでは、C1 というディレクトリ名を使用しています。別のディレクトリ名を使用する場合は、バッチファイルを変更し、パス情報を含めることができます。ただし、ルートの場所に変数を使用しないでください。

たとえば、

```
\zenworks\clssp
```

を、¥C1 というディレクトリ名の代わりに使用できます。

6 ワークステーションの snapinprefs.ser ファイルを

c:¥documents and settings¥user_ID¥.consoleone (Windows 2000)

ネットワークサーバ上の ¥C1 ディレクトリにコピーします。

258 ページの「ConsoleOne のバッチファイルの作成と使用」に示されているバッチファイルを使用している場合は、このファイルがマスタ snapinprefs.ser ファイルになり、新しい .spk のパス情報が更新されます。

7 258 ページの「ConsoleOne のバッチファイルの作成と使用」に進みます。

ConsoleOne のバッチファイルの作成と使用

バッチファイルの概要、作成、および使用については、以下の節を参照してください。

- 259 ページの「サンプルバッチファイル」
- 259 ページの「バッチファイルによる処理の内容」
- 259 ページの「バッチファイルの作成」
- 260 ページの「バッチファイルに対するその他の変更」
- 261 ページの「ConsoleOne バッチファイルの使用」

サンプルバッチファイル

```
@echo off
REM map a network drive
net use m:\\server1.servers.novell.com\vol1

REM create a backup copy of the workstation's .ser file
copy "%USERPROFILE%\.consoleone\snapinprefs.ser"
"%USERPROFILE%\.consoleone\snapinprefs.tmp"

REM copy the master .ser to the workstation
copy m:\c1\snapinprefs.ser "%USERPROFILE%\.consoleone\snapinprefs.ser"

REM start ConsoleOne
c:\Novell\ConsoleOne\1.2\bin\ConsoleOne.exe

REM batch file control returns after exiting ConsoleOne
REM copy the updated .ser to server
copy "%USERPROFILE%\.consoleone\snapinprefs.ser" m:\C1\snapinprefs.ser

REM restore the backup copy of the workstation's .ser file
copy "%USERPROFILE%\.consoleone\snapinprefs.tmp"
"%USERPROFILE%\.consoleone\snapinprefs.ser"

REM delete the mapped network drive
net use m:/delete
@echo on
```

バッチファイルによる処理の内容

- .spkおよび.cpkファイルを保存しているサーバにアクセスするためにネットワークドライブをマッピングします。
- Windowsの%USERPROFILE%変数を使用して、Server Managementの/¥.consoleoneディレクトリを検索します。また、この変数は、Server Managementによって、/¥.consoleoneディレクトリを作成し、snapinprefs.serファイルを書き込む場所を判断するために使用されます。
- snapinprefs.serファイルのバックアップコピーである.tmpを作成します。
- マスタsnapinprefs.serファイルを、サーバの¥C1ディレクトリから、ワークステーションの/¥.consoleoneディレクトリにコピーします。
- ConsoleOneを起動します。
- ConsoleOneを終了した後、バッチファイルは更新されたsnapinprefs.serファイルをワークステーションの/¥.consoleoneディレクトリからコピーして、サーバ上の¥C1ディレクトリにあるバージョンを置き換えます。これが新しいマスタsnapinprefs.serファイルになります。
- .tmpファイルからsnapinprefs.serファイルのバックアップコピーを復元します。
- サーバへのドライブ名のマッピングを解除します。

バッチファイルの作成

1. 前に示したサンプルバッチファイルのテキストをテキストエディタにコピーします。
2. ドライブ名m:を各ワークステーションで空いているドライブ名に置き換えます。この作業をバッチファイル内のすべてのm:について行います。

3 net use m: ¥¥server1.servers.novell.com¥vol1 の行を編集し、.spk および .cpk ファイルを保存しているサーバボリュームまたはサーバの共有フォルダへのパスに置き換えます。

4 このバッチファイルをワークステーションに保存し、次のような名前を付けます。

```
C1SSP.BAT
```

5 このバッチファイルを、ソフトウェアパッケージの管理に使用する各ワークステーションにコピーします。

バッチファイルに対するその他の変更

- ConsoleOne を、バッチファイルのサンプルに示されているワークステーション上の場所とは異なる場所にインストールしている場合は、c:¥novell¥consoleone¥1.2¥bin¥consoleone.exe の行を、ワークステーション上の consoleone.exe ファイルの場所に合わせて変更します。

  この変更は、デフォルトの ConsoleOne のパスが使用されていないワークステーション上の個々のバッチファイルで行う必要があります。

- このバッチファイルをワークステーションで使用して、サーバにインストールされている ConsoleOne のインスタンスを起動することもできます。c:¥novell¥consoleone¥1.2¥bin¥consoleone.exe の行を、サーバ上の consoleone.exe ファイルの場所に合わせて変更します。ドライブ名がサーバにアクセスするために使用されているドライブ名であることを確認します。257 ページのステップ 1 を参照してください。

- %USERPROFILE% 変数が使用されていなかったために、/¥.consoleone ディレクトリのパスがワークステーションによって異なる場合は、必要に応じて、この変数を含む行をすべて編集します。%USERPROFILE% 変数が使用されていなかったワークステーションでバッチファイルのコピーを開き、この変数を含む行を編集して、/¥.consoleone ディレクトリへの正しいパスを反映させます。

- サーバに ¥C1 以外のディレクトリを作成した場合は、バッチファイル内のすべての ¥C1 を 258 ページのステップ 5 で指定したディレクトリに置き換えます。

- このバッチファイルは snapinprefs.ser ファイルの。tmp バージョンを作成します。これによって、バッチファイルを使用する前に存在していたワークステーション上の .ser ファイルを保持しておくことができます。ただし、ワークステーションのバージョンをサーバにコピーされたマスタバージョンと常に一致させる場合は、バッチファイルから次の 2 行を削除します。

  ```
  copy "%USERPROFILE%\.consoleone\snapinprefs.ser"
  "%USERPROFILE%\.consoleone\snapinprefs.tmp"

  copy "%USERPROFILE%\.consoleone\snapinprefs.tmp"
  "%USERPROFILE%\.consoleone\snapinprefs.ser"
  ```

- すべてのワークステーションで同じドライブ名を使用できない場合は、バッチファイルで引数 %1 を使用できます。ただし、すべての .spk ファイルで UNC パスを使用している場合だけです。引数 %1 を使用するには、m: の記述をすべて %1 に置き換えます。次に、コマンドラインからバッチファイルを実行するときに、バッチファイル名の後にドライブ名を追加します。たとえば、

  C1SSP R:

  と入力すると、snapinprefs.ser ファイルのマスタコピーを検索するドライブとして、バッチファイルは R: を使用します。

ConsoleOne バッチファイルの使用

- このバッチファイルを実行する前に、ソフトウェアパッケージの管理に使用する各ワークステーションの ¥.consoleone ディレクトリに snapinprefs.ser ファイルを配置します。このバッチファイルでは、コピーや置換において .ser ファイルが存在していることを前提としています。
- このバッチファイルを実行する前に、ソフトウェアパッケージのファイルを保存するサーバの ¥C1 ディレクトリに snapinprefs.ser ファイルのマスタコピーを配置します。このバッチファイルでは、コピーや置換においてこの .ser ファイルが存在していることを前提としています。
- ソフトウェアパッケージを追加、削除、またはコンパイルする場合には、常にこのバッチファイルを実行します。
- ソフトウェアパッケージのプロパティを表示または編集する場合は、このバッチファイルを使用する必要はありません。snapinprefs.ser ファイルを更新するアクションは、追加、削除、およびコンパイル機能だけです。

261 ページの「Server Software Package の作成」に進みます。

Server Software Package の作成

1 ConsoleOne で、Server Software Packages ネームスペースを右クリックし、[New Package] をクリックします。

Create New Server Software Package ウィザードが表示されます。

2 最初のダイアログボックスに表示される情報を読んで、[Next] をクリックします。

3 ソフトウェアパッケージの名前を指定します。

わかりやすい名前を指定します。この名前は、ConsoleOne の Server Software Packages オブジェクトの下に表示されます。

重要： ソフトウェアパッケージ名に 2 バイト文字を使用しないでください。このソフトウェアパッケージについてレポートを実行したときにエラーの原因になります。

4 ソフトウェアパッケージはファイルをベースにしているので、拡張子 .spk を含むフルパスおよびファイル名を指定します。

拡張子を入力しなかった場合、拡張子を追加するよう求めるメッセージが表示されます。

UNC パスを使用することもできます。

.spk ファイルはワークステーションまたはサーバに保存できます。.spk ファイルのサイズは、通常 100KB 未満です。ただし、コンパイル済みのソフトウェアパッケージ (.cpk ファイル) は、数百メガバイトになる場合があります。.spk および .cpk ファイルの保存については、248 ページの「Server Software Package の管理」を参照してください。

警告： ソフトウェアパッケージのフルパスおよびファイル名はドライブに依存します。パッケージを作成した後でドライブマッピングを変更した場合、ソフトウェアパッケージが使用できなくなることがあります。このフィールドのエントリが変更されていないことを確認してください。ただし、UNC パスを使用している場合は、この問題は発生しません。

5 [Finish] をクリックします。

6 262 ページの「Server Software Package の環境設定」に進みます。

Server Software Package の環境設定

ソフトウェアパッケージを作成した後、パッケージに含まれるファイルやアプリケーションのインストールの前提条件を設定することによりパッケージの環境を設定する必要があります。

パッケージを環境設定するには

1 ConsoleOne で、ソフトウェアパッケージを右クリックし、[Properties] をクリックします。

[Identification] タブが表示されます。表示されない場合は、このタブを選択します。

[Name] フィールドには、パッケージの作成時に指定したパッケージ名が表示されます。

2 ソフトウェアパッケージのわかりやすい説明を入力します。

3 新しいバージョンをインストールした後、サーバのファイルやアプリケーションを以前のバージョンにロールバックする必要がない場合は、[Disable Rollback] チェックボックスをオンにします。ただし、これはお勧めできません。

ソフトウェアパッケージのインストールのロールバックについては、254 ページの「ソフトウェアパッケージのインストールのロールバック」を参照してください。

4 [Requirements] タブを選択します。

5 [Add] をクリックし、要件を選択します。

423 ページの「オペレーティングシステム」
426 ページの「Memory (RAM)」
426 ページの「ディスク領域」
427 ページの「SET Commands」
427 ページの「レジストリ」
428 ページの「File」
428 ページの「Products.dat」

6 各要件について、ステップ 5 を繰り返します。

7 変数を使用してインストールをカスタマイズする場合は、[Variables] タブを選択し、[Add] をクリックします。

8 変数名と値を入力します。

変数については、363 ページの「変数を使用したファイルの抽出の制御」を参照してください。

9 各変数について、手順 7 とステップ 8 を繰り返します。

10 環境設定が終了したら [OK] をクリックします。

[Cancel] をクリックすると、どのタブで行った環境設定の変更も保存されません。

11 262 ページの「ソフトウェアパッケージコンポーネントの作成」に進みます。

ソフトウェアパッケージコンポーネントの作成

ソフトウェアパッケージを作成し、環境設定を行った後、パッケージの個々のファイルやアプリケーションを含む、パッケージのコンポーネントを作成する必要があります。

ソフトウェアパッケージコンポーネントを作成するには

1 ConsoleOne の左側のペインで、ソフトウェアパッケージを右クリックし、[New Component] を選択します。

2 ConsoleOne に表示されるコンポーネントの名前を入力し、[OK] をクリックします。

名前を付けたコンポーネントがソフトウェアパッケージオブジェクトの下に表示されます。

3 必要な各コンポーネントについてこの手順を繰り返します。

4 263 ページの「ソフトウェアパッケージコンポーネントの環境設定」に進みます。

ソフトウェアパッケージコンポーネントの環境設定

ソフトウェアパッケージコンポーネントを作成した後、コンポーネントのファイルやアプリケーションの識別など、各コンポーネントの前提条件を設定する必要があります。

パッケージコンポーネントの前提条件をすべて同じにすることができ、これによって時間を節約し、ユーザエラーを最小限に抑えることができます。

コンポーネントを環境設定するには

1 ConsoleOne で、コンポーネントを右クリックし、[Properties] をクリックします。

[Identification] タブが表示されます。表示されない場合は、このタブを選択します。

2 コンポーネントのわかりやすい説明を入力します。

3 [After Package Installation Is Complete] ドロップダウンリストから、インストール処理の完了後にソフトウェアパッケージについて実行する追加のアクションを選択します。

4 コンポーネントの環境設定を続行するには、設定する必要がある以下の各項目を参照してください。

264 ページの「要件」
264 ページの「インストール前のロード / アンロード」
265 ページの「インストール前のスクリプト」
265 ページの「Local File Copy」
266 ページの「Copy File」
270 ページの「テキストファイル」
271 ページの「SET Commands」
272 ページの「レジストリの設定」
272 ページの「Products.dat」
273 ページの「インストール後のアンロード / ロード」
274 ページの「インストール後のスクリプト」

必要に応じて、これらのすべての項目の設定が完了するまで、コンポーネントのプロパティページで [OK] をクリックしないでください。

5 [OK] をクリックします。

[Cancel] をクリックすると、どのタブで行った環境設定の変更も保存されません。

6 ソフトウェアパッケージの配布の準備をするには、274 ページの「ソフトウェアパッケージのコンパイル」に進みます。

要件

サーバのファイルやアプリケーションをインストールの要件を指定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Requirements] タブを選択し、[Add] をクリックします。

2 次のいずれかの要件を選択します。

423 ページの「オペレーティングシステム」
426 ページの「Memory (RAM)」
426 ページの「ディスク領域」
427 ページの「SET Commands」
427 ページの「レジストリ」
428 ページの「File」
428 ページの「Products.dat」

項目の設定方法の詳細については、これらの各項目を参照してください。

[OK] をクリックする前に、設定する次の項目に進みます。

インストール前のロード / アンロード

サーバにソフトウェアパッケージをインストールする前に特定の NLM ファイルまたはプロセスをロードまたはアンロードするように設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Pre-Installation] タブを選択し、[Load/Unload] をクリックします。

2 [Add] をクリックします。

3 次のいずれかを選択します。

421 ページの「Load NLM/Process」
422 ページの「Load Java Class」
422 ページの「Unload Process」
422 ページの「Start Service」
422 ページの「Stop Service」

項目の設定方法の詳細については、これらの各項目を参照してください。

重要： ソフトウェアパッケージによってプロセスをロードすることを選択し、そのプロセスがターゲットサーバ上ですでに実行されている場合、パッケージのインストールは失敗し、ロールバックされます (ロールバックが有効になっている場合)。このプロセスをアンロードするのにユーザの操作が必要な場合は、ソフトウェアパッケージをインストールする前に、手動でプロセスをアンロードする必要があります。

ソフトウェアパッケージにプロセスを含めている場合に、プロセスがロードされていないことを保証するには、ロードオプションを追加する前に、そのプロセスのアンロードオプションを追加します。ただし、この方法を使用できるのは、プロセスをアンロードするときにユーザによるキーボードからの入力を必要としない場合だけです。

4 パッケージに含める各 NLM またはプロセスについて、手順 1 からステップ 3 までを繰り返します。

5 方向キーを使用して、NLM ファイルおよびプロセスを実行する順序を指定します。

[OK] をクリックする前に、設定する次の項目に進みます。

インストール前のスクリプト

サーバにソフトウェアパッケージをインストールする前にサーバスクリプトの実行を設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Pre-Installation] タブを選択し、[Script] をクリックします。

2 [Add] をクリックします。

3 スクリプト名を入力します。

4 スクリプトの種類 (NCF、NetBasic、PERL) を選択します。

重要： NetBasic は NetWare 6.5 サーバではサポートされていません。

5 スクリプトのテキストを入力します。

警告： ソフトウェアパッケージがすべての要件を満たしており、スクリプトを実行する場合、スクリプトで実行された処理をロールバックによって元に戻すことはできません。

6 追加する各スクリプトについて、手順 2 からステップ 5 までを繰り返します。

7 方向キーを使用して、スクリプトを実行する順序を指定します。

[OK] をクリックする前に、設定する次の項目に進みます。

Local File Copy

Local File Copy コンポーネントによって、ソフトウェアパッケージを使用してサーバ上のファイルをある場所から別の場所にコピーできます。ファイルをコピーすることも、移動することもできます。

Local File Copy コンポーネントを設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Local File Copy] タブを選択します。

2 [Add] をクリックします。

Local File Copy #1 がデフォルトの名前です。この名前は編集できます。

3 次のフィールドに情報を入力します。

[Source Path] : コピーするファイルが保存されている場所のフルパスを指定します。

パスにはワイルドカードを使用できます。

* = 任意の数の文字
? = その位置にある任意の 1 文字
??? = それらの位置にある任意の文字

[Target Path] : コピーするファイルの保存先のフルパスを指定します。

このパスにはワイルドカードを使用できます。このパスにはソースパスを反映させる必要はありません。ただし、既存のターゲットパスを反映させることができます。

[Include Subdirectories] : パスの最後にあるディレクトリから始めて、すべてのサブディレクトリとその中にあるファイルを含めます。このオプションを選択しない場合は、パスの最後にあるディレクトリ内のファイルだけがコピーされます。

[Maintain Attributes] : ソースのファイルシステムに存在するファイル属性をターゲットのファイルシステムでも保持します。

[Overwrite Destination Files]：ファイルの日付に関係なく、コピー先のディレクトリで同じ名前のファイルを上書きします。このオプションを選択しない場合、同じ名前のファイルは置き換えられません。

[Maintain Trustees]：ファイルのトラスティ属性を保持します。

[When a File Is Locked]：次のいずれかまたは両方を選択します。

- [Retry __ Times]：指定した回数だけロックされたファイルの上書きを再試行した後、ファイルの置換に失敗したことにします。このチェックボックスをオフのままにすると、ターゲットファイルシステム上のロックされたファイルは置換されません。
- [Kill Connection of Open Files]:（NetWare のみ）ロックされたファイルに上書きできるように、ロックされたファイルへの接続を強制終了しようとします。このオプションは、ファイルを抽出している場合にのみ適用され、Distribution を構築するためにファイルにアクセスしている場合には適用されません。Distribution を構築しているときに、Distribution に属するファイルがロックされている場合、構築は失敗します。サーバと NLM の接続は強制終了できません。

[Error Processing]：デフォルトでは、[Fail On Error] が選択されています。これによって、コピー中にエラーが発生した場合、ファイルのコピー処理は中止されます。エラーが発生してもファイルのコピーを続行するには、[Continue On Error] を選択します。

[Operation]：[Source Path] で指定されたファイルをコピーするか、移動するかを設定します。

[OK] をクリックする前に、設定する次の項目に進みます。

Copy File

Copy File コンポーネントを設定することによって、ソフトウェアパッケージのインストール中にファイルをコピーする方法を制御できます。これには、既存のディレクトリへのファイルの追加、新しいディレクトリの作成、新しいディレクトリへのファイルやサブディレクトリの追加、既存のファイルやディレクトリの削除が含まれます。

ファイルグループは、コンポーネントの展開可能なツリー構造のルート項目です。Copy File コンポーネントでは、複数のファイルグループを指定できます。ファイルグループは、関連するディレクトリおよびファイルのセットです。ファイルグループは最上位レベルの項目であり、他のファイルグループを含めることはできません。

ファイルグループに含まれるその他の構造項目には、ディレクトリとファイルがあります。ディレクトリには他のディレクトリやファイルを含めることができますが、ファイルグループを含めることはできます。

重要： ファイルグループまたはディレクトリを追加する場合、ファイルのソースパスではなく、ファイルのコピー先のターゲットパスを作成します。ソースファイルまたはディレクトリを選択したときに、ソースパスは自動的に設定されます。

ソフトウェアパッケージのインストール時のファイルのコピーを設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Copy File] タブを選択します。

2 初めてファイルグループを作成する場合は、次の操作を行います。

2a [Add] ボタンの横にあるドロップダウンリストの下向きの矢印をクリックし、[Add File Group] を選択し、[Add] をクリックします。

ファイルおよびディレクトリはファイルグループに含まれている必要があるので、追加する対象に関係なく、最初に［Add］をクリックしたときにファイルグループを作成するよう求めるメッセージが表示されます。

特定のコピー先ごとにファイルグループを 1 つ作成する必要があります。たとえば、C: ドライブ上の複数の場所 c:¥files、c:¥data¥accounting、c:¥data¥personnel に、関連性のない異なるファイルのグループをコピーできます。

2b ファイルグループに名前を付けた後、ターゲットパスを指定します。

ファイルグループのターゲットパスは、そのグループ内のすべてのディレクトリおよびファイルがインストールされるベースパスを指定します。

2c ファイルグループの場所がロックされている場合の処理を指定するには、次のいずれかのチェックボックスをオンにします。

1. ［Retry］（再試行の回数を入力します）
2. ［Kill Connection of Open Files］(NetWare のみ）
3. ［Fail With Error］

再試行は約 5 秒間隔で行われます。したがって、再試行の回数を 12 にした場合、約 1 分かかります。

3 ファイルグループまたは別のディレクトリの下にターゲットディレクトリを作成するには、ファイルグループまたはディレクトリを選択し、ドロップダウンボックスで［Add Directory］を選択して、［Add］をクリックした後、次の操作を行います。

3a Directory はデフォルトのディレクトリ名なので、ディレクトリ名を変更するには、Directory を右クリックし、［Rename］をクリックして適切なディレクトリ名を入力し、(Enter) キーを押します。

このフィールドに情報を入力するときは、(Enter) キーを押して変更を保存する必要があります。

一致する既存のターゲットディレクトリを検索してファイルを削除またはコピーするには、正確な名前を入力する必要があります。

重要： 既存のディレクトリ名を指定し、コピー先サーバのファイルシステムでそのディレクトリが Read Only としてマークされている場合、Subscriber が Distribution を抽出しようとしたときに、そのディレクトリに書き込みできないので、Software Package Distribution は失敗します。したがって、既存のターゲットディレクトリの属性を調べて、Read Only ディレクトリ属性を削除しておく必要があります。

コピー先の場所に存在しているものと同じディレクトリ構造を File Copy コンポーネントで作成し、ここで指定したディレクトリ名がパスと同じ順序になるようにする必要があります。

3b ディレクトリを作成するか、削除するかを指定するには、［Copy Mode］ドロップダウンリストでモードを選択します。

[Create]：［Create］を選択し、そのディレクトリが存在しない場合、ディレクトリが作成されます。［Create］を選択し、そのディレクトリが存在する場合、ディレクトリは作成されず、エラーも発生しません。

[Delete]：［Delete］を選択し、そのディレクトリが存在する場合、ディレクトリおよびそのディレクトリに含まれるすべてのサブディレクトリとファイルが削除されます。［Delete］を選択し、そのディレクトリが存在しない場合、ディレクトリは削除されず、エラーも発生しません。

警告： 追加したディレクトリについて［Copy Mode］を［Delete］に設定する場合に、追加した親ディレクトリは削除しない場合は、ファイルグループの［Target Path］フィールドでこれらの親ディレクトリを指定します。たとえば、c:¥winnt¥cookies を削除するが、¥winnt ディレクトリは削除しない場合は、［Target Path］フィールドに c:¥winnt と入力し、［Add］をクリックしてツリー構造の/¥cookies ディレクトリを入力して、［Copy Mode］フィールドで［Delete］をクリックします。たとえば、次のように入力します。

ターゲット = c:¥winnt

ツリー構造 = cookies

である場合、cookies ディレクトリおよびそのディレクトリ内のすべてのファイルとサブディレクトリだけが削除されます。

逆に、［Target Path］フィールドに c:¥ と入力し、［Add］をクリックしてツリー構造の ¥winnt ディレクトリを入力し、［Add］をクリックしてツリー構造の ¥winnt の下にある/¥cookies ディレクトリを入力した後、［Copy Mode］フィールドで［Delete］をクリックすると、¥winnt ディレクトリと/¥cookies ディレクトリの両方が削除されます。たとえば、次のように入力します。

ターゲット = c:¥

ツリー構造 = winnt¥cookies

である場合、winnt ディレクトリおよびそのディレクトリ内のすべてのファイルとサブディレクトリが削除されます。

4 ツリー構造のファイルグループまたはディレクトリの下にファイルやソースディレクトリを追加するには、ファイルグループまたはディレクトリを選択し、ドロップダウンボックスで［Add File］を選択し、［Add］をクリックした後、次の操作を行います。

4a ［Open］ダイアログボックスを使用してファイルまたはディレクトリを選択します。

これらのディレクトリやファイルは、ステップ 3 で選択したファイルグループやディレクトリのすぐ下に表示されます。

コピー先サーバのファイルシステムでは、コピーされるファイルやディレクトリの属性は保持されません。詳細については、ステップ 4c を参照してください。

［Open］ダイアログボックスでディレクトリを選択した場合は、展開して表示されません。ディレクトリの下に追加した既存の構造を展開するには、プラス記号をクリックします。

［Open］ダイアログボックスでは、デフォルトで［Recurse Directories］オプションが選択されています。このディレクトリ内のファイルだけを選択するには、［Recurse Directories］チェックボックスをクリックしてオフにし、どのサブディレクトリも選択されないようにします。

ファイルやサブディレクトリを選択から除外するには、［Exclude Selected Subdirectory］オプションを選択し、除外するファイルやディレクトリを選択し（複数選択する場合は（Shift）キーや（Ctrl）キーを使用する）、［Open］をクリックします。

ファイルやサブディレクトリを除外しても、ファイルシステムからは削除されません。単に選択されないようになるだけです。

ファイルやディレクトリを追加した後でツリー構造から削除する方法については、ステップ 8 を参照してください。

4b 追加したサブディレクトリを設定するには、次の操作を行います。

- サブディレクトリを選択した後、[Copy Mode]（ディレクトリをコピーするか、削除するか）を選択します。

  警告： [Copy Mode] を [Delete] に設定した場合、ターゲットディレクトリおよびそのすべてのファイルとサブディレクトリが削除されます。

- 追加したサブディレクトリの名前を変更するには、サブディレクトリを右クリックし、[Rename] をクリックして新しいディレクトリ名を入力し、(Enter) キーを押します。

  このフィールドに情報を入力するときは、(Enter) キーを押して変更を保存する必要があります。

  [Open] ダイアログボックスで選択したディレクトリの名前を変更する場合は、新しい名前がコピー先の場所での条件を満たしていることを確認します。

  選択したファイルのパスだけがコピーのために記憶されるので、ディレクトリ名を変更してもファイルの選択には影響しません。つまり、ターゲットディレクトリにソースとは別の名前を付けても、そのディレクトリに同じファイルがコピーされます。

4c 追加したファイルを設定するには、ファイルを選択し、次の操作を行います。

- ファイルのコピーモードを指定するには、[Copy Mode] ドロップダウンリストからモードを選択します。

  すべてのファイルについてオプションを選択する必要があります。同じモードを指定する場合は、複数のファイルを選択できます。

  指定できるオプションには、[Copy Always]、[Copy If Exists]、[Copy If Does Not Exist]、[Copy If Newer]、[Copy If Newer and Exists]、および [Delete] があります。

  警告： [Copy Mode] を [Delete] に設定した場合、選択したファイルがターゲットサーバから削除されます。

- 選択したファイルに適用する各属性のチェックボックスをオンにします。

  属性はデフォルトでは設定されません。コピー先サーバに合わせて属性を設定する必要があります。属性はファイルのコピー元からは引き継がれません。

  重要： 1 つのファイルについてすべての属性をオンにしないでください。すべての属性をオンにすると、サーバで例外が発生します。

  実行可能ファイルの属性を設定する場合は、[Read Only] に設定します。この属性を [Execute] に設定しないでください。ファイルを [Execute] としてマークすると、NetWare® CLIB API によって、ユーザはファイルの属性を変更できなくなります。ソフトウェアパッケージのインストール後、この属性を Execute から Read Only に変更するには、手動でファイルを削除し、ファイルを置換して、もう一度属性を設定する必要があります。

5 別のファイルグループを作成する場合は、次の操作を行います。

5a [Add] ボタンの横にあるドロップダウンリストの下向きの矢印をクリックし、[Add File Group] を選択し、[Add] をクリックします。

ツリー構造で何を選択していてもかまいません。ファイルグループは、表示されている他のファイルグループと同じ、ツリーの第 1 レベルに自動的に配置されます。

5b グループ名を指定します。

5c ターゲットベースパスを指定します。

5d グループの場所がロックされている場合の処理を指定するには、次のいずれかのチェックボックスをオンにします。

1. [Retry]（再試行の回数を入力します）
2. [Kill Connection of Open Files]（NetWare のみ）
3. [Fail With Error]

6 追加するファイル、ディレクトリ、またはファイルグループごとに、手順 5 からステップ 5d までを繰り返します。

7 ファイルグループを特定の順序でコピーする場合は、方向キーを使用してファイルグループの順序を指定します。

選択したファイルグループを上下に移動できない場合、矢印は淡色表示されます。

8 ファイルグループ、ディレクトリ、またはファイルを削除するには、削除する対象を選択し、[Remove] をクリックします。

[Remove] ボタンを使用して、ツリー構造から余分なファイルやディレクトリを削除できます。

(Shift) キーや (Ctrl) キーを使用して、削除する複数の項目を選択できます。

重要： ファイルグループやディレクトリを削除すると、その下に表示されているすべてのファイルやディレクトリも削除されます。ただし、このツリー構造から削除されるだけで、ソースファイルシステムからは削除されません。

[OK] をクリックする前に、設定する次の項目に進みます。

テキストファイル

ソフトウェアパッケージのインストール時のテキストファイルに対する変更を設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Text Files] タブを選択します。

2 [Add] をクリックします。

1 つのテキストファイルを追加した後、別のテキストファイルを追加するか、または選択したテキストファイルの変更する項目を追加するかを選択できます。

別のテキストファイルを追加するには テキストファイルを選択します。左側のペインでどのテキストファイルまたは変更項目が選択されていてもかまいません。テキストファイルは最も左のレベルに追加されます。

テキストファイルに別の変更を追加するには 左側のペインで変更するテキストファイルを選択し、[Add] をクリックして、[Change] を選択します。選択したテキストファイルの下に変更項目が追加されます。

3 テキストファイルを追加している場合は、テキストファイルの名前を指定します。

4 デフォルトの名前 (Change #1 など) を受け入れるか、この名前を変更します。

テキストファイルを追加する場合は、[OK] をクリックします。

5 [Change Mode] フィールドの下向きの矢印をクリックし、ドロップダウンリストから変更モードを選択します。

6 [Search Type] フィールドの下向きの矢印をクリックし、ドロップダウンリストから検索の種類を選択します。

7 検索文字列を正確に入力します。

8 大文字と小文字を区別して文字列を検索する場合は、チェックボックスをオンにします。

9 検索文字列のすべての出現箇所を検索するには、チェックボックスをオンにします（デフォルト）。このチェックボックスをオフにすると、最初の出現箇所だけが検索されます。

10 [Result Action] フィールドの下向きの矢印をクリックし、ドロップダウンリストから、文字列が一致する場合のアクションを選択します。

11 文字列を置き換えたり、新しい文字列を入力する場合は、[New String] テキストボックスにテキストを入力します。

12 追加する各テキストファイルまたは各変更について、手順 2 からステップ 11 までを繰り返します。

13 テキストファイルや変更項目の順序を変更するには、方向キーを使用します。

[OK] をクリックする前に、設定する次の項目に進みます。

SET Commands

NetWare のみ。

ターゲットサーバの SET コマンドを設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Set Commands] タブを選択します。

2 [Add] をクリックして、NetWare Server SET Commands ウィザードを開きます。

3 SET コマンドが保存されているサーバを選択し、[Next] をクリックします。

重要： SET コマンドを取得するサーバでは、Server Management および Java が実行されている必要があります。

4 ターゲットサーバについて設定するすべての SET コマンドを選択します。

カテゴリのチェックボックスをオンにしてカテゴリ全体を選択することも、プラス記号をクリックして SET コマンドカテゴリを展開し、含める個々の SET コマンドのチェックボックスをオンにすることもできます。

警告： SET コマンド Set Developer Option を選択し、Off を On に変更しないでください。このパラメータは、開発者がサーバの異常終了をデバッグできるようにするためのものです。特定の異常終了の発生を防止するために用意されているオペレーティングシステムの一部のチェック機能を無効にします。また、Set Developer Option がオンになっている場合、キーボード入力を要求する NCP™ スクリプトを実行するとサーバが異常終了する可能性があります。

5 SET コマンドの選択が完了したら、[Finish] をクリックします。

選択した SET コマンドが、ファイルまたはアプリケーションコンポーネントの [Set Commands] タブに表示されます。

6 SET コマンドを編集するには、プラス記号をクリックしてその属性を展開します。

7 属性を編集するには、属性を選択して、[Edit] をクリックします。

属性を変更できるダイアログボックスが表示されます。

8 特定の SET コマンドの編集する各属性について、ステップ 7 を繰り返します。

9 別の SET コマンドの属性を編集するには、手順 6 からステップ 8 までを繰り返します。

[OK] をクリックする前に、設定する次の項目に進みます。

レジストリの設定

NetWare サーバまたは Windows サーバのレジストリの変更を設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Registry Settings] タブを選択し、[HKEY_LOCAL_MACHINE] をクリックします。

HKEY_LOCAL_MACHINE は Windows のレジストリキーです。NetWare についても、Server Management によって、HKEY_LOCAL_MACHINE は My Server と等価であると認識されます。したがって、このキーを使用して、NetWare と Windows の両方のレジストリを編集できます。

2 [Add] をクリックします。

3 次のいずれかを選択します。

429 ページの「Key」
430 ページの「Binary」
430 ページの「Expand String」
431 ページの「(Default)」
431 ページの「DWord」
431 ページの「Multi-Value String」
432 ページの「String」

項目の設定方法の詳細については、これらの各項目を参照してください。

4 作成する各レジストリエントリについて、手順 2 およびステップ 3 を繰り返します。

5 方向キーを使用して、レジストリエントリを作成する順序を指定します。

[OK] をクリックする前に、設定する次の項目に進みます。

Products.dat

NetWare のみ。

products.dat ファイルをソフトウェアパッケージによって更新し、将来の更新でファイルやアプリケーションの最後にインストールされたバージョンを識別することができます。

警告： products.dat を変更すると、NetWare サーバ上で実行やインストールが妨げられる場合があります。Novell から提供されたすべてのエントリを変更しないでください。

products.dat について実行するアクションを指定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Products.dat] タブを選択します。

2 次のいずれかを選択します。

オプション	Description
Add	新規エントリを追加します。
Modify Existing Entry	一致する ID を検索し、バージョンおよび説明を変更します。
Replace Existing Entry	特定の ID を検索し、新しい ID に置換します。
No Action	これはデフォルトです。products.dat に対して何も行いません。

3 [Add] を選択した場合は、

3a 追加する項目の ID を指定します。

これは大文字と小文字が区別されます。この項目は、.dat ファイル用の新しい製品の ID です。

3b 追加する正確なバージョン番号を指定します。

3c 追加する説明を指定します。

4 [Modify Existing Entry] を選択した場合は、

4a 検索する項目の ID（大文字と小文字を区別する）を指定します。

4b 新しいバージョン番号を指定します。

4c 新しい説明を指定します。

5 [Replace Existing Entry] を選択した場合は、

5a 検索する項目の ID（大文字と小文字を区別する）を指定します。

5b 検索する正確なバージョン番号を指定します。

5c 新しい ID を指定します。

5d 新しいバージョンを指定します。

5e 新しい説明を指定します。

[OK] をクリックする前に、設定する次の項目に進みます。

インストール後のアンロード / ロード

サーバにソフトウェアパッケージをインストールした後に特定の NLM ファイルやプロセスをロードまたはアンロードするように設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Post-Installation] タブを選択し、[Load/Unload] をクリックします。

2 [Add] をクリックします。

3 次のいずれかを選択します。

421 ページの「Load NLM/Process」
422 ページの「Load Java Class」
422 ページの「Unload Process」
422 ページの「Start Service」
422 ページの「Stop Service」

項目の設定方法の詳細については、各項目を選択してください。

4 パッケージに含める各 NLM またはプロセスについて、手順 2 とステップ 3 を繰り返します。

[OK] をクリックする前に、設定する次の項目に進みます。

インストール後のスクリプト

サーバにソフトウェアパッケージをインストールした後に NetWare サーバスクリプトの実行を設定するには

1 ソフトウェアパッケージコンポーネントのプロパティを表示しているときに、[Post-Installation] タブをクリックし、[Script] をクリックします。

2 [Add] をクリックします。

3 スクリプト名を入力します。

4 スクリプトの種類 (NCF、NetBasic、PERL) を選択します。

重要： NetBasic は NetWare 6.5 サーバではサポートされていません。

5 スクリプトのテキストを入力します。

警告： ソフトウェアパッケージがすべての要件を満たしており、スクリプトを実行する場合、スクリプトで実行された処理をロールバックによって元に戻すことはできません。

6 追加する各スクリプトについて、手順 2 からステップ 5 までを繰り返します。

7 方向キーを使用して、スクリプトを実行する順序を指定します。

[OK] をクリックする前に、設定する次の項目に進みます。

ソフトウェアパッケージのコンパイル

ソフトウェアパッケージ (.spk ファイル) は、コンパイルして拡張子を .cpk にするまでは、Policy and Distribution Services によってインストールできません。

ソフトウェアパッケージをコンパイルするには

1 ConsoleOne で、ソフトウェアパッケージを右クリックし、[Compile Package] をクリックします。

Compile Server Software Package ウィザードが表示されます。

2 最初のダイアログボックスに表示される情報を読んで、[Next] をクリックします。

3 コンパイル済みソフトウェアパッケージの名前とパスを指定して (拡張子 .cpk を使用)、[Next] をクリックします。

.cpk ファイル用に十分な空きディスク容量がある場所を選択します。コンパイル済みのソフトウェアパッケージ (.cpk ファイル) は、通常、コンパイル前のソフトウェアパッケージ (.spk) よりもサイズが大きくなります。

重要： コンパイル済み (.cpk) ファイル名の指定を求められたときに .spk ファイルのパスとファイル名を指定すると、その .spk ファイルは上書きされ、編集できなくなります。したがって、コンパイル済みバージョンの名前を指定するときには、.cpk という拡張子を使用してください。

含まれるファイルの数によっても異なりますが、コンパイル処理には時間がかかる場合があります。

4 コンパイルが終了したら、[Finish] をクリックします。

5 ソフトウェアパッケージ (.cpk) を配布するには、275 ページの「ソフトウェアパッケージの配布」に進みます。

ソフトウェアパッケージの配布

ソフトウェアパッケージの配布の準備ができたら、次のようにしてソフトウェアパッケージを配布できます。

- Tiered Electronic Distribution を使用します。Tiered Electronic Distribution による配布の手順については、3 章 87 ページの「Tiered Electronic Distribution」を参照してください。
- ソフトウェアパッケージファイル (.cpk) を手動でサーバにコピーし、サーバのコンソールプロンプトから PACKAGE コマンドを使用して実行します。このコマンドを使用する手順については、417 ページの付録 C 、「サーバコンソールコマンド」を参照してください。

ソフトウェアパッケージをターゲットサーバにインストールした後、サーバを再起動しなければならない場合があります。たとえば、パッケージによって tcpip.nlm が変更された場合、この NLM を停止することはできません。サーバを再起動して、もう一度この NLM を実行する必要があります。ただし、ソフトウェアパッケージでサーバを停止し、自動的に再起動することができます。

古いバージョンの Server Software Package の ZENworks 6.5 Server Management への変換

Server Management には、古いバージョンの Server Software Package を ZENworks 6.5 Server Management に変換するためのウィザードが用意されています。ZENworks for Servers 1.0、2、および 3.*x* のソフトウェアパッケージを変換できます。

このウィザードは、*ZENworks 6.5 Server Management Program* CD には含まれていません。このウィザードを入手するには、技術情報ドキュメント 2962260 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2962260.htm) を参照してください。Readme ファイルにウィザードのインストール手順が記載されています。

ウィザードのインストール後に、古いバージョンの .spk または .cpk ファイルを ZENworks 6.5 Server Management に変換するには

1 変換したバージョンのソフトウェアパッケージファイルを配置する場所に対して書き込み権限があることを確認します。

2 ConsoleOne で、次のいずれかの操作を行います。

- Server Software Package ネームスペースを右クリックし、[Convert Software Packages to Version 6.5] をクリックします。
- Server Software Package ネームスペースを選択し、[File] > [Actions] の順にクリックして、[Convert Software Package to Version 6.5] を選択します。

Convert Server Software Package Wizard が起動します。

3 [Server Software Packages to Convert] ページで、[Add] をクリックし、.spk ファイルおよび .cpk ファイルを参照して選択します。

ウィザードによってソフトウェアパッケージのバージョンが自動的に確認されます。ZENworks 6.5 Server Management のファイルを選択した場合は、ファイルがすでにバージョン 6.5 になっていることを示すメッセージが表示されます。

このページには、古い変換不能なファイル (破損しているファイルや異なる種類のファイルで拡張子だけが .spk または .cpk に変更されたものなど) も表示されません。

選択した古いファイルについて、ウィザードのページの［Old Software Packages］列には、元のファイル名が表示されます。［New Software Packages］列には、新しいファイル名が表示されます。新しいファイル名は、ファイル拡張子の前に _v65 が挿入されるだけです。

列のサイズを変更してファイル名とパスの全体を表示することができます。

4 新しいソフトウェアパッケージの名前またはパスを変更するには、いずれかの列のファイル名をクリックします。次に、［Edit］をクリックして、名前またはパスを編集し、［OK］をクリックします。

新しいソフトウェアパッケージの名前とパスのみを変更できます。ただし、このウィザードを実行するユーザは、［New Software Packages］列に表示される場所に対する書き込み権限が必要です。

警告： 新しいファイルを古いファイルと同じ名前に変更することはできません。同じ名前に変更すると、古いファイルは変換したファイルに置換されます。ウィザードの次のページで［Cancel］をクリックすると、すべての変換したファイルが削除されます。したがって、古いソフトウェアパッケージファイルの元のバージョンが失われる場合があります。新しいファイルを古いファイルと同じ名前に変更した場合、変更を確認する警告メッセージが表示されます。

5 ファイル（.spk または .cpk）を変換から除外するには、［Old Software Packages］列のファイル名を選択し、［Delete］をクリックします。

これにより、ファイルはリストからは削除されますが、ハードドライブの場所からは削除されません。

6 ファイルの選択を終了した後で、［Convert］をクリックして変換プロセスを開始します。

変換プロセスの進行を示すメッセージが表示されます。

変換後のファイルは、［New Software Packages］列の指定した場所に配置されます。ウィザードの次のページで［Close］をクリックしてウィザードを終了すると、ファイルは指定した場所に残り、使用することができます。

すべてのファイルの変換が完了すると、［Converted Server Software Packages］ページが表示されます。

［Status］列に、表示されている各ファイルの変換ステータスが表示されます。変換に失敗したファイルを確認できます。

7 変換したソフトウェアパッケージを自動的に ConsoleOne の Server Software Packages ネームスペースに追加するには、［Converted Server Software Packages］ページの［Add the Above Software Packages to ConsoleOne］チェックボックスをオンにします。

このオプションを使用すると、新しい各パッケージを ConsoleOne に手動で追加する必要がありません。

8 ［Close］をクリックして、ウィザードを終了します。

［Add the Above Software Packages to ConsoleOne］チェックボックスをオンにした場合は、変換したソフトウェアパッケージが自動的に ConsoleOne の Server Software Packages ネームスペースに追加されます。

警告： ［Cancel］をクリックすると、変換したソフトウェアパッケージファイルは、［Server Software Packages to Convert］ページの［New Software Packages］列で指定したハードドライブの場所から削除されます。新しいファイルを古いファイルと同じ名前に変更した場合は、［Cancel］をクリックしたときに古いファイルが削除されます。

変換したソフトウェアパッケージは、ZENworks 6.5 Server Management サーバで使用できます。

Server Software Packages によるサーバ上のディレクトリの削除

種類の異なるネットワークサーバ (NetWare、Windows、Linux、および Solaris) から特定のディレクトリを削除する場合、通常、この作業を実行するための自動化された方法はありません。ただし、ZENworks 6.5 Server Management Policy and Distribution Services を使用している場合は、Server Management の Server Software Packages 機能によって、指定したディレクトリを Subscriber サーバのファイルシステムから削除できます。

複数のサーバ上の指定したディレクトリの削除を自動化するには、まず、必要に応じてパス変数を設定し、ConsoleOne でそのネームスペースに Server Software Package を作成し、そのソフトウェアパッケージをコンパイルした後、Tiered Electronic Distribution を使用してパッケージを配布します。その他のユーザの操作は不要です。

サーバ上の指定したディレクトリを削除するソフトウェアパッケージを作成するには、次の操作を行います。

1. 277 ページの「Server Software Package で使用する変数の設定」
2. 278 ページの「Server Software Package の作成」
3. 279 ページの「Server Software Package コンポーネントの作成と環境設定」
4. 280 ページの「Server Software Package のコンパイル」
5. 281 ページの「ディレクトリの削除の手動によるテスト」
6. 281 ページの「次のタスク」

Server Software Package で使用する変数の設定

パスに変数を使用する場合 (たとえば、ターゲットサーバで、NetWare と Windows のようにオペレーティングシステムが異なる場合) は、ソフトウェアパッケージを作成する前に、Subscriber オブジェクトのプロパティで変数を設定する必要があります。

1 削除するディレクトリを指定します。

1a パスのルートを指定します。ボリューム名 (NetWare)、ドライブ名 (Windows)、または /var/opt/novell/zenworks (Linux や Solaris の場合) などです。たとえば、data: と指定します。

1b 削除するディレクトリの親ディレクトリを含め、パスの残りの部分を指定します。たとえば、dist が親ディレクトリである場合は、¥zenworks¥pds¥ted¥dist と指定します。

1c 削除するディレクトリを指定します。たとえば、olddist.Distributions.ZENworks.Novell のように指定します。

フルパスと削除されるディレクトリは次のようになります。

```
data:\zenworks\pds\ted\dist\olddist.Distributions.ZENworks.Novell
```

サーバによってパスの要素は異なる場合があります。必要に応じて変数を使用することによって、これらの違いに対応できます。ステップ 2 とステップ 3 を参照してください。

2 ConsoleOne で、削除するディレクトリが存在している各 Subscriber の data:、D:、または /var/opt/novell/zenworks を表す変数（DELETEDDIRROOT など）を作成します。

削除するディレクトリとしてターゲットサーバに存在しないディレクトリを指定しても、サーバ上ではそのディレクトリについて何も行われません。

Tiered Electronic Distribution ポリシーを使用して、変数をグローバルに定義することもできます。このポリシーでは、変数のデフォルト値を定義する必要があり、適用可能な Subscriber オブジェクトのプロパティで例外を定義することもできます。

3 ConsoleOne で、Subscriber サーバに対してパス要素の異なる部分を表す Subscriber 変数を作成します。

変数については、9 章 355 ページの「変数」を参照してください。

4 必要に応じて、ステップ 2 とステップ 3 を繰り返します。

5 278 ページの「Server Software Package の作成」に進みます。

Server Software Package の作成

1 ZENworks 6.5 Server Management スナップインがインストールされている ConsoleOne の左側のペインで、Server Software Packages ネームスペースを右クリックします。

2 [File] > [New] > [Software Package] の順にクリックし、Create New Server Software Package ウィザードを起動します。

3 [Next] をクリックします。

4 ソフトウェアパッケージの名前を指定します。たとえば、Delete Old Directories のように指定します。

5 ソフトウェアパッケージテンプレートファイル（.spk）のパスとファイル名を指定します。たとえば、c:¥temp¥deletedirs.spk のように指定します。

重要： .spk ファイルをネットワークサーバに保存する場合は、ドライブ名を変更しても、そのソフトウェアパッケージファイルにアクセスできるように UNC パスを使用します。

.spk ファイルのサイズは大きくならないので、.spk ファイルはワークステーションやサーバに保存することもできます。この例で使用しているソフトウェアパッケージ（ディレクトリを削除する操作だけを指定し、データファイルをコンパイルしない）の場合は、.cpk（コンパイル済みソフトウェアパッケージ）バージョンも同じ程度のサイズになります。したがって、管理のために、これらの .spk ファイルと対応する .cpk ファイルを、ワークステーションまたはサーバの同じ場所に保存できます。

6 [Finish] をクリックします。

7 必要に応じて、プラス記号をクリックして Server Software Package ネームスペースを展開し、新しいパッケージを表示します。

8 279 ページの「Server Software Package コンポーネントの作成と環境設定」に進みます。

特に指示のない限り、以降の節の手順は、これまでの手順で使用したものと同じ ConsoleOne のインスタンスで行ってください。作成した .spk ファイルはこのインスタンスからアクセスできます。

Server Software Package コンポーネントの作成と環境設定

1 作成したソフトウェアパッケージオブジェクトを右クリックし、[New Component] をクリックします。

2 コンポーネントの名前を指定します。たとえば、Delete Directories のように指定します。

3 必要に応じて、プラス記号をクリックして、Server Software Package オブジェクトを展開します。

4 コンポーネントを右クリックし、[Properties] をクリックします。

5 [Copy File] タブを選択します。

6 [Add] ボタンの横にあるドロップダウンリストボタンをクリックし、[Add File Group] を選択します。

7 [Add] をクリックします。

8 ファイルグループの名前を指定します。たとえば、Delete Working Directories のように指定します。

9 [Group Target Path] フィールドで、削除するディレクトリの場所が含まれている作成済みの変数の名前を指定し、この変数に含まれていないパス情報を追加します。ただし、このパスの一部として削除するディレクトリの名前を指定しないでください。

   たとえば、削除するディレクトリの場所がすべてのターゲットサーバで同じである場合は、パス情報（変数も使用できる）で実際のボリューム (NetWare) またはドライブ (Windows) を指定します。

   ただし、サーバのオペレーティングシステムが異なるために変数を使用する必要がある場合は、% 記号で囲まれた変数名と、削除するディレクトリのすぐ上のディレクトリまでのフルパス（変数も使用できる）を指定します。たとえば、%DELETEDDIRROOT%（変数名）と %TARGET%¥pds¥ted¥dist（削除するディレクトリの親ディレクトリへのフルパス）を指定します。

   重要： 変数を使用する場合、指定するパスは、削除するディレクトリが含まれているディレクトリである必要があります。ステップ 11 では、削除する実際のディレクトリ名を追加します。

10 [OK] をクリックしてダイアログボックスを閉じます。

11 ドロップダウンリストのボタンをもう一度クリックし、[Add Directory] を選択します。

   最初に、このディレクトリを追加するツリー項目を選択していることを確認します。

12 [Add] をクリックします。

13 ツリー構造のデフォルトである名前 ("Directory") を、削除する実際のディレクトリ名 (olddist.Distributions.ZENworks.Novell など) に変更するには、ディレクトリ名を編集し、(Enter) キーを押して変更を保存します。

   (Enter) キーを押さなかった場合、再び "Directory" と表示されます。[Rename] ボタンを使用して、ディレクトリ名を編集できます。

14 [Copy Mode] コンボボックスの横にあるドロップダウンリストボタンをクリックし、[Delete] を選択します。

15 [Apply] をクリックします。

16 このソフトウェアパッケージで、このコンポーネントのファイルグループを使用して削除する各ディレクトリについて、ステップ 10 からステップ 15 までを繰り返します。

他のファイルグループを追加する場合は、ステップ 6 から始め、新しいコンポーネントを追加する場合は、ステップ 1 から始めます。ステップ 6 で作成したファイルグループに、削除するすべてのディレクトリを追加できない場合は、これらの手順から繰り返すことができます。

17 ソフトウェアパッケージコンポーネントの設定が終了したら、[OK] または [Close] をクリックします。

これまでの手順の例に従って、次のように入力したとします。

%DELETEDDIRROOT%

および

%TARGET%¥pds¥ted¥dist

および

olddist.Distributions.ZENworks.Novell

この場合、次のパスにあるディレクトリが削除されます。

```
data:\zenworks\pds\ted\dist\olddist.Distributions.ZENworks.Novell
d:\zfs\zenworks\pds\ted\dist\olddist.Distributions.ZENworks.Novell
```

18 280 ページの「Server Software Package のコンパイル」に進みます。

Server Software Package のコンパイル

削除する対象のテンプレートとして機能する .spk ファイルを作成しました。この .spk ファイルを .cpk ファイルにコンパイルする必要があります。

1 ソフトウェアパッケージ (Delete Old Directories など) を右クリックします。

2 [Compile] を選択して、Compile Software Package ウィザードを起動します。

3 ウィザードの最初のページの [Next] をクリックします。

4 生成する .cpk ファイルのフルパスおよびファイル名を指定します。

重要： このファイル名に .spk という拡張子を使用しないでください。保存場所が同じである場合、テンプレートファイルがコンパイル済みバージョンによって上書きされる可能性があります。これによって、ソフトウェアパッケージをさらに編集することができなくなります。DELETEDIRS など、ファイル名を同じにすることはできますが、ファイル名の拡張子には .cpk だけを使用してください。

5 [Next] をクリックし、[Finish] をクリックします。

6 281 ページの「ディレクトリの削除の手動によるテスト」に進みます。

ディレクトリの削除の手動によるテスト

ソフトウェアパッケージは、Software Package Distribution として送信する準備ができました。ただし、テストのために、いずれかのターゲットサーバでソフトウェアパッケージを手動で処理し、意図したとおりにディレクトリが削除されることを確認できます。

1 ディレクトリを削除するサーバで、¥zenworks¥pds¥ted¥dist の下に、ソフトウェアパッケージに含まれるディレクトリ（olddist.Distributions.ZENworks.Novell など）を作成します。

2 .cpk ファイル（deletedirs.cpk など）をそのサーバの ¥temp ディレクトリにコピーします。

3 サーバの ZENworks Server Management コンソールのプロンプトで、PACKAGE PROCESS コマンドを実行してソフトウェアパッケージを処理します。

たとえば、NetWare サーバの場合は、ZENworks Server Management のプロンプトで次のコマンドを実行します。

```
package process data:¥temp¥deletedirs.cpk
```

Server Management によって、パッケージが処理され、処理が終了したことがレポートされます。サーバのファイルシステムを調べて、
¥olddist.Distributions.ZENworks.Novell ディレクトリ、つまり指定したディレクトリが削除されたことを確認します。

次のタスク

テストの結果に問題がなければ、Tiered Electronic Distribution を使用して、新しい Software Package Distribution によって deletedirs.cpk ファイルをすべてのターゲット Subscriber サーバに配布し、Subscriber サーバのファイルシステム上のディレクトリを削除できます。

6 Desktop Application Distribution

Novell® ZENworks® Server Management の Policy and Distribution Services は、ZENworks 6.5 Desktop Management の Novell Application Management と統合されています。

次の節では、ZENworks Server Management と ZENworks Desktop Management の統合機能の理解、設定、および使用方法について説明します。

- 283 ページの「Desktop Application Distribution の理解」
- 299 ページの「要件」
- 300 ページの「Desktop Application Distribution の作成」
- 308 ページの「Desktop Application Distribution の再構築」
- 310 ページの「Desktop Application Distribution ファイルのクリーンアップ」
- 310 ページの「ツリー間での Desktop Application Distribution の送信」

Desktop Application Distribution の理解

Server Management では、Novell Application Launcher™ によって配布されたアプリケーションの地理的、負荷、および冗長の問題を解決できます。これらの問題解決には、Server Management を使用しなければ Desktop Management での手作業による設定に多くの時間を必要とします。Server Management がデスクトップアプリケーションの作業の自動化にどのように役立つかについては、次の節を参照してください。

- 283 ページの「Desktop Application Distribution の目的」
- 286 ページの「配布されたアプリケーションの問題」
- 297 ページの「その他の問題」

Desktop Application Distribution の目的

- 284 ページの「Desktop Management のアプリケーション」
- 285 ページの「Server Management の配布されたアプリケーション」

Desktop Management のアプリケーション

Desktop Management では、Novell Application Launcher を経由してユーザやワークステーションがアプリケーションを受信するために、アプリケーションオブジェクトを作成できます。アプリケーションオブジェクトにはアプリケーションに属するファイルへのポインタが含まれ、アプリケーションをどのようにインストールしてデスクトップ上に設定するかを定義する環境設定パラメータも含まれます。

Desktop Management では、アプリケーションに属するファイルを任意のサーバに配置でき、関連するアプリケーションオブジェクトをツリーの任意の場所に配置できます。したがって、Novell Application Launcher を経由してアプリケーションを受信するワークステーションに対して、アプリケーションのファイルがサーバからコピーされ、ワークステーションにインストールされます。

ただし、Desktop Management 管理者に対しては次のような問題が発生する可能性があります。

- **ネットワークトラフィック：** アプリケーションを入手する場合に、多くのユーザやワークステーションでネットワークトラフィックが大きくなる可能性があります（特に低速な WAN リンクを経由した場合）。

  Desktop Management のみを使用している場合にネットワークトラフィックが大きくなる地理的な問題に対処するには、多くの手作業を必要とします。アプリケーションオブジェクトの再作成とカスタム設定を何度も行い、ワークステーションにサービスをローカルに提供するさまざまなサーバにファイルをコピーする必要があります。

- **ローカルアプリケーションアクセス：** ユーザは、ネットワークに接続している場所に関係なくアプリケーションにローカルアクセスできる必要があります。

  手作業でアプリケーションオブジェクトを複製し、アプリケーションオブジェクトの各コピーにサイトリストを作成する必要があります。

  サイトリストの詳細については、『*ZENworks 6.5 Desktop Management 管理ガイド*』の「サイトリストのセットアップ」を参照してください。

- **サーバの負荷：** さまざまなアプリケーションファイルを 1 つのサーバにロードしていると、すべてのワークステーションにサービスを提供するには負担が大きすぎる場合があります。

  Desktop Management のみを使用している場合は、アプリケーションオブジェクトの負荷分散を設定してサーバ間で配布負荷を共有し、複数のサーバが同じサービスを実行できるようにすることでサーバの過重負荷に対処できます。ただし、この機能を使用するには多くの手作業が必要になります。

- **サーバの冗長性：** さまざまなアプリケーションファイルをロードされたサーバが停止した場合は、ワークステーションがアプリケーションを受信できません。

  Desktop Management のみを使用している場合は、アプリケーションオブジェクトの障害対策を設定してサーバを冗長化し、アプリケーションオブジェクトにリストされているバックアップサーバを複数にすることでサーバが停止している状況に対処できます。ただし、この機能を使用するには多くの手作業が必要になります。

Server Management には、このような地理的な問題や手作業の問題を解決するソリューションが用意されています。方法を参照するには、285 ページの「Server Management の配布されたアプリケーション」に進みます。

Server Management の配布されたアプリケーション

Server Management には、ネットワークトラフィック、アプリケーションへのローカルアクセス、サーバの帯域幅、および冗長の問題を最小限にし、管理者の負担を軽減する Desktop Application Distribution が用意されています。

例：

- **ネットワークトラフィック：** アプリケーションを含む Desktop Application Distribution を作成した後、各地域の Subscriber がアプリケーションのローカルコピーを作成します。そこでは、Novell Application Launcher がローカルアプリケーションを使用して Subscriber サーバのユーザとワークステーションにサービスを提供できます。
- **ローカルアプリケーションアクセス：** Desktop Application Distribution を作成して送信した後、リンクアップサイトがリストされ、地理的な場所を移動したユーザが自分のアプリケーションにローカルアクセスできるようになります。

  Server Management によるサイトリストのセットアップ方法については、307 ページのステップ 13 を参照してください。
- **サーバの負荷：** 負荷分散機能を使用すると、Novell Application Launcher によって複数のサーバを利用して多くのユーザやワークステーションにサービスを提供できます。Desktop Application Distribution を受信する各サーバに、共通の作業コンテキストを使用します。これで、複数のサーバが負荷分散を使用できます。

  重要： 負荷分散は Subscriber サーバ上のソースパスへのアクセスに関係し、配布されたアプリケーションオブジェクトへのアクセスには関係しません。
- **サーバの冗長性：** 障害対策機能を使用すると、冗長化が行われ、Novell Application Launcher によって、サーバが停止したときに他のサーバがユーザとワークステーションにサービスを同じように提供できます。Desktop Application Distribution を受信する各サーバに、共通の作業コンテキストを使用します。これで、複数のサーバが障害対策を使用できます。

  重要： 障害対策は Subscriber サーバ上のソースパスへのアクセスに関係し、配布されたアプリケーションオブジェクトへのアクセスには関係しません。

負荷分散や障害対策を行うには、次の作業のみを実行します。

1. アプリケーションまたはアプリケーションのグループに対して Desktop Application Distribution を 1 つ作成します。
2. Distribution を複数のサーバに送信します。

   Server Management が各サーバの環境に基づいてアプリケーションを自動的に設定します。
3. 新しいアプリケーションオブジェクトに関連するグループに必要なユーザやワークステーションを手作業で割り当てます。
4. 1 つのボタンをクリックしてサイトリストにリンクします。

これにより各サーバは次のようになります。

- アプリケーションのファイルのサーバ自体のコピーをファイルシステム上に持ちます。
- そのファイルを指定するアプリケーションオブジェクトへのアクセス権を持ちます。

  アプリケーションオブジェクトは、Novell Application Launcher を経由してワークステーションにアプリケーションをインストールするために使用されます。

Distribution プロセスは、複数のアプリケーションオブジェクトの作成、カスタム環境設定、およびファイルコピー作業を自動的に実行します。

これらの問題を Server Management が解決する方法について理解を深めるには、286 ページの「配布されたアプリケーションの問題」に進みます。

配布されたアプリケーションの問題

Desktop Application Distribution を送信する場合は、アプリケーションオブジェクトの内容の一部は保持され、一部は保持されず、一部は変更されます。次の節では、このことについて説明します。

- 286 ページの「配布準備のできたアプリケーションオブジェクトと配布されたアプリケーションオブジェクトの理解」
- 287 ページの「配布準備のできたアプリケーションの属性の保持」
- 289 ページの「オブジェクト配布時の関連付けの保持」
- 290 ページの「アプリケーションのファイル権利の保持」
- 291 ページの「Subscriber 作業コンテキストの競合」
- 292 ページの「ソースパスの保持」

配布準備のできたアプリケーションオブジェクトと配布されたアプリケーションオブジェクトの理解

Desktop Application Distribution を作成する場合は、配布するアプリケーションオブジェクトを選択します。Server Management では、これは「配布準備のできた」アプリケーションオブジェクトと呼ばれます。Distribution によって作成されたすべてのアプリケーションオブジェクトは、「配布された」アプリケーションオブジェクトと呼ばれます。

配布準備のできたアプリケーションの固有性

管理者は Distribution に対する配布準備のできたアプリケーションオブジェクトがどれであるかを知っておく必要があります。アプリケーションオブジェクト同士は ConsoleOne® で見分けがつかないからです。

アプリケーションオブジェクトに関連した Desktop Management の通常の作業がオブジェクトの内部リビジョン番号を変更する可能性があるため、Distribution の不必要なデルタがトリガされ、送信される場合があります。たとえば、Distribution の再構築が、Distribution に含まれるアプリケーションに関連付けられたユーザグループオブジェクトの単純な変更によってトリガされる可能性があります。この情報は配布されたアプリケーションにまったく転送されません。したがって、配布準備のできたアプリケーションをユーザやワークステーションで使用しないでください。

配布準備のできたアプリケーションオブジェクトを固有の Novell eDirectory™ コンテキストに保持し、ユーザとワークステーションを配布されたアプリケーションオブジェクトだけに関連付けることをお勧めします。詳細については、308 ページの「Desktop Application Distribution の再構築」を参照してください。

配布準備のできたアプリケーションと配布されたアプリケーションの同期化

Distribution が再構築され、再送信された場合は、すべての配布されたアプリケーションオブジェクトが配布準備のできたアプリケーションオブジェクトと同期化されます。つまり、配布されたアプリケーションオブジェクトに重要な変更を加えたが配布準備のできたアプリケーションオブジェクトには加えなかった場合に Distribution を再構築して再送信すると、変更が失われる可能性があります。Distribution は配布準備のできたアプリケーションオブジェクトの内容だけを使用して配布されたオブジェクトを更新するからです。したがって、Distribution を再送信する場合に変更するオブジェクトは、配布準備のできたアプリケーションオブジェクトのみです。

ただし、配布されたアプリケーションオブジェクトが上書きされない場合は、再送信される Distribution によって一般的に上書きされない属性を変更できます。これは、次の節で説明します。

287 ページの「配布準備のできたアプリケーションの属性の保持」に進みます。0201 納品ここまで

配布準備のできたアプリケーションの属性の保持

Server Management は、配布準備のできたアプリケーションオブジェクトの属性のすべてではなく、大部分を配布します。したがって、Distribution が再構築されたときに配布されたアプリケーションオブジェクトに含まれる属性に応じて、さまざまな結果が発生する可能性があります。

次の節では、属性が配布された場合と配布されなかった場合について説明します。

- 287 ページの「配布される属性」
- 287 ページの「配布されない属性」
- 288 ページの「一度だけ送信される属性」
- 288 ページの「変更される属性」

配布される属性

属性が ConsoleOne で変更できる場合は、配布準備のできたアプリケーションオブジェクトに存在する、次の 3 つの節でリストされないすべての属性が配布されます。これらの属性は Distribution 構築時に配布準備のできたアプリケーションオブジェクトから読み取られ、Server Management が配布されたアプリケーションオブジェクトを作成または更新するたびに送信されます。

配布準備のできたアプリケーションオブジェクトの属性は、更新されたものだけではなくすべてが、Distribution の再構築、送信、および抽出時に、配布されたアプリケーションオブジェクトで更新されます。つまり、すべての配布されたアプリケーションオブジェクトは、次の 3 つの節に記載されているものを除き、配布準備のできたアプリケーションと同期化されています。

配布されない属性

eDirectory 属性名ごとにリストされた次の属性は、Distribution 構築プロセスで読み取られず、Server Management によって配布されたアプリケーションオブジェクトに設定されません。

属性名	アプリケーションオブジェクトのプロパティ内のロケーション
App:FS Rights Path	[Common] タブ > [File Rights] サブタブ > [Path] 列

属性名	アプリケーションオブジェクトのプロパティ内のロケーション
App:FS Rights Volume	[Common] タブ > [File Rights] サブタブ > [Volume] 列
App:Printer Ports	[Common] タブ > [Drives/Ports] サブタブ > [Ports to be Captured] リストボックス

このリストには、ConsoleOne で変更できる属性のみが含まれています。

一度だけ送信される属性

eDirectory 属性名ごとにリストされた次の属性は、最初のアドレス帳を提供するために一度だけ送信されます。

属性名	アプリケーションオブジェクトのプロパティ内のロケーション
App:Contacts	[Identification] タブ > [Contacts] サブタブ

この属性は、2 回目以降の Distribution 更新では更新されません。このため、配布されたアプリケーションオブジェクトのこの属性の変更が、配布準備のできたアプリケーションオブジェクトのオリジナルまたは更新済みアドレス帳によって上書きされることがありません。

この属性は、ConsoleOne で変更できます。

変更される属性

eDirectory 属性名ごとにリストされた次の属性は、Distribution 構築時に配布準備のできたアプリケーションオブジェクトから読み取られ、ターゲットサーバの作業コンテキストにおける配布されたアプリケーションオブジェクト作成時にアプリケーションオブジェクトの新環境に合わせて変更されます。

属性名	アプリケーションオブジェクトのプロパティ内のロケーション
ACL	[NDS Rights] タブ > [Trustees of This Object] サブタブ
App:Alt Back Link	[Fault Tolerance] タブ > [Remote Alternate App] サブタブ
App:Associations	[Associations] タブ
App:Back Link	[Run Options] タブ > [Application Dependencies] サブタブ > [Show Chain] ボタン
App:Fault Tolerance	[Fault Tolerance] タブ > [Fault Tolerance] サブタブ
App:Load Balancing	[Fault Tolerance] タブ > [Load Balancing] サブタブ
App:Site List	[Distribution] タブ > [Link Up Site List] ボタン (Server Management スナップインが ConsoleOne にインストールされている場合のみ表示される)。このボタンの使用方法と理由については、307 ページのステップ 13 を参照してください。
アプリケーション GUID	[Distribution Options] タブ > [Options] サブタブ > [GUID] フィールド
creatorsName	[Listed on the Other] タブ (表示するには [Show Read Only] をクリック)。

属性名	アプリケーションオブジェクトのプロパティ内のロケーション
modifiersName	[Other] タブ (表示するには [Show Read Only] をクリック)。
Object Class	[Listed on the Other] タブ。
Revision	[Listed on the Other] タブ (表示するには [Show Read Only] をクリック)。
Used By	[Listed on the Other] タブ (表示するには [Show Read Only] をクリック)。

このリストには ConsoleOne で変更できる属性のみが含まれ、属性はアプリケーションを定義する必要がある場合にのみアプリケーションオブジェクトに表示されます。

289 ページの「オブジェクト配布時の関連付けの保持」に進みます。

オブジェクト配布時の関連付けの保持

Desktop Application Distribution を設定する場合は、関連付けの保持を指定できます。つまり、配布準備のできたアプリケーションオブジェクトに設定されている属性の関連付けが、Distribution によって作成される配布されたアプリケーションオブジェクトに保持されます。

Desktop Application Distribution では、適用可能なユーザやワークステーションを配布されたアプリケーションオブジェクトに追加するなど、手作業がいくつか必要です。Desktop Application Distribution オブジェクトにはその情報がありません。これは、ユーザとワークステーションが、配布されたアプリケーションを受信するサーバによって異なる可能性があるためです。

[Maintain Associations] オプションを選択すると、属性の関連付けが次の方法で処理されます。

- **[Maintained]** : ユーザグループ、ワークステーショングループ、組織、および部門の各オブジェクト。

  これらは信頼されるグループおよびコンテナです (ソースのルートコンテナ内)。これらは次の方法で保持されます。

  - **[Created New]** : グループおよびコンテナのオブジェクトが存在しない場合、それらのオブジェクト。

    配布されたアプリケーションを必要とするユーザやワークステーションにそのオブジェクトを手作業で設定する必要があります。

  - **[Not Overwritten]** : グループおよびコンテナのオブジェクトがすでに存在する場合、それらのオブジェクト。

    グループオブジェクトとコンテナオブジェクトがすでに存在して配布されたアプリケーションオブジェクトに割り当てられている場合、設定が上書きされません。配布されたアプリケーションを使用する必要があるユーザやワークステーションにすでに設定されている可能性があるからです。既存のグループやコンテナに他のユーザやワークステーションを追加する場合は、手動で追加する必要があります。

- **[Not Created]** : ユーザおよびワークステーションオブジェクト。

  Distribution の抽出後に、適用可能なユーザやワークステーションを配布されたアプリケーションオブジェクトに追加できます。

チェーンアプリケーションの情報やフォルダを配布する場合は、[Maintain Associations] オプションが必要です。これは 298 ページの「Distribution のチェーンアプリケーション」に記載されています。

290 ページの「アプリケーションのファイル権利の保持」に進みます。

アプリケーションのファイル権利の保持

配布準備のできたアプリケーションオブジェクトに設定したファイル権利は、配布されたアプリケーションオブジェクトに渡されません。ファイルの場所はサーバによって異なり、予想できないからです。

Desktop Application Distribution では、ファイルアクセス権の追加など、いくつかの手作業が必要です。このような処理は、配布されたアプリケーションオブジェクト作成時の ZENworks による最小セット以外の作業となります。(通常のアプリケーションには最低限の権限で十分です。)

Desktop Application Distribution でのファイル権利処理方法については、次の節を参照してください。

- 290 ページの「配布されないファイル権利」
- 290 ページの「ファイル権利とグループ」
- 290 ページの「チェーンアプリケーションとファイル権利」
- 291 ページの「ファイル権利の設定」
- 291 ページの「ファイル権利の代わりとしてのトラスティと共有の設定」

配布されないファイル権利

[Rights to Files and Folders] タブを使用してアプリケーションオブジェクトに明示的に割り当てられているファイル権利は転送されませんが、ユーザが配布されたアプリケーションを使用するのに必要な最小限度 (読み込み権およびファイルスキャン権) にリセットされます。配布されたアプリケーションオブジェクトが作成された後でコンテナやグループに関連付けられたときに、ファイル権利は設定されます。

アプリケーションオブジェクトの [Common] > [File Rights] タブで割り当てられたファイル権利も、配布されません。

配布されたアプリケーションオブジェクトのこれらのタブで後に追加の権利を付与でき、権利は削除も置換もされません。

ファイル権利とグループ

ユーザやワークステーションが Desktop Application Distribution の配布グループのメンバーである場合は、ユーザやワークステーションのファイル権利を個別に設定する必要はありません。ユーザやワークステーションは、アプリケーションに対する自分の権利をグループのメンバーシップによって取得します。

チェーンアプリケーションとファイル権利

チェーンアプリケーションを使用する場合は、ディレクトリに対する権利を必要とするチェーンのすべてのアプリケーションが、配布準備のできたアプリケーションのツリー構造のユーザグループ、ワークステーショングループ、またはコンテナに関連付けられている必要があります。ユーザやワークステーションのオブジェクトの権利は、配布されたアプリケーションオブジェクトに個別に保持されないからです。

ファイル権利の設定

チェーンアプリケーションに属するファイルへの読み取りと書き込みのアクセス権を付与するには、ユーザグループオブジェクトまたはワークステーショングループオブジェクトの［Rights to Files and Folders］タブでファイル権利を割り当てます。

ファイル権利の代わりとしてのトラスティと共有の設定

Server Management では NetWare® 用のファイルに権利が個別に設定されません。そのファイルを含むディレクトリにトラスティのみが設定され、権利は常に読み込み権利およびファイルスキャン権利になります。したがって、NetWare サーバ上では、アプリケーションのファイルが配布されるディレクトリにユーザの読み込み権を付与してください。たとえば、ファイルを ¥apps ディレクトリにコピーした場合は、そこにファイルがコピーされたアプリケーションをユーザが使用するには、¥apps ディレクトリへの読み込み権が必要です。

Server Management では、Windows でもファイル権利が設定されません。したがって、アプリケーションの配布ファイルにアクセスするユーザごとに共有を設定します。

291 ページの「Subscriber 作業コンテキストの競合」に進みます。

Subscriber 作業コンテキストの競合

Subscriber のすべてが同じ作業コンテキストを使用するか固有の作業コンテキストを使用するかは、アプリケーション配布の設計ニーズによって異なります。負荷分散または障害対策を使用する場合は、Desktop Application Distribution を受信するすべての Subscriber が同じ作業コンテキストを使用している可能性があります。詳細については、283 ページの「Desktop Application Distribution の目的」を参照してください。

同じ作業コンテキストを使用する Subscriber が複数存在する場合は、eDirectory が衝突する可能性があります。つまり、複数の Subscriber は同時に同じ Desktop Application Distribution からツリーの同じ作業コンテキストにコピーを抽出できません。

たとえば、2 つの Subscriber が同時にアプリケーションを抽出し、2 つの異なる eDirectorys レプリカにアプリケーションオブジェクトを作成した場合は、eDirectory の同期化に問題が発生します。eDirectory は 2 つの異なるオブジェクトを検出しますが、2 つの異なるレプリカに同じ名前と同じタイムスタンプがあるため、eDirectory は重複したオブジェクトの名前に数字を付けてオブジェクトのうち 1 つの名前を変更し、これを解決します。（詳細については、技術情報 10062001（http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062001.htm）を参照）。

Subscriber のグループに同じ作業コンテキストを使用する場合は、各 Subscriber の抽出スケジュールが異なる時間に開始されるか確認し、Subscriber が抽出を完了してから次の Subscriber が抽出を開始できるように、スケジュールの間に十分な時間をあける必要があります。

各 Subscriber が固有の作業コンテキストを使用する場合は、すべての Subscriber が同時に同じ Desktop Application Distribution のコピーを抽出でき、eDirectory の衝突は発生しません。

すぐに抽出するように Distribution が設定されている場合、同じシナリオになります。

292 ページの「ソースパスの保持」に進みます。

ソースパスの保持

アプリケーションの多くはサポートするファイルを必要とし、ソースファイルへのパスが Desktop Management のアプリケーションオブジェクトに設定されている必要があります。これは「ソースパス」と呼ばれます。

この節では、ソースパスを使用するアプリケーションオブジェクトを含む Desktop Application Distribution について説明します。notepad.exe などの実行可能ファイルのみを必要とするアプリケーションの場合は、アプリケーションオブジェクトにソースパスは必要ありません。

Desktop Application Distribution でのソースパス使用方法については、次の節を参照してください。

- 292 ページの「Server Management でのソースパスの使用方法」
- 294 ページの「SOURCE_PATH マクロの目的」
- 295 ページの「SOURCE_PATH マクロの値の解釈方法」
- 295 ページの「MSI アプリケーションとソースパス」
- 295 ページの「Server Management の変数の定義」
- 296 ページの「Distribution の［Source Path］オプションの使用方法」

Server Management でのソースパスの使用方法

Desktop Application Distribution プロセス時に配布準備のできたアプリケーションオブジェクトと配布されたアプリケーションオブジェクト間の属性に起きることを示すために、次の表に ConsoleOne で表示および設定できるソースパス、その目的、場所の設定方法、および配布ステータスをリストします。

ソースパス名（タイプ）	アプリケーションオブジェクト内の場所	目的	設定方法	配布情報
SOURCE_PATH（マクロ[1]）	［Distribution Options］>［Application Files］>［Source］列	SOURCE_PATH マクロからパスを解決します。	SOURCE_PATH マクロから	これは、［Name］列の下にリストされる、それを使用する各アプリケーションファイルに配布されます。
SOURCE_PATH（マクロ）	［Common］>［Macros］>［Name］列	アプリケーションオブジェクトによって使用されるソースパスを［Value］列で定義します。	配布されたアプリケーションオブジェクト作成時にこのページ上で作成するエントリから	これは、Subscriber の環境に合わせて変更された状態で配布されます。配布準備のできたアプリケーションオブジェクトで変更されている場合は、必要な変更が加えられ、配布されたアプリケーションオブジェクトで更新されます。 Novell Application Launcher の配布に問題が発生しないように、配布準備のできたアプリケーションオブジェクトでこのソースパスを変更しないでください。

ソースパス名（タイプ）	アプリケーションオブジェクト内の場所	目的	設定方法	配布情報
Package Source List（ボックス）	[Common] > [Sources]	使用する負荷分散プロパティと障害対策プロパティのソースパスリストを提供します。	SOURCE_PATH マクロから、Disribution を受信および抽出する同じ作業コンテキストを使用する各 Subscriber から、および [Add] ボタンを使用して作成するエントリから	SOURCE_PATH マクロのエントリのみがパスの長いバージョン (DNS) を使用して Server Management によって複製されます。 リストされたソースパスは、有効な UNC パス、または有効な UNC パスを解決する変数のいずれかである必要があります。 リストされた各ソースパスは、Distributor サーバのファイルシステム上にあるアプリケーションファイルの完全なセットを指定します。(Distributor は他のサーバからそれ自体の Desktop Application Distribution のファイルを収集できません。) ソースパスによって指定される実際のソースファイルは、Distribution が再構築されて再送信されるたびに上書きされます。 配布されたアプリケーションオブジェクトのこのフィールドは累積的であり、Distribution 再送信時に上書きされません。同じ作業コンテキストを使用する Distribution を受信する Subscriber に対して負荷分散や障害対策を選択するか、配布されたアプリケーションオブジェクトの [Add] ボタンを使用すると、エントリが行われます。ただし、配布準備のできたアプリケーションオブジェクトの SOURCE_PATH マクロに変更を加えると、このリストボックスのソースパスが更新され、リストの最初に挿入されます。前のソースパスは置き換えられず、リストに残ります。前のソースパスは有効でなくなり、削除できます。
Source List（ボックス）	[Fault Tolerance] > [Fault Tolerance]	サーバのリストを提供し、Novell Application Launcher の作業に使用しているサーバが停止した場合に備えて冗長化を可能にします。 リストされたソースパスはすべて、同じアプリケーションファイルセットを指定する必要があります。それ以外の場合、配布されたアプリケーションが正しく作成されないことがあります。	Disribution を受信および抽出する、同じ作業コンテキストを使用する各 Subscriber から実行します。	この情報は、配布準備のできたアプリケーションオブジェクトからは配布されません。同じ作業コンテキストを使用する複数の Subscriber に Distribution を送信することにより、このフィールドを設定する必要があります。

ソースパス名（タイプ）	アプリケーションオブジェクト内の場所	目的	設定方法	配布情報
Source List（ボックス）	[Fault Tolerance] > [Load Balancing]	サーバのリストを提供し、Novell Application Launcher が作業できるようにサーバ間の負荷分散を実行できます。 リストされたソースパスはすべて、同じアプリケーションファイルセットを指定する必要があります。それ以外の場合、配布されたアプリケーションが正しく作成されないことがあります。	Disribution を受信および抽出する、同じ作業コンテキストを使用する各 Subscriber から実行します。	この情報は、配布準備のできたアプリケーションオブジェクトからは配布されません。同じ作業コンテキストを使用する複数の Subscriber に Distribution を送信することにより、このフィールドを設定する必要があります。

[1] Desktop Management の「マクロ」は、Server Management の「変数」と同じ機能を持っています。

SOURCE_PATH マクロの目的

SOURCE_PATH マクロは、Distributor サーバのファイルシステム上のアプリケーションオブジェクトのファイルがある場所に、アプリケーションオブジェクトのソースパスを定義します。これは、Desktop Application Distribution を構築するために Distributor がアプリケーションファイルにアクセスする場所です。

SOURCE_PATH マクロの値は、Subscriber サーバのファイルシステムに場所を作成するために使用されます。そこには配布されたアプリケーションオブジェクト作成時に Subscriber がアプリケーションファイルを配置します。

SOURCE_PATH マクロの値に含まれる情報は、次のとおりです。

- サーバ名、IP アドレス、またはフル DNS 名のいずれかによるサーバ識別（Distributor サーバ）
- Distributor サーバ上のボリュームまたはドライブ
- ユーザ定義パス情報（ウィザードで提供される場合）
- アプリケーションパス情報（ウィザードで選択）

次に例を示します。

```
server1.novell.com\sys\apps\acrobat
```

```
server1.novell.com\n\apps\acrobat
```

これは次のような有効な UNC パスとして解決されます。

```
\\server1\sys\apps\acrobat
```

SOURCE_PATH マクロの値にマクロまたは変数が含まれていると、Server Management が埋め込まれた情報を解決しません。Server Management は SOURCE_PATH マクロの値を有効な UNC パスとしてのみ解決します。

グローバルポリシー変数が定義されている場合、マップされたドライブ文字を使用することもできます。

SOURCE_PATH マクロの値の解釈方法

Tiered Electronic Distribution では、配布準備のできたアプリケーションオブジェクトのソースパスと一致するものを見つけるために変数が検索されます。たとえば、配布準備のできたアプリケーションオブジェクトのソースパスが ¥apps¥acrobat である場合、次の順序で一致するものが検索されます。

n:¥
N:¥
n:
N:
n
N

ただし、配布準備のできたアプリケーションオブジェクトのソースパスが N:¥apps¥acrobat である場合、次の順序で一致するものが検索されます。

N:¥
n:¥
N:
n:
N
n

MSI アプリケーションとソースパス

.mst ファイルは、ファイルのフルパスを指定せずに入力できます（［MSI］>［Transforms］タブ）。Server Management が、アプリケーションオブジェクトに定義されたソースパスを使用して、Desktop Application Distribution 構築時に .mst ファイルを検索するからです。ただし、このことが適用されるのは .mst ファイルが MSI ファイルと同じディレクトリに存在する場合のみです。

Server Management の変数の定義

従来、マップされたドライブは、デスクトップ上のマップされたドライブからアプリケーションを起動する手段として、アプリケーションオブジェクトに埋め込まれてきました。Server Management では変数を使用して、ドライブマッピングに使用するアプリケーションを配布します。

Distributor および Distribution を受信するすべての Subscriber のボリューム名とマップされたドライブが異なっている可能性があるため、変数を使用することで Distributor と各 Subscriber によって解釈される値でこれらの場所を識別できるようになります。

変数は、次のようにグローバルおよび個別に定義できます。

- **SLP のプロパティパッケージの Tiered Electronic Distribution ポリシーによるグローバルな定義**

  Tiered Electronic Distribution ポリシー（SLP のプロパティパッケージ）に定義された変数は、ポリシーパッケージを Subscriber オブジェクトの親コンテナに関連付けるなど、そのポリシーに関連付けられたすべての Subscriber オブジェクトで使用できます。各 Subscriber に対して有効にするポリシーについて、［Variables］のプロパティページで［Include Policy］チェックボックスが選択されていることを確認してください。

ポリシーパッケージは、Distributor オブジェクトの親コンテナにも関連付けられている必要があります。ポリシーの変数定義によって、Distributor にアプリケーションファイルを収集する場所を確実に通知できます。

Distributor と Subscriber の両方が同じ変数値を使用している場合は、Tiered Electronic Distribution ポリシーが 1 つだけ必要で、その SLP のプロパティパッケージを Distributor と Subscriber 両方の親コンテナに関連付けることができます。

たとえば、配布準備のできたアプリケーションオブジェクトのマップされたドライブのソースパスが n:¥applications¥acrobat であり、Distributor サーバの sys:¥public ディレクトリを n: で表すとします。変数を作成するには、Tiered Electronic Distribution ポリシーで［Variables］タブを選択した後、変数の n: とその値の sys:¥public を入力します。これで、Distributor は Distribution を構築する必要がある場合に、sys: ボリュームの ¥applications¥acrobat ディレクトリを見つけることができます。

このポリシーの詳細については、213 ページの「Tiered Electronic Distribution」を参照してください。

- **各ターゲット Subscriber のプロパティでの個別の定義**

  任意の Subscriber オブジェクトに対して変数を定義できます。この定義は、Subscriber が関連付けられている Tiered Electronic Distribution ポリシーに定義されている場合は、同じ変数を上書きします。

  これは、Subscriber サーバのボリューム名またはマップされたドライブが Distributor サーバのものと異なる場合（同じ Tiered Electronic Distribution ポリシーを使用できないため）、または Distribution を受信する Subscriber 同士のボリューム名やマップされたドライブが異なる場合に便利です。

  Subscriber の変数定義方法については、361 ページの「変数の定義」を参照してください。

Distribution の［Source Path］オプションの使用方法

配布準備のできたアプリケーションオブジェクトがマップされたドライブを使用する場合は、Desktop Application Distribution ウィザード実行時に［Keep the Same Source Paths for the Replicated Objects］オプションを有効にします。このオプションを有効にすると、配布されるアプリケーションがマップされたドライブの指定を使用できるよう、Distribution が配布準備のできたアプリケーションのソースパスを保持するようになります。マップされたドライブの値によって、アプリケーションファイルのコピー先が決まります。

配布準備のできたアプリケーションのソースパスがドライブにマップされているが、抽出ディレクトリに基づいて配布されたアプリケーションに UNC パスを使用させる場合は、このオプションを選択する必要はありません。しかし、マップされたドライブに定義された変数を使用して、SLP のプロパティパッケージの Tiered Electronic Distribution ポリシーを定義する必要があります。このパッケージは、Distribution を構築するために、変数によって Distributor に関連付けられている必要があります。また、ドライブマッピングが同じ場合、Subscriber オブジェクト、またはその上位のすべてのコンテナにも関連付けられている必要があります。

このオプションについては、次の点に注意する必要があります。

- 配布準備のできたアプリケーションオブジェクトの［Package Source List］ボックスにマップされたドライブが含まれている場合は、[Keep the Same Source Paths for the Replicated Objects］オプションを有効にする必要があります。マップされたドライブ文字は、有効な UNC パスを完了するために Distributor および Subscriber の両方で解決する必要がある変数のように扱われます。
- 配布準備のできたアプリケーションオブジェクトの［Package Source List］ボックスに Distributor サーバと異なるサーバへのローカルなドライブマッピングが含まれる場合は、アプリケーションファイルを収集も配布もできません。Distribution に含まれるすべてのファイルは Distributor サーバのファイルシステムに含まれている必要があるからです。
- このオプションを有効にすると、チェーンアプリケーションを含む、Distribution のすべてのアプリケーションオブジェクトに影響します。したがって、Distribution に含まれる各アプリケーションオブジェクトのマップされたドライブの全プロパティが、配布準備のできたアプリケーションのソースパスを保持するために配布され、各アプリケーションとチェーンアプリケーションはソースパスのマップされたドライブを持っている必要があります。
- このオプションを選択すると、アプリケーションオブジェクトの［Default Directory Path］のみが使用されます。次のウィザードページの［Application Destination Directory Path］フィールドが無効になっているからです。したがって、パスを変更できません。
- このオプションを選択するか、未選択にしておくと、Distribution のこのオプションに対してその選択が永続的に使用されます。これは、アプリケーションオブジェクトのマップされたドライブを使用したり、使用しなかったりと変更することによる問題の発生を防止するためです。
- チェーンアプリケーションの場合、他のチェーンアプリケーションが依存している最初のアプリケーションのソースパスと同じように、すべてのチェーンアプリケーションのソースパスが処理されます。

その他の問題

- 297 ページの「アプリケーションの依存関係と要件」
- 298 ページの「Distribution のチェーンアプリケーション」
- 298 ページの「ディレクトリパスの拡張文字」
- 299 ページの「ツリー間の Distribution 」
- 299 ページの「Site Distribution オブジェクト」

アプリケーションの依存関係と要件

依存関係と要件は、属性の配布に関して次のように設定できます。

- **依存関係：** チェーンアプリケーションなど、アプリケーションの依存関係は、Distribution の再構築、送信、および抽出時に配布されたアプリケーションオブジェクトで更新されます。

  アプリケーションの依存関係を表示するには：アプリケーションオブジェクトのプロパティで、［Run Options］>［Application Dependencies］をクリックします。

- **システム要件:** アプリケーションを実行するオペレーティングシステムなどのシステム要件は、Distribution の再構築、送信、および抽出時に配布されたアプリケーションオブジェクトで更新されます。

  システム要件を表示するには：アプリケーションオブジェクトのプロパティで、[Availability] > [Distribution Rules] をクリックします。

  例外には、Distribution の再構築、送信、および抽出時に、アプリケーション要件が配布されたアプリケーションオブジェクトで更新されないことがあります。代わりにアプリケーションの依存関係を使用することをお勧めします。

Distribution のチェーンアプリケーション

複数のアプリケーションに同じチェーンアプリケーションが含まれる場合は、アプリケーションのファイルは Distribution に一度だけ含まれます。これによって Distribution のファイルサイズが小さくなります。

たとえば、複数のアイコンを配布し、それぞれがそれ自体のアプリケーションオブジェクトを持ちオフィスソフトウェアスイートを必要とする場合は、そのスイートソフトウェアは Distribution に一度だけ含まれます。

Desktop Application Distribution がチェーンアプリケーションを持つ場合は、Distribution 構成時に [Maintain Associations] オプションを有効にする必要があります。

Distribution のチェーンアプリケーションは、ZENworks for Desktops 4.*x* 以降でのみ使用できます。

チェーンアプリケーションの理解とセットアップの詳細については、『*ZENworks 6.5 Desktop Management 管理ガイド*』の「高度な配布： アプリケーションの依存関係とチェーンの設定」を参照してください。

ディレクトリパスの拡張文字

AOT アプリケーションオブジェクトの .fil ファイルへのパスに拡張文字（など）が含まれる場合、Distributor とその Subscriber の両方に対してコードページ変数を定義する必要があります。

Distributor が Distribution を構築するときに、ファイルシステムからアプリケーションファイルを収集できるようにするために、Distributor にはコードページ変数が必要です。Subscriber が Distribution からファイルシステムにアプリケーションファイルを正常にコピーできるようにするために、Subscriber にもコードページ変数が必要です。つまり、Distributor および Subscriber によって使用されるコードページには、Distribution に含まれるパスで使用される拡張文字が必要です。

コードページ変数を作成するには

1 Distribution で使用される各国文字について、ConsoleOne で使用されるコードページを決定します。

  コードページは、AOT ファイルへのパスに拡張文字を含む、配布準備のできたアプリケーションオブジェクトの作成に使用されるワークステーションから受け取る必要があります。

  ZENworks 6.5 Companion 2 CD の ¥codepageutility ディレクトリに収録されている encoding.cmd ユーティリティを使用して、必要なコードページを決定できます。このユーティリティの使用方法の詳細については、¥codepageutility ディレクトリに収録されている readme.doc ファイルを参照してください。

2 ConsoleOne で SLP のプロパティパッケージを作成して、プロパティにアクセスします。

3 Tiered Electronic Distribution ポリシーをクリックして有効にし、[Properties] をクリックします。

4 ポリシーに変数 CODE_PAGE を追加します。

5 変数の値として、目的のコードページを入力します。

たとえば、Cp1252 などです。

コードページの値では、大文字と小文字が区別されます。ト

6 [OK] をクリックしてポリシーを保存します。

7 ポリシーパッケージを Distributor オブジェクトのコンテナに関連付けます。

8 Subscriber がコードページにアクセスできるようにするには、次のいずれかの操作を行います。

- ポリシーパッケージを、Distribution を受信する Subscriber オブジェクトのコンテナに関連付けます。

  これにより、Subscriber で変数を使用できるようになり、コードページにアクセスできるようになります。

- Subscriber オブジェクトのプロパティごとに、同じコードページ変数を定義します（ステップ 4 およびステップ 5 の場合と同様）。

  これにより、Subscriber がコードページにアクセスできるようになります。

9 Distribution がすでに作成されている場合は、再構築します。

ツリー間の Distribution

Desktop Application Distribution を他のツリーに送信できます。ただし、ZENworks 6.5 以上には新しいスキーマ拡張が使用されているため、ZENworks for Servers 3.0.2 Subscriber に ZENworks 6.5 または 6.5 SP1 Distribution を送信することはできません。

Site Distribution オブジェクト

ZENworks 6.5 Server Management は Site Distribution オブジェクトを使用しません。ZENworks の以前のバージョンでは、この Distribution タイプと共に Site Distribution オブジェクトを使用していました。

要件

Tiered Electronic Distribution を使用して Desktop Application Distribution を作成および送信するには、次の要件を満たしている必要があります。

- ❑ Desktop Application Distribution は、NetWare サーバおよび Windows サーバにのみ送信できます。この Distribution タイプは、Solaris サーバではサポートされていません。

- ❑ Novell Application ManagementをZENworks 6.5 Server Managementと共に使用するには、ZENworks for Desktops 4.01またはZENworks 6.5 Desktop Managementがインストールされている必要があります。Desktop Application Distributionのチェーンアプリケーションは、ZENworks for Desktops 4.01以降でのみサポートされます。
- ❑ Desktop ManagementとServer Managementは、それぞれのスキーマ拡張も含めて、両方とも同じツリーにインストールされている必要があります。
- ❑ 配布準備のできたアプリケーションオブジェクトをDesktop Application Distributionで機能させるには、Server ManagementとDesktop Managementの両方のスナップインがConsoleOneにインストールされている必要があります。
- ❑ 配布準備のできたアプリケーションオブジェクトのすべての関連付けがソースのルートコンテキストまたはその下位で行われていることを確認します。

  重要： 関連付けが1つでもソースのルートコンテキストの外部で行われている場合は、Distributorは Distributionの構築に失敗します。
- ❑ WindowsおよびLinuxサーバの場合、Distributionのファイルの抽出先となる共有場所を確立しておく必要があります。この場所から、すべてのユーザはDistributionファイルにアクセスすることができます。
- ❑ ソースパスがDistributorサーバのファイルシステム上にあるアプリケーションファイルを指定する必要があります。Distributorは他のサーバのファイルシステムからファイルを収集できないからです。

  [Package Source List]ボックスにローカルドライブマッピングが含まれている場合、アプリケーションファイルは収集または配布されません。

  [Package Source List]ボックスにマップされたドライブが含まれている場合、[Keep the Same Source Paths for Replicated Objects]が選択されている必要があります。ドライブ文字は、有効なUNCパスを完了するためにDistributorおよびSubscriberの両方で解決する必要がある変数のように扱われます。

  ポリシーを使用してDistributorの変数を定義します。Subscriberでは、Subscriberオブジェクトの変数リスト、またはSubscriberオブジェクトが存在するコンテナに関連したポリシーを使用できます。
- ❑ Subscriberオブジェクトには、Working Context属性が定義されている必要があります。これは、Subscriberが受信するDesktop Application Distributionに関連したオブジェクトを作成するeDirectoryコンテキストです。

  負荷分散や障害対策を使用する複数のSubscriberは、同じ作業コンテキストを使用できます。
- ❑ AOTアプリケーションオブジェクトの.filファイルへのパスに拡張文字(など)が含まれる場合、DistributorとSubscriberの両方にコードページ変数を定義する必要があります。詳細については、298 ページの「ディレクトリパスの拡張文字」を参照してください。

Desktop Application Distributionの作成

- 301 ページの「Desktop Application Distributionウィザードの理解」
- 301 ページの「Distributionの作成」

Desktop Application Distribution ウィザードの理解

ZENworks では、Tiered Electronic Distribution を使用して、アプリケーションオブジェクトを同じツリーの別の場所または別のツリーに配布できます。Desktop Application Distribution では、アプリケーションに関連付けられたオリジナルのファイルをサーバの適切な場所にコピーします。この場所から、配布されたアプリケーションオブジェクトに関連付けられたユーザグループとワークステーショングループにローカルにサービスを提供できます。

アプリケーションを配布するには、Server Management Desktop Application Distribution ウィザードを使用して Distribution を設定します。これには次のような作業が含まれます。

- 配布先のツリーコンテキストの確認
- ユーザ / ワークステーショングループまたはコンテナとアプリケーションとの関連付けを保持するかどうかの確認
- 負荷分散と障害対策を自動化するかどうかの確認
- Distribution の再構築をトリガする方法の確認
- アプリケーションの選択
- ファイルコピーパスの確認

ウィザードを使用して Desktop Application Distribution を作成するには、301 ページの「Distribution の作成」に進みます。

Distribution の作成

重要： このウィザードを ConsoleOne で実行する代わりに、この手順を iManager で実行することもできます。詳細については、iManager のコンテキストに応じたヘルプを参照してください。

1 299 ページの「要件」に記載されているすべての要件を満たします。必要に応じて、コードページ変数も作成します。

2 ConsoleOne で、Distribution オブジェクトを保存するコンテナを右クリックし、[New]、[Object] の順にクリックし、[TED Distribution] を選択して、[OK] をクリックします。

3 Distribution の名前を指定します。

重要： Distribution 名にピリオド (.) は使用できません。代わりに、単語の区切り文字としてはダッシュ (-) またはアンダースコア (_) を使用します。Distribution 名にピリオドを使用した場合、Distribution は送信されず、Distributor は終了後も再ロードされません。

4 Distributor に Distribution の所有権を与えるには、Distributor オブジェクトを参照して選択し、[Define Additional Properties] をクリックし、[OK] をクリックします。

Distribution オブジェクトのプロパティが表示されます。

5 [General] タブを選択し、[Settings] フィールドに入力します。

[Active]： 必須。Distribution を Subscriber で利用できるようにするには、アクティブにする必要があります。

[Use Digests]： ダイジェストは、送信中に Distribution が改ざんされていないことを確認するために、Distributor と Subscriber によって使用されます。このダイジェストは、Subscriber が照合する MD5 チェックサムを提供します。

ダイジェストは、Distribution のパッケージの破損も検出します。破損があると、Subscriber は Distribution の distfile.ted ファイルの名前を distfile.corrupt に変更し、次回に Channel のスケジュールが開始されたときに Distribution を再構築して送信します。

[Encrypt]： セキュリティで保護されていない接続を介して送信する場合に、Distribution を暗号化できます。暗号化によって、同一ファイアウォール内にない Distributor と Subscriber の間で送信される Distribution のセキュリティが向上します。[Strong] または [Weak] のいずれかの暗号化を選択します。

暗号化を実行する各サーバに NICI 2.6.4 以降をインストールしている必要があります（51 ページの「NICI 2.6.4 のインストール」を参照）。旧バージョンの NICI とバージョン 2.6.4 以降は互換性がありません。

[Maximum Revisions]： この数値は、Distributor と Subscriber の作業ディレクトリに特定の Distribution のバージョンをいくつまで保存できるかを指定することによって、ディスク容量の使用状況を制御するのに役立ちます。デフォルトは 10 です。データが頻繁に変更され、変更が最小限である（デルタファイルが小さい）場合は、この数値を大きくします。データが頻繁に変更されない場合や、大部分のデータが変更される（デルタファイルが大きい）場合は、この数値を小さくします。[1] を選択すると、[Delete Previous Revision] フィールドが選択されます。

リビジョンの最大数に近づくと、SMTP 通知が設定されている場合、SMTP 電子メール通知が送信されます。SMTP 電子メール通知の設定については、212 ページの「SMTP Host」を参照してください。

[Delete Previous Revision Before Receiving Next]： このオプションは、[Maximum Revisions] フィールドで [1] を選択した場合に、利用できます。Distribution のサイズが大きく、Subscriber サーバ上の利用可能なディスク容量が犠牲になる場合は、このオプションをオンにして、以前のバージョンを削除してから次のバージョンを受信することによって、ディスク容量を節約できます。このチェックボックスをオフにした場合、以前のバージョンが削除される前に、新しいバージョン全体が受信されます。いずれの場合も、Distribution を受信した後、Subscriber の作業ディレクトリに保存できる Distribution のバージョンは 1 つだけです。

[Priority]： Distribution に優先度を指定して、他の Distribution との関係で Distribution をどのように送信するかを指定できます。優先度が [High] の場合、その Distribution は、優先度が [Medium] や [Low] の Distribution よりも先に送信されます。

Distributor: この Distribution を構築および送信する Distributor オブジェクトの DN を表示します。Distributor は、Distribution オブジェクトの作成時に選択しています。

説明： Distribution に関する役に立つ詳細情報を入力します。たとえば、デスクトップアプリケーションの名前、含まれているファイルやディレクトリ、対象になるユーザグループなどです。

6 [General] > [Restrictions] の順にクリックします。

Distribution 自体のプラットフォームを制限するかどうかを選択できます。これは配布されたアプリケーションオブジェクトの制限ではありません。

[No Restrictions]： デフォルトではこのオプションが選択されています。プラットフォームの制限を指定するには、このオプションをクリックして無効にした後、この Distribution を受信するプラットフォームに対応するチェックボックスをオンにします。

チェックボックスがオンになっていないプラットフォームでは、Distribution を受信できません。つまり、[No Restrictions] オプションを無効にし、プラットフォームを選択しないことによって、そのプラットフォームへの送信を制限します。

使用できるオプションは次のとおりです。

[No Restrictions]
[NetWare All]
[NetWare 4.*x*]（以前のバージョンの ZfS でサポートされていたプラットフォーム）
[NetWare 5.0]（以前のバージョンの ZfS でサポートされていたプラットフォーム）
[NetWare 5.1]
[NetWare 5.*x*]（以前のバージョンの ZfS でサポートされていたプラットフォーム）
[NetWare 6.*x*]
[Windows Server]

[No Restrictions] は、Distribution をすべてのプラットフォームに送信できるという意味です。

[NetWare All] を選択した場合、個々の NetWare プラットフォームを選択する必要はありません。

7 [Type] タブを選択し、[Select Type] ドロップダウンボックスで [Desktop Application] を選択して、[Setup] をクリックします。

Desktop Application Distribution ウィザードが起動されます。iManager では、このウィザードの代わりに独自のインタフェースが使用されます。

[Modify] をクリックして [Desktop Application Agent] プロパティページからこのウィザードを起動することもできます。

7a 導入情報を読んだ後、[Next] をクリックします。

7b フィールドに入力し、[Next] をクリックします。

[Maintain Source Tree Structure]： 配布されたアプリケーションオブジェクトを配置するために、ソースツリーの構造を配布先（ターゲット Subscriber の作業コンテキスト）に複製します。チェーンアプリケーションを選択している場合は、このオプションを選択する必要があります。

詳細については、292 ページの「ソースパスの保持」を参照してください。

[Source Root Context]： 配布する配布準備のできたアプリケーションオブジェクトのルートコンテナとして使用されるコンテナを選択します。このルートコンテナとその従属コンテナからのみ配布準備のできたアプリケーションオブジェクトを選択してください。

[Maintain Associations]： ターゲットの場所に存在しない場合に、関連付けられたグループやコンテナを配布します。ただし、複製元のグループやコンテナに含まれるユーザやワークステーションは配布されません。

詳細については、289 ページの「オブジェクト配布時の関連付けの保持」を参照してください。

Distribution にチェーンアプリケーションがある場合は、このオプションを有効にする必要があります。詳細については、298 ページの「Distribution のチェーンアプリケーション」を参照してください。

重要： 以前に保持される関連ユーザ / ワークステーショングループまたはコンテナに設定した権限は配布されませんが、配布されたグループまたはコンテナでユーザがアプリケーションを使用するのに必要な最小限度に設定されます。

[Always Replicate Association Flags]： 配布準備のできたアプリケーションオブジェクトに関連付けられた各グループやコンテナに対して、起動設定フラグを各配布されたアプリケーションに複製します。

[Load Balance and Fault Tolerance Support]： 自動化された負荷分散または障害対策を使用するか、またはどちらも使用しないかを選択します。

- **[Load Balance]：** サーバの負荷を Desktop Application Distribution 用に使用されるサーバに自動的に分散させます。障害対策の機能（冗長）は負荷分散によって自動的に実行されます。
- **[Fault Tolerance]：** Desktop Application Distribution 用に使用されるサーバが、停止した別のサーバの配布処理を引き受けることができます。[Fault Tolerance] は負荷分散機能を提供しません。
- **[None]：** いずれのオプションも適用されません。個別にサポートする場合は、各配布されたアプリケーションオブジェクトの負荷分散や障害対策を個別に設定する必要があります。

これら 2 つを機能をさせるには

- Distribution を受信する複数の Subscriber が同じ作業コンテキストを使用している必要があります。
- アプリケーションオブジェクトの [Fault Tolerance] > [Fault Tolerance] のプロパティページまたは [Fault Tolerance] > [Load Balancing] のプロパティページで [User Source List] ボタンを選択している必要があります。

選択したオプションに応じて、この作業コンテキストを共有するすべてのサーバ上のファイルの場所に [Load Balancing] または [Fault Tolerance] のページが入力されます。

詳細については、285 ページの「Server Management の配布されたアプリケーション」を参照してください。

[Rebuild Only If Any Application Version Number Changes]： 構築スケジュールに基づいて Distribution の再構築を制御できます。配布できるようになるまで、配布準備の整ったアプリケーションオブジェクトの変更を保持するには、このチェックボックスを選択します。

このチェックボックスのステータスに関係なく、アプリケーションが Distribution に追加されるか Distribution から削除されると、Distribution がその構築スケジュールに基づいて再構築されます。

詳細については、308 ページの「再構築のトリガ」を参照してください。

7c [Add] をクリックし、配布準備のできたアプリケーションオブジェクトを参照して選択します。

ウィザードの前のページで設定したルートディレクトリよりも上の階層を参照しないでください。特に [Maintain Source Tree Structure] オプションを選択している場合には注意してください。

重要： Desktop Application のソースファイルは Distributor サーバのファイルシステムに存在している必要があります。Distribution は、別のサーバのファイルシステムから収集することはできません。

7d マップされたドライブの機能を配布されたアプリケーションで使用するときに、配布準備のできたアプリケーションオブジェクトのソースパスを保持する場合、[Keep the Same Source Paths for the Replicated Objects] オプションを選択します。

詳細については、292 ページの「ソースパスの保持」を参照してください。

7e 配布先ボリュームまたは共有フォルダを指定します。

配布されるアプリケーションファイルは、ウィザードの前のページで選択した配布準備のできたアプリケーションオブジェクトに関連付けられているファイルです。

代わりに変数を指定することもできます。変数を使用する場合、その変数は、配布先 Subscriber サーバのプロパティで、ターゲットサーバのボリュームまたは共有フォルダを指すように定義されている必要があります。

このボリューム (NetWare) または共有フォルダ (Windows および Linux) は、アプリケーションファイルがコピーされる従属ディレクトリを配置するためのルートになります。

7f アプリケーションのデフォルトパスだけを使用するには、Application の [Default Directory Path] をクリックします。デフォルトパスは、ステップ 7e で指定したルートから始まるように配置されます。

または

ユーザ定義のディレクトリパスをアプリケーションのファイルに提供する場合は、[User-Defined Directory Path] をクリックし、パス情報を指定します。

指定するパスは次のように使用されます。

- ボリュームまたは共有フォルダ名は変更されません (ステップ 7e で指定したとおりです)。
- パス情報は、ボリュームまたは共有フォルダ名の後に挿入されます。
- アプリケーションのデフォルトパスの一部がユーザのパス情報に追加されます。追加されるのは、デフォルトパスの、アプリケーションのファイルのすぐ上の親ディレクトリから始まる部分です。親ディレクトリよりも上の階層にあったデフォルトパス情報は、ユーザのパスエントリに置き換えられます。

最終的にカスタマイズされたディレクトリパスは、ボリュームまたは共有フォルダで始まり、次にユーザ定義のパス情報が続き、最後はアプリケーションのすぐ上の親ディレクトリで終わります。たとえば、アプリケーションの実行可能ファイル (application.exe) のデフォルトパスが次のようになっているとします。

```
\application_root_directory\application_subdirectory
```

ここで、ユーザ定義のパスとして「mypath」と入力すると、実行可能ファイルの新しいフルパスは次のようになります。

```
c:\mypath\application_subdirectory\application.exe
```

共有フォルダとして「C:」、ユーザ定義パスとして「¥mypath」と入力しました。¥application_root_directory は ¥mypath に置き換えられています。¥application_subdirectory は application.exe のすぐ上の親ディレクトリです。

7g［Next］をクリックして続行します。

［Summary］ページが表示されます。

7h 変更する場合は、［Back］をクリックします。

7i Distribution オブジェクトの設定が終了したら、［Finish］をクリックしてウィザードを終了します。

Distribution オブジェクトの［Type］タブで［Modify］をクリックすることによって、いつでも Distribution を編集できます。

8 ［Channels］タブを選択し、［Add］をクリックした後、この Distribution の Channel を参照して選択します。

Channel を使用して Subscriber にデータをプッシュする場合は、各 Distribution に最低 1 つの Channel を関連付ける必要があります。Distribution は、選択した Channel を購読しているすべての Subscriber に送信されます。

9 ［Schedule］タブを選択し、［Build schedule］を選択します。

412 ページの「曜日」
413 ページの「間隔（Interval）」
413 ページの「月」
413 ページの「Never」
414 ページの「すぐに実行（Run Immediately）」
414 ページの「Time」
415 ページの「年」

10 ［Apply］をクリックして［Distribution］を作成します。

追加のセキュリティ証明書をコピーするよう求めるメッセージが表示されます。

11 ［Yes］を選択して証明書を解決します。

これによって、セキュリティ証明書が、Distributor から、Channel を購読している Subscriber にコピーされます。

詳細については、317 ページの「証明書の解決」を参照してください。

12 ［OK］をクリックして Distribution オブジェクトを閉じます。

Distributor は、次回 eDirectory を読み込むとき（このスケジュールは Distributor オブジェクトのプロパティで設定される）、新しい Desktop Application Distribution に関するすべての情報（配布の詳細や構築スケジュールなど）を取得します。

Distribution は構築スケジュールに従って構築され、Channel オブジェクトで設定されているスケジュールに従って送信され、Subscriber オブジェクトで設定されているスケジュールに従って抽出されます。

ファイル収集プロセス時に Distributor が例外処理を実行した場合は、その Distribution は構築されません。Distributor はエラーをレポーティングデータベースに記録します。

抽出中に Subscriber が例外処理を実行した場合は、プロセスが完了しません。Distributor はこの情報を Subscriber から受信し、エラーをレポーティングデータベースに記録します。

抽出後、Desktop Management ユーザのオブジェクトが関連付けられたコンテナにあるか、配布されたグループのメンバーである場合は、そのユーザは配布されたデスクトップアプリケーションへのアクセス権を持ちます。

重要： Desktop Application Distribution の場合、同時に複数のアプリケーション（1 つずつまたは複数の Distribution）を配布しているときのディレクトリの同期に対処するために、遅延が組み込まれています。

Subscribers はすべての Desktop Application Distribution を同時に受信できますが、抽出は一度に 1 つずつ行います。1 つの Distribution に複数のアプリケーションがある場合、Subscriber は配布されたアプリケーションオブジェクトを作成し、アプリケーションのファイルを一度に 1 つずつコピーします。組み込まれた遅延は、新規作成されたアプリケーションオブジェクトを円滑にディレクトリの同期化に役立ちます。

組み込まれた遅延によって配布プロセスの時間がどれほど余計にかかるか確認するには、Desktop Application Distribution のアプリケーション個数に 30 秒をかけてください。

一般的に、配布されるアプリケーションに、基本バージョンが 1 つと、デルタバージョンが 2 つなど、複数のバージョンが含まれている場合、それぞれのバージョンについて 30 秒間の遅延が発生します。たとえば、10 個のデスクトップアプリケーションを送信するときに、それぞれ 3 つのバージョンがある場合は、Distribution の抽出が完了するまでに最低でも 15 分かかります。

13 任意の地理的な場所からアプリケーションに自動的にアクセスする Desktop Management ユーザおよびワークステーションの場合は、次のサイトリストをリンクする必要があります。

13a Desktop Application Distribution が配布され、受信する Subscriber サーバによって抽出されるのを待ちます。サイトリストをリンクするには、配布されたアプリケーションオブジェクトが作成され、アプリケーションのファイルがインストールされている必要があるからです。

13b ConsoleOne で、Distribution を構築するために使用した、配布準備のできたアプリケーションオブジェクトを右クリックし、[Properties] をクリックします。

13c [Distributions] をクリックし、[Link Up Site Lists] ボタンをクリックします。

この配布準備のできたアプリケーションオブジェクトから作成されたすべての配布されたアプリケーションオブジェクトは、[Replicated Applications] リストボックスに表示されます。また、配布されたアプリケーションオブジェクトを含むすべての Distribution は、[Distributions Currently In] リストボックスに表示されます。

[Link Up Site List] ボタンの動作は、次のとおりです。

1. 配布準備のできたアプリケーションオブジェクトに対しては、Distribution から作成された各配布されたアプリケーションオブジェクトを検索し、配布準備のできたアプリケーションオブジェクトのプロパティ（[Replicated Applications] リストボックス）にオブジェクトの完全 DN をリストします。
2. 配布された各アプリケーションオブジェクトに対しては、Distribution から作成された他の配布アプリケーションオブジェクトを検索します。配布準備のできたアプリケーションオブジェクトに対しては、配布されたアプリケーションオブジェクトのプロパティ（[Replicated Applications] リストボックス）にオブジェクトの完全 DN をすべてリストします。
3. 配布された各アプリケーションオブジェクトに対して手順 1 と手順 2 を繰り返します。
4. [Replicated Applications] リストボックスに表示される各アプリケーションオブジェクトに対しては、そのオブジェクトに関連付けられている Distribution が各アプリケーションオブジェクトの [Distributions Currently In] リストボックスに表示されます。

したがって、配布準備のできたアプリケーションオブジェクトとすべての配布されたアプリケーションオブジェクトは、その［Replicated Applications］リストボックスに相互に表示され、ユーザは接続しているネットワークの場所に関係なく、同じアプリケーションに対してローカルアクセス権を持つことができます。

13d ［OK］をクリックして、配布準備のできたアプリケーションオブジェクトのプロパティを閉じます。

13e Desktop Application Distribution の構築に使用された配布準備のできたアプリケーションオブジェクトごとにステップ 13b からステップ 13d までを繰り返します。

サイトリストのリンクを実行する必要があるのは、配布準備のできたアプリケーションオブジェクトに対してのみです。

Desktop Application Distribution の再構築

次の節では、再構築のトリガ方法を含む、Desktop Application Distribution の再構築に関するさまざま問題について説明します。

- 308 ページの「すべての属性の更新」
- 308 ページの「再構築のトリガ」

すべての属性の更新

変更された属性だけでなく、配布準備のできたアプリケーションオブジェクトに含まれるすべての属性は、Distribution が再構築、送信、および抽出される場合に配布されたアプリケーションオブジェクトで更新されます。このことは、配布されたアプリケーションオブジェクトのソースパスなどの属性を変更する場合は、配布準備のできたアプリケーションオブジェクトのソースパスデータによってソースパスが上書きされることを意味しています。つまり、すべての配布されたアプリケーションオブジェクトは配布準備のできたアプリケーションオブジェクトと同期しています。これの例外は 287 ページの「配布準備のできたアプリケーションの属性の保持」に記載されています。

再構築された Desktop Application Distribution には、前回 Distribution が構築された後に加えられたすべての変更が含まれます。

再構築のトリガ

Desktop Application Distribution ウィザードの［Rebuild Only If Any Application Number Changes］チェックボックスを選択するかどうかによって Distribution が再構築される時期を指定できます。

- 309 ページの「チェックボックスの選択」
- 309 ページの「チェックボックスの無効」

チェックボックスの選択

この機能は、オブジェクトの配布の準備が整うまで配布準備のできたアプリケーションオブジェクトに変更を保持しておく場合に便利です。

Distribution は、設定されている構築スケジュールに基づいて再構築されます。ただし、これは配布準備のできたアプリケーションオブジェクトまたはその従属アプリケーションの［Version Number］フィールドを手作業で増やし、かつ Distributor が eDirectory を読み込んで［Version Number］フィールドの変更を検出した後だけです。

Distribution に複数のアプリケーションがある場合、アプリケーションの 1 つのバージョン番号が変更されるだけで、すべてのアプリケーションの Distribution 再構築がトリガされます。

［Version Number］フィールドは、アプリケーションオブジェクトのプロパティの［Distribution Options］>［Options］タブにあります。

このチェックボックスのステータスに関係なく、アプリケーションが Distribution に追加されるか Distribution から削除されると、Distribution はその構築スケジュールに基づいて再構築されます。

チェックボックスの無効

このオプションを選択しない場合（デフォルトでは無効に設定）、Distribution は設定されている構築スケジュールに基づいて再構築されます。この場合には、次の 2 つのシナリオを実行できます。

- 309 ページの「オブジェクトの変更」
- 309 ページの「配布されたアプリケーションオブジェクトの削除」

オブジェクトの変更

Distribution オブジェクトまたはそのいずれかの配布準備のできたアプリケーションオブジェクトを変更すると、内部リビジョン番号が自動的に変更され、設定されている構築スケジュールに基いた Distribution の再構築がトリガされます。

変更には、Distribution からのアプリケーションの追加や削除が含まれます。ただし、Distributor サーバのファイルシステムのアプリケーションファイルを更新、追加、または削除するだけの場合は、Desktop Application Distribution オブジェクトの内部リビジョン番号は変更されません。ZENworks のファイル同期機能は、アプリケーションオブジェクトのファイルには適用されません。したがって、再構築はトリガされません。

配布準備のできたアプリケーションオブジェクトに属するファイルを追加、削除、または更新すると、次回に再構築がトリガされたときにその変更が反映されます。

配布されたアプリケーションオブジェクトの削除

配布されたアプリケーションオブジェクトを削除すると、そのオブジェクトが変更されずに配布準備のできたアプリケーションオブジェクトにバックリンクします。したがって、内部リビジョン番号が配布準備のできたアプリケーションオブジェクトの番号に変更され、設定されている構築スケジュールに基づいた Distribution の再構築がトリガされます。

Desktop Application Distribution ファイルのクリーンアップ

Tiered Electronic Distribution は、Desktop Management の配布準備のできたアプリケーションオブジェクトを削除した場合などに Desktop Management ファイルをクリーンアップするようには設計されていません。Desktop Application Distribution が作成した配布されたアプリケーションオブジェクトは、自動的に削除されません。サーバのファイルシステム上でこの eDirectory オブジェクトおよび関連するアプリケーションファイルを手作業で削除する必要があります。

このためには、配布準備のできたアプリケーションオブジェクトを削除する前に、ConsoleOne でアプリケーションオブジェクトを検索してそのファイル名をメモしておきます。これにより、配布準備のできたアプリケーションを削除した後で手作業で簡単にクリーンアップできます。

配布準備のできたアプリケーションオブジェクトとそのファイルを削除した後で配布されたアプリケーションが存在するか確認してから、配布されたバージョンを削除できます。

1 ConsoleOne で、配布準備のできたアプリケーションオブジェクトを選択します。

2 ファイルブラウザで、アプリケーションに関連するファイルを削除します。

3 ConsoleOne で、配布準備のできたアプリケーションオブジェクトの Distribution に関連付けられている Distributor オブジェクトを右クリックします。

4 ドロップダウンメニューから［Refresh Distributor］をクリックした後、［Yes］>［OK］の順にクリックします。

5 配布されたアプリケーションオブジェクトの配布場所を確認します。

そのオブジェクトはまだ存在していても、Distribution には存在しなくなっています。

6 ConsoleOne で、配布されたアプリケーションオブジェクトを削除します。

7 ファイルブラウザで、配布されたアプリケーションに関連するファイルを削除します。

ツリー間での Desktop Application Distribution の送信

Desktop Application Distribution をツリー間で送信できます。ただし、このためには次のような作業を行う必要があります。

1 Distributor のツリーで、Desktop Application Distribution の送信先となる他のツリー内のターゲットサーバを指す External Subscriber オブジェクトを作成します。

これによって、Distributor サーバは、External Subscriber オブジェクトにリストされている IP アドレスを使用して、Distribution をターゲットサーバに直接送信できます。

2 Desktop Application Distribution を受信することになっているターゲットサーバでは、それ自体のツリー内に Subscriber オブジェクトがあり、eDirectory に対して、配布されたアプリケーションオブジェクトを新規作成するための権利をそのツリー内に持っていることを確認します。

この Subscriber は、稼動している Tiered Electronic Distribution システム内にある必要があります。

3 インストール中に設定されていない場合は、Subscriber オブジェクト内でターゲットサーバの作業コンテキストを設定します。

ターゲットサーバの作業コンテキストが設定されていない場合、抽出中に認証が失敗します。

4 Desktop Application Distribution を作成します。300 ページの「Desktop Application Distribution の作成」を参照してください。

Desktop Application Distribution の定義は、ツリー内で送信する場合も、ツリー間で送信する場合も同じ処理です。

5 External Subscriber オブジェクトを、Desktop Application Distribution がリストされている Channel に追加します。

6 証明書をターゲットツリー内の Subscriber に手動でコピーします。

または

マップされたドライブを使用する場合は、プロンプトが表示されたときに参照して正しいパスを指定します。

7 Distribution を送信します。

7 Policy and Distribution Servicesのセキュリティ

Novell® ZENworks® Server Management では、Policy and Distribution Services について、次のようなタイプのセキュリティが用意されています。

- 313 ページの「署名付き証明書とダイジェストを使用した配布のセキュリティ」
- 324 ページの「暗号化を使用した Distribution のセキュリティ」
- 328 ページの「セキュリティ保護されていない接続でのサーバ間通信のセキュリティ」

署名付き証明書とダイジェストを使用した配布のセキュリティ

Tiered Electronic Distribution には、セキュリティを処理するための機能が 2 つあります。

- **証明書（必須）：** セキュリティ証明書は、Distribution が信頼されるソースから送信されたものであるか、改ざんされているかを検証するために、各 Distributor から Distribution を受信するすべての Subscriber に対して発行されます。このセキュリティは、Policy and Distribution Services によって、すべての Distribution について自動的に使用されます。ただし、Policy and Distribution Services で証明書を作成および処理するために操作が必要になる場合もあります。

  Subscriber が最初の Distribution を Distributor から受け付けるには、...¥security ディレクトリ内にその Distributor からの証明書が必要です。最初の Distribution を Distributor から受信すると、証明書はまず .keystore ファイルに保存され、次に ...¥security ディレクトリから削除されます。

  .keystore ファイルは、Subscriber に Distribution を送信する各 Distributor からの署名済み証明書のリポジトリです。つまり、Subscriber にとって Distribution に関する信頼されるソースが蓄積される場所です。

  .keystore ファイルの内容は Novell iManager で表示できます。

  暗号化された Distribution のセキュリティ証明書については、324 ページの「暗号化を使用した Distribution のセキュリティ」を参照してください。

- **ダイジェスト（省略可能）：** Distributionの構築時に、各Distributionについてダイジェストを作成できます。このダイジェストは、Distributor から送信された後の Distribution が改ざんされているかどうかを調べるために、Subscriber が照合する MD5 チェックサムを提供します。

  ダイジェストは、Distribution のパッケージの破損も検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。

以下の節では、証明書とダイジェストの概要、作成および使用方法について詳しく説明します。

- 314 ページの「ダイジェストについて」
- 314 ページの「Policy and Distribution Services での証明書の使用について」
- 315 ページの「証明書に関する重要な点」
- 317 ページの「ConsoleOne ユーザの権利と証明書のコピー」
- 317 ページの「証明書ファイルの場所」
- 317 ページの「証明書の解決」
- 318 ページの「無効な証明書の処理」
- 322 ページの「証明書とプライベートキーのディレクトリ」
- 322 ページの「暗号化されていない Distribution 用のセキュリティ証明書の作成」
- 323 ページの「暗号化されていない Distribution 用の証明書の手動によるコピー」

ダイジェストについて

ダイジェストに関して重要な点は次のとおりです。

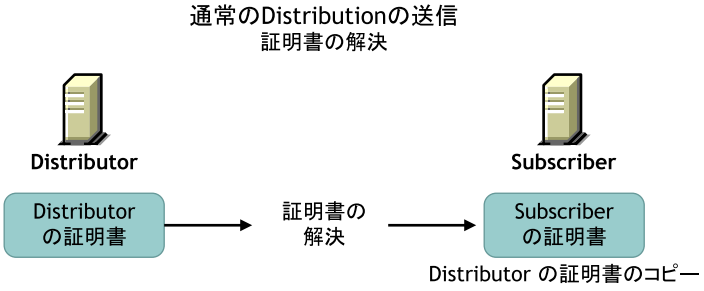
- ダイジェストは、Distribution の構築時に、各 Distribution について作成できます。ダイジェストは、Distribution が Distributor から送信された後、改ざんされているかどうかを調べるために、Subscriber によって使用されます。
- ダイジェストは Distribution のパッケージの破損を検出します。破損が検出された場合、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更して、次回に Channel のスケジュールが開始されたときに、Distribution を再構築して送信します。
- [Digest] オプションは、すべてのタイプの Distribution について使用できます。[Digest] チェックボックスは、Distribution オブジェクトのプロパティの [General] タブに表示されます。
- ダイジェストによって、構築時間が長くなります。ダイジェストを使用した場合の構築時間に影響する要因としては、CPU およびハードドライブの速度、RAM の容量、サーバの負荷などがあります。

Policy and Distribution Services での証明書の使用について

証明書は Policy and Distribution Services によって使用されるセキュリティメカニズムであり、Subscriber が受信した Distribution が、その Distribution を所有する Distributor が実際に送信したものであることを保証します。Subscriber には環境設定情報も送信できるので、環境設定情報が既知の Distributor から送信されたものであり、データが変更されていないことを保証します。

すべての Subscriber は、Distribution の送信元である各 Distributor から有効なセキュリティ証明書を受信する必要があります。一致する証明書がない場合、Subscriber は Distributor から Distribution を受信できません。

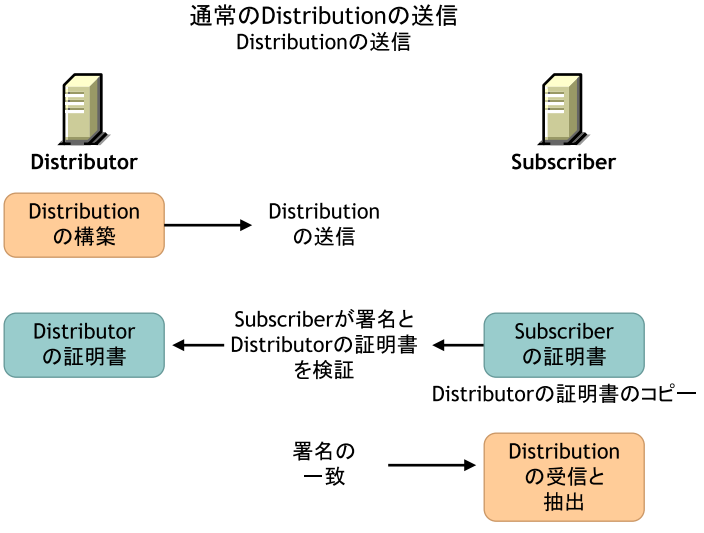
次の図は、Distribution で証明書を使用する処理を示しています。



Distribution が送信される前に、証明書を解決する必要があります。これによって、Subscriber が受信した Distribution が、Distribution を所有する Distributor によって実際に送信されたものであることが確認されます。

証明書の解決については、317 ページの「証明書の解決」を参照してください。

証明書が解決された後、次の図のように、Subscriber は証明書を使用して有効な Distribution を受信していることを確認します。



証明書に関する重要な点

- 証明書は、各 Distributor によって、その Distributor から Distribution を受信するすべての Subscriber に対して発行されます。Subscriber が Distributor から Distribution を受け付けるには、その Distributor からの証明書を受け取っている必要があります。
- セキュリティのために、証明書のキーのペアが Distributor によって作成されます。
- パブリックキーは Distributor サーバのファイルシステムに書き込まれ、証明書は自己署名され、Novell eDirectory™ に保存されます。
- プライベートキーは、Distributor オブジェクトのプロパティに保存され、暗号化のために使用されます。
- Subscriber ソフトウェアは、サーバに証明書をコピーするために、Subscriber サーバ上で実行されている必要はありません。

- Distribution（Distributor が所有）と Subscriber の Channel に対する関連付けによって、どの Subscriber がどの Distributor から証明書を受信するかが決まります。
  - Distributor は、Distributor が Distribution を提供する Channel を購読するすべての Subscriber に証明書を送信します。
  - Subscriber は、購読している Channel に Distribution を持つすべての Distributor に証明書を要求します。
- 証明書は、次のような場合に Distributor から Subscriber に渡すことができます。
  - Subscriber が最初に Channel を購読するときに、[OK] をクリックして変更を適用した場合。
  - Subscriber オブジェクトを右クリックし、[Resolve Certificates] を選択した場合。Subscriber は、Distribution の送信元であるすべての Distributor に証明書を要求します。
  - Distribution が Channel にリストされており、[OK] をクリックして変更を適用した場合。
  - Distributor オブジェクトを右クリックし、[Resolve Certificates] を選択した場合。Distributor は、Distribution の送信先であるすべての Subscriber に証明書を送信します。

    証明書の解決については、317 ページの「証明書の解決」を参照してください。
  - Distribution または Subscriber を Channel に追加した場合。[OK] をクリックすると、[Resolve Certificates?] ダイアログボックスが表示されます。[Yes] をクリックすると、Distribution をその Channel に関連付けているすべての Distributor によって、その Channel を購読しているすべての Subscriber に証明書が送信されます。
  - 手動で証明書ファイルを転送メディア（フロッピーディスクやローカルドライブなど）にコピーし、サーバ上の ¥zenworks¥pds¥ted¥security ディレクトリにコピーします。

  基本的に、Subscriber、Channel、または Distribution との間で関係が変更されたときにはいつでも証明書を渡すことができます。
- Distributor オブジェクトを削除し、同じサーバを指すように再作成した場合、従属 Subscriber 上のすべての証明書は無効になります。Subscriber の ¥security ディレクトリから証明書を削除した後、Distributor は新しい証明書を Subscriber に送信する必要があります。
- ConsoleOne は証明書ファイルを Subscriber サーバにコピーします。したがって、ConsoleOne を実行するワークステーション上のクライアントソフトウェアは、Subscriber サーバのファイルシステムにアクセスできる必要があります。Windows の Subscriber サーバの場合は、ワークステーションで Domain and Workgroup の権利を設定し、証明書のコピーを自動化する必要があります。この設定を行わない場合、1204a エラーが発生します。

ConsoleOne ユーザの権利と証明書のコピー

ConsoleOne® を使用する管理者は、管理者が ConsoleOne で証明書を解決するときに、サーバに証明書をコピーできるように、Subscriber サーバに対して十分な権利を持っている必要があります。これは、ConsoleOne を使用して、特定の Channel から Distribution を受信するように Subscriber オブジェクトを設定する場合、その Channel 内の Distribution を所有している Distributor は、Subscriber のサーバに証明書を送信する必要があるからです。

NetWare® Subscriber の場合は、Subscriber オブジェクトを設定できるので、ConsoleOne ユーザは自動的に十分な権利を持っています。

Windows Subscriber の場合、[Active Directory Users and Computers] を選択するか、[Local Users and Groups] を選択して、Windows で ConsoleOne ユーザの管理者権限を設定する必要があります。

証明書ファイルの場所

証明書は、NetWare および Windows Subscriber サーバでは ¥zenworks¥pds¥ted¥security ディレクトリに保存され、Linux および Solaris サーバでは /var/opt/novell/zenworks/zfs/pds/ted/security ディレクトリに保存されます。

警告： ノ¥security ディレクトリが非パブリックディレクトリであることを確認します。このディレクトリは、管理者以外のユーザが読み込めないようにします。.keystore ファイルはノ¥security¥private ディレクトリにあり、デフォルトでは管理者以外のユーザに対して非表示になっています。

証明書には、通常、Distributor サーバの完全修飾 DNS 名に基づいた名前が付けられます。たとえば、Distributor_Server001.Distributions.ZENworks.Novell.com.cer や Distributor_Server001.Distributions.ZENworks.Novell.com.csr などです。DNS 名が解決できない場合は、サーバの TCP/IP アドレスが .csr ファイルに使用されます。証明書には、155.55.155.55.csr のように、IP アドレスを使用した名前が付けられます。

証明書の解決

重要： ConsoleOne は証明書ファイルを Subscriber サーバにコピーします。したがって、ConsoleOne を実行するワークステーション上のクライアントソフトウェアは、Subscriber サーバのファイルシステムにアクセスできる必要があります。Windows の Subscriber サーバの場合は、ワークステーションで Domain and Workgroup の権利を設定し、証明書のコピーを自動化する必要があります。この設定を行わない場合、1204a エラーが発生します。

ConsoleOne で証明書を解決するためのオプションが自動的に表示された場合は、次の点を考慮して［Yes］または［No］のいずれをクリックするかを判断してください。

- 現在、Distributor がこの Channel に関連付けられた Distribution を持っており、現在 Channel を購読しているすべての Subscriber が以前にこの Distributor から証明書を受信したことがある場合は、［No］を選択します。
- これが Distributor によってこの Channel に追加された最初の Distribution であるか、または Subscriber が新しく Channel に追加された場合は、［Yes］を選択して証明書を解決します。

  これによって、セキュリティ証明書が、Distributor から、Channel を購読している Subscriber にコピーされます。
- サーバが、証明書の解決に使用するワークステーションから（Samba を使用するなどして）ドライブがマッピングされていない Linux または Solaris Subscriber である場合は、323 ページの「暗号化されていない Distribution 用の証明書の手動によるコピー」を参照してください。

通常、次のような追加を行うと、証明書をコピーするよう求めるメッセージが表示されます。

- Channel を Distribution に追加
- Distribution を Channel に追加
- Subscriber を Channel に追加
- Channel を Subscriber に追加

証明書の解決を開始するには

1 ConsoleOne で Distributor オブジェクトを右クリックし、[Resolve Certificates] をクリックします。

2 [Copy Certificates Automatically to Subscribers]オプションが選択されていることを確認した後、[OK] をクリックします。

これによって、新しい証明書が各 Subscriber にコピーされ、Distribution をこの Distributor から受信できるようになります。ただし、ConsoleOne を実行しているワークステーションが、すべての Subscriber サーバにアクセスできる必要があります。証明書をコピーする場所を指定するよう求めるメッセージが表示された場合は、コピー先のサーバにドライブがマッピングされている必要があります。

無効な証明書の処理

Distributor の証明書が無効になっている場合、Subscriber は Distributor から Distribution を受信できません。Subscriber の暗号化証明書が無効になっている場合、Subscriber は暗号化された Distribution を受信できません。暗号化証明書については、324 ページの「暗号化を使用した Distribution のセキュリティ」を参照してください。

Distributor の DNS 名または IP アドレスが変更された場合、Distributor の証明書が無効になる可能性があります。ただし、Distributor が DNS を使用するように設定されている場合（推奨されるアドレス指定方法）、Distributor で IP アドレスを変更しても証明書は無効になりません。また、DNS アドレス指定が使用されている場合、Subscriber の DNS 名や IP アドレスを変更しても、Subscriber は Distribution を受信できます。

ただし、Subscriber の DNS 名や IP アドレスが変更されると、Subscriber の暗号化証明書が無効になる場合があります。この場合、新しい暗号化証明書を作成する必要があります。

DNS によるアドレス指定方法が使用されている場合は DNS 名の変更に、IP アドレスによるアドレス指定方法が使用されている場合は IP アドレスの変更に、以下の項目が適用されます。

- 319 ページの「Distributor の DNS 名または IP アドレスの変更」
- 321 ページの「Subscriber の DNS 名または IP アドレスの変更」

Distributor の DNS 名または IP アドレスの変更

Distributor はそのサーバの DNS 名または IP アドレスによって Subscriber に識別されるので、Distributor サーバ上で使用されている識別子を変更すると、Subscriber は Distributor を Distribution の有効なソースとして認識しなくなります。

Distributor の DNS 名または IP アドレスを変更すると、その Distributor によって作成された証明書は、この Distributor から証明書を受信したすべての Subscriber で無効になります。したがって、Distributor は、この Distributor から Distribution を受信しているすべての Subscriber に新しい証明書を送信する必要があります。

Distributor の証明書を再作成して解決するには、次の操作を順に行います。

1. 319 ページの「Distributor サーバの識別属性の変更」
2. 320 ページの「新しい証明書の作成と送信」

Distributor サーバの識別属性の変更

最初に、Distributor および Subscriber オブジェクトのプロパティの［Other］タブで、［Network Address］属性を変更する必要があります。

サーバが識別情報として［DNS Name］属性を使用している場合は、次の操作を行います。

1 ConsoleOne で Distributor オブジェクトを右クリックし、［Properties］をクリックして［Other］タブを選択します。

2 ［NetWork Address］の左側にある + 記号をクリックします。

3 変更するフィールドの左側にあるアイコンを選択します。

右側に［Browse］ボタンが表示されます。

4 ［Browse］ボタンをクリックします。

5 ［DNS Name］フィールドを変更している場合は、Type 13 と表示されているボックスの上部にあるドロップダウンリストをクリックします。

6 値を［Type 13］から［IP］に変更した後、［IP］を［Type 13］に戻します。

これによって値がリセットされ、新しい DNS 名が認識されます。

7 ボックスの下部の［NetAddress］フィールドの右側にある［Browse］ボタンをクリックします。

8 ボックスの右側にある［Servers DNS Name］を選択し、新しい名前に変更します。

9 ［OK］をクリックして［Other］タブに戻ります。

10 ［OK］をクリックして終了します。

サーバが識別情報として［IP Address］属性を使用している場合は、次の操作を行います。

1 ConsoleOne で Distributor オブジェクトを右クリックし、［Properties］をクリックして［Other］タブを選択します。

2 ［NetWork Address］の左側にある + 記号をクリックします。

3 変更するフィールドの左側にあるアイコンを選択します。

右側に［Browse］ボタンが表示されます。

4 ［Browse］ボタンをクリックします。

ダイアログボックスの下部に IP アドレスが表示されます。

5 IP アドレスを新しいアドレスに変更します。

6 [OK] をクリックして [Other] タブに戻ります。

7 [OK] をクリックして終了します。

320 ページの「新しい証明書の作成と送信」に進みます。

新しい証明書の作成と送信

1 Distributor サーバで、Distributor Agent をシャットダウンします。

[NetWare]： ZENworks Server Management コンソールのプロンプトで、「**exit**」と入力します。

[Windows]： [Services] ダイアログボックスで、Novell ZENworks Service Manager サービスを停止します。

エージェントの起動と停止については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Server Management Services の起動と停止」を参照してください。

2 Distributor サーバの ¥zenworks¥pds¥ted¥security¥private ディレクトリで、.keystore ファイルを削除します。

このファイルには Distributor の証明書が含まれています。

3 Distributor サーバの ¥zenworks¥pds¥ted¥security¥csr ディレクトリで、以前の DNS 名または以前の IP アドレスと一致する名前を持つ .csr ファイルを削除します。

4 Distributor Agent を再開します。

Distributor の新しい証明書および .keystore ファイルが自動的に作成されます。

5 ステップ 1 で選択した Distributor から、Distribution を受信するすべての Subscriber に新しい証明書を送信するには

5a 証明書を解決するには、ConsoleOne で Distributor オブジェクトを右クリックし、[Resolve Certificates] をクリックします。

重要： ConsoleOne は証明書ファイルを Subscriber サーバにコピーします。したがって、ConsoleOne を実行するワークステーション上のクライアントソフトウェアは、Subscriber サーバのファイルシステムにアクセスできる必要があります。Windows の Subscriber サーバの場合は、ワークステーションで Domain and Workgroup の権利を設定し、証明書のコピーを自動化する必要があります。この設定を行わない場合、1204a エラーが発生します。

5b [Copy Certificates Automatically to Subscribers] オプションが選択されていることを確認した後、[OK] をクリックします。

これによって、新しい証明書が各 Subscriber にコピーされ、Distribution をこの Distributor から受信できるようになります。ただし、ConsoleOne を実行しているワークステーションが、すべての Subscriber サーバにアクセスできる必要があります。証明書をコピーする場所を指定するよう求めるメッセージが表示された場合は、コピー先のサーバにドライブがマッピングされている必要があります。

Subscriber の DNS 名または IP アドレスの変更

Distributor は Subscriber のアドレスを、eDirectory 内の Subscriber のオブジェクトから取得するので、Subscriber オブジェクト内でこの情報を更新し、Subscriber が Distribution を受信できるようにする必要があります。

Subscriber の DNS 名または IP アドレスを変更すると、Subscriber 上で格納されているすべての暗号化証明書が無効になります。Subscriber は、暗号化された Distribution を送信する Distributor ごとに 1 つの暗号化証明書を持つことができます。

Subscriber は、DNS 名または IP アドレスが変更された場合でも、暗号化されていない Distribution を受信することはできます。

次の節では、DNS 名と IP アドレスの変更を解決するための手順を説明します。

- 321 ページの「Subscriber サーバの識別属性の変更」
- 322 ページの「新しい証明書の解決」

Subscriber サーバの識別属性の変更

最初に、Distributor および Subscriber オブジェクトのプロパティの［Other］ページで、［Network Address］属性を変更する必要があります。この作業のために、必要に応じて次の操作を行います。

サーバが識別情報として［DNS Name］属性を使用している場合は、次の操作を行います。

1. ConsoleOne で、Subscriber オブジェクトを右クリックし、［Properties］をクリックして［Other］タブを選択します。
2. ［NetWork Address］の左側にある + 記号をクリックします。
3. 変更するフィールドの左側にあるアイコンを選択します。

   右側に［Browse］ボタンが表示されます。
4. ［Browse］ボタンをクリックします。
5. ［DNS Name］フィールドを変更している場合は、Type 13 と表示されているボックスの上部にあるドロップダウンリストをクリックします。
6. 値を［Type 13］から［IP］に変更した後、［IP］を［Type 13］に戻します。

   これによって値がリセットされ、新しい DNS 名が認識されます。
7. ボックスの下部の［NetAddress］フィールドの右側にある［Browse］ボタンをクリックします。
8. ボックスの右側にある［Servers DNS Name］をクリックし、新しい名前に変更します。
9. ［OK］をクリックして［Other］タブに戻ります。
10. ［OK］をクリックして終了します。

サーバが識別情報として［IP Address］属性を使用している場合は、次の操作を行います。

1. ConsoleOne で、Subscriber オブジェクトを右クリックし、［Properties］をクリックして［Other］タブを選択します。
2. ［NetWork Address］の左側にある + 記号をクリックします。

3 変更するフィールドの左側にあるアイコンを選択します。

右側に［Browse］ボタンが表示されます。

4 ［Browse］ボタンをクリックします。

ダイアログボックスの下部に IP アドレスが表示されます。

5 IP アドレスを新しいアドレスに変更します。

6 ［OK］をクリックして［Other］タブに戻ります。

7 ［OK］をクリックして終了します。

新しい証明書の解決

Subscriber の有効な暗号化証明書を作成し直すには、324 ページの「暗号化を使用した Distribution のセキュリティ」の手順に従ってください。

証明書とプライベートキーのディレクトリ

Policy and Distribution Services の証明書とプライベートキーは、次の場所にある .keystore ファイルに保存されます。

- NetWare Distributor サーバ上の Distributor のプライベートキーの場合：

  sys:¥zenworks¥pds¥ted¥security¥private

- Windows Subscriber サーバ上の Distributor のプライベートキーの場合：

  c:¥zenworks¥pds¥ted¥security¥private

- NetWare Subscriber サーバ上の Distributor から受信した証明書の場合：

  sys:¥zenworks¥pds¥ted¥security

  Distribution が送信された後、証明書は .keystore ファイルに移動されます。

暗号化されていない Distribution 用のセキュリティ証明書の作成

Distributor で証明書を作成し、関連付けられた Subscriber にコピーするには

1 Distributor がインストールされているサーバ上で、Distributor Agent が実行されていることを確認します。NetWare サーバでは、zfs.ncf を使用します。Windows サーバでは、Novell ZENworks Service Manager サービスを再起動します。Linux または Solaris サーバでは、**/etc/init.d/novell zfs start** を実行します。

この Java プロセスは、証明書を作成し、eDirectory に書き込みます。

2 次のいずれかの方法で、証明書を各 Subscriber にコピーします。

- Channel および Distribution が設定されている場合は、ConsoleOne で Distributor オブジェクトを右クリックし、［Resolve Certificates］をクリックして［OK］をクリックします。［Copy Certificates Automatically to Subscribers］オプションが選択されていることを確認した後、［OK］をクリックします。これによって新しい証明書が各 Subscriber にコピーされ、Subscriber はこの Distributor から Distribution を受信できるようになります。

  証明書の解決については、317 ページの「証明書の解決」を参照してください。

- 必要に応じて、Subscriber を Channel に関連付けて、Distributor 用の Distribution を作成した後、この Distribution を Channel に関連付けます。[OK] をクリックすると、証明書を解決するかどうかを確認するメッセージが表示されます。[Yes] をクリックすると、すべての Subscriber の証明書が解決されます。証明書は関連付けられたすべての Subscriber にコピーされます。Subscriber の Java プロセスは Subscriber サーバ上で実行されている必要はありません。このサーバが稼動していることだけが必要です。
- Distributor の証明書を各 Subscriber サーバの *installation_path*¥zenworks¥pds¥ted¥security ディレクトリ (Linux または Solaris では、/var/opt/novell/zenworks/zfs/pds/ted/security) に手動でコピーします。この方法は、Linux または Solaris サーバにドライブがマッピングされていない場合に、証明書を解決するために使用しているワークステーションに対して必要です。
- Subscriber オブジェクトを右クリックし、[Resolve Certificates] をクリックします。各 Subscriber オブジェクトについてこの手順を繰り返します。このオプションを利用できるのは、セキュリティ証明書をコピーするかどうかを確認するメッセージが表示されたときに [No] を選択した場合だけです。

複数の Subscriber が 1 つの Distributor から Distribution を受信する場合は、最初の 2 つの選択肢が最も容易です。

3 各 Distributor はそれぞれセキュリティ証明書を作成するので、ツリー内の各 Distributor オブジェクトについて、ステップ 1 とステップ 2 を繰り返します。

暗号化されていない Distribution 用の証明書の手動によるコピー

ConsoleOne を使用して証明書を Subscriber に手動でコピーするには

1 Distributor、Subscriber、または External Subscriber オブジェクトを右クリックし、[Resolve Certificates] をクリックします。

または

[File] をクリックし、[Resolve Certificates] をクリックします。

2 [Save Certificates to Disk] オプションを選択します。

3 証明書ファイルのコピー先のパスを指定し、[OK] をクリックします。

このパスにコピーされる証明書ファイルには、次の構文を使用して名前が付けられます。

DNS_Name.cer

4 *DNS_name*.cer ファイルを、指定したパスから Subscriber サーバの ¥zenworks¥pds¥ted¥security ディレクトリ (Linux または Solaris では、/var/opt/novell/zenworks/zfs/pds/ted/security) にコピーします。

暗号化を使用した Distribution のセキュリティ

Policy and Distribution Services には、Distribution をセキュリティで保護されたネットワークの外部に送信するときに、その内容への承認されていないアクセスを防止するために、Distribution を暗号化するオプションが用意されています。通常、セキュリティで保護されているネットワーク内で送信される Distribution を暗号化する必要はありません。

Distribution の暗号化は 2 段階の処理です。

1. ConsoleOne で Distribution のプロパティの［Encrypt］チェックボックスをオンにして、暗号化のレベル（強または弱）を選択します。
2. 暗号化セキュリティ証明書ファイルを手動で作成し、Distributor サーバと Subscriber サーバの間でコピーします。

   重要： セキュリティのために、フロッピーディスクなどの物理メディアを使用して、ネットワークサーバ間で証明書を転送します。

その後、Distribution は暗号化された Distribution として送信されます。

Distribution の暗号化については、次の節を参照してください。

- 324 ページの「暗号化証明書の作成とコピー」
- 327 ページの「暗号化された Distribution の送信」
- 327 ページの「暗号化された Distribution の抽出」

暗号化証明書の作成とコピー

RSA PKI には、暗号化された Distribution で使用されるセキュリティプロセスが用意されています。

暗号化証明書は証明書署名要求（.csr）ファイルから作成されます。各 Subscriber サーバには、特定の Distributor 用の暗号化証明書を作成するためのテンプレートとして使用できる .csr ファイルが含まれています。

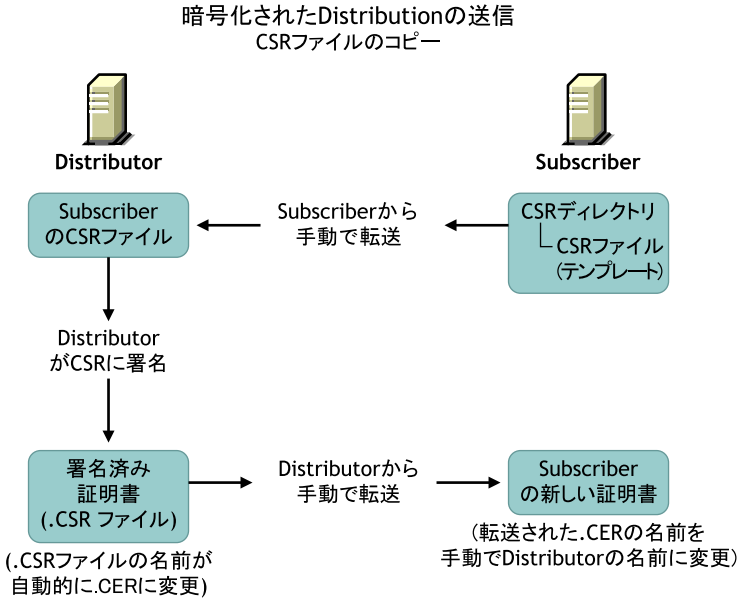
暗号化証明書（.cer）は、暗号化された Distribution の安全な送信を保証するために Subscriber によって使用されます。.cer ファイルの受け渡しをネットワーク経由で行うと、Distribution の暗号化キーが漏洩する可能性があります。したがって、証明書ファイルに含まれている暗号化キーを保護するには、暗号化セキュリティ証明書を手動でコピーする必要があります。

重要： ファイルブラウザは伝送ケーブルを使用し、漏洩の可能性があるので、ファイルブラウザを使用して証明書を手動でコピーしないでください。代わりに、フロッピーディスクなどの外部メディアに証明書をコピーし、それを物理的に Distributor サーバから Subscriber サーバに運びます。

Subscriber で暗号化証明書を使用するには、まず証明書を解決し、暗号化されていない Distributor を各 Subscriber に送信する必要があります。

証明書の解決については、317 ページの「証明書の解決」を参照してください。

次の図は、暗号化証明書を手動でコピーする処理を示しています。



Distributor は .csr に署名して暗号化 .cer ファイルを作成します。このファイルを手動で Distributor から Subscriber にコピーして、Subscriber サーバ上の現在の暗号化されていない .cer ファイルを置き換えます。

Distribution を抽出するには、暗号化証明書が必要です。Subscriber が、Distribution の Channel を購読している Subscriber に暗号化された Distribution を渡す親 Subscriber としてのみ機能している場合は、親 Subscriber サーバに暗号化証明書は必要ありません。

暗号化された Distribution の証明書を作成するには

1 暗号化する Distribution を指定します。

2 この Distribution を所有している Distributor を指定します。

3 暗号化された Distribution を受信する Subscriber を指定します。

4 選択した Distributor の証明書を選択した Subscriber に解決して、暗号化されていない Distribution を Distributor から Subscriber に送信します。

証明書の解決については、317 ページの「証明書の解決」を参照してください。

5 この Distributor および Subscriber のファイルシステムにアクセスします。

6 各 Subscriber の次のディレクトリにあるすべての .csr 証明書ファイルを、Distributor の同じパスにコピーします。

¥zenworks¥pds¥ted¥security¥csr

このパスは、ZENworks Server Management のインストールに使用した場所から始まります。

証明書署名要求 (.csr) を使用して暗号化証明書ファイルが作成されます。

7 ConsoleOne で、Distributor オブジェクトを右クリックし、[Sign CSR Files] をクリックし、署名する .csr ファイルを選択して [Sign] をクリックします。[Success] ダイアログボックスの [OK] をクリックし、[Close] をクリックします。

複数の .csr ファイルを選択して、同時に署名できます。

これによって、Subscriber からコピーした .csr ファイルと同じ Distributor のディレクトリに、証明書 (.cer) ファイルが作成されます。.csr ファイルごとに .cer ファイルが 1 つ作成されます。

iManager を使用してこの手順を実行することもできます。

7a [Remote Web Console] を選択します。

7b Distributor の IP アドレスを選択または指定します。

7c [Available Services] ドロップダウンボックスで、[Tiered Electronic Distribution] を選択します。

7d [Security] タブをクリックし、[Sign CSR] リンクをクリックします。

8 各ターゲット Subscriber について、次の操作を行います。

8a Subscriber サーバの対応する .cer ファイルを、Distributor のファイルシステム上の次の場所

¥zenworks¥pds¥ted¥security¥csr

から、Subscriber のサーバのファイルシステム上の次のパスにコピーします。

¥zenworks¥pds¥ted¥security

各 .cer ファイルには、Subscriber サーバの名前が含まれています。

8b Subscriber サーバにコピーした .cer ファイルの名前を、Subscriber の DNS 名ではなく、Distributor の DNS 名を使用するように変更します。

9 暗号化された Distribution を送信します。

警告： 次のような状況では、作成した暗号化証明書を上書きして使用できます。

1. 暗号化された Distribution に関連する Channel、Subscriber、または Distribution を変更します。
2. これによって、証明書をコピーするかどうかを確認するメッセージが表示されます。
3. [Yes] を選択すると、暗号化された Distribution が送信され、Subscriber によって受信される前に、

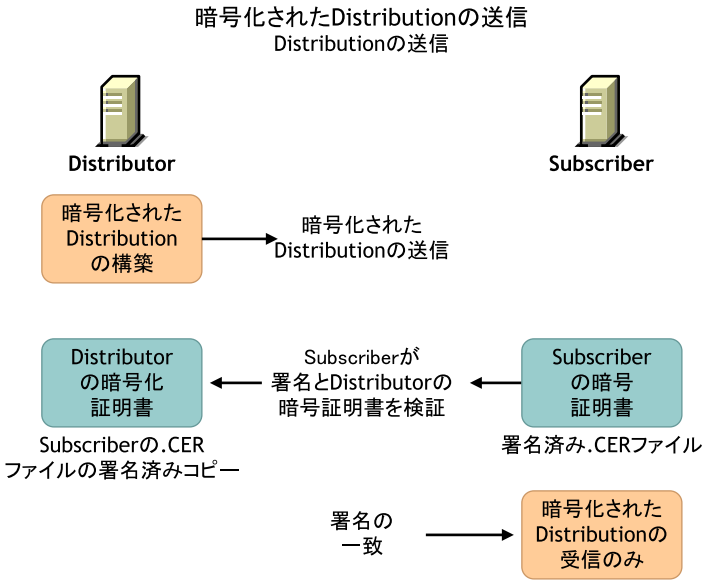
   a. 暗号化 .cer ファイルは各 Subscriber 上で暗号化されていない .cer ファイルによって上書きされます。

   b. Subscriber は Distribution を受信したときに暗号化を解除できません。これは、.cer ファイルが暗号化キーを含まない .cer ファイルによって上書きされたからです。

暗号化された Distribution が各 Subscriber に送信されると、暗号化 .cer ファイルが Subscriber サーバのファイルシステム上の .keystore ファイルに移動されるので、上書きできません。これ以降は、このような状況で [Yes] を選択して証明書をコピーできます。

暗号化された Distribution の送信

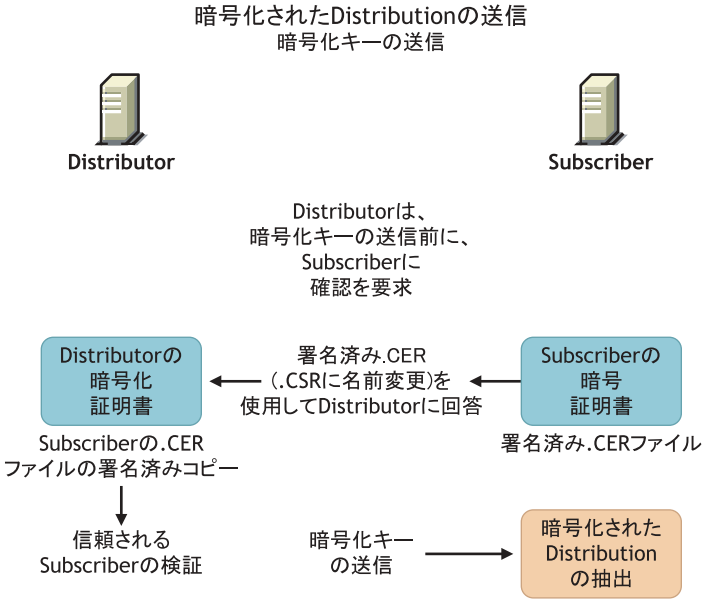
次の図は、Subscriber サーバ上で暗号化証明書を設定した後の暗号化された Distribution の送信処理を示しています。



暗号化キーを受信する必要があるのは、Distribution を抽出する Subscriber だけです。したがって、親 Subscriber や Distributor のルーティング階層内の Subscriber は、Distribution を抽出しない場合は暗号化キーを受信する必要はありません。

暗号化された Distribution の抽出

暗号化された Distribution を Subscriber サーバ上で抽出するには、Subscriber が暗号化キーを受信している必要があります。次の図は、キーの送信の処理を示しています。



各 Distribution について、それぞれ暗号化キーが送信されます。

セキュリティ保護されていない接続でのサーバ間通信のセキュリティ

Policy and Distribution Services では、通常のサーバ間通信に XMLRPC (Extensible Markup Language Remote Procedure Call) を使用します。XMLRPC は、オプションで、セキュリティ保護されていない接続でのサーバ間通信に対してセキュリティを提供します。Policy and Distribution Services では、セキュリティ保護されていない接続でのサーバ間の通信や、セキュリティ保護されていない接続での管理ワークステーションとサーバの間の通信に、このセキュリティを使用します。たとえば、ファイアウォール、イントラネット、NAT 構成などです。

このサーバ間通信のセキュリティによって、セキュリティで保護されていない接続を介して受信したデータが信頼されるソースから送信されたものであり、途中で改ざんされておらず、受信したデータは他のコンピュータでも信頼できることが保証されます。これは、署名付きのセキュリティ証明書とデジタル署名を使用することによって実現されます。

このセキュリティでは特定のテキストファイルを編集する必要があり、Server Management ウィザードを使用してインストールされます。

サーバ間通信のセキュリティが必要になるのは、次のような場合です。

- **ConsoleOne の管理：** ワークステーションを使用して、セキュリティで保護されていない接続を介して Distributor サーバを管理する場合。
- **パラメータ：** SET Parameterポリシーや SETパラメータのソフトウェアパッケージを作成する場合、ターゲットサーバの SET パラメータ情報を提供するためにサーバ間通信が行われます。この通信は、セキュリティで保護されていない接続を介する場合があります。
- **Server Down Policy:** このポリシーを使用してサーバを停止する場合、停止するサーバとそのサーバが再び稼動するのを監視する別のサーバとの間の通信がセキュリティで保護されていない接続を介することがあります。

XMLRPC セキュリティのインストール手順については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「セキュリティ保護されていない接続のための追加セキュリティのインストール」を参照してください。

XMLRPC を使用したサーバ間通信のセキュリティについては、次の節を参照してください。

- 329 ページの「この節で使用される用語」
- 329 ページの「セキュリティ証明書」
- 329 ページの「SSL の使用」
- 330 ページの「パスワードファイルの形式」

この節で使用される用語

サーバ間通信のセキュリティに関する説明では、次の用語および頭字語を使用します。

用語	説明
CA	Certificate Authority（認証機関） 他のサーバの x.509 証明書にデジタル署名する信頼される証明書の発行元。
CS	Certificate Signer 他のサーバの ＸＭＬＲＰＣ 証明書にデジタル署名する信頼される証明書の発行元。
証明書 または セキュリティ証明書	Distribution など、証明書が関連付けられている対象を検証するための電子署名を含む電子ドキュメント。
CSR	Certificate Signing Request 信頼される CS による XMLRPC 証明書の署名をサーバが要求すること。これは、VeriSign* や Thawte Consulting などのルート CA によって署名される X.509 証明書ではありません。
self-signed certificate（自己署名された証明書）	作成者によって署名された有効な証明書。
署名付き証明書	CS によって署名された証明書。受信側のサーバによる受け入れで有効になります。
SSL	Secure Socket Layer
XMLRPC	Extensible Markup Language Remote Procedure Call Server Management および Tiered Electronic Distribution によってサーバ間通信で使用されるソフトウェア。

セキュリティ証明書

サーバ間通信のセキュリティでは、Certificate Signer (CS) によって発行された署名付き証明書を使用します。これは、Novell ZENworks ファミリの製品のコンテキスト内でのみ有効です。

使用される証明書は X.509 準拠ではないので、e コマースや SSL アプリケーションでは使用できません。

SSL の使用

CS サーブレットが Certificate Signing Request (CSR) に署名する場合、要求元のクライアントは HTTP 基本認証によりユーザ名とパスワードを使用して認証する必要があります。SSL を使用して、ユーザ名とパスワードのセキュリティを保護できます。商用 Web サーバ用に SSL を有効にする方法については、SSL のドキュメントを参照してください。

パスワードファイルの形式

サーバ間通信のセキュリティでは、CSR の署名のために認証されるユーザ名とパスワードについてパスワードファイルを使用します。パスワードファイルはテキストエディタで作成し、セキュリティで保護された場所に保存できます。このファイルへのアクセスは、ファイルにリストされているユーザだけに制限します。

ユーザ名とパスワードではいずれも大文字と小文字が区別されます。パスワードファイルの構文は次のとおりです。

username=password

例：

admin=adminpassword
CSsigner=cspassword
JohnDoe=jdpassword

このパスワードファイルへのアクセスは、このファイルに含まれているユーザだけに制限します。

TCP/IP アドレスと DNS 名

サーバ間通信のセキュリティを設定する場合、インストールプログラムは、このセキュリティを有効にするサーバのアドレスまたは名前を使用します。TCP/IP アドレスまたは完全識別 DNS サーバ名のいずれかを使用できます。

重要： NetWare サーバの場合は、DNS 名にアンダースコアを使用できません。サーバの DNS 名にアンダースコアが含まれている場合、Distribution の送受信エラーが発生します。単語の区切り文字としてアンダースコアの代わりにダッシュを使用することをお勧めします。

これらのアドレスやサーバ名の取得に使用できる各種の方法については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「インストールに関する情報の収集」を参照してください。

8 スケジュール設定

次のスケジュール設定に関する情報は、Novell® ZENworks® Server Management の Policy and Distribution Services に適用されます。

- 331 ページの「Policy and Distribution Services でのスケジュール設定の理解」
- 333 ページの「スケジュール設定とTiered Electronic Distributionオブジェクト」
- 353 ページの「スケジュール設定とサーバポリシー」

Policy and Distribution Services でのスケジュール設定の理解

次の節を参照してください。

- 331 ページの「配布にスケジュール設定が必要な理由」
- 332 ページの「スケジュール設定を必要とするサーバポリシー」
- 332 ページの「サーバポリシーと Tiered Electronic Distribution のスケジュール設定の相違点」
- 333 ページの「Tiered Electronic Distribution ポリシーの優先設定」

配布にスケジュール設定が必要な理由

Distribution を作成する場合、それを必要とする適切な Subscriber サーバに向けて、適切な時間に配布する必要があります (Distribution を作成するには Distribution オブジェクトを作成して設定します)。そのためには、配布プロセスをスケジュール設定する必要があります。

配布プロセスの基本的な流れは次のとおりです。

1. Distribution オブジェクトを作成して設定します。
2. Distribution オブジェクトを割り当てた Distributor オブジェクトによって eDirectory が読み込まれ、新しい Distribution が検出されます。
3. 設定情報に基づいて Distributor サーバにより Distribution ファイルが構築されます。
4. Distribution オブジェクトを Channel オブジェクトに関連付けます。
5. Distributor サーバから、その Channel に登録している Subscriber サーバに Distribution ファイルが送信されます。
6. Subscriber サーバにより、Distribution の内容が抽出されてインストールされます。

この配布プロセスにスケジュール設定が必要な理由は、次のとおりです。

- **配布プロセスの統制：** Distribution を適切な時間に配布して使用するために、あるプロセスから別のプロセスへの Distribution の流れを統制する必要があります。

  スケジュール設定が競合すると、Distribution がプロセスを通過しないか、配布と使用が遅れる場合があります。

- **ネットワークトラフィックの最小化：** スケジュール設定により、ネットワーク帯域幅の使用を柔軟に制御できます。たとえば、ネットワークのトラフィックが最も少ないときに大きな Distribution を送信するようにスケジュールを設定できます。

- **サーバの負荷の軽減：** スケジュール設定により、Distribution の構築、送信、および抽出に伴う関連サーバの負荷を軽減できます。たとえば、大きな Distribution の構築と抽出をピーク時や週末を避けてスケジュール設定することができます。

スケジュール設定は Distribution によって使用されるネットワークリソース全体には影響しません。リソースの使用時期だけに影響します。

スケジュール設定を必要とするサーバポリシー

一部のポリシーは、スケジュール設定をした後で適用する必要があります。

ポリシーを有効にしてもスケジュール設定をしないと、デフォルトパッケージスケジュールに現在指定されているスケジュールに従って実行されます。デフォルトパッケージスケジュールは、ポリシーのデフォルトスケジュールを提供します。デフォルトスケジュールは、システム起動時に実行されます。

複数の異なるサーバポリシーで同じスケジュールを使用すると、ポリシーの適用順序が保証されません。ポリシーの適用順序を確保するには、ポリシーのスケジュールに時間差が必要です。

ポリシーのスケジュール設定の詳細については、353 ページの「スケジュール設定とサーバポリシー」を参照してください。

ポリシーの詳細については、4 章 197 ページの「Server Policies（サーバポリシー）」を参照してください。

サーバポリシーと Tiered Electronic Distribution のスケジュール設定の相違点

ポリシーは現地時間に従ってスケジュール設定されます。Tiered Electronic Distribution オブジェクトは、グリニッジ標準時（GMT）からのオフセットに従ってスケジュール設定されます。

サーバポリシーの例： ユタ州に居住していてポリシーをユタ時間の午後 5 時に実行するように設定すると、ユタ州に存在するサーバに対してユタ時間の午後 5 時にポリシーが実行されます。カリフォルニア州では、カリフォルニア時間の午後 5 時にポリシーが実行されます。つまり、ポリシーの実行時間を午後 5 時に設定すると、サーバの場所に関係なしに現地時間の午後 5 時にポリシーが実行されます。

Tiered Electronic Distribution の例： ユタ州に居住していて Tiered Electronic Distribution オブジェクトのスケジュールを夏時間の午後 5 時に設定すると、ユタ時間の午後 5 時にポリシーが実行されます。カリフォルニア州では、州内のサーバに対してカリフォルニア時間の午後 4 時（ユタ時間の午後 5 時）にポリシーが実行されます。つまり、Tiered Electronic Distribution のスケジュールは GMT のオフセットに相対的となり、Tiered Electronic Distribution のスケジュールは世界中で同時に実行されます。

Distribution に利用できる日中の時間帯として、スケジュールのアクションを実行する開始時刻と終了時刻を定義することができます。通常、配布スケジュールはピーク時を避けて設定します。一部のネットワークでは、スケジュールを設定できる時間帯が狭く限られる場合があります。ピーク時を避けた時間は、ネットワークの他のシステムによる処理（バックアップなど）に使用される場合もあります。

配布に利用できる時間帯が制限される場合があるため、使用するリソースに関係なしに、いかに配布時間を短縮できるかが重要な条件になります。時間とリソースの最善の関係を確認するために多少の試行錯誤が必要になる場合があります。

Tiered Electronic Distribution ポリシーの優先設定

[Schedule] タブで、(SLP のプロパティパッケージの)Tiered Electronic Distribution ポリシーに対してスケジュールを設定すると、このスケジュールがポリシー適用先のすべての Distributor および Subscriber のデフォルトになります。ただし、ConsoleOne で Tiered Electronic Distribution オブジェクトに個別にスケジュールを設定した場合を除きます。つまり、Distributor および Subscriber のスケジュールを個別に変更すると、その変更は自動的に Tiered Electronic Distribution ポリシーのスケジュールよりも優先されます。

Distributor のスケジュールと Subscriber のスケジュールは異なります。Distributor の更新スケジュールと Subscriber の抽出スケジュールには異なる [Schedule] タブが用意されています。

デフォルトでは、Tiered Electronic Distribution ポリシーにスケジュールを設定すると、すべての Distributor および Subscriber に対して [General] タブと [Schedule] タブの両方に [Use Policy] チェックボックスが表示されます。さらに、スケジュールを変更していない Distributor オブジェクトおよび Subscriber オブジェクトに対しては、このチェックボックスが自動的に選択されます。スケジュールを変更したオブジェクトに対しては、このボックスが選択解除されます。

特定の Distributor オブジェクトまたは Subscriber オブジェクトのプロパティで [Use Policy] チェックボックスを選択解除すると、そのオブジェクトに対する Tiered Electronic Distribution ポリシーのデフォルトスケジュールを無効にすることができます。デフォルトスケジュールの変わりに個別のスケジュールを使用する場合は、オブジェクトのプロパティで新しいスケジュールを定義します。

Distributor または Subscriber の個別のスケジュールを無効にする場合は、オブジェクトのプロパティで [Use Policy] チェックボックスを選択します。その Distributor または Subscriber に対して、Tiered Electronic Distribution ポリシーのスケジュールが適用されます。

Tiered Electronic Distribution ポリシーの作成、設定、およびスケジュール設定の方法については、213 ページの「Tiered Electronic Distribution」を参照してください。

スケジュール設定と Tiered Electronic Distribution オブジェクト

スケジュール設定を円滑に行うには、スケジュール設定の基本的な原則を理解する必要があります。次の節のガイドラインに従って、Distribution の効果的なスケジュールを設定してください。

- 334 ページの「Tiered Electronic Distribution オブジェクトおよびスケジュールの理解」
- 339 ページの「Tiered Electronic Distribution のスケジュール間の相互関係」

- 340 ページの「スケジュール設定に影響する 3 つの時間要因」
- 344 ページの「スケジュール設定の指針」
- 346 ページの「スケジュール設定に関する問題」

Tiered Electronic Distribution オブジェクトおよびスケジュールの理解

Distributor サーバから Subscriber サーバに Distribution を送信する場合、この配布プロセスにはいくつかの Tiered Electronic Distribution オブジェクトが関与します。そのため、配布プロセスを効率化して配布の目的を達成するには、一部の関与するオブジェクトにスケジュールを設定する必要があります。

次の節では、それぞれのスケジュールについて説明します。

- 334 ページの「Tiered Electronic Distribution のスケジュール」
- 335 ページの「Distributor オブジェクトの更新スケジュール」
- 336 ページの「Distribution オブジェクトの構築スケジュール」
- 337 ページの「Channel オブジェクトの送信スケジュール」
- 338 ページの「Subscriber オブジェクトの抽出スケジュール」

Tiered Electronic Distribution のスケジュール

次の Tiered Electronic Distribution オブジェクトにスケジュールを設定できます。

Tiered Electronic Distribution オブジェクト	スケジュール名	スケジュール設定の目的
Distributor	更新	Distribution に加えられた変更を検出するための eDirectory の再読み込みを行う時期を Distributor に通知します。変更を検出すると、Distribution オブジェクトの構築スケジュールに従って Distribution を再構築します。
Distribution	構築	特定の Distribution を構築できる時期を Distributor に通知します。
Channel	Send	Distributor が所有する Channel 内の Distribution を送信できる時期を Distributor に通知します。
Subscriber	Extract	受信したがまだ抽出していない Distribution を抽出およびインストールできる時期を Subscriber に通知します。

これらの Tiered Electronic Distribution オブジェクトにスケジュールを設定する必要があります。スケジュールを設定しない場合、そのオブジェクトは、Distribution の検出、構築、配布、抽出などの Distribution に関連するアクションを実行できません。

次の Tiered Electronic Distribution オブジェクトにはスケジュールを設定しません。

External Subscriber
Subscriber Group
Policy Package [1]

[1] Container Package と Service Location Package のみ。Distributed Policy Package には、Distribution オブジェクトで［Schedule］タブを使用してスケジュールを設定できます。

スケジュール別のサーバ CPU 使用率

スケジュールは、Distribution で使用されるリソース全体（CPU サイクル、帯域幅、ディスク領域など）には直接影響せず、リソースの使用時期に影響します。つまり、Tiered Electronic Distribution のスケジュールは、Distribution の構築、送信、および抽出の時期を制御します。

ただし、CPU 使用率は、スケジュールのアクションを実行するために使用するサーバの影響を受けます。サーバの CPU 時間は、そのサーバで実行している Tiered Electronic Distribution の機能によって異なります。

サーバの CPU 時間	スケジュール
Distributor	更新、構築、送信
Subscriber	Extract
parent Subscriber（親 Subscriber）	送信、抽出

スケジュールタイプ

オブジェクトのスケジュールを設定する場合、次のスケジュールタイプから選択できます。

Never
曜日
月
年
間隔（Interval）
Time
Run Immediately（Distributor オブジェクトを除く）

スケジュールタイプの詳細については、340 ページの「頻度」および 411 ページの「スケジュールタイプ」を参照してください。

スケジュール変更時の証明書の解決

いずれかのスケジュールに変更を加えるときは、証明書の解決が必要になることがあります。詳細については、317 ページの「証明書の解決」を参照してください。

Distributor オブジェクトの更新スケジュール

Distributor のスケジュールは、Distributor が Novell eDirectory™ を読み込んで設定の変更を検出する時期を決定します。これにより、Distributor は Distribution の構築に対する要求に応じることができます。Distribution オブジェクトのスケジュールに従って構築が要求されると、Distributor は Distribution を再構築します。

Channel の送信スケジュールが開始されると、Distributor は直接の配布先の Subscriber に最新の Distribution バージョンがあるかどうかを確認します。ただし、

- シーケンシャルでない Distribution の場合、Distributor は最新バージョンの有無のみを確認します。

- シーケンシャルなDistributionの場合(DistributionのタイプがFileまたはDesktop Application の場合のみ) は、Subscriber にすべての Distribution バージョンがあるかどうかを確認するために、ベースラインから開始してベースライン以降の各変更をチェックします。

Subscriber に Distribution の全体が揃っていない場合は、その下位の Subscriber がチェックされ、さらにルーティング階層の下方に向かってチェックが継続されます。

Channel のすべての Distribution がすべての配布先に受信されているかどうかは、短時間で確認されます。

重要： Distribution の構築または送信に要する時間よりも更新スケジュールが短いと、Distribution の送信が完了しない場合があります。更新スケジュールが短すぎると、Distributor を更新したときに、構築中または送信中の Distribution は構築または送信が完了する前にキャンセルされます。したがって、Distributor の更新スケジュールは日単位で設定し、Distribution の変更頻度がより高い場合にのみ時間単位で設定することをお勧めします。Distributor の更新間隔は最低 5 分とし、それ以下には設定しないでください。

Distributor のスケジュール設定

1 ConsoleOne で、Distributor オブジェクトを右クリックし、[Properties] をクリックします。

2 [Schedule] タブ > ドロップダウンボックスの矢印 > [Interval] の順にクリックし、[Daily] などの間隔を選択します。

3 必要に応じて、開始時刻と終了時刻を設定します。

[Start Time] と [End Time] は、スケジュールのアクションを実行する時間帯を指定します。

指定した時間帯の中で、設定した間隔ごとに更新を繰り返すことができます。

指定した時間帯の中で更新をランダムに実行することもできます。詳細については、351 ページの「Distributor の更新スケジュールにおける [Randomly Dispatch] オプションの使用」を参照してください。

4 [OK] をクリックします。

Distribution オブジェクトの構築スケジュール

Distribution のスケジュールは、Distribution オブジェクト内の定義に基づいて Distribution を作成する時期を Distributor に指示します。

大半の Distribution を構成するファイルセットは時間の経過とともに変更されるため、定期的に再配布する必要があります。Distribution 別に独自の構築スケジュールがあり、それに従って Distributor による Distribution の再構築の頻度が決まります。Distributor では、Distribution を構築するときに前のバージョンと自動的に比較して変更の有無を確認します。

File Distribution である場合は、現在の構築内容に変更がないと、新しいバージョンは作成されません。変更があると、変更のみで構成されたデルタが構築されて配布されます。

Distribution タイプが FTP、HTTP、および Software Package である場合は、前回のバージョン以降に変更があるときに限り、新しいバージョンが作成されます。Distributor は、すべての配布先の Subscriber に新しいバージョン全体を送信します。

ランダムな実行イベントの終了時刻を指定するには、Distribution の [End Time] を使用します。つまり、Distributor は Distribution の構築が完了するまで構築を停止しません。

削除したファイルとディレクトリの同期化は構築スケジュールで処理します。

Distribution のスケジュール設定

1 ConsoleOne で、Distribution オブジェクトを右クリックし、[Properties] をクリックします。

2 [Schedule] タブ > ドロップダウンボックスの矢印の順にクリックし、[Run Immediately] などのスケジュールタイプを選択します。

指定した間隔でアクションを繰り返すことができます。

[Start Time] と [End Time] は、スケジュールのアクションを実行する時間帯を指定します。

指定した時間帯の中で構築をランダムに実行することもできます ([Daily] スケジュールタイプを選択した場合)。詳細については、351 ページの「Distribution の構築スケジュールにおける [Randomly Dispatch] オプションの使用」を参照してください。

3 [OK] をクリックします。

Channel オブジェクトの送信スケジュール

Channel の送信スケジュールを使用すると、その Channel に関連する Subscriber に Distribution の送信を開始する時間帯を設定できます。

Channel のスケジュールは、Distributor およびその直接の配布先 (最初の階層の Subscriber) にのみ適用されます。送信スケジュールが終了すると、Distributor から最初の階層の Subscriber に対する配布が終了します。

2 番目の階層の配布先およびそれより下位の配布先は、Channel のスケジュールに拘束されません。親 Subscriber から他の Subscriber への Distribution の送信は、送信スケジュールの終了後も続行されます。下位の Subscriber でも、送信スケジュールは無視されます。

送信スケジュールの [End Time] は、送信スケジュールの終了時に Distribution の送信を中断することを Distributor に強制します。送信スケジュールが再開されると、Distributor は送信を中断した箇所から送信を再開します。Distribution は全体が再送信されるのではありません。たとえば、60MB の Distribution のうち、50MB が中断前に送信済みであった場合、Channel の送信スケジュールが再開されると、Distributor は残りの 10MB の送信を再開します。

Channel のスケジュールに対する時間帯の影響については、348 ページの「タイムゾーンが異なる Tiered Electronic Distribution オブジェクトのスケジュール設定」を参照してください。

[Cache and Forward] は、Channel の送信スケジュールの終了時に親 Subscriber が Distribution の送信を続行するかどうかには影響しません。送信スケジュールの終了前に Distribution を完全に受信した親 Subscriber は、その Distribution を下位の Subscriber に対して引き続いて送信します。送信スケジュールの終了時に親 Subscriber による送信の続行を制御する手段はありません。

重要： Distribution の送信に要する時間よりも送信スケジュールが短い場合は、Distribution は送信されません。したがって、Channel の送信スケジュールは日単位または時間単位で設定することをお勧めします。送信スケジュールは、Channel のすべての Distribution を送信するのに必要な時間よりも長く設定してください。

Channel のスケジュール設定

1 ConsoleOne で、Channel オブジェクトを右クリックし、[Properties] をクリックします。

2 [Schedule] タブ > ドロップダウンボックスの矢印 > [Interval] の順にクリックし、[Repeat the Action Every] フィールドで間隔 (1 時間など) を選択して、[OK] をクリックします。

[Start Time] と [End Time] は、スケジュールのアクションを実行する時間帯を指定します。

送信スケジュールをランダムに開始する方法 ([Daily] スケジュールタイプを選択した場合) については、352 ページの「Channel の送信スケジュールにおける [Randomly Dispatch] オプションの使用」を参照してください。

Subscriber オブジェクトの抽出スケジュール

Subscriber のスケジュールは、Subscriber が受信した Distribution を抽出できる時期を決定します。

ランダムな実行イベントの終了時刻を設定するには、Subscriber の [End Time] を使用します。Subscriber は、Distribution の抽出プロセスを完了するまで、抽出を中断しません。

Subscriber のスケジュール設定

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [Channels] タブ > [Add] の順にクリックし、Channel を参照して選択します。次に、[Select] > [OK] の順にクリックします。

Channel が [Active in the Channels] リストに表示されていることを確認します。

3 [Schedule] タブ > ドロップダウンボックスの矢印の順にクリックし、[Run Immediately] などのスケジュールタイプを選択して、[OK] をクリックします。

[Run Immediately] スケジュールタイプを選択した場合は、Distribution の受信と同時に抽出が開始されます。

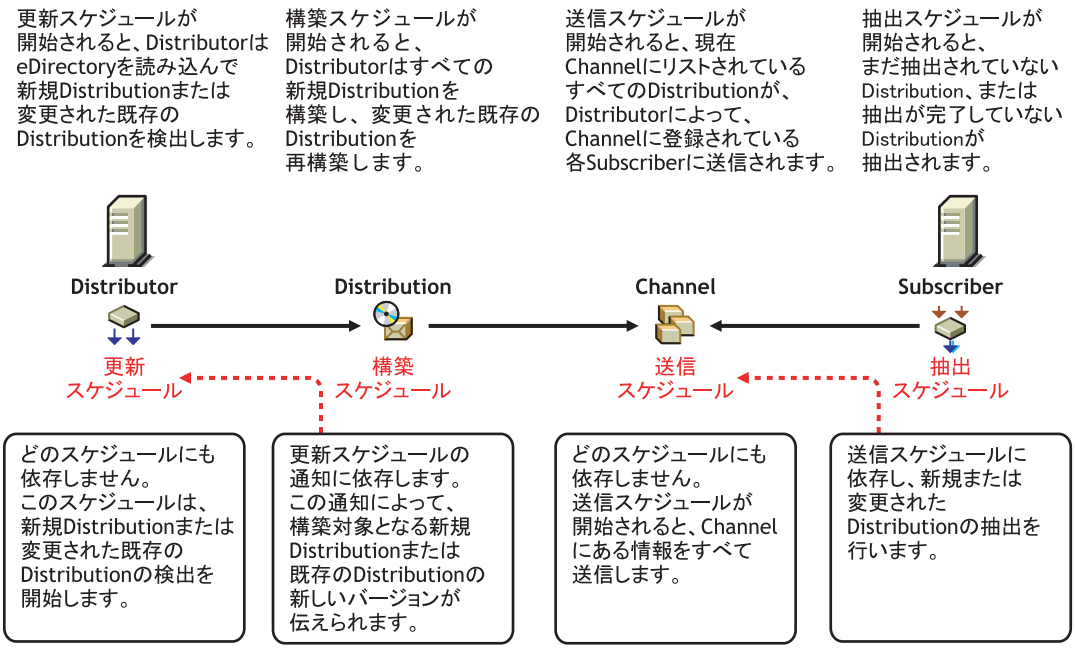
[Start Time] と [End Time] は、スケジュールのアクションを実行する時間帯を指定します。

抽出スケジュールをランダムに開始する方法 ([Daily] スケジュールタイプを選択した場合) については、352 ページの「Subscriber の抽出スケジュールにおける [Randomly Dispatch] オプションの使用」を参照してください。

4 この手順を Subscriber ごとに繰り返します。

Tiered Electronic Distribution のスケジュール間の相互関係

Tiered Electronic Distribution オブジェクトの各スケジュールは、他のすべてのスケジュールと直接関係するわけではありません。次の例に示すように、スケジュール間は一定の順序に従って関係付けられます。



最も重要な点は、指定した時間帯内で Distribution を正常に検出、構築、送信、および抽出できるように、Refresh、Build、Send、および Extract の順に各スケジュールを設定する必要があることです。

いずれかのスケジュールが他の 3 つのスケジュールと同期しない場合は、Distribution を作成して最終的に使用するまでに大幅に遅れる場合があります。

スケジュールの設定例と結果を次に示します。

- **更新スケジュールの間隔を 1 時間に設定した場合：** Distributor は、新規の Distribution または変更された Distribution を検出するために、1 時間ごとに eDirectory を読み込みます。この間隔は、Distributor が各更新後に構築する Distribution の大きさに基づいて決定する必要があります。通常は、更新間の時間が短いほど理想的です。
- **構築スケジュールをすぐに実行するように設定した場合：** Distributor は、更新スケジュールに従って eDirectory を読み込み、新しい Distribution または変更された Distribution を検出すると同時にその構築を開始します。ただし、特に大きな Distribution については、ピーク外の時間に構築する必要があります。
- **送信スケジュールを深夜 0 時に設定した場合：** Distributor は、ネットワークの帯域幅が比較的空いているピーク外の時間に Distribution を送信します。
- **送信スケジュールをすぐに実行するように設定した場合：** Distributor は、Distribution の構築を完了すると同時に送信します。
- **抽出スケジュールを午前 3 時に設定した場合：** 受信された Distribution は、サーバが最も空いているピーク外の時間に抽出されます。この設定は、抽出とインストールを急がない大きな Distribution を受信するサーバに最適です。

- **抽出スケジュールをすぐに実行するように設定した場合：** Subscriber は、Distribution を受信すると同時に抽出します。ウィルスパターンなどの重要な Distribution を受信するサーバに便利な設定です。

次のような設定をした場合は、配布プロセスの流れが混乱します。

- Distributor の更新スケジュールの設定間隔が、新しい Distribution または変更された Distribution を構築する時間よりも短い場合。
- Distributor の更新スケジュールの設定間隔が長すぎて、重要な Distribution が適時に構築および送信されない場合。
- Distribution の構築スケジュールの設定間隔が短すぎて、構築中の Distribution を完了する前にスケジュールが終了してしまう場合。
- Distribution の構築スケジュールの設定間隔が長すぎて、重要な Distribution が適時に構築および送信されない場合。
- Channelの送信スケジュールがDistributorの構築スケジュールと同期していないために、Distribution の送信が遅延する場合。
- Channel の送信スケジュールの設定間隔が短すぎて、すべての Distribution の送信を完了できない場合。

スケジュール設定に影響する 3 つの時間要因

スケジュール設定に影響する 3 つの時間に関連する要因があります。

- 340 ページの「頻度」
- 341 ページの「Duration」
- 342 ページの「間隔 (Interval)」
- 343 ページの「Distributor での間隔の使用」

頻度

スケジュールを設定する場合、特定の Distribution を構築、送信、および抽出する頻度を決定します。

Distribution の処理頻度を決定するには、次のスケジュールタイプを使用できます。

スケジュールタイプ	機能
曜日	毎日同じ時間に当該機能を実行します。
月	毎月同じ日に当該機能を実行します。
年	毎年同じ日に当該機能を実行します。
間隔 (Interval)	指定した間隔で当該機能を実行します。
Time	指定した日時にのみ当該機能を実行します。
すぐに実行 (Run Immediately)	スケジュールの標準設定を無視して、当該機能を直ちに開始します。

配布プロセスのスケジュールを設定するときに選択する頻度は、Distribution の目的に応じて決定します。たとえば、次のように入力します。

- ウィルス保護パターンファイルは、利用可能になると同時に配布してインストールできるようにします。
- ソフトウェアのアップデートは、1 回だけ送信してインストールできるようにします。

Duration

スケジュールタイプによっては、時間帯を設定する必要があります。時間帯を定義するには、開始時刻と終了時刻を使用して、スケジュール設定したアクションを実行できる時間を指定します。

一部のスケジュールは、スケジュールの時間帯の終了時に機能が全面的に停止します。したがって、スケジュールの時間帯は、Distribution のサイズに応じて構築、送信、および抽出に要する時間を判断し、それよりも長く設定する必要があります。

時間帯に関する問題は、次に説明するように、スケジュールごとに異なります。

- 341 ページの「Distributor オブジェクトの更新スケジュール」
- 342 ページの「Distribution オブジェクトの構築スケジュール」
- 342 ページの「Channel オブジェクトの送信スケジュール」
- 342 ページの「Subscriber オブジェクトの抽出スケジュール」

Distributor オブジェクトの更新スケジュール

更新スケジュールが開始すると、次の動作が発生します。

- **Distribution の構築が中断する：** Distributor は、構築中の Distribution の構築を中断します。一時的な構築ファイルは削除されず、未完了の Distribution の構築は中断した箇所から再開されません。未完了の Distribution の構築は、次回の構築スケジュールが開始されたときに最初からやり直されます。
- **Distribution の送信が中断される：** Distributor は、送信中の Distribution の送信を中断します。ただし、送信スケジュールが再開されると、Distributor は中断した箇所から送信を再開して Distribution の送信を完了します。

したがって、更新スケジュールは構築スケジュールまたは送信スケジュールと重複することはできません。更新スケジュールは、他のスケジュールが終了した後で開始し、他のスケジュールが開始する前に終了する必要があります。

更新スケジュールによって Distributor による Distribution の構築が妨げられる可能性があるので、必要に応じてシステムに複数の Distributor を確保し、作成する Distribution の種類別に処理を分担します。詳細については、344 ページの「Distributor の追加に関する判断」を参照してください。

更新スケジュールの終了時刻に達すると、Distributor は中断した箇所から Distribution の送信を開始します。ただし、更新スケジュールの開始によって中断された構築中の Distribution については、中断箇所から再開されずに最初から構築がやり直されます。

Distribution オブジェクトの構築スケジュール

構築スケジュールが開始すると、その時点で Distributor によって認識されている Distribution のみが構築スケジュールの時間中に構築が開始されます。Distributor は、Distributor の更新スケジュールに従って eDirectory を読み込むことにより、変更された既存の Distribution および新しく作成された Distribution を検出します。

構築スケジュールの終了時刻に達しても、構築が開始されていたすべての Distribution の構築は完了または失敗するまで続行されます。

Channel オブジェクトの送信スケジュール

送信スケジュールが開始されると、Channel に表示されている Distribution の中で、送信スケジュールの開始時に Distributor に認識されているものに限り、その送信が開始されます。

送信スケジュールの終了時刻に達すると、Distribution の送信が完了していない場合でも、Distributor は送信を中断します。ただし、次回に送信スケジュールが開始されると、送信を中断した Distribution の送信を中断箇所から再開して完了します。さらに、Distributor が更新スケジュールの時間内に検出した新しい Distribution または変更された Distribution の送信を開始します。

Subscriber オブジェクトの抽出スケジュール

抽出スケジュールが開始されると、受信済みの Distribution または抽出スケジュールの時間中に受信されたすべての Distribution が同時に抽出されます。

抽出スケジュールの終了時刻に達しても、Subscriber で開始されていたすべての Distribution の抽出は完了または失敗するまで続行されます。

間隔 (Interval)

間隔は、スケジュールの時間帯でスケジュールの機能を繰り返す頻度を表します。

間隔は、スケジュール全体をより小さいスケジュールに分割して連続的に実行することと同じです。スケジュールの時間帯で、間隔は開始 / 終了位置を指定し、スケジュール内で開始 / 終了位置の数に応じた回数だけ同じアクションを繰り返します。

間隔に関する問題は、次に説明するように、スケジュールごとに異なる場合があります。

- 342 ページの「Distributor オブジェクトの更新スケジュール」
- 343 ページの「Distribution オブジェクトの構築スケジュール」
- 343 ページの「Channel オブジェクトの送信スケジュール」
- 343 ページの「Subscriber オブジェクトの抽出スケジュール」

Distributor オブジェクトの更新スケジュール

間隔を使用して、Distributor の更新頻度と、Distribution、Channel、Subscriber、またはポリシーの設定情報の変更を検出する頻度を同期化します。

間隔として設定する時間は、Distributor が eDirectory を読み込んで検出した新しい Distribution または変更された Distribution を構築する時間よりも長くなければなりません。

Distribution オブジェクトの構築スケジュール

内容が頻繁に変更される Distribution を適時に配布するには、各変更を構築スケジュールによって効率よく検出し、再構築した Distribution を適時に送信できるように間隔を設定します。

Channel オブジェクトの送信スケジュール

送信スケジュールの時間帯に間隔を設定すると、間隔が開始されるたびに現在送信中の Distribution は中断され、前に送信が中断されていた Distribution は中断箇所から送信が再開されます。さらに、キューに追加された新しい Distribution の送信も開始されます。

間隔を使用しない場合は、送信スケジュールの開始後に送信スケジュールのキューに追加された Distribution は、次回に送信スケジュールが開始されるまで送信されません。したがって、送信スケジュールに間隔を設定すると、新しくキューに追加された Distribution を送信スケジュールの時間帯に含めることができます。

Subscriber オブジェクトの抽出スケジュール

間隔は抽出プロセスには無意味です。抽出スケジュールの開始前に受信された Distribution、または抽出スケジュールが開いている間に受信された Distribution は、すべてが抽出されます。抽出スケジュールの終了後も抽出は続行されるため、間隔を設定しても抽出プロセスによって無視されます。

Distributor での間隔の使用

間隔を設定したスケジュールタイプでは、Distributor によって eDirectory が再読み込みされるまでイベントが開始されません。たとえば、次のように入力します。

- **[Daily]：** 当日の時間帯が経過する前に Distribution が更新されると、イベントは当日に実行され、以後毎日実行されます。それ以外の場合は、翌日の時間帯中に 1 回実行され、以後毎日実行されます。
- **[Interval]：** 間隔を 3 日に設定すると、Distributor によって eDirectory が再読み込みされた日から 3 日後にイベントが実行され、以後 3 日ごとに実行されます。
- **[Weekly]、[Monthly]、または [Yearly]：** イベントは、Distributor による eDirectory の再読み込み後から最初の曜日、月、または特定の日付（［Yearly］オプション）に実行されます。たとえば、日曜日ごとに実行する［Weekly］イベントを水曜日に設定したとします。この場合、Distributor による eDirectory の再読み込みは木曜日に、イベントの実行日は次の日曜日になります。イベントは、以後日曜日ごとに実行されます。
- **[Run Immediately]：** Distributor が更新されると同時にイベントが実行されます。以後、イベントは設定した間隔に従って実行されます。

［Run Immediately］とは別に、間隔を設定したスケジュールタイプで予定外の時間にイベントを実行するには、iManager の ZENworks Server Management ロールを使用できます。詳細については、2 章 69 ページの「Novell iManager」を参照してください。

スケジュール設定の指針

スケジュールの設定方法を決める際に、次の指針を参考にしてください。

- 344 ページの「Distributor の追加に関する判断」
- 344 ページの「Channel の制御」
- 345 ページの「Distributor の負荷分散機能の有効化」
- 345 ページの「スケジュールの停止」
- 345 ページの「他のソフトウェアと競合するスケジュール」

Distributor の追加に関する判断

Distributor の必要数は、Distributor サーバの負荷および Distribution の構築作業を完了できるかどうかによって決まります。

たとえば、ピーク外の時間中に構築し、すぐには送信する必要がない大きな Distribution と、すぐに送信する必要があるウィルスパターン Distribution がある場合は、2 つの異なる Distributor を使用します。最初の Distribution については、Distribution を毎日 1 回のみ構築するので、更新スケジュールとして毎日を設定します。2 番目の Distribution については、新しいウィルスパターンの変更を検出するために頻繁な更新スケジュールを設定し、Distribution を適時に構築および送信できるようにします。

Channel の制御

Tiered Electronic Distribution を使用する目的は、Subscriber が Distribution を使用する時期を制御することにあります。その方法として、Subscriber が Distribution を使用するときに Distribution を構築することができます。この場合、必要な Distribution が適時に Subscriber に到着するように他のスケジュールを調整することが重要です。

このスケジュールの調整に最も役立つのが Channel の送信スケジュールです。次の例を参考にしてください。

1. Distribution の構築スケジュールは、Distribution の情報が変更される頻度に依存します。たとえば、次のように入力します。
   - Distribution が毎月更新されるフォームで構成され、更新されたフォームをすぐに配布する必要がある場合は、構築スケジュールを［Daily］に設定します。これにより、フォームの変更の有無が毎日チェックされ、変更があれば、その日または 24 時間以内に検出されます。フォームの変更が検出されると、新しい Distribution が構築されます。
   - Distributionが6ヶ月ごとに1回変更されるソフトウェアアプリケーションで構成されている場合は、Distribution を毎週構築するように設定します。Distribution のアプリケーションが変更された場合は、1 週間以内に Distribution が構築されます。
2. Subscriber のすべての抽出スケジュールを［Run Immediately］に設定します。これにより、Distribution の構築および送信の時期に関係なしに、Subscriber は受信した Distribution をすぐに使用できます。

   Subscriber のすべての抽出スケジュールを［Run Immediately］に設定した場合、大きな Distribution を受信してもピーク時の Subscriber サーバへの影響を心配する必要はありません。Channel の送信スケジュールを使用すると、Subscriber による特定の Distribution の受信と抽出の時期を制御できます。

3. Channel の送信スケジュールを、Distribution の再構築のスケジュールと相関させ、Subscriber による抽出時に実行するように設定します。
   - 毎月変更される Distribution の場合は、Channel の送信スケジュールを［Monthly］に設定します。
   - 6ヶ月単位などで変更される Distribution の場合は、Channel の送信スケジュールを［Yearly］または *xxx* 日間の間隔に設定します。
   - ピーク時を避けて抽出する必要がある大きな Distribution の場合は、Channel の送信スケジュールをすぐに実行するように設定します。Distribution の抽出については、ピーク時以外に抽出するように Subscriber の抽出スケジュールを設定できます。

簡単にまとめると、Distribution が必要になったときに構築し、Subscriber が Distribution を受信すると同時に抽出して使用できるように準備を完了します。次に、Channel から Subscriber に対して Distribution を最適な時間に送信するように設定します。

Distributor の負荷分散機能の有効化

Distributor サーバの配布作業に伴う負荷を分散するには、次の操作を行います。

1. Distribution オブジェクトで［Maximum Number of Concurrent Distributions］オプションを選択します。
2. Distribution オブジェクトに対して、［Daily］、［Monthly］、または［Yearly］の各スケジュールタイプの［Randomly Dispatch］オプションを使用します。

   ［Randomly Dispatch］オプションの詳細については、351 ページの「［Randomly Dispatch During Time Period］オプションの使用」を参照してください。

これにより、多数の Distribution の送信に伴うネットワークトラフィックは、スケジュールの時間帯全体に分散されます。

スケジュールの停止

Distribution を［Active］または［Inactive］に設定することができます。

- **［Active］**：［Active］チェックボックスは、Distribution オブジェクトの［General］タブにあります。
- **［Inactive］**：Distribution を Subscriber に送信できる準備が完了するまで Distribution を停止状態にするには、Distribution を構築するときに［Inactive］を使用します。

Distribution オブジェクトを作成または変更する場合は、Distribution パッケージの配布を開始する準備が整うまで、関連する Channel を［Inactive］に設定することをお勧めします。これにより、設定が未完了の Distribution が間違えて送信されるのを防止できます。

他のソフトウェアと競合するスケジュール

大半の配布はピーク時を避けた時間に実行します。ネットワークによっては、ピーク時を避けた時間帯が短く限られる場合があります。ピーク時を避けた時間が、ネットワークの他のシステムによる処理（バックアップなど）に使用される場合もあります。

Distribution に利用できる時間帯が制限される場合があるため、使用するリソースに関係なしに、いかに配布時間を短縮できるかが重要な条件になります。時間とリソースの最善の関係を確認するために多少の試行錯誤が必要になる場合があります。

スケジュール設定に関する問題

以下の節では、スケジュール設定に関する問題について説明します。

- 346 ページの「スケジュール間の相互関係」
- 348 ページの「タイムゾーンとスケジュール設定」
- 351 ページの「［Randomly Dispatch During Time Period］オプションの使用」
- 352 ページの「アクションの繰り返し」

スケジュール間の相互関係

4 つのスケジュール（更新、構築、送信、および抽出）の相互関係は、配布プロセスの成功または適時性を左右します。

- 346 ページの「相互関係に関する全体的な問題」
- 347 ページの「更新スケジュールと構築スケジュールの関係」
- 347 ページの「更新 / 構築スケジュールと送信スケジュールの関係」
- 347 ページの「構築スケジュールと送信スケジュールの関係」
- 347 ページの「送信スケジュールと抽出スケジュールの関係」

相互関係に関する全体的な問題

配布プロセスは、4 つのスケジュール間の適時の相互関係に依存します。Distribution の目的に応じて、配布プロセスに関与する各スケジュールの役割を決定できます。

たとえば、ウィルスパターン Distribution は、その設定または変更が終了すると同時に送信し、ターゲットサーバで受信してすぐに使用できるように、Tiered Electronic Distribution の 4 つの各オブジェクトに関連するスケジュールを設定します。

一方、特に大きな Distribution で、送信に要する帯域幅と構築および抽出に要するサーバ時間が余分に必要な場合は、ピーク時を避けた時間帯に構築、送信、および抽出するように各スケジュールで調整します。

目的とサイズが異なる Distribution を同じ Distributor サーバで構築する場合が少なくありません。したがって、このような状況にも対応できるスケジュールを設定する必要があります。たとえば、Distributor の更新スケジュールを 5 分ごとに実行するように設定すると、Distribution をすぐに送信するとともに、ピーク時を避けた時間に送信することもできます。これは、Distribution の構築スケジュールは、特定の Distribution が構築されたとき（即時またはピーク時を避けた時間）に実行されることによります。

Subscriber の抽出スケジュールでは、Distribution の即時抽出とピーク時を避けた時間帯の抽出が競合する場合があります。しかし、Distribution をすぐに抽出してインストールするように Subscriber のスケジュールを設定する場合に、構築スケジュールと送信スケジュールを使用して特定の Distribution を受信する時期を制御できます。このようにして、ウィルスパターン Distribution は（小さくてサーバに負担を与えないので）すぐに抽出し、大きな Distribution はピーク時を避けた時間に受信して抽出することができます。

Distribution ごとに構築時間を制御できること、および通常は Distribution 別に Channel を作成することから、Distributor の更新スケジュールと Subscriber の抽出スケジュールはきめ細かく設定できます。つまり、大半のスケジュールの食い違いは構築スケジュールと送信スケジュールで制御できます。

更新スケジュールと構築スケジュールの関係

Distributor は、Distribution オブジェクトの構築スケジュールに従って Distribution を構築します。ただし、この構築が行われるのは、Distributor が更新スケジュールに従って eDirectory を読み込み、新しい Distribution や既存の Distribution の変更など、再構築が必要となるような変更を検出した後です。つまり、構築スケジュールは更新スケジュールに依存します。

したがって、新しい Distribution オブジェクトを作成して設定した直後に Distribution を構築するには、そのような直後の構築を可能にするために Distributor の更新スケジュールの実行間隔を短くする必要があります。たとえば、Distributor の更新スケジュールを 5 分間隔に設定します。

ただし、Distributor サーバでピーク時を避けた時間にのみ Distribution を構築する場合は、更新スケジュールの開始時刻と終了時刻をピーク時を避けた時間帯に設定します。したがって、そのような時間帯を指定できる更新スケジュールタイプを選択する必要があります。たとえば、[Daily]、[Monthly]、および [Yearly] を選択すると、時間帯を設定できます。さらに、[Daily] を使用すると、eDirectory を読み込んで変更を検出する曜日を指定することもできます。

更新 / 構築スケジュールと送信スケジュールの関係

Distribution は、最初の構築が終了済みのものだけが Channel に表示されます。したがって、Channel の送信スケジュールは、新しく構築された場合でも変更のために再構築された場合でも、既存の Distribution に適用されます。Distributor は、Channel オブジェクトの送信スケジュールに従って Distribution を送信します。つまり、送信スケジュールは更新スケジュールまたは構築スケジュールには依存しません。

ただし、Subscriber サーバは送信スケジュールが開始されるまで Distribution を受信しないので、更新スケジュールおよび構築スケジュールは送信スケジュールに依存します。

構築スケジュールと送信スケジュールの関係

Channel には、送信可能な Distribution のみが表示されます。Channel は、既存の Distribution が再構築を要するかどうかには関知しません。送信スケジュールは、Channel に登録している Subscriber サーバに Distribution を送信できる時期を Distributor に指示するだけです。

したがって、Channel の送信スケジュールの開始時に送信できるように Distribution の最初の構築または再構築が完了している必要があるという点で、構築スケジュールは送信スケジュールに依存します。また、構築後の Distribution を送信するには、送信スケジュールの開始を待つ必要があります。

送信スケジュールと抽出スケジュールの関係

送信スケジュールが開始されると、Distributor から Channel に登録している Subscriber サーバに対して、Channel に表示されている Distribution が送信されます。ただし、受信された Distribution は、Subscriber の抽出スケジュールが開始されるまで抽出されません。

したがって、Distribution の抽出は抽出スケジュールにのみ依存します。ただし、Distribution を抽出できる時期は送信スケジュールによって決定されます。つまり、抽出スケジュールは送信スケジュールに依存します。

送信された Distribution は抽出スケジュールが開始されるまで抽出およびインストールされないという点に限り、送信スケジュールは抽出スケジュールに依存します。これは、送信スケジュールだけでは Distribution を完全に処理できないことを意味します。

タイムゾーンとスケジュール設定

複数のタイムゾーンによってスケジュール設定作業が混乱する場合があります。次の節では、この種の問題について説明します。

- 348 ページの「タイムゾーンが異なる Tiered Electronic Distribution オブジェクトのスケジュール設定」
- 348 ページの「時差の計算」
- 350 ページの「地域をベースにした Channel の使用」

タイムゾーンが異なる Tiered Electronic Distribution オブジェクトのスケジュール設定

タイムゾーンのオフセットに関する次の情報は Channel オブジェクトを基準にしています。ただし、この情報はスケジュールを設定できるすべての Tiered Electronic Distribution オブジェクトに該当します。

Channel は特定のサーバに関連付けられていないツリー内のオブジェクトであるため、Channel の時間は、ConsoleOne® を実行し、Channel のスケジュールを設定するワークステーションのローカルタイムゾーンに常に設定されます。

たとえば、管理者がニューヨーク市に居住している場合、この管理者が同市からスケジュールを設定する Channel のローカル時間はニューヨーク時間になります。

この Channel とは異なるタイムゾーンの Distributor がこの Channel に Distribution を持っている場合、その Distributor はこの Channel のローカル時間のスケジュールに従って Distribution を送信する必要があります。たとえば、次のように入力します。

1. Channel のスケジュールをロサンゼルス時間の午前 1 時～午前 5 時に設定したとします。
2. ニューヨークで、このロサンゼルスの Channel に Distributor の Distribution を表示することを選択します。
3. ニューヨークでは、Distribution を午前 4 時～午前 8 時の間にのみ送信できます。ニューヨーク時間はロスアンゼルスよりも 3 時間進むために、ロサンゼルスの午前 1 ～ 5 時の時間帯はニューヨークの午前 4 ～ 8 時の時間帯になります。

Distributor が Distribution を送信できる正しいローカル時間を決定するには、タイムゾーンのオフセットを使用する必要があります。また、Channel のスケジュールによって Distribution を送信できる時期が決まるため、Distribution に設定した構築スケジュールが Channel のスケジュールよりも前に実行されることを確認する必要があります。

時差の計算

World Time Server (http://www.worldtimeserver.com) は、世界の 2 地点間の時差を確認できる Web サイトです。

このサイトを参照する場合は、次の点に留意してください。

- 左のフレームに表示される場所は、国または主要都市の別に表示できます。
- 国際日付変更線を基準にした現在の GMT 時間は、右のフレームに表示されます。

- 左のフレームで場所を選択すると、右のフレームに曜日、日付、標準時または夏時間の別、および GMT オフセットが表示されます。

このサイトを利用して 2 つの Tiered Electronic Distribution の場所間の時差を計算するには、次の手順に従ってください。

1 一方の Tiered Electronic Distribution サイトの場所を選択します。

2 表示される時間、曜日 / 日付、GMT オフセット、および夏時間であるかどうかを（後の参考のために）書き留めます。

3 別の Tiered Electronic Distribution サイトの場所を選択します。

4 表示される時間、曜日 / 日付、GMT オフセット、および夏時間であるかどうかを書き留めます。

5 スケジュールを調整するすべての Tiered Electronic Distribution の場所について、このプロセスを繰り返します。

6 収集した情報を使用して、Tiered Electronic Distribution の場所間の時差を計算します。

7 Tiered Electronic Distribution の異なる各場所でイベントがローカルに発生する時間を考慮し、時差を使用して適切なスケジュールを設定します。

例として、

- ハワイのDistributorがNew YorkのChannelにDistributionをリストする場合を考えます。
- World Time Server Web サイトを使用して、2 の場所間の時差が夏時間の実施中は -6 時間であることを確認できます。負の数値は時間が遅れることを意味します。したがって、ハワイの時間はニューヨークの時間から引き算すると、正しい時間を得られます。
- Channel の開始時刻がニューヨークで午前 1 時である場合は、ハワイの Distributor のスケジュールとして午後 7 時を選択します。
- 結果として、Distributor は Distribution の送信を午後 7 時に開始できます。
- ニューヨークでは夏時間を採用しているがハワイでは採用していないので、ニューヨークが標準時間に戻ったときの結果は午後 8 時になります。

ハワイの夜遅くに Distribution を送信する場合は、Channel の時間帯をニューヨークの午前 1 時よりも後に開始する必要があります。たとえば、次のように入力します。

- ハワイの午後 11 時に Distribution の送信を開始するとします。
- この場合、Channel の開始時刻をニューヨークの午前 5 時に設定する必要があります。

Channel のスケジュールを設定する場合は、どのオブジェクトの時間帯がより重要であるかを判断する必要があります。たとえば、Distributor にとってピーク時を避けた時間帯に Distribution を送信することがより重要である場合があります。したがって、ニューヨークとハワイの例で言うと、Distribution の送信をハワイ時間の深夜 0 時以降に開始するには、ニューヨークの Channel の開始時刻を午前 6 時以降に設定する必要があります。

地域をベースにした Channel の使用

タイムゾーンが異なる Subscriber があるときに、同じローカル時間（午前 3 時など）に Distribution を受信するように設定する必要がある場合は、地域をベースにした Channel を使用します。

Distribution に単一の Channel を使用した場合は、この Distribution を送信と同時に受信することしかできません。つまり、Subscriber がすべて同じタイムゾーンにあるわけではない場合、Distribution は別々のローカル時間に到着することになります。たとえば、次のように入力します。

1. Distribution_A が作成されて、Channel_A にリストされています。
2. Channel_A の送信スケジュールは、Distributor のローカル時間の午前 3 時に Distribution_A を送信するように設定されています。
3. Subscriber001 のタイムゾーンは Distributor と同じです。
4. Subscriber002 のタイムゾーンは、Distributor のタイムゾーンより 2 時間遅れています。
5. Subscriber001 と Subscriber002 は、Channel_A に登録されています。
6. Channel_A の送信スケジュールは、Distribution_A を所有する Distributor のローカル時間午前 3 時に開始されます。
7. Distribution_A は、Distributor のローカル時間午前 3 時に Subscriber001 および Subscriber002 に送信されます。
8. Subscriber001 は、Subscriber001 のローカル時間午前 3 時に Distribution を受信します。
9. Subscriber002 は、Subscriber002 のローカル時間午前 1 時に Distribution を受信します。

ただし、本来の意図は、これら両方の Subscriber それぞれのローカル時間の午前 3 時に Distribution_A が受信されるようにすることです。

Subscriber002 もローカル時間の午前 1 時ではなく午前 3 時に Distribution_A を受信するようにするには、次の手順に従ってください。

1. Subscriber002 を Channel_A から登録解除します。
2. Distribution_A の Channel_A2 を作成します。
3. Subscriber002 を Channel_A2 に登録します。
4. Channel_A2 の送信スケジュールを、Distributor のローカル時間の午前 5 時に Distribution_A を送信するように設定します。

次のように動作します。

1. Channel_A2 の送信スケジュールは、Distribution_A を所有する Distributor のローカル時間午前 5 時に開始されます。
2. Subscriber002 は、Subscriber002 のローカル時間午前 3 時に Distribution を受信します。

地域をベースにした Channel を使用することにより、Distributor は、同じ日の異なる時間に同じ Distribution を送信することができます。

[Randomly Dispatch During Time Period] オプションの使用

[Randomly Dispatch During Time Period] オプションは、各スケジュール (Distributor、Subscriber、Channel、および Distribution) で使用できます。このオプションは、[Daily]、[Monthly]、または [Yearly] の各スケジュールタイプに設定できる時間帯 (開始時刻と終了時刻) と組み合わせて使用します。

ランダムな実行では、スケジュール設定されたアクションが指定した時間帯の任意な時間に実行されます。これにより、サーバに対する負荷を分散できます。ただし、アクションをすぐに実行したい場合は、ランダムに実行されるスケジュールを設定していると混乱することがあります。

次の節では、[Randomly Dispatch] オプションに関する問題について説明します。

- 351 ページの「Distributor の更新スケジュールにおける [Randomly Dispatch] オプションの使用」
- 351 ページの「Distribution の構築スケジュールにおける [Randomly Dispatch] オプションの使用」
- 352 ページの「Channel の送信スケジュールにおける [Randomly Dispatch] オプションの使用」
- 352 ページの「Subscriber の抽出スケジュールにおける [Randomly Dispatch] オプションの使用」

Distributor の更新スケジュールにおける [Randomly Dispatch] オプションの使用

Distributor の更新スケジュールで [Randomly Dispatch] オプションを使用し、eDirectory からの Distribution の更新に伴う負荷を分散することができます。これにより、多数の Distributor が同時に eDirectory を読み込むことを避けてネットワークトラフィックを最小限に抑えることができます。

Distributor の更新スケジュールは、その Distributor に関連する Distribution の構築スケジュールおよび Channel の送信スケジュールと調整する必要があります。

Distributor の更新スケジュールは、Tiered Electronic Distribution の情報が eDirectory で更新される頻度を考慮して決定します。たとえば、新しい Distribution が作成される頻度、既存の Distribution オブジェクトのプロパティが変更される頻度、新しい Channel が追加される頻度などを考慮します。Distributor は、Tiered Electronic Distribution オブジェクトへの変更を検出するために、eDirectory を再読み込みする必要があります。eDirectory の更新は、構築スケジュールおよび送信スケジュールが開始される前に終了する必要があります。

重要： Distributor の更新間隔は最低 5 分とし、それより短くしないでください。Distribution の構築、eDirectory の複製、およびツリーの検索 (検索ポリシーが定義されていない場合) には、最大で 5 分を要する場合があります。

[Randomly Dispatch] オプションを使用する場合は、構築スケジュールと送信スケジュールの開始時刻を設定する際に更新スケジュールの終了時刻を考慮する必要があります。

Distribution の構築スケジュールにおける [Randomly Dispatch] オプションの使用

Distribution の構築スケジュールで [Randomly Dispatch] オプションを使用し、Distributor による Distribution の構築作業に伴う負荷を分散することができます。Distributor の Distribution 数が増大するほど、負荷を分散することが必要になります。

Distribution の構築スケジュールは、その Distributor の更新スケジュールおよび関連する Channel の送信スケジュールと調整する必要があります。Distribution の構築は、更新スケジュールの終了後に開始し、送信スケジュールの開始前に終了します。

重要： Distributor の更新間隔は最低 5 分とし、それより短くしないでください。Distribution の構築、eDirectory の複製、およびツリーの検索（検索ポリシーが定義されていない場合）には、最大で 5 分を要する場合があります。

[Randomly Dispatch] オプションを使用する場合は、構築スケジュールの開始時刻を設定する際に Distributor の更新スケジュールの終了時刻を考慮し、送信スケジュールの開始時刻を設定する際に構築スケジュールの終了時刻を考慮する必要があります。

Channel の送信スケジュールにおける [Randomly Dispatch] オプションの使用

Channel の送信スケジュールで [Randomly Dispatch] オプションを使用し、Subscriber に対する Distribution の送信をスケジュールの時間帯内でランダムに開始することができます。Channel に Distribution を持つ各 Distributor は、指定された開始時刻と終了時刻の間のランダムな時間を計算して、Distribution の送信を開始します。これにより、ネットワークの配布負荷を一定時間内で分散することができます。

たとえば、Distributor A および Distributor B の Distribution が Channel にあるとします。各 Distributor は、各自のランダムな時間を計算して Distribution の送信を開始します。

多数の Channel があり、すべての Channel にあるすべての Distribution を午後 10 時から午前 4 時までの 6 時間中に送信する場合なども、送信スケジュールで [Randomly Dispatch] オプションを使用できます。各 Channel で [Randomly Dispatch] オプションを使用すると、すべての Channel にある Distribution の送信時間をその 6 時間内で分散することができます。

[Randomly Dispatch] オプションを使用する場合は、送信スケジュールの開始時刻を設定する際に関連する各 Distribution の構築スケジュールの終了時刻を考慮し、すべての関連する Subscriber の抽出スケジュールの開始時刻を設定する際に送信スケジュールの終了時刻を考慮する必要があります。

Subscriber の抽出スケジュールにおける [Randomly Dispatch] オプションの使用

Subscriber の抽出スケジュールで [Randomly Dispatch] オプションを使用し、Subscriber での Distribution の抽出作業に伴う負荷を分散することができます。

[Randomly Dispatch] オプションを使用する場合は、抽出スケジュールの開始時刻を設定する際に、Subscriber が登録している Channel の送信スケジュールの終了時刻を考慮する必要があります。

アクションの繰り返し

[Repeat the Action Every] フィールドがあるスケジュールタイプの場合、このオプションの動作は他のスケジュールや Distributor による eDirectory の読み込み頻度などの他の要因に依存します。

例：

- Channel の送信スケジュールとして [Daily] を選択します。
- 送信の時間帯を午前 1:00 時から深夜 0 時 (23 時間) に設定します。
- [Repeat the Action Every] フィールドに繰り返す値として 1 時間を設定します。

アクション（Distribution の送信）は、次のように繰り返されます。

1. 午前 1:00 時に開始して 1 時間ごとに、Distributor は送信する Distribution をキューに入れます。
2. 送信中の Distribution については、送信が続行されます。
3. Distribution が送信されてキューからなくなると、Distributor は次のより新しいバージョンを送信キューに入れます。

   Distribution の前のバージョンが送信されずにキュー内に残っていた場合は、このバージョンの次に新しいバージョンがキューに挿入されます。つまり、送信中のバージョンの Distribution がある場合は、別のバージョン（最新のビルド）の Distribution が 1 つだけキューに挿入されます。

最新の Distribution が Subscriber にすでに存在する場合でも、Distributor は常に最新のバージョンを送信します。

スケジュール設定とサーバポリシー

すべてのポリシーでデフォルトスケジュール（パッケージスケジュール）が使用されます。ただし、このデフォルトスケジュールを特定のポリシーで変更した場合を除きます。デフォルトのパッケージスケジュールは、編集することができます。

以下の節を参照してください。

- 353 ページの「ポリシースケジュールと Distribution スケジュールの比較」
- 354 ページの「サーバポリシーのスケジュール設定」
- 354 ページの「デフォルトパッケージスケジュールの編集」

ポリシースケジュールと Distribution スケジュールの比較

スケジュール設定を要するポリシーでは、2 つの方法でスケジュールを設定できます。

- 個別のポリシースケジュール。このスケジュールは、ポリシーのプロパティで設定します。
- デフォルトのパッケージスケジュール。このスケジュールは、個別のスケジュールが設定されていないパッケージ内のすべての有効なポリシーに適用されます。

配布する必要があるポリシーについては、ポリシースケジュールと Distribution スケジュールの用途が異なります。

- **実行：** ポリシースケジュールは、ポリシーを実行できる時期を決定します。
- **Distribution:** ポリシーパッケージの Distribution スケジュールは、ポリシーパッケージを送信、受信、および抽出できるようにポリシーの Distribution を構築する時期を決定します。抽出後に、ポリシースケジュールはポリシーを実行できる時期を決定します。

つまり、Distribution スケジュールはポリシーの実行時期を直接は決定しません。ただし、Distribution スケジュールを Channel の送信スケジュールおよび Subscriber の抽出スケジュールと併用すると、ポリシーの実行を遅延させることができます。

サーバポリシーのスケジュール設定

個別のポリシーのスケジュールを設定するには

1 ConsoleOne で、ポリシーパッケージオブジェクトを右クリックし、[Properties] をクリックして、[Policies] タブを選択します。

2 ポリシーを選択し、[Properties] をクリックして、[Policy Schedule] タブを選択します。

3 [Schedule Type] フィールドでスケジュールを選択し、そのスケジュールを設定します。

412 ページの「曜日」
412 ページの「イベント」
413 ページの「間隔 (Interval)」
413 ページの「月」
413 ページの「Never」
413 ページの「パッケージスケジュール」
414 ページの「相対 (Relative)」
414 ページの「すぐに実行 (Run Immediately)」
414 ページの「Time」
415 ページの「週」
415 ページの「年」

重要： [Relative] スケジュールと [Run Immediately] スケジュールは、[Scheduled Down] ポリシーでは使用できません。

デフォルトパッケージスケジュールの編集

デフォルトパッケージスケジュールを編集するには

1 ConsoleOne で、ポリシーパッケージオブジェクトを右クリックし、[Properties] をクリックします。

2 [Edit] をクリックします。

3 [Schedule Type] フィールドでスケジュールを選択し、そのスケジュールを設定します。

412 ページの「曜日」
412 ページの「イベント」
413 ページの「間隔 (Interval)」
413 ページの「月」
413 ページの「パッケージスケジュール」
414 ページの「相対 (Relative)」
414 ページの「すぐに実行 (Run Immediately)」
414 ページの「Time」
415 ページの「週」
415 ページの「年」

9 変数

Novell® ZENworks® Server Management の変数については、次の節を参照してください。

- 355 ページの「変数の理解」
- 359 ページの「変数の種類」
- 361 ページの「変数の定義」
- 363 ページの「 iManager でのすべての変数の表示」
- 363 ページの「変数を使用した Subscriber のコンソールプロンプトの変更」
- 363 ページの「変数を使用したファイルの抽出の制御」

変数の理解

次の節を参照してください。

- 355 ページの「変数を使用する理由」
- 356 ページの「変数の使用」
- 358 ページの「変数の使用方法の違い」
- 358 ページの「使用する変数を決定する際の優先順位」
- 358 ページの「 Distribution の変数の例」

変数を使用する理由

Server Management で変数を使用することによって、さまざまなパス情報をより簡単に管理できるので時間を節約できます。たとえば、すべてのサーバの同じ場所に対する変更をグローバルに制御するには、スクリプト内のすべてのボリュームやドライブを表す変数を使用できます。

- 各サーバの Subscriber オブジェクトに変数を作成し、その変数の値を場所が存在するサーバのボリュームやドライブにします。
- スクリプトを実行すると、スクリプトは変数を各サーバに渡し、サーバは Subscriber オブジェクトのプロパティにある変数の定義から変数の値を判断します。
- この値は、適切な場所が含まれているボリュームやドライブを示します。

この情報として変数を使用することによって、スクリプト内で各サーバの名前とそのボリュームやドライブを個々にリストする必要がなくなりました。

変数を使用することによって、個々のサーバやサーバ上のソフトウェアに固有なものの参照が容易になります。たとえば、次のように入力します。

サーバ名
対象ボリュームまたはドライブ
作業ディレクトリ
DNS 名
IP アドレス
変更するテキストファイルの名前
実行するスクリプトの内容

これらはサーバごとに異なるデータである場合があります。変数によって、これらの違いを容易に処理できます。

変数の使用

- 356 ページの「変数の構文」
- 357 ページの「ネストされた変数」
- 357 ページの「リテラル % 記号」

変数の構文

変数は、名前、値、および使用の 3 つの部分を持つと考えることができます。それぞれの構文は次のとおりです。

名前の構文： *variable_name*

例　DEST

値の構文： *value_of_variable*

例　sys:

使用の構文： %*variable_name*%

例　%DEST%

したがって、変数 DEST はこの変数が定義されている特定のサーバでは sys: と同一と見なされます。

変数を定義する場合、変数の名前や値に % 記号は指定しません。ただし、変数を使用するときには、名前の前後に % 記号を使用します。

ソフトウェアでは、% 記号を使用して変数名の先頭と最後を識別します。たとえば、次のように入力します。

1. %DEST% はソフトウェアに DEST が変数名であることを通知します。
2. ソフトウェアは受信側のサーバ上の変数定義テーブルで DEST を検索し、その値を見つけます。
3. その値を使用して、パスの指定が完了します。

ネストされた変数

変数は任意のレベルでネストできます。たとえば、次のようにして対象の指定を自動化できます。

1. DEST を対象ボリュームおよびディレクトリとして定義します。
   - **変数名：** DEST
   - **値：** %VOL_DRV%%DIR%

     ここで、DEST 内に 2 つの変数をネストして値を設定しています。
   - **使用方法：** %DEST%
2. NetWare Subscriber で、VOL_DRV 変数を定義します。
   - **変数名：** VOL_DRV
   - **値：** *属性*

     たとえば、data: と指定します。
   - **使用方法：** %VOL_DRV%
3. NetWare Subscriber で、VOL_DRV 変数を定義します。
   - **変数名：** VOL_DRV
   - **値：** *属性*

     インストールされません。
   - **使用方法：** %VOL_DRV%
4. DIR 変数を定義します。
   - **変数名：** DIR
   - **値：** *属性*

     ¥apps などのディレクトリを指定します。
   - **使用方法：** %DIR%

この結果、対象を単に DEST と指定することができ、この変数は各ターゲットサーバで指定されているディレクトリとボリュームまたはドライブに解決されます。たとえば、次のように入力します。

NetWare Subscriber: data:¥apps

Windows Subscriber: c:¥apps

リテラル % 記号

% 記号は、ファイル名やディレクトリ名で有効な文字です。したがって、リテラル文字としての % 記号の使用を区別する必要があります。この区別を行わないと、ソフトウェアはネストされた変数名が指定されていると認識します。

リテラル文字の % を区別するには、変数の値に使用されている % 記号の直前にもう 1 つ % 記号を追加します。これによって、ソフトウェアは % 記号を変数の指示子ではなく、リテラル文字として認識します。たとえば、次のように入力します。

変数名： DEST

変数のパス： temp%abc%xyz

変数の値： temp%%abc%%xyz

最初の % によって、ソフトウェアは次の % 記号がパス名のリテラル部分であり、ネストされた変数名が続くことを示す指示子ではないことを認識します。2 つ連続した % 記号がない場合、"abc" はネストされた変数名として解釈されます。

変数の使用方法の違い

Tiered Electronic Distribution ポリシーでの変数の定義など、一般的な変数の定義では、何も定義されていない Subscriber 用のデフォルトの変数値が用意されています。Subscriber オブジェクトで定義された変数は、このようなデフォルトの変数値を上書きします。

Server Software Packages の場合、変数名の解決方法が異なります。

1. 変数が Server Software Package コンポーネントで定義された変数である場合は、その値が使用されます。

   重要： ソフトウェアパッケージで定義された変数は、Subscriber で定義されたすべての値を上書きします。

2. 変数が定義済みの変数である場合は、その値が使用されます。
3. 変数が Java 環境変数である場合は、その値が使用されます。

使用する変数を決定する際の優先順位

使用する変数を決めるために、変数は特定の順序で確認されます。順序は次のとおりです。

1. Server Software Packages [1]
2. Subscriber オブジェクト [1]
3. Tiered Electronic Distribution ポリシー [1]
4. デフォルト変数 [2]
5. 環境変数 [2]

[1] Server Management でユーザ定義
[2] 定義済み

変数は、最初に見つかった場所から使用されます。

Distribution の変数の例

変数を使用して、フルパスなど、Distribution を抽出する場所を指定することもできます。

たとえば、20 の Subscriber がある単一の Distribution があるとします。この Distribution を、Subscriber の各サーバ上の特定のボリュームに抽出するとします。ただし、ボリューム名はサーバによって異なり、15 台のサーバでは data: ボリュームを使用しており、5 台では vol1: を使用しています。

これらの Subscriber の一部では Distribution Volume 変数を編集して、vol1: を使用している 5 台の Subscriber 上の［Resolve To］フィールドを data: から vol1: に変更します。

この Distribution を抽出すると、20 台のサーバのそれぞれにおいて適切なボリュームに抽出されます。

変数の種類

変数には 2 つの種類があります。

- 359 ページの「定義済みの変数」
- 360 ページの「ユーザ定義変数」

定義済みの変数

定義済みの変数は ZENworks Server Management を起動したときに作成されます。定義済みの変数は、Server Software Packages および Tiered Electronic Distribution で使用され、ポリシーパッケージによって認識されます。

定義済みの変数は、サーバコンソールやこのマニュアルではすべて大文字で表示されていますが、大文字と小文字が区別されません。

構文：

%*predefined_variable_name*%

ここで、*predefined_variable_name* は Server Management によって定義された名前で、% 記号は変数名がこの記号で囲まれていることをソフトウェアに通知します。たとえば、次のように入力します。

%WORKING_PATH%

定義済みの変数を使用するには、その値を Server Software Package コンポーネントまたは Tiered Electronic Distribution オブジェクトで設定する必要があります。

Java 環境では、.ncf ファイルの Java プロセスコールで使用される SERVER_DN など、定義済みの変数を使用できます。

ポリシーパッケージで定義済みの変数を使用する例として、サーバダウンプロセスポリシーの Broadcast Message テキストがあります。このテキストにサーバ名の変数 (%SERVER_DN%) を含めることにより、ブロードキャストメッセージにサーバの名前を表示できます。

Server Management で利用できる定義済みの変数は次のとおりです。

変数	説明と値
BASE_PATH	Policy Manager の場所。 sys:¥zenworks¥pds¥smanager¥
CONF_PATH	環境設定ファイルの場所。 sys:¥zenworks¥pds¥ted¥
IP_ADDRESS	サーバの IP アドレス。たとえば、 192.68.1.255
LOAD_DIR	(NetWare® のみ) サーバのロード元のディレクトリ。 c:¥nwserver

変数	説明と値
LOG_PATH	ログファイルの場所。 sys:¥zenworks¥pds¥smanager¥
PLUGINS_PATH	Server Management プラグインがインストールされた場所。 sys:¥zenworks¥pds¥smanager¥plugins¥
POLICY_PATH	ポリシーファイル (.pol) が保存されている場所。 sys:¥zenworks¥pds¥smanager¥policy¥
PROP_PATH	Where Novell eDirectory™ オブジェクトのプロパティが保存されている場所。 sys:¥zenworks¥pds¥smanager¥prop¥
SERVER_DN	eDirectory 内の識別されたサーバ名。たとえば、 server01.servers.novell
SERVER_NAME	NetWare をインストールしたときにサーバに指定した名前。たとえば、 server01
TED_PATH	ノ¥ted ディレクトリへのパス。 sys:¥zenworks¥pds¥ted¥
TREE_NAME	Server Management サーバが存在する eDirectory ツリーの名前。これはインストール時に設定されます。
VOL	デフォルトのボリューム。 sys:
WORKING_PATH	Server Policies and Server Software Packages コンポーネントの作業ディレクトリ。 sys:¥zenworks¥pds¥smanager¥working¥
ZWS_PATH	ZENworks Web Server のファイルが保存されている場所。 sys:¥zenworks¥zws¥
ZWS_PROP_FILE_PATH	ZENworks Web Server のプロパティファイルが保存されている場所。 sys:¥zenworks¥zws¥
ZWS_SECURITY_PATH	ZENworks Web Server のセキュリティファイルが保存されている場所。 sys:¥zenworks¥zws¥security¥

ユーザ定義変数

ユーザ定義変数は、Server Software Package コンポーネント、Subscriber オブジェクト、および Tiered Electronic Distribution ポリシーで作成されます。ポリシーパッケージでは、ユーザ定義変数は認識されません。

ユーザ定義変数では大文字と小文字は区別されません。

構文：

%*variable_name*%

ここで、*variable_name* は変数を定義するときに指定した名前です。変数名には空白は使用できません。単語を区切るにはハイフン (-) またはアンダースコア (_) を使用します。

Subscriber オブジェクトで定義された変数は簡単なテキストの置き換えです。変数の値として入力したテキストが、変数名の代わりに使用されます。

変数の定義

変数は 3 つの場所で作成できます。

- 361 ページの「すべての Subscriber に関するデフォルトの変数の定義」
- 362 ページの「特定の Subscriber の変数の定義」
- 362 ページの「Server Software Package の変数の定義」

すべての Subscriber に関するデフォルトの変数の定義

Tiered Electronic Distribution ポリシーを使用して、すべての Subscriber に関するデフォルトの変数を定義できます。このポリシーですべての Subscriber のデフォルトとして設定した変数は、Subscriber で定義された同じ名前の変数によって上書きされます。362 ページの「特定の Subscriber の変数の定義」を参照してください。

デフォルトの変数を定義するには

1 ConsoleOne® で、SLP オブジェクトを右クリックし、[Properties] をクリックし、Tiered Electronic Distribution ポリシーのチェックボックスをオンにして有効にした後、[Properties] をクリックし、[Variables] タブを選択します。

2 [Add] をクリックします。

3 変数の名前を指定します。

名前には、ユーザ定義名、環境変数 (Java またはネイティブ)、または定義済みの変数を指定できます。

4 変数の値を指定します。

変数はこの値に解決されます。変数をネストするために、別の変数を指定することもできます。

抽出が確実に行われるようにするには、すべての Subscriber への絶対パスを指定します。たとえば、パスが data: ボリュームだけである場合でも、コロン (:) が含まれていることを確認します。コロンがフルパスに必要な部分であるからです。

5 説明 (省略可能) を入力し、[OK] をクリックします。

6 Subscriber に別の変数を定義するには、ステップ 2 からステップ 5 までを繰り返します。

7 デフォルトの変数を定義したら [OK] をクリックします。

8 Service Location Package のプロパティページで、[Associations] タブを選択します。

9 すべての Subscriber オブジェクトを含む関連付けがリストされていない場合は、[Add] をクリックします。

10 すべての Subscriber オブジェクトを含む eDirectory コンテナを参照し、[OK] をクリックします。

これによって、このポリシーはすべての Subscriber に強制的に適用されます。詳細については、213 ページの「Tiered Electronic Distribution」を参照してください。

11 [OK] をクリックして、ポリシーパッケージのプロパティを閉じます。

特定の Subscriber の変数の定義

1 ConsoleOne で Subscriber オブジェクトを右クリックし、[Variables] タブを選択します。

2 [Add] をクリックします。

3 変数の名前を指定します。

名前には、ユーザ定義名、環境変数 (Java またはネイティブ)、または定義済みの変数を指定できます。

変数の名前だけを入力します。使用時に変数に付ける % 記号は含めないでください。

4 変数の値を指定します。

変数はこの値に解決されます。変数をネストするために、別の変数を指定することもできます。

抽出が確実に行われるようにするには、Subscriber への絶対パスを指定します。たとえば、パスが data: ボリュームだけである場合でも、コロン (:) が含まれていることを確認します。コロンがフルパスに必要な部分であるからです。

5 説明 (省略可能) を入力し、[OK] をクリックします。

6 この Subscriber に別の変数を定義するには、ステップ 2 からステップ 5 までを繰り返します。

7 [OK] をクリックして、Subscriber のプロパティを閉じます。

Server Software Package の変数の定義

1 ConsoleOne でソフトウェアパッケージを右クリックし、[Variables] タブを選択します。

2 [Add] をクリックします。

[Variables] 列のデフォルトは [New Variable #1] です。

変数の名前だけを入力します。使用時に変数に付ける % 記号は含めないでください。

3 変数に別の名前を付ける場合は、(Backspace) キーを使用してデフォルト名を削除し、新しい変数名を入力した後、(Tab) キーを押します。

名前には、ユーザ定義名、環境変数 (Java またはネイティブ)、または定義済みの変数を指定できます。

4 変数の値を指定します。

変数はこの値に解決されます。変数をネストするために、別の変数を指定することもできます。

5 別の変数を定義するには、ステップ 2 からステップ 4 までを繰り返します。

6 [OK] をクリックして、Server Software Package のプロパティを閉じます。

iManager でのすべての変数の表示

Novell iManager では、Server Management オブジェクトによって使用されるすべての変数を表示することができます。

1 iManager で、ZENworks Server Management の役割の下にある [Remote Web Console] をクリックします。

2 Distributor オブジェクトまたは Subscriber オブジェクトを選択して、[OK] をクリックします。

3 [Display] リストボックスで [Policy/Package Agent] を選択します。

この操作により、[Configurations] タブが自動的に表示されます。

4 スクロールダウンして、[Variables] の右側にリストされる変数を確認します。

オブジェクトで使用できる変数がすべて表示されます。

変数を使用した Subscriber のコンソールプロンプトの変更

Subscriber では、PROMPT 変数の値をサーバコンソールプロンプトとして使用できます。

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、[Properties] をクリックします。

2 [Variables] タブを選択し、[Add] をクリックします。

3 [Variables] ダイアログボックスで、次のフィールドの情報を指定します。

[Variable]： 変数名として「PROMPT」と入力します。

値： 表示されるプロンプトのテキストを入力します。たとえば、「%SERVER NAME%」と入力すると、Subscriber は次のように表示します。

```
Provo_01 Subscriber >
```

[Description]： わかりやすい説明を入力します（省略可能）。

4 [OK] を 2 回クリックします。

変数を使用したファイルの抽出の制御

変数を使用して、Subscriber 上でファイルが抽出される場所を制御できます。任意の対象を、パーセント記号 (%) で囲むことによって、Subscriber オブジェクトで定義された変数として使用できます。

重要： Tiered Electronic Distribution ポリシーで指定された変数値がデフォルト値であり、Subscriber オブジェクトで設定された変数値によって上書きされます。

ファイルを抽出する場所の場合、抽出先のルートは [File Grouping] ダイアログボックスで destroot という名前のディレクトリとして指定されます。これは、ファイルを抽出する場所を決定するために Subscriber が使用する最上位レベルのディレクトリです。このダイアログボックスで、¥destroot ディレクトリの下にディレクトリのグループを構築できます。

抽出先を既知の場所（%APP_DIR% など）として指定できます。Subscriber オブジェクトの［Variables］タブをクリックし、この変数の値を指定できます。

例：

変数	値
APP_DIR	sys:¥apps

変数を使用して、ファイルを抽出する場所を設定するには

1 ConsoleOne で、Subscriber オブジェクトを右クリックし、［Properties］をクリックします。

2 ［Variables］タブを選択し、［Add］をクリックします。

3 変数の名前を指定します。

名前には、ユーザ定義名、環境変数（Java またはネイティブ）、または定義済みの変数を指定できます。

4 変数の値を指定します。

変数はこの値に解決されます。変数をネストするために、別の変数を指定することもできます。

抽出が確実に行われるようにするには、Subscriber への絶対パスを指定します。たとえば、パスが data: ボリュームだけである場合でも、コロン（:）が含まれていることを確認します。コロンがフルパスに必要な部分であるからです。

5 説明（省略可能）を入力し、［OK］を 2 回クリックして、プロパティを閉じます。

6 Distribution オブジェクトを新規作成します。

詳細については、125 ページの「Distribution の作成」を参照してください。

7 Distribution オブジェクトのプロパティで、［Type］タブを選択し、［Select Type ］ドロップダウンボックスで［File］を選択して、［New Target］をクリックします。

8 デフォルトの %DEST_VOLUME% を変数名に置き換えて、必要に応じて［OK］をクリックしてプロパティを閉じます。

デフォルトでは、［Destination］列に ¥dest_volume という名前のディレクトリが作成されます。このディレクトリを選択して、抽出先のルートを変更します。このディレクトリを選択するには、実際のディレクトリ名（destroot）を選択します。既知の場所を指定することも、パーセント記号で囲まれた変数を使用することもできます。

10 ZENworks Database

次の節では、Policy and Distribution Services で使用される Novell® ZENworks® Server Management データベースとその使用方法について説明します。

- 365 ページの「ZENworks データベースの理解」
- 368 ページの「必要なデータベースの数の決定」
- 371 ページの「Server Management データベースのインストールと接続」
- 374 ページの「ZENworks データベースオブジェクトの作成」
- 375 ページの「データベースのパージ」

ZENworks データベースの理解

次の節では、ZENworks データベースについて説明します。

- 365 ページの「データベースエンジン」
- 365 ページの「データベースファイル」
- 366 ページの「データベースオブジェクト」
- 366 ページの「データベースの実行」
- 366 ページの「データベースのキャッシュ」
- 366 ページの「データベース情報」
- 367 ページの「データベースの共存」

データベースエンジン

ZENworks Server Management には、Sybase データベースエンジンが付属しています。この製品は 1 台のサーバに 1 回だけインストールできます。ただし、Sybase は複数のサーバにインストールできます。

Oracle* および SQL はサポートされていません。

データベースファイル

Policy and Distribution Services では、zfslog.db という名前の Sybase データベースを使用します。Server Management は、通常、データベースがなくても機能します。これは、Policy and Distribution Services のレポーティングのための情報を記録するためにのみ zfslog.db を使用するからです。

zfslog.db は、通常、サーバ上の ¥zenworks¥pds¥db ディレクトリにあります。この場所は、インストールプログラムの実行に決定されます。NetWare® サーバと Windows サーバのどちらにも保存できます。

データベースオブジェクト

インストール時に、Novell eDirectory™ データベースオブジェクトが作成され、Server Management Database_*server_name* という名前が付けられます。インストール時に設定されている場合、このオブジェクトのプロパティに、データベースファイル (zfslog.db) の場所が表示されます。それ以外の場合、ZENworks データベースポリシー (SLP のプロパティパッケージ) を設定して、データベースオブジェクトを指定できます。情報を記録するためのデータベースファイルを見つけるには、この場所とポリシーが必要です。

データベースの実行

NetWare サーバでは、データベースは mgmtdbs.ncf ファイル (sys:¥system ディレクトリにある) を使用して実行され、このファイルは autoexec.ncf から実行されます。

Windows サーバでは、データベースは Novell Database - Sybase サービスを使用して実行されます。

データベースのキャッシュ

データベースファイルはサイズが非常に大きくなる場合があります。このため、データベースを実行しているサーバでは 32MB のキャッシュを推奨します。キャッシュによって、情報の zfslog.db への記録の頻度が減少し、サーバのパフォーマンスが向上します。

データベース情報

zfslog.db は、Policy and Distribution Services によって、Server Policies または Tiered Electronic Distribution コンポーネントの成功と失敗をログに記録するために使用されます。ポリシーの設定にしたがってポリシー情報を自動的にパージできます。Tiered Electronic Distribution の情報は、手動でデータベースオブジェクトからパージできます。パージの詳細については、375 ページの「データベースのパージ」を参照してください。

zfslog.db には環境設定情報は含まれていません。

次のような情報がエージェントによって zfslog.db に書き込まれます。

エージェント	情報
Policy/Package	失敗および成功したポリシー
	検出されたが適用できなかったポリシー
	Down Server ポリシーのステータス
	Server Software Packages およびコンポーネント

エージェント	情報
Distributor	Distribution のステータス ◆ 構築、送信、抽出された時刻 ◆ 構築および抽出の成功（および理由） ◆ 構築、送信、受信、および抽出の失敗（および理由） Subscriber のステータス リビジョン履歴

データベース情報に関するレポートの取得については、11 章 379 ページの「レポート機能」を参照してください。

データベースのデータの収集時に、情報は次のように提供されます。

- Distributor はそのルーティング階層にある各 Subscriber を把握しており、どの親 Subscriber が Distribution を受信したかを認識します。
- Distributor はどの Subscriber が特定のルートの最後にあるかを認識しており、階層の上位にある Subscriber が Distribution を受信できなかったために、Subscriber が Distribution を受信できなかったことを認識できます。
- Subscriber は、Distribution を受信したことを示すメッセージを直接 Distributor に送信します。Distributor は、Subscriber のメッセージを受信したことの確認を返信しません。
- Subscriber から "Successfully Received" メッセージが送信されたときに Distributor が実行されていない場合、この情報はデータベースに書き込まれません。メッセージの受信確認は Subscriber によって受信されないので、Subscriber はメッセージを再送信しません。

データベースの共存

ツリー内で複数の Server Management データベースを使用できます。データベースの数は、レポーティングを統合するかどうか、および WAN 環境でのネットワークトラフィックの増加に対応できるかどうかによって異なります。

統合されたレポーティングが不要である場合は、WAN セグメントごとに、異なるサーバに 1 つのデータベースファイルとオブジェクトをインストールできます。これによって、Distributor による WAN リンクを介したデータベースファイルの書き込みが回避されます。

データベースファイル用に選択したサーバについて、Policy and Distribution Services 用に ZENworks Server Management データベースが存在する場合、ZENworks Desktop Management データベースをインストールしないでください。Desktop Management データベースファイルによって、ZENworks Server Management データベースファイルが置き換えられるので、すべての ZENworks Server Management データベース情報が失われます。ただし、Desktop Management データベースが存在する場所に ZENworks Server Management データベースをインストールすることができ、この場合、Desktop Management データベース情報は失われません。

Management and Monitoring Services、Server Inventory、および Policy and Distribution Services のデータベースは、データベースファイルのファイル名が異なるので、1 台のサーバ上で共存できます。ただし、データベースオブジェクトにはそれぞれ異なる名前を付ける必要があります。これらのデフォルトのオブジェクト名はすべて ZENworks Database であるからです。

必要なデータベースの数の決定

データベースは NetWare サーバと Windows サーバの両方にインストールできます。

インストールプログラムは、Sybase エンジンのバージョンを確認した後、エンジンを更新します。Sybase エンジンが存在しない場合やバージョンが古い場合は、Sybase ソフトウェアがインストールされます。

重要： [Subscriber/Policies] オプションをインストールしているデータベースのサーバを選択していることを確認します。ZENworks Server Management ポリシー (Distributed Server Package) の [Purge Database] オプションが機能するのは、Policy/Package Agent ソフトウェアと zfslog.db ファイルが同じサーバ上にある場合だけです。

インストールプログラムでは、インストールされているデータベースのインスタンスごとに、データベースオブジェクトが自動的に作成されます。インストール時にそのオブジェクトのデータベースを選択できます。インストールプログラムを実行するたびに、データベースのインスタンスを 1 つだけインストールできます。データベースオブジェクトは、データベースファイル zfslog.db もインストールされているサーバのサーバオブジェクトと同じ eDirectory コンテナにインストールされます。

複数のデータベースファイルを使用するかどうかについては、次の節を参照してください。

- 368 ページの「データベースのログの記録と Tiered Electronic Distribution のレポーティング」
- 369 ページの「複数のデータベース」

データベースのログの記録と Tiered Electronic Distribution のレポーティング

Policy and Distribution Services は、Server Management データベースを使用しなくても正常に機能します。これは、レポート用の情報を記録するためにのみ zfslog.db ファイルを使用するからです。Policy and Distribution Services の zfslog.db には、環境設定情報は含まれていません。Distribution のステータス情報を取得するには、Novell iManager の ZENworks Server Management の役割で、[Tiered Distribution] ビューおよび [Remote Web Console] のオプションを使用します。(データベースファイルに書き込まれている) ポリシー情報は、Novell ConsoleOne® の [Tools] メニューから利用できる標準のレポートを介して取得できます。

Distributor Agent は、その配布のステータス情報 (構築、受信、抽出) および Server Software Package のインストール情報をデータベースファイル (zfslog.db) に書き込みます。Policy/Package Agent は、ポリシー適用の成功と失敗をこのデータベースファイルに書き込みます。このデータベースは、Policy and Distribution Services のレポートで使用されます。

書き込み先とするデータベースをエージェントが識別するためには、エージェントに対してポリシーを作成する必要があります。インストール時に設定されていない場合、ZENworks Database ポリシーで (SLP のプロパティパッケージを使用して) 関連付けることで、Distributor Agent は書き込み先を認識できます。ZENworks データベースポリシーは、Policy/Package Agent が書き込み先を識別できるように、Distributed Server Package を使用して Subscriber に配布されます。

Policy and Distribution Services には、Server Policies コンポーネント用に 6 つの定義済みレポートと、Tiered Electronic Distribution コンポーネント用に 4 つのレポートが用意されています。レポート情報は、データベースファイルのログに記録された情報から取得されます。次のようなレポートを利用できます。

Server Policies レポート	Tiered Electronic Distribution レポート
[Discovered Policies]	[Distribution Detail]
[Server Down Policy]	[Revision History]
[Packages]	[Revision History Failure]
[Failed Policies]	[Subscriber Detail]
[Successful Policies]	
[Unenforceable Policies]	

選択したレポートには、現在データベースに記録されている、該当する Server Policies または Tiered Electronic Distribution の情報がすべて表示されます。指定できるレポートの条件には、日付の範囲、特定の Distribution、Distribution のバージョンなどがあります。

特殊なレポートでは、複数のデータベースが必要になる場合があります。詳細については、370 ページの「利点」を参照してください。

レポーティングについては、11 章 379 ページの「レポート機能」を参照してください。

複数のデータベース

Policy and Distribution Services では、ツリーごとに、Server Management データベースの複数のインスタンスがサポートされています。ただし、ツリーごとに、データベースのインスタンスを 1 つだけインストールすることをお勧めします。次の節を参照してください。

- 370 ページの「利点」
- 370 ページの「Distributor オブジェクトのコンテキストと複数のデータベース」
- 371 ページの「複数のデータベースが必要であるかどうかの判断」

利点

データベースを 1 つだけ使用することの利点は、すべての Distributor Agent と Policy/Package Agent によって提供される Distribution 情報を 1 つのレポートに表示できることです。

たとえば、単一のレポートを使用すると、次のようなソフトウェアパッケージ情報を 1 つのレポートに含めることができます。

- Software Package Distribution の構築と送信に関する Distributor Agent の情報
- ソフトウェアパッケージの抽出とインストールに関する Policy/Package Agent の情報

複数のデータベースを使用することの利点は、次のとおりです。

- 低速な WAN リンク上のトラフィックの最小化

  たとえば、WAN リンクのサーバ側で Policy/Package Agent のログ用に別のデータベースを使用できます。

- 特殊なレポーティング用に個別データベースを提供

  たとえば、Distributor Agent（配布）用にデータベースが 1 つあり、Policy/Package Agent（ポリシー）用にデータベースが 1 つある場合、Software Package および Policy Package タイプの Distribution に関する構築および送信情報はデータベースの配布インスタンスに書き込まれ、ソフトウェアパッケージのインストールおよびポリシーの適用の情報はデータベースのポリシーインスタンスに書き込まれます。

Distributor オブジェクトのコンテキストと複数のデータベース

1 つの zfslog.db ファイルで複数の Distributor からのログエントリを受信することができ、Distributor は 1 つの zfslog.db ファイルにログを記録できます。理由は次のとおりです。

- Distributor Agent がデータベースファイルを検出するには、ZENworks データベースポリシー (Service Location Package) がデータベースオブジェクト（ファイルの場所とそのプロパティを格納する）を指す Distributor のオブジェクトよりも上の階層のコンテキストに関連付けられている必要があります。Distributor は、関連付けによってポリシーを受信します。
- 個別のデータベースを複数の Distributor サーバにインストールしている場合、各データベースにはデータベースを特定するための独自の ZENworks データベースポリシー（ファイルの場所を格納するデータベースのオブジェクトを指すポリシー）が必要です。
- Distributor オブジェクトを保持しているコンテナなど、特定のコンテキストに関連付けることができる Service Location Package（ZENworks データベースポリシーを格納する）は 1 つだけです。
- 特定のコンテキストに関連付けることができる Service Location Package は 1 つだけなので、複数の Distributor が個別のデータベースファイルに書き込むことができるようにするには、Distributor オブジェクトを異なるコンテキストにインストールする必要があります。各 Distributor には、それぞれの親コンテナに関連付けられたデータベースの場所ポリシーがそれぞれ必要です。

管理を容易にするために、通常すべての Distributor オブジェクトを配置するコンテナの下に、各オブジェクト用の個別のコンテナを作成することによって、Distributor オブジェクトを近い場所にまとめておくことができます。これによって、異なる Service Location Package を適切な Distributor の一意の親コンテナに関連付けることができます。

- すべての Distributor が同じデータベースファイルに書き込むようにするには、それぞれの Distributor オブジェクトを、Service Location Package を関連付けるコンテナの下の階層に配置します。すべての Distributor は、同じデータベースの場所ポリシーを使用します。

複数のデータベースが必要であるかどうかの判断

ツリー内にいくつのデータベースが必要であるかを判断するには、次の点を検討します。

- **WAN トラフィック：** Tiered Electronic Distribution は大量のデータベースの更新を実行しないので、システムリソースに対する実際の影響は最小限です。最も大きな影響は、トランザクションの実行にかかる時間です。ただし、WAN 接続が低速である場合、WAN を介してデータベースのログの記録を実行しないことも可能です。
- **複数の Distributor：** ツリー内に複数の Distributor がある場合、それぞれに 1 つのデータベースを使用することも、1 つ以上のデータベースを共有させることもできます。必要な Distributor のレポーティングのタイプによって、それぞれに個別のデータベースを使用するかどうかが決まります。たとえば、Distributor が、送信する Distribution のタイプ専用であるかどうかなどです。
- **統合されたレポーティング：** すべての Tiered Electronic Distribution 情報についてレポートを 1 つだけ生成する場合は、WAN トラフィックの注意事項に関係なく、データベースオブジェクトとファイルを 1 つだけインストールします。ZENworks データベースポリシー (Service Location Package) を使用して、すべての Distributor がそのデータベースファイルを使用するように指定します。
- **特殊なレポーティング：** サーバの特定の領域やグループに固有のレポートが必要になる場合があります。データベースオブジェクトとファイルをこのような各領域にインストールし、Distributor でその領域またはサーバグループのログをそのデータベースに記録することができます。個別の ZENworks データベースポリシー (Service Location Package) を使用して、各 Distributor が適切なデータベースファイルを使用するように指定します。

Server Management データベースのインストールと接続

ポリシーを適用するサーバ上に、Server Management データベースをインストールする必要があります。これは、ZENworks データベースポリシーを使用してデータベースファイル zfslog.db を見つけるために必要です。

Server Management データベースオブジェクトは、インストールプログラムを実行してデータベース用のサーバを選択すると、ツリー内に自動的に作成されます。

インストールプログラムでは、一度にデータベース 1 つだけをインストールできます。ツリーに別のデータベースを追加インストールするには、インストールするデータベースごとに次の各節の手順を実行する必要があります。

次の各節の手順を実行して、データベースをインストールおよび設定します。

- 372 ページの「データベースのインストール」
- 373 ページの「データベースへの接続」

データベースのインストール

Policy and Distribution Services データベースをインストールするには

1 ワークステーションに、*ZENworks 6.5 Server Management Program* CD を挿入します。

起動画面が表示されます。CD 挿入後、起動画面が自動的に表示されない場合は、CD のルートにある winsetup.exe を実行すると起動できます。

重要： リモート CD からのインストールは、ワークステーション上にその CD にマップされるドライブがない限り、サポートされません。たとえば、Windows サーバの CD ドライブに CD を挿入してワークステーションからインストールを実行する場合、ドライブをその Windows サーバの CD ドライブにマッピングしておく必要があります。

2 [Server Management] オプションを選択します。

3 [Policy-Enabled Server Management] をクリックして、インストールプログラムを起動します。

4 ソフトウェアの使用許諾契約に同意する場合は、[Accept] をクリックして [Next] をクリックすると、[Installation Type] ページが表示されます。同意しない場合は、[Decline] を選択し、[Cancel] をクリックして終了します。

5 [Installation Type] ページで、[Next] をクリックして新規インストールを実行し、[Installation Options] ページを表示します。

6 [Installation Options] ページで、[Next] をクリックしてデフォルトを受け入れ、[eDirectory Tree for Creating Objects] ページを表示します。

7 インストール先のツリーを参照して 1 つだけ選択し、[Next] をクリックします。

ツリー名では、大文字と小文字は区別されません。

8 [Server Selection] ページで、[Add] をクリックし、データベースのインストール先にするサーバを参照します。

インストールプログラムを 1 回実行するたびにサーバを 1 台だけ選択できます。

各 Distributor のデータベースがそれぞれの固有の情報を書き込むためのデータベースが必要になる場合があります。ただし、Distributor はデータベースを共有することができます。Distributor はすべての Tiered Electronic Distribution オブジェクトについてデータベースに情報を書き込むため、ネットワークトラフィックを最小化するにはデータベースを Distributor と同じサーバにインストールする必要があります。

重要： ポリシーをインストールしているデータベースのサーバを選択していることを確認します。[Purge Database] オプションは、zfs.ncf ファイルおよび zfslog.db ファイルが同じサーバ上にある場合に限り機能します。

9 [Additional Options] で、[Server Management Database] チェックボックスを選択して有効にし、[Next] をクリックして [File Installation Paths and Options] ページを表示します。

インストールプログラムにより、サーバにマウントされたすべてのボリュームについて、zfslog.db があるかどうかが確認されます。zfslog.db がない場合は、ファイルとデータベースオブジェクトの両方がインストールされます。zfslog.db がある場合でも、データベースオブジェクトはインストールされます。

10 [Next] をクリックしてデフォルトを受け入れ、[Database Settings] ページを表示します。

11 データベースファイルへのデフォルトのパスを変更するには、[Database Path] フィールドを編集します。

重要： データベースファイルはサイズが非常に大きくなる可能性があるため、NetWare のデフォルトのボリュームを、sys: からそのサーバ上の別のボリュームに変更することをお勧めします。

12 [Next] をクリックして [Database Settings] ページのその他のデフォルトを受け入れ、[Policy and Distribution Services Database Logging] ページを表示します。

13 前のインストールページで設定した Server Management データベースに関するログを指定するには、次のいずれかを選択します。

[Log to an Existing Server Management Database] : 関連付けるデータベースオブジェクトを参照して選択することにより、ログ対象の既存のデータベースファイルを選択します。

[Log to a Server Management Database That Will Be Installed] : 前のインストールページで設定したデータベースオブジェクト名がデフォルトになります。ただし、既存のデータベースオブジェクトを参照して選択することができます。

[Do Not Log to a Server Management Database]: 前のインストールページでデータベースを設定している場合でも、ここでデータベースにログを記録しないことを選択できます。

14 [Summary] ページで、選択内容を確認して [Finish] をクリックします。

インストールプログラムは、ファイルをコピーして、データベースオブジェクトをインストールします。

警告： [Cancel] をクリックした場合、インストールプログラムで実行した作業は何も保存されません。

インストールの終了後は、インストールに失敗したコンポーネントがないことをインストールログファイルで確認できます（ステップ 10 を参照してください）。

ZENworks データベースポリシーは、この新しいデータベースのインストール中に自動的に作成および設定されます。

15 373 ページの「データベースへの接続」に進みます。

データベースへの接続

Policy/Package Agent がデータベースに書き込みできるようにするには

1 サーバで、次に従ってエージェントをロードします。

サーバプラットフォーム	エージェントの起動方法
Windows:	1. [コントロール パネル] を開きます。 2. [管理ツール] をダブルクリックし、[サービス] をダブルクリックします。 3. [Click Novell ZENworks Service Manager] を右クリックし、[開始] をクリックします。
NetWare	**sys:\zenworks\pds\smanager\zfs.ncf**
Solaris または Linux	**/etc/init.d/Novell-ZfS Start**

エージェントがデータベースに接続されたことを示すメッセージが表示されることを確認します。

2 エージェントがデータベースに書き込んでいるかどうかを判断するには、次の操作を行います。

2a NetWare サーバのコンソールプロンプトで、エージェントのロード中にモニタを確認します。

エージェントがデータベースと接続されているかどうかを示すメッセージが表示されます。

2b エージェントがデータベースに接続されていないことを示すメッセージが表示された場合は、次の項目を確認します。

- データベースがサーバ上で稼動しているかどうか。
- [Policy/Distribution Management] タブを持つデータベースオブジェクトが、データベースファイルがインストールされているサーバで設定されているかどうか。
- データベースオブジェクトを指す有効な ZENworks データベースポリシーがあるかどうか。

ZENworks データベースオブジェクトの作成

誤って ZENworks データベースオブジェクトを削除した場合、この ZENworks データベースオブジェクトは存在しなくなっていることがあります。

データベースオブジェクトを当初からインストールしていないためにデータベースオブジェクトがツリーに存在しない場合は、GUI インストールプログラムを使用して作成する必要があります。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「インストールプログラムの起動」を参照してください。対象となるデータベースの作成に必要な手順とオプションのみを実行および選択します。

誤って削除したデータベースオブジェクトを再作成するには

1 ConsoleOne で、eDirectory ツリー内のデータベースオブジェクトを作成する場所を右クリックし、[New] > [Object] > [ZENworks Database] > [OK] の順にクリックします。

2 データベース名を指定します。

3 [Define Additional Properties] チェックボックスをオンにして、[OK] をクリックします。

4 [ZENworks Database] タブで、[Server DN] または [Server IP Address] のいずれかのオプションを選択します。

これらの場所の ID のいずれかが、すでにデフォルトになっている場合があります。デフォルトになっていない場合は、zfslog.db が存在しているサーバの情報を指定します。

5 [eDirectory Rights] タブを選択し、[Trustees of This Object] をクリックして [Add Trustee] をクリックし、[Public] を選択します。

データベースオブジェクトには Public のトラスティを割り当てる必要があります。このトラスティが割り当てられていない場合、Policy/Package Agent は、データベースに接続できない、または ZENworks Server Management ポリシーを読み込むことができないというメッセージを表示します。

6 [OK] をクリックします。

[Cancel] をクリックすると、どのタブで追加または変更した情報も保存されません。ただし、データベースオブジェクトはツリー内に残ります。

7 ZENworks データベースポリシーを設定します。

データベースの場所を指定する手順については、233 ページの「 ZENworks Database 」を参照してください。

8 Service Location Package を、Distributor オブジェクトが存在する場所よりも上のコンテナに関連付けます。

データベースのパージ

Policy and Distribution Services は、Server Policies または Tiered Electronic Distribution コンポーネントのすべての成功と失敗をログに記録するので、zfslog.db のサイズがすぐに大きくなる場合があります。したがって、このデータベースファイルを定期的にパージする必要があります。

次のデータベース情報のタイプによって、パージの方法は異なります。

- 375 ページの「 Tiered Electronic Distribution の情報」
- 375 ページの「サーバポリシー情報」

Tiered Electronic Distribution の情報

指定した日時よりも古いすべての Tiered Electronic Distribution 情報を、選択したデータベースから手動でパージするには

1 ConsoleOne で、データベースオブジェクトを右クリックし、[Purge] をクリックします。

2 [Purge Database] ダイアログボックスで、日時を選択し、[OK] をクリックします。

入力した日付よりも古いレコードがデータベースからパージされます。

パージが完了すると、パージに成功したことを示すダイアログボックスが表示されます。

サーバポリシー情報

ポリシー情報のパージは、ZENworks Server Management ポリシーの設定および次のどのイベントが発生するかによって自動的に実行されます。

- ポリシー情報をデータベースに書き込む Policy/Package Agent が実行されているサーバが再起動された場合。
- ポリシー情報をデータベースに書き込む Policy/Package Agent が実行されているサーバで、Server Management が再起動された場合。
- ポリシー情報をデータベースに書き込む Policy/Package Agent が実行されているサーバで、ZENworks Server Management コンソールのプロンプトから REFRESH コマンドを実行することによって、Policy/Package Agent が手動で更新された場合。

REFRESH コマンドや [Refresh] オプションによってデータベースがパージされるのは、データベースファイルが存在しているサーバ上で実行した場合だけです。

これらのいずれかのイベントが発生した場合、パージされるデータベースは関連付けられた Policy/Package Agent によって書き込まれていたデータベースです。

ポリシー情報のパージを設定するには

1 ConsoleOne で、次のいずれかの操作を行います。

- 情報パージするために、既存の Distributed Server Package（ステップ 5 を参照）で使用しているものとは異なるポリシーパッケージスケジュールを使用する場合は、ConsoleOne で、[File] > [New] > [Policy Package] の順にクリックし、[Distributed Server Package] を選択して、目的を示す名前を入力します。たとえば、Purge_Policy_*server_name* のように入力します。ここで、*server_name* は zfslog.db ファイルが存在しているサーバです。
- 他のポリシーが有効になっている同じポリシーパッケージを使用するには、ConsoleOne で既存の Distributed Server Package を右クリックし、[Properties] をクリックします。

  この場合には、ステップ 5 で、パッケージスケジュールとして [Run Immediately] を選択することをお勧めします。これによって、ステップ 3 で行う日数の変更は、次回パージがトリガされるときに直ちに有効になります。

2 Distributed Server Package で、ZENworks Server Management ポリシーのチェックボックスをオンにして、[Properties] をクリックします。

3 [ZENworks Server Management Configuration] タブを選択し、日数を選択します。

デフォルトは 100 日間です。指定した日数よりも古いレコードはパージされます。

適切なデータベースファイルのサイズを維持する数値を選択します。データベース内でポリシー関連の情報が増加する量は、このデータベースに書き込むサーバによってポリシーが実行される頻度によって決まります。データベースをパージする頻度に応じて、最適な日数を決定するために時間をかけて実験をしなければならない場合があります。

4 [OK] をクリックして、ポリシーのプロパティを閉じます。

5 パッケージのスケジュールを設定するには、次のいずれかの操作を行います。

- デフォルトのパッケージスケジュール [Run Event: System Startup] を受け入れる場合は、[OK] をクリックしてパッケージのプロパティを閉じます。
- デフォルトのスケジュールを変更する場合は、[Edit] をクリックし、スケジュールを選択し、[OK] を 2 回クリックしてパッケージのプロパティを閉じます。

  スケジュールの詳細については、238 ページの「ポリシーのスケジュール設定」を参照してください。

パッケージスケジュールによって、変更した環境設定がいつ有効になるかが決まります。たとえば、パッケージスケジュールとして以前に [Event: System Startup] を選択していた場合に、後で 100 日を 60 日に変更したとします。このとき、Policy/Package Agent を更新してパージをトリガしても、変更は認識されません。この変更が認識されるのは、システムが起動されたときだけです。

6 このポリシーの Policy Package Distribution を作成します。

詳細については、54 ページの「Distribution の作成と設定」を参照してください。

7 zfslog.db ファイルが保存されている Subscriber サーバに Distribution を送信します。

詳細については、57 ページの「Distribution の送信」を参照してください。

このポリシーパッケージがパージのための ZENworks Server Management ポリシー専用である場合、必要なことは、この Distribution をデータベースファイルが存在している各サーバにだけ送信することです。このポリシーのインスタンスはデータベースファイルごとに 1 つだけ必要であるためです。

11 レポート機能

Novell® ZENworks® Server Management には、Policy and Distribution Services コンポーネント用の定義済みのレポートが用意されています。

- 379 ページの「Policy and Distribution Services のレポーティングの理解」
- 381 ページの「レポートの説明」
- 386 ページの「レポートの生成」
- 387 ページの「カスタマイズしたレポートの作成」

Policy and Distribution Services のレポーティングの理解

次の節を参照してください。

- 379 ページの「レポーティングカテゴリ」
- 380 ページの「レポーティングスコープ」
- 380 ページの「レポートへのアクセス」
- 380 ページの「レポート情報の作成と保存」

レポーティングカテゴリ

Server Policies には 6 つの定義済みレポートがあり、Tiered Electronic Distribution は 4 つの定義済みレポートがあります。各定義済みレポートの詳細については、381 ページの「レポートの説明」を参照してください。

次の節では、Policy and Distribution Services のレポートの目的について説明します。

- 379 ページの「Server Policies レポートの目的」
- 379 ページの「Tiered Electronic Distribution レポートの目的」

Server Policies レポートの目的

Server Policies レポートには、どのサーバがどのポリシーを処理したか、ポリシーがいつ処理されたか、およびポリシーの適用が成功したかどうかの情報が表示されます。

Tiered Electronic Distribution レポートの目的

Distribution レベルのレポートには Distributor 側からのビューが示され、どの Subscriber が特定の Distribution の受信および抽出に成功したか、失敗したかを確認するのに便利です。Subscriber レポートは、単一の Subscriber がどの Distribution を受信したかを確認するために使用します。

レポートを使用することにより、どのノードが成功したかについての詳細情報を得ることができます。既知のすべてのエラー状況が捕捉され、エラー状況がデータベースにレポートされます。ただし、プロセスのステータスが実行中である場合、ノードで捕捉されないエラーや障害が発生することがあります。たとえば、コンピュータが停止したり、プロセスが強制終了されるなどです。

Distribution を受信しようとしなかった Subscriber（正しく設定されていない場合や実行されていない場合）では、レポートに情報が表示されません。予測される数値と実際の数値を比較して、レポートに示されていない Subscriber を検索できます。Subscriber が設定され、機能している場合、これは一般的な問題ではありません。

レポーティングスコープ

選択したレポートには、現在データベースに記録されている、該当する Server Policies または Tiered Electronic Distribution の情報がすべて表示されます。一部のレポートに表示される日付範囲などのデータの選択条件を定義したり、ポリシーパッケージオブジェクトや Tiered Electronic Distribution オブジェクトを選択したりするためのオプションがあります。

レポートへのアクセス

Policy and Distribution Services のレポートには、2 つのアクセスポイントがあります。

オブジェクト経由

1 ConsoleOne で、ZENworks データベースオブジェクトを右クリックします。

2 [Reporting] をクリックします。

Policy and Distribution Services の標準のレポートに関するレポートダイアログボックスが表示されます。

メニュー経由

1 ConsoleOne で、[Tools] > [ZENworks Reports] の順にクリックします。

2 [Reporting] をクリックします。

Policy and Distribution Services の標準のレポートに関するレポートダイアログボックスが表示されます。

レポート情報の作成と保存

Policy and Distribution Services データベースファイル (zfslog.db) は、レポート情報を保存するために使用されます。データベースをインストールして実行し、データが zfslog.db に配置されると、Policy and Distribution Services のレポーティングが有効になります。

各 Subscriber サーバで実行される Policy/Package Agent が Server Policies 情報をデータベースに書き込みます。Distributor Agent は、Tiered Electronic Distribution 情報および Server Software Package 情報をデータベースに書き込みます。

各 Distributor には通常はそれぞれ固有の ZENworks データベースオブジェクトおよびデータベースファイル (zfslog.db) があるため、選択された ZENworks データベースオブジェクトに関連付けられている特定の Distributor に関するレポート情報だけが提供されます。

次のアクションのいずれかが発生したときに、情報が Zfslog.db ファイルに記録されます。

- ZENworks データベースポリシー (Service Location Package) が設定されて有効になったとき (219 ページの「ZENworks Database」を参照)
- ZENworks データベースポリシー(Distributed Server Package) が設定されて有効になったとき (219 ページの「ZENworks Database」を参照)
- Policy/Package Agent がサーバコンソールから更新されたか、ZENworks Server Management が再起動されたとき

  Policy/Package Agent がデータベースファイルに情報を記録するためには、Subscriber サーバで ZENworks データベースポリシー (Distributed Server Package) を受信済みおよび抽出済みである必要があります。
- ZENworksデータベースポリシーが有効になった(Distributorオブジェクトのコンテナとの関連付けを含む) 後に、Distributor Agent が再起動されたとき (更新は行われないとき)

レポートの説明

次の節では、Policy and Distribution Services のレポートについて説明します。

- 381 ページの「Tiered Electronic Distribution レポート」
- 383 ページの「サーバポリシーレポート」

Tiered Electronic Distribution レポート

定義済みの Tiered Electronic Distribution レポートは 4 つあります。

- 381 ページの「Distribution Detail レポート」
- 382 ページの「Revision History レポート」
- 382 ページの「Revision History Failure レポート」
- 383 ページの「Subscriber Detail レポート」

Distribution Detail レポート

選択した Subscriber について Distribution の詳しい時系列的な履歴を表示します。次の項目が含まれます。

- 送信された Distribution
- 受信された Distribution
- 抽出された Distribution(開始時刻、終了時刻、完了コードを含む)

時刻によってソートされ、Distribution の名前とバージョンによってグループ化されます。

このレポートの条件は次のとおりです。

- **Subscriber:** Subscriber オブジェクトを選択した場合、[Subscriber] フィールドにそのオブジェクトが表示され、レポートにはこの Subscriber によって実行される受信および抽出アクションの情報だけが表示されます。親 Subscriber に関する情報では、[Received Stage] という見出しも表示されます。

  Database または Distribution オブジェクトを選択した場合、レポートには Distribution に関して実行されたすべてのアクションが含まれます。つまり、関連するすべての Subscriber の情報が表示されます。

- **[Latest Version Only]：** 指定した日付の範囲内のバージョンを含める場合は、選択を解除します。

- **[Select the Date Range Criteria for the Report]：** 範囲を指定します。

Revision History レポート

Distribution パッケージのバージョンの履歴を表示します。次の項目が含まれます。

- Distribution(パッケージの DN)
- Distributor(オブジェクトの DN)
- バージョン番号
- 作成日時
- Distribution のサイズ

バージョン番号によってソートされます。

このレポートの条件は次のとおりです。

- **Distribution:** Distribution オブジェクトを選択した場合、[Distribution] フィールドにそのオブジェクトが表示されます。データベースオブジェクトを選択した場合は、Distribution オブジェクトを参照する必要があります。

Revision History Failure レポート

作成中に失敗した Distribution のバージョンを表示します。次の項目が含まれます。

- Distribution(パッケージの DN)
- Distributor(オブジェクトの DN)
- 作成日時
- エラーの説明

バージョンによってソートされます。

このレポートの条件は次のとおりです。

- **Distribution:** Distribution オブジェクトを選択した場合、[Distribution] フィールドにそのオブジェクトが表示されます。データベースオブジェクトを選択した場合は、Distribution オブジェクトを参照する必要があります。

Subscriber Detail レポート

Distribution を受信した Subscriber のステータス情報を表示します。次の項目が含まれます。

- Distribution およびバージョン
- Subscriber（オブジェクトの DN）および Subscriber のアドレス
- チャネル名
- ソース（Distributor の DN）
- ステージ
- Status
- 日時
- エラーの説明

Subscriber/ 親 Subscriber によってソートされ、次にステージによってソートされます。

このレポートの条件は次のとおりです。

- **Distribution:** Distribution オブジェクトを選択した場合、[Distribution] フィールドにそのオブジェクトが表示されます。データベースオブジェクトを選択した場合は、Distribution オブジェクトを参照する必要があります。
- **[Version Number]：** Distribution の複数のバージョンが存在する場合、ドロップダウンメニューからバージョンを選択できます。[Select All] を選択すると、すべてのバージョンが含まれます。
- **[Distribution Stage]：** [All]、[Extract]、[Receive] のいずれかを選択できます。
- **[Distribution Status]：** [All]、[Success]、[Not Success] のいずれかを選択できます。

サーバポリシーレポート

すべてのサーバポリシーレポートについて、デフォルトの日付の範囲は現在の日付（深夜から深夜まで）になっています。

定義済みのサーバポリシーレポートは 6 つあります。

- 384 ページの「Discovered Policies レポート」
- 384 ページの「Server Down Process レポート」
- 384 ページの「Failed Policies レポート」
- 385 ページの「Packages レポート」
- 385 ページの「Successful Policies レポート」
- 386 ページの「Unenforceable Policies レポート」

Discovered Policies レポート

指定したパッケージ内でポリシーを検出したサーバを表示します。次の項目が含まれます。

- パッケージ (DN)
- サーバ (DN)
- サーバ名
- OS 名と OS のバージョン
- 検出の日時

パッケージによってソートされ、次にコンテキスト / サーバ名によってソートされます。ツリーの階層は維持されます。たとえば、myserver.servers.novell は novell、servers、myserver の順にソートされます。

このレポートの条件は次のとおりです。

- **[Package] :** ドロップダウンリストからポリシーパッケージを選択するか、[All] を選択します。
- **[Policy Type] :** [All]、[Server Down Process]、[Scheduled Down]、[SNMP Trap Targets]、[Community Strings]、[Set Parameters]、[Script]、[Text File]、[Scheduled Load/Unload]、[Database Location] のいずれかを選択できます。
- **[Select the Date Range Criteria for the Report] :** 範囲を指定します。

Server Down Process レポート

ツリー内のすべてのサーバまたは選択したサーバについて、サーバダウンプロセスポリシー情報を表示します。次の項目が含まれます。

- 各ポリシーの停止アクションおよびコード

サーバ名によってのみソートされます。

このレポートの条件は次のとおりです。

- **サーバ :** ドロップダウンリストからサーバを選択するか、[All] を選択します。
- **[Select the Date Range Criteria for the Report] :** 範囲を指定します。

Failed Policies レポート

ツリー内のすべてのサーバについて、失敗したすべてのポリシーを表示します。次の項目が含まれます。

- パッケージ (DN)
- サーバ (DN)
- サーバ名
- OS 名
- 失敗の日時
- 失敗の理由 (説明)

コンテキスト / サーバ名によってソートされます。ツリーの階層は維持されます。たとえば、myserver.servers.novell は novell、servers、myserver の順にソートされます。

このレポートの条件は次のとおりです。

- **[Package]：** ドロップダウンリストからポリシーパッケージを選択するか、[All] を選択します。
- **[Failure Type]：** [All]、[Failed]、[Unenforceable]、[Partial Enforcement] のいずれかを選択できます。
- **[Policy Type]：** [All]、[Server Down Process]、[Scheduled Down]、[SNMP Trap Targets]、[Community Strings]、[Set Parameters]、[Script]、[Text File]、[Scheduled Load/Unload]、[Database Location] のいずれかを選択できます。
- **[Select the Date Range Criteria for the Report]：** 範囲を指定します。

Packages レポート

Server Software Packages およびそのコンポーネントに関する情報を表示します。次の項目が含まれます。

- 各パッケージの成功ステータス
- 各コンポーネントの成功ステータス

コンテキスト / サーバ名によってソートされます。ツリーの階層は維持されます。たとえば、myserver.servers.novell は novell、servers、myserver の順にソートされます。

このレポートの条件は次のとおりです。

- **[Package]：** ドロップダウンリストからソフトウェアパッケージを選択するか、[All] を選択します。
- **サーバ：** ドロップダウンリストからサーバを選択するか、[All] を選択します。
- **[Select the Date Range Criteria for the Report]：** 範囲を指定します。

Successful Policies レポート

ツリー内のすべてのサーバについて、正常に適用されたすべてのポリシーを表示します。次の項目が含まれます。

- パッケージ (DN)
- サーバ (DN)
- サーバ名
- OS 名
- 実行の日時
- アクションコード

コンテキスト / サーバ名によってソートされます。ツリーの階層は維持されます。たとえば、myserver.servers.novell は novell、servers、myserver の順にソートされます。

このレポートの条件は次のとおりです。

- **[Package]：** 単一のポリシーパッケージを指定するか、[All] を選択できます。
- **[Success Type]：** [All]、[Change]、[No Change] のいずれかを選択できます。

- **[Policy Type]**：[All]、[Server Down Process]、[Scheduled Down]、[SNMP Trap Targets]、[Community Strings]、[Set Parameters]、[Script]、[Text File]、[Scheduled Load/Unload]、[Database Location] のいずれかを選択できます。
- **[Select the Date Range Criteria for the Report, From/To]**：範囲を指定します。

Unenforceable Policies レポート

ツリー内のすべてのサーバについて、サーバにエンフォーサがなかったために適用できなかったすべてのポリシーを表示します。次の項目が含まれます。

- パッケージ (DN)
- サーバ (DN)
- サーバ名
- OS 名と OS のバージョン

パッケージによってソートされ、次にサーバ名によってソートされます。

このレポートの条件は次のとおりです。

- **[Package]**：ドロップダウンリストからポリシーパッケージを選択するか、[All] を選択します。
- **[Select the Date Range Criteria for the Report]**：範囲を指定します。

レポートの生成

1 ConsoleOne で、ZENworks データベースオブジェクトを右クリックします。

ZENworks データベースオブジェクトは、[Policy/Distribution Management] タブ ([Inventory Management] タブではない) が適切に設定されたオブジェクトである必要があります。

2 [Reports] をクリックします。

3 レポートを選択します。

- サーバポリシーレポート

  [Discovered Policies]
  [Failed Policies]
  [Packages]
  [Server Down Process Policy]
  [Successful Policies]
  [Unenforceable Policies]

- Tiered Electronic Distribution レポート

  [Distribution Detail]
  [Revision History]
  [Revision History Failure]
  [Subscriber Detail]

4 レポーティングの条件を選択します。

レポーティングの条件や内容の詳細については、381 ページの「レポートの説明」を参照してください。

5 [Run Selected Report] をクリックします。

[View Report] ダイアログボックスを使用して、生成されたレポートを表示します。このダイアログボックスには、次の機能が用意されています。

- 画面に表示できるレポートの領域を拡大するには、ダイアログボックスのサイズを調整します。

  レポートは、印刷できるように横長の配置で表示されます。

- 次のナビゲーションオプションを使用して、そのレポートに関するページ間を移動します。

  [First Page]
  [Previous Page]
  [Next Page]
  [Last Page]
  [Go To Page]

- レポートを印刷するには、[File] > [Print] の順にクリックします。

  デフォルトのプリンタが選択されています。

- レポートをエクスポートするには、[File] > [Export Report] の順にクリックします。

  次の形式にエクスポートできます。

  [Text]
  [HTML]
  [PDF]
  [SDF]

カスタマイズしたレポートの作成

次のデータベース情報を使用して、Server Policies および Tiered Electronic Distribution コンポーネントのカスタムレポートを作成できます。

ただし、Subscriber または External Subscriber などの Tiered Electronic Distribution オブジェクトについては、Distribution やポリシーのステータスを確認するために、ZENworks レポーティングオプション（11 章 379 ページの「レポート機能」を参照）または iManager（2 章 69 ページの「Novell iManager」）を使用する必要があります。

データベースファイル（zfslog.db）には、次の情報が含まれます。

- 387 ページの「デフォルトの Sybase データベースのユーザ ID およびパスワード」
- 388 ページの「サーバポリシーデータベースの内容」
- 394 ページの「Tiered Electronic Distribution データベースの内容」

デフォルトの Sybase データベースのユーザ ID およびパスワード

Server Management に付属している Sybase データベース（zfslog.db）では、デフォルトのユーザ ID およびパスワードは次のとおりです。

ユーザ ID： dba

パスワード： sql

サーバポリシーデータベースの内容

サーバポリシーのデータベーステーブルの定義は次のとおりです。

SERVERS

Policy/Package Agent を実行する各サーバについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
SERVERID	integer	null 以外	自動的に割り当てられる一意の番号。
SERVERNAME	varchar	null 以外	コンソールプロンプトに表示されるサーバの短い名前。
SERVERDN	varchar		eDirectory 内のサーバオブジェクトの DN (ドット区切り)。
REVERSEDN	varchar	null 以外	逆の順序の SERVERDN。バックスラッシュ (¥) で区切られます。
OSNAME	varchar		オペレーティングシステムの名前。NetWare 5.1 など。
OSVERSION	char		オペレーティングシステムのバージョン。5.1、6.0 など。
TREENAME	varchar		サーバを含んでいる eDirectory ツリーの名前。

Primary key (SERVERID)

SERVERIP

Policy/Package Agent を実行する各サーバについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
SERVERIPKEY	integer	null 以外	自動的に割り当てられます。デフォルトは自動インクリメント。
SERVERID	integer	null 以外	SERVERS テーブルにリンクします。
IPADDRESS	varchar	null 以外	サーバの IP アドレス。

Primary key (SERVERID) REFERENCES SERVERS
Primary key (SERVERIPKEY)

PACKAGES

Policy/Package Agent が処理しようとしたソフトウェアパッケージの各バージョンについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
PACKAGEGUID	char	null 以外	自動的に割り当てられます。

フィールド名	Type	使用方法	
PACKAGENAME	char		.cpk ファイルまたはポリシーパッケージの名前。
PACKAGEDESC	char		Server Software Package コンポーネントに含まれている説明。
PACKAGEVERSION	char		ソフトウェアパッケージのバージョン。
BUILDDATE	integer		ソフトウェアパッケージがコンパイルされた日付。

Primary key (PACKAGEGUID)

POLICIES

各ポリシーまたはポリシーパッケージの組み合わせについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
POLICYID	integer	null 以外	グローバルに一意な ID。
POLICYDN	varchar		eDirectory ポリシーオブジェクトの DN。
POLICYPACKAGE	varchar		ポリシーが属しているポリシーパッケージの DN。
POLICYCLASS	varchar		ポリシーのクラスまたは型。定義については、389 ページの「POLICYCLASS の有効なエントリ」を参照してください。
POLICYTREENAME	varchar		ポリシーオブジェクトが存在しているツリーの名前。

Primary key (POLICYID)

POLICYCLASS の有効なエントリ

zenZFSServerDowningPolicy
zenZFSScheduleDownPolicy
zenZFSSetServerParamPolicy
zenZFSServerScriptPolicy
zenZFSTextFilePolicy
zenZFSScheduledRunPolicy
zenZFSZFSPolicy
zenZFSCommunityPolicy
zenZFSSNMPTrapTargetPolicy
zenZFSSMTPHostPolicy
zenZFSDatabaseLocationPolicy
zenZFSLicenseLocationPolicy
zenZFSTEDPolicy

POLICYACTION

実行される各アクションについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
POLICYACTIONKEY	integer	null 以外	自動的に割り当てられます。デフォルトは自動インクリメント。
POLICYID	integer	null 以外	POLICIES テーブルにリンクします。
SERVERID	integer	null 以外	SERVERS テーブルにリンクします。
CREATIONDATE	timestamp		アクションのタイムスタンプ。
DESCRIPTION	varchar		エラーを示す未定義の文字列。
CODE	integer		アクションの結果を表すコード。定義については、390 ページの「CODE の有効なエントリ」を参照してください。
ACTIONCODE	integer		実行されるアクション。定義については、390 ページの「ACTIONCODE の有効なエントリ」を参照してください。

Primary key (POLICYACTIONKEY)

CODE の有効なエントリ

RC_POL_SUCCESS	= 0
RC_POL_PARTIAL_SUCCESS	= 1
RC_POL_FAILURE	= -1
RC_POL_EMPTY	= 2

例外： ACTIONCODE フィールドの値が AC_POL_DOWN_CONNECTIONS または AC_POL_DOWN_DISCONNECTIONS である場合、CODE の値は現在のアクティブな接続の数、または強制切断の数のいずれかです。

CODE フィールドの値が 1 である場合は、次のいずれかを意味します。

- 部分的に成功した
- アクティブな接続が 1 つ存在する
- 強制切断が 1 つ行われた

これは、CODE フィールドのエントリの意味が、ACTION CODE フィールドの内容によって決まるためです。

ACTIONCODE の有効なエントリ

AC_POL_DISCOVERED	= 101
AC_POL_SCHEDULED	= 102
AC_POL_APPLIED	= 103

AC_POL_APPLIED_CHANGE	= 104
AC_POL_NO_ENFORCER	= 105
AC_POL_DOWN_CONNECTIONS	= 106
AC_POL_DOWN_DISCONNECTIONS	= 107
AC_POL_DOWN_UNLOAD	= 108
AC_POL_DOWN_EMAIL	= 109
AC_POL_DOWN_NOTIFY	= 110
AC_POL_DOWN_CANCELED	= 111
AC_POL_DOWN_IGNORED	= 112
AC_POL_DOWN_REQUESTED	= 113

PACKAGEACTION

Server Software Package に対して実行される各アクションについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
PACKAGEACTIONID	integer	null 以外	自動的に割り当てられます。デフォルトは自動インクリメント。
PACKAGEGUID	char	null 以外	PACKAGES テーブルにリンクします。
SERVERID	integer	null 以外	SERVERS テーブルにリンクします。
CREATIONDATE	timestamp		アクションのタイムスタンプ。
DESCRIPTION	varchar		定義については、391 ページの「DESCRIPTION の有効なエントリ」を参照してください。
CODE	integer		アクションの結果を表すコード。定義については、392 ページの「CODE の有効なエントリ」を参照してください。
ACTIONCODE	integer		実行されるアクションを表すコード。定義については、392 ページの「ACTIONCODE の有効なエントリ」を参照してください。
STARTEDPACKAGEACTIONID	integer		0 = パッケージの実行が開始されました。 または 新しいアクションがログに記録されると、0 の代わりに新しいアクションの PACKAGEACTIONID が格納されます。

Primary key (PACKAGEACTIONID)

DESCRIPTION の有効なエントリ

Started package
Finished rollback
Error description
Or it is empty

CODE の有効なエントリ

Success	= 0
Failure	= 1
Partial	= 2

ACTIONCODE の有効なエントリ

AC_PACKAGE_INSTALL	= 0
AC_PACKAGE_ROLLBACK	= 1
AC_PACKAGE_INSTALL_STARTED	= 2
AC_PACKAGE_ROLLBACK_STARTED	= 3

SOFTWARECOMPONENTACTION

各 Server Software Package コンポーネントについて 1 つのレコードを格納します。

フィールド名	Type	使用方法	
SOFTWARECOMPONENTACTIONKEY	integer	null 以外	自動的に割り当てられます。デフォルトは自動インクリメント。
PACKAGEACTIONID	integer	null 以外	PACKAGEACTION テーブルにリンクします。
NAME	char	null 以外	ソフトウェアコンポーネント名。
CREATIONDATE	timestamp		アクションのタイムスタンプ。
DESCRIPTION	varchar		説明がコンポーネントの作成時にユーザが指定した説明であるコンポーネントの最初のレコード。コンポーネントが終了する場合、説明は 392 ページの「DESCRIPTION の有効なエントリ」で定義されている説明のいずれかです。
CODE	integer		アクションの結果を表すコード。定義については、393 ページの「CODE の有効なエントリ」を参照してください。
ACTIONCODE	integer		実行されるアクションを表すコード。定義については、393 ページの「ACTIONCODE の有効なエントリ」を参照してください。

Primary key (SOFTWARECOMPONENTACTIONKEY)

DESCRIPTION の有効なエントリ

Did not meet requirements
Error processing requirements
Pre-install load/unload
Error pre-install load/unload
Pre-Installation Scripts
Error pre-install scripts

Copy file changes
Error processing copy file
Text File Changes
Error processing text files
NetWare SET Parameters
Error processing NetWare SET parameters
Registry process
Error processing Registry
NetWare products process
Error in NetWare products process
Post-install script process
Error in post-install script process
Post-install load/unload process
Error in post-install load/unload process

CODE の有効なエントリ

Success	= 0
Failure	= 1
Partial	= 2

ACTIONCODE の有効なエントリ

Started	= 200
Pre-Load	= 201
Pre-Scripts	= 202
Copy File Changes	= 203
Text File Changes	= 204
Set Parameters	= 205
レジストリ	= 206
Products.dat	= 207
Post Scripts	= 208
Post Load	= 209
Requirements	= 210

外部キー

外部キーはテーブル間の関係を設定します。

POLICYACTION

"add foreign key (POLICYID) references POLICIES (POLICYID)"

POLICYACTION

"add foreign key (SERVERID) references SERVERS (SERVERID)"

PACKAGEACTION

"add foreign key (PACKAGEGUID) references PACKAGES (PACKAGEGUID)"

PACKAGEACTION

"add foreign key (SERVERID) references SERVERS (SERVERID)"

SOFTWARECOMPONENTACTION

"add foreign key (PACKAGEACTIONID) references PACKAGEACTION (PACKAGEACTIONID)"

Tiered Electronic Distribution データベースの内容

Tiered Electronic Distribution のデータベーステーブルの定義は次のとおりです。

- 394 ページの「TAB_NODE」
- 395 ページの「TAB_CHANNEL」
- 395 ページの「TAB_DISTRIBUTION」
- 395 ページの「TAB_DIST_VERSION」
- 396 ページの「TAB_DIST_ACTION」
- 397 ページの「TAB_CHANNEL_DISTRIBUTION」
- 397 ページの「外部キー」

TAB_NODE

ツリー内の各 Distributor、Subscriber、および External Subscriber について 1 つのレコードを格納します。

フィールド名	Type	使用方法		
ID	numeric(8,0)	identity	null 以外	自動的に割り当てられる一意の番号。
NAME	varchar(255)		null 以外	Tiered Electronic Distribution オブジェクトの DN。
TYPE	char		null 以外	"D"=Distributor "T"=Subscriber (Transceiver)
NETWORK_ADDRESS	varchar(255)			サーバの IP アドレス。
SERVER_NAME	varchar(255)			現在使用されていません。

Primary key (ID)
Unique (NAME)

TAB_CHANNEL

ツリー内の各 Channel オブジェクトについて 1 つのレコードを格納します。

フィールド名	Type	使用方法		
ID	numeric(8,0)	identity	null 以外	自動的に割り当てられる一意の番号。
NAME	varchar(255)		null 以外	Channel オブジェクトの DN。

Primary key (ID)
Unique (NAME)

TAB_DISTRIBUTION

eDirectory 内の各 Distribution オブジェクトについて 1 つのレコードを格納します。

フィールド名	Type	使用方法		
ID	numeric(8,0)	identity	null 以外	自動的に割り当てられる一意の番号。
NAME	varchar(255)		null 以外	Distribution オブジェクトの DN。
DISTRIBUTOR_ID	numeric(8,0)		null 以外	TAB_NODE テーブルにリンクします。

Primary key (ID)
Unique (NAME)

TAB_DIST_VERSION

Distribution の各バージョンについて 1 つのレコードを格納し、TAB_DISTRIBUTION テーブルにリンクされます。

フィールド名	Type	使用方法		
ID	numeric(10.0)	identity	null 以外	自動的に割り当てられる一意の番号。
DISTRIBUTION_ID	numeric(8,0)		null 以外	TAB_DISTRIBUTION テーブルにリンクします。
VERSION	bigint		null 以外	バージョンのタイムスタンプ。
SIZE	integer		null 以外	distfile.ted (Distribution を格納しているファイル) のサイズ。
TIMESTAMP	datetime		null 以外	データベースにエントリが作成されたときのタイムスタンプ。
DIRECT_ROUTING	bit		null 以外	現在使用されていません。
LATEST_VERSION	bit		null 以外	Distribution の最新バージョン。再新バージョンを追跡するために内部的に使用されます。

Primary key (ID)
Unique (DISTRIBUTION_ID, VERSION)

TAB_DIST_ACTION

各 Distribution のバージョンについて、送信、受信、および抽出の複数のレコードを格納します。

フィールド名	Type	使用方法		
ID	numeric(12.0)	identity	null 以外	自動的に割り当てられる一意の番号。
DIST_VERSION_ID	numeric(10.0)		null 以外	TAB_DIST_VERSION テーブルにリンクします。
NODE_ID	numeric(8,0)		null 以外	次のタスクを実行するノードの TAB_NODE テーブルにリンクします。 Create Send Receive Extract Post process
TIMESTAMP	datetime		null 以外	アクションのログがデータベースに記録されたときのタイムスタンプ。
STAGE	char		null 以外	"C"=Create "S"=Send "R"=Receive "E"=Extract "P"=Post process
STATUS	char		null 以外	"S"=Success "F"=Failure "P"=In process
STATUS_TIMESTAMP	datetime		null 以外	レコードが更新されたときのタイムスタンプ。
REASON_TEXT	varchar(255)			成功または失敗の理由。定義については、396 ページの「REASON_TEXT の有効なエントリ」を参照してください。
CHANEL_DIST_ID	numeric(8,0)			TAB_CHANNEL_DISTRIBUTION テーブルにリンクします。

Primary key (ID)

REASON_TEXT の有効なエントリ

REASON_TEXT フィールドの有効なエントリは次のとおりです。

- "The Distribution was not received because this Subscriber does not meet the platform restrictions."

  文字どおりの内容です。

- "The Distribution was shut down before it was received."

  このメッセージが表示されるのは、2 つの状況のいずれかです。1)Subscriber 上に新しい設定があるため Distribution を受信する前に更新する必要がある場合、または 2) 署名の例外が発生した場合、たとえば、Subscriber が、信頼する Distributor からの Distribution を信頼できない場合などです。

- ″The Distribution was terminated before it was received.″

  管理上の理由で Distribution がキャンセルされました。

- ″There was an error receiving the Distribution.″

  予期していない何らかの処理に失敗しました。たとえば、ソケットの例外、トランスポートの例外などです。

TAB_CHANNEL_DISTRIBUTION

各 Channel/Distribution について 1 つのレコードを格納します。

フィールド名	Type	使用方法		
ID	numeric(8,0)	identity	null 以外	自動的に割り当てられる一意の番号。
CHANNEL_ID	numeric(8,0)		null 以外	TAB_CHANNEL テーブルにリンクします。
DISTRIBUTION_ID	numeric(8,0)		null 以外	TAB_DISTRIBUTION テーブルにリンクします。
TIMESTAMP	datetime		null 以外	Distribution が構築されたときのタイムスタンプ。

```
Primary key (ID)
Unique (CHANNEL_ID, DISTRIBUTION_ID)
```

外部キー

外部キーはテーブル間の関係を設定します。

TAB_DISTRIBUTION

```
″ add foreign key FK_TAB_DIST_REF_591_TAB_NODE (DISTRIBUTOR_ID)″ + ″ references
TAB_NODE (ID) on update restrict on delete restrict;″;
```

TAB_DIST_VERSION

```
″ add foreign key FK_TAB_DIST_REF_37_TAB_NODE (DISTRIBUTOR_ID)″ + ″ references
TAB_DISTRIBUTION (ID) on update restrict on delete restrict;″;
```

TAB_DIST_ACTION

```
″ add foreign key FK_TAB_DIST_REF_380_TAB_NODE (DIST_VERSION_ID)″ + ″
references TAB_DIST_VERSION (ID) on update restrict on delete restrict;″;
```

TAB_DIST_ACTION

```
″ add foreign key FK_TAB_DIST_REF_1525_TAB_NODE (NODE_ID)″ + ″ references
TAB_NODE (ID) on update restrict on delete restrict;″;
```

TAB_CHANNEL_DISTRIBUTION

```
″ add foreign key FK_TAB_DIST_REF_572_TAB_DIST (DISTRIBUTION_ID)″ + ″
references TAB_DISTRIBUTION (ID) on update restrict on delete restrict;″;
```

TAB_CHANNEL_DISTRIBUTION

″ add foreign key FK_TAB_DIST_REF_572_TAB_CHAN (CHANNEL_ID)″ + ″ references TAB_CHANNEL (ID) on update restrict on delete restrict;″;

A Distribution のタイプ

次の節では、Ditribution のタイプを設定する方法について説明します。

- 399 ページの「Desktop Application」
- 400 ページの「File」
- 402 ページの「FTP」
- 404 ページの「HTTP」
- 405 ページの「MSI」
- 408 ページの「ポリシーパッケージ」
- 409 ページの「RPM」
- 410 ページの「Software Package」

Desktop Application

このオプションを使用すると、ZENworks Desktop Management で作成されたアプリケーションで構成される Distribution を作成できます。

Desktop Application Distribuiton を作成するには

1 [Setup] ボタンをクリックします。

Desktop Application Distribution ウィザードが起動します。

初めてウィザードを起動して Desktop Application Distribution を作成した後は、[Setup] ボタンの名前が [Modify] に変更されます。

このウィザードの使用方法については、300 ページの「Desktop Application Distribution の作成」のステップ 7 を参照してください。

このウィザードを終了すると、[Current Configuration] フィールドに Desktop Application Distribution の現在の設定が表示されます。同じ情報は Desktop Application Distribution ウィザードの [Summary] ページにも表示されます。

2 Desktop Application Distribution の設定を変更するには、[Modify] をクリックします。

Desktop Application Distribution ウィザードが開き、表示された設定を変更できます。

File

Distributor のファイルシステム上に存在するファイルを Subscriber サーバのファイルシステムにコピーするとき、Distribution をこのようなファイルで構成するには、このオプションを使用します。

次のフィールドとボタンを使用して、File Distribution を設定します。

- 400 ページの「New Target」
- 400 ページの「Add Directory」
- 401 ページの「Add Files」
- 401 ページの「削除」
- 401 ページの「Synchronize Directories」
- 401 ページの「Verify Distributions」
- 402 ページの「Retry __ Times」
- 402 ページの「Kill Connection on Open Files」
- 402 ページの「Maintain Trustees」
- 402 ページの「Error Handling」

New Target

ターゲットファイルシステムで Distribution を抽出する場所です。

デフォルトは %DEST VOLUME% です。

重要： デフォルトを変更する場合は、(Enter) キーを押して変更を保存する必要があります。

すべての種類の変数や、実際の場所の名前を使用できます。リテラル文字による場所の例は次のとおりです。

- **[NetWare] :**
  sys:¥files
  data:¥files
- **[Windows] :**
  c:¥files
  ¥¥MyServer¥Files *（共有フォルダ）*
- **Linux または Solaris:**
  /usr/files

ただし、UNC パスは使用しないでください。すべての Distribution が 1 か所だけに送信される原因となります。代わりに、変数を使用します。詳細については、9 章 355 ページの「変数」を参照してください。

Add Directory

デフォルト名は New Directory です。この名前は、送信先のディレクトリ名に変更する必要があります。

重要： デフォルトを変更する場合は、(Enter) キーを押して変更を保存する必要があります。

このボタンを使用すると、ターゲット Subscriber のファイルシステムに追加するファイルおよびディレクトリのディレクトリ構造を作成できます。

Add Files

Distributor のファイルシステムで、ターゲット Subscriber のファイルシステムにコピーするディレクトリまたはファイルを参照します。

選択した各ディレクトリまたはファイルは、ソースファイルシステムのフルパスで表示されます。このパスは、ターゲットファイルシステムへのコピー時にディレクトリまたはファイルを取得する場所を指定します。ターゲットファイルシステムに作成されるのは、[New Target] ボタンと [Add Directory] ボタンを使用して作成されたパスだけです。[Add Files] ボタンで選択したディレクトリは、このパスの下に追加されます。

ディレクトリを選択すると、その下のすべてのファイルとサブディレクトリも選択され、コピーされます。Server Software Package の Copy File コンポーネントとは異なり、選択したディレクトリからファイルおよびサブディレクトリを削除できません。参照して追加したすべてのディレクトリは展開できません。削除できるのは、[Files To Be Distributed] ボックスのツリー構造に表示される項目だけです。

削除

[Files To Be Distributed] ボックスのツリー構造で選択したものだけが削除されます。

- [File]: ツリー構造からファイルを削除します（ハードディスクからは削除しません）。
- [Directory] : ツリー構造から、ディレクトリとそのディレクトリに属するファイルおよびサブディレクトリをすべて削除します。
- [Volume] : ツリー構造から、このボリュームのディレクトリとファイルをすべて削除します。

Synchronize Directories

ターゲットサーバのディレクトリが、Distribution に含まれるディレクトリと同期されるようにします。

警告： Distribution に含まれないディレクトリがターゲットサーバに存在する場合、これらのディレクトリとすべてのファイルおよびサブディレクトリは、Distribution の抽出時にターゲットサーバのファイルシステムから削除されます。

この機能は、特にターゲットディレクトリがルートディレクトリの場合は、大きな問題が発生することがあります。ディレクトリの同期は、Distribution に含まれない既存ディレクトリを意図的に削除する場合にのみ有効にしてください。

この Distribution の作成に使用されたファイルシステムを所有する Distributor が、Distribution に登録された Subscriber でもある場合、Distributor のファイルシステムは他の Subscriber と同様に処理されます。

同期の詳細については、180 ページの「File Distribution のディレクトリ同期の細分性」を参照してください。

Verify Distributions

ファイルの変更や追加など、Distribution が変更されるたびに新しいバージョンが構築され、Subscriber に送信されます。ただし、Subscriber は、新しいバージョンが送信されない場合でも、Distribution に含まれるファイルがすべての Subscriber に抽出され、インストールされていることを検証する必要があります。

この検証オプションを使用すると、送信スケジュールの開始時に新しいバージョンの Distribution が送信されない場合、ファイルを確実にインストールするために現在のバージョンを再抽出する要求を Distributor から Subscriber に送信するよう指定できます。

Retry __ Times

指定した回数だけロックされたファイルの上書きを再試行した後、ファイルの置換に失敗したことにします。このチェックボックスをオフのままにすると、ターゲットファイルシステム上のロックされたファイルは置換されません。

Kill Connection on Open Files

ロックされたファイルに上書きできるように、ロックされたファイルへの接続を強制終了しようとします。このオプションは、ファイルを抽出している場合にのみ適用され、Distribution を構築するためにファイルにアクセスしている場合には適用されません。Distribution を構築しているときに、Distribution に属するファイルがロックされている場合、構築は失敗します。

サーバと NLM™ の接続は強制終了できません。

Maintain Trustees

ターゲットファイルシステムの各ファイルのトラスティ属性を、ソースファイルシステムと同じになるように維持します。

追加のみが実行されます。ターゲットファイルシステムのトラスティは削除されません。

Error Handling

2 つのオプションがあります。

- **[Fail on Error]**：Distribution が停止するため、再送信前にエラーを修正できます。これはデフォルトの設定です。
- **[Continue on Error]**：エラーが発生した部分は終了されずに、Distribution の作成が続行されます。

FTP

このタイプでは、1 つまたは複数の FTP ソースのファイルで構成される Distribution を作成できます。各ソースには、1 つまたは複数のディレクトリやファイルを含めることができます。

抽出時にターゲットファイルがロックされている場合、Subscriber はファイルをコピーできなかったことを示す例外処理を実行します。Distributor はこの情報を Subscriber から受信し、エラーをレポーティングデータベースに記録します。

次のフィールドとボタンを使用して、FTP Distribution を設定します。

- 403 ページの「New FTP Source」
- 403 ページの「New Target」
- 403 ページの「Add Directory」

- 403 ページの「Add Files」
- 403 ページの「削除」
- 403 ページの「プロパティ」
- 403 ページの「Files To Be Distributed」
- 404 ページの「Binary Transfer」
- 404 ページの「Include Symbolic Link Files」

New FTP Source

[FTP File Group] ダイアログボックスに、サーバ名、ログイン名（デフォルトは「anonymous」）、およびこの FTP Distribution のパスワードを指定します。

New Target

ボリュームを指定します。デフォルトは、変数 %DEST VOLUME% です。

Add Directory

ファイルが存在するディレクトリを参照します。ディレクトリに親ディレクトリがある場合は、その親ディレクトリも含まれます。複数のディレクトリを追加できます。

このフィールドに情報を入力するときは、(Enter) キーを押して変更を保存する必要があります。

Add Files

ファイルを参照します。複数のファイルを追加できます。

削除

選択したものをすべて削除します。

- [File]：ツリーからファイルを削除します (FTP からは削除しません)。
- [Directory]：ツリーから、ディレクトリとそのディレクトリに属するファイルおよびサブディレクトリをすべて削除します。
- [Volume]：ツリーから、このボリュームのディレクトリとファイルをすべて削除します。

プロパティ

選択した FTP ソースのプロパティを表示します。

Files To Be Distributed

パスとファイル名を示す展開可能なツリー構造です。

Binary Transfer

バイナリ形式でのファイル転送を有効にします。

Include Symbolic Link Files

追加したディレクトリのシンボリックリンクファイル（すべてのサブディレクトリからのファイルも含む）がすべて FTP Distribution に含まれるようにする場合は、このボックスを選択します。これは、ディレクトリを追加したときのみ適用されます。

個別に追加したシンボリックリンクファイルについては、このボックスを選択する必要はありません。

このチェックボックスでは、ディレクトリとファイルを参照して追加するときに、シンボリックリンクファイルの表示について制御できません。

HTTP

このタイプでは、1 つまたは複数の HTTP ソースで構成される Distribution を作成できます。各ソースには、1 つまたは複数のターゲットエントリを含むことができます。

抽出時にターゲットファイルがロックされている場合、Subscriber はファイルをコピーできなかったことを示す例外処理を実行します。Distributor はこの情報を Subscriber から受信し、エラーをレポーティングデータベースに記録します。

次のフィールドとボタンを使用して、Distribution を設定します。

- 404 ページの「New Target」
- 404 ページの「Add Directory」
- 404 ページの「Add Files」
- 405 ページの「削除」
- 405 ページの「Files To Be Distributed」

New Target

ボリュームを指定します。デフォルトは、変数 %DEST VOLUME% です。

Add Directory

ファイルが存在するディレクトリを参照します。ディレクトリに親ディレクトリがある場合は、その親ディレクトリも含まれます。複数のディレクトリを追加できます。

このフィールドに情報を入力するときは、(Enter) キーを押して変更を保存する必要があります。

Add Files

ファイルの URL を指定します。複数のファイルを追加できます。

削除

選択したものをすべて削除します。

- [File] : ツリーからファイルを削除します (HTTP からは削除しません)。
- [Directory] : ツリーから、ディレクトリとそのディレクトリに属するファイルおよびサブディレクトリをすべて削除します。
- [Volume] : ツリーから、このボリュームのディレクトリとファイルをすべて削除します。

Files To Be Distributed

パスとファイル名を示す展開可能なツリー構造です。

MSI

MSI(Microsoft Software Installer) パッケージを Windows ベースのアプリケーション用 Windows サーバに配布します。MSI エンジンは、MSI Distribution に含まれる Windows ソフトウェアのインストールに使用されます。MSI Distribution は、ConsoleOne と iManager の両方で作成および設定できます。

次のいずれかを使用して、Distribution を設定します。ト

- 405 ページの「追加」
- 405 ページの「削除」
- 405 ページの「設定」
- 408 ページの「並べ替え」

追加

次のいずれかを使用して、1 つまたは複数の MSI または MSP パッケージを追加します。

[Add From Distributor] : .msi ファイルと .msp ファイルは、この MSI Distribution を所有する Distributor サーバのファイルシステムに保存されている必要があります。

[Add From FTP Site] : .msi ファイルと .msp ファイルは、FTP サイトから取得できます。

削除

リストから MSI パッケージを選択し、[Remove] をクリックしてリストから削除します。

設定

各 MSI パッケージを設定するには、[Selected Packages] 列でパッケージを選択し、[Edit Parameter List] をクリックして [Edit Parameters] ダイアログボックスを開き、次のフィールドに入力します。

- 406 ページの「[Distribution Includes Box]」
- 406 ページの「[Options] ボックス」
- 407 ページの「[Transforms Box]」
- 408 ページの「[Custom Parameters] フィールド」
- 408 ページの「[Command] フィールド」

[Distribution Includes Box]

次のオプションのいずれかを選択します。

[Package File Only]：MSI パッケージのみが Distribution に含まれます。

[Package Files and Folders]：MSI パッケージ、同じフォルダ内のすべてのファイル、すべてのサブフォルダとそのファイルが含まれます。これは、MSI パッケージに必要なすべてのサポートファイルが、このフォルダおよびサブフォルダに含まれていることを前提としています。

[Options] ボックス

次のオプションから選択します。

[Install]：MSI パッケージがインストールされます。

[Uninstall]：MSI パッケージがアンインストールされます。

[Patch]：このフィールドは MSP パッケージにのみ適用されるため、淡色表示になっています。

[Administrative Install]：(標準の方法として)MSI パッケージを削除せずに MSI パッケージがインストールされるため、自己修復に使用できます。このオプションは、パッケージの管理イメージと組み合わせて使用されます。詳細については、『InstallShield Tip from AdminStudio (http://www.installshield.com/news/newsletter/0302-articles/setupexe.asp)』を参照してください。

[Repair]：このオプションを選択した場合は、次のいずれかのチェックボックスを選択します。これは、MSI エンジンに渡して修正の種類を指定する共通 MSI フラグです。

- [Missing File]：失われているファイルがある場合のみ、そのファイルを再インストールするように Windows Installer に指示します。
- [Older File]：ファイルが失われている場合、またはインストールされているファイルのバージョンが MSI パッケージに含まれているバージョンより古い場合に、そのファイルを再インストールするように Windows Installer に指示します。
- [Equal or Older File]：ファイルが失われている場合、またはインストールされているファイルのバージョンが MSI パッケージに含まれているバージョンと同じか古い場合に、そのファイルを再インストールするように Windows Installer に指示します。
- [Force All]：すべてのファイルを再インストールするように Windows Installer に指示します。
- [Use Registry Keys]：ユーザごとのエントリすべてを、MSI パッケージから Windows のシステムレジストリに記述し直すように Windows Installer に指示します。ユーザごとのエントリとは、HKEY_CURRENT_USER レジストリハイブおよび HKEY_USERS レジストリハイブに含まれているエントリです。

- [Computer Registry Keys]：コンピュータごとのエントリすべてを、MSI パッケージから Windows のシステムレジストリに記述し直すように Windows Installer に指示します。コンピュータごとのエントリとは、HKEY_LOCAL_MACHINE レジストリハイブおよび HKEY_CLASSES_ROOT レジストリハイブに含まれているエントリです。
- [Failed Checksum]：ファイルが失われている場合、またはファイルが破損していることがチェックサムで検証された場合、すべての実行可能ファイルに対するチェックサムを実行してファイルを再インストールするように Windows Installer に指示します。MSI パッケージの File Table の Attributes 列に msidbFileAttributesChecksum があるファイルのみが修復されます。
- [Install and Re-Cache]：ソースパッケージではなく、再キャッシュ（ローカル）ソースからファイルをインストールするように Windows Installer に指示します。
- [Shortcuts]：MSI アプリケーションのショートカットを再インストールして既存のショートカットやアイコンを上書きするように Windows Installer に指示します。
- [Different File Version]：ファイルが失われている場合、またはインストールされているファイルのバージョンが MSI パッケージに含まれているバージョンと異なる場合に、そのファイルを再インストールするように Windows Installer に指示します。

[Transforms Box]

Distribution に変換を含めるには、変換する MSI パッケージ (MSP パッケージではない）を選択し、[Edit Parameters] ボタンを選択して、次の操作を実行します。MSI パッケージの変換ごと、および MSI パッケージごとに、必要に応じてこれらの手順を繰り返します。

- 407 ページの「追加」
- 407 ページの「削除」
- 407 ページの「並べ替え」

追加

次のいずれかを使用して、1 つまたは複数の変換を追加します。

[Add From Distributor]：.msi ファイルは、この MSI Distribution を所有する Distributor サーバのファイルシステムに保存されている必要があります。

[Add From FTP Site]：.msi ファイルは、FTP サイトから取得できます。

変換ファイルは、[Type] タブの [Selected Packages] 列で選択した MSI パッケージの動作を変更するために使用されます。

複数の変換が同じ MSI パッケージプロパティに適用されると、そのプロパティは、最後に適用された変換によって適用された値を保持します。

変換の作成と設定の詳細については、ソフトウェアアプリケーションに付属のマニュアルを参照してください。

削除

リストから変換を選択し、[Remove] をクリックしてリストから変換を削除します。

並べ替え

[Up] ボタンと [Down] ボタンを使用して、変換が適用される順序を並べ替えます。

実行順序を並べ替えるときは、MSP パッケージが特定の MSI パッケージにパッチを適用することを考慮して、MSP パッケージが MSI パッケージの後に配置されるようにしてください。

[Custom Parameters] フィールド

MSI パッケージに記載されたコマンドラインパラメータを変更できます。

一部の MSI Distribution は、Windows 2000 サーバでは抽出できない場合があります。この問題を解決するには、118 ページの「MSI Distribution の抽出エラー」を参照してください。

[Command] フィールド

このフィールドは表示専用です。

このフィールドに表示されるパラメータは、[Parameters] ダイアログボックスを最初に表示したときのデフォルトのオプションです。[Distribution Includes]、[Options]、または [Transforms] ボックスでオプションを変更した場合、または [Custom Parameters] フィールドにパラメータを追加した場合、これらのパラメータは自動的に更新されます。

並べ替え

[Up] ボタンと [Down] ボタンを使用して、MSI パッケージが適用される順序を並べ替えます。

ポリシーパッケージ

このオプションを使用すると、有効化され設定済みのポリシーを含む 1 つまたは複数のポリシーパッケージで構成される Distribution を作成できます。

External Subscriber オブジェクトを使用して Policy Package Distribution を Subscriber に送信するには、agentinfo.properties ファイルを編集して、信頼されるツリーでのエラーの発生を防ぐ必要があります。詳細については、165 ページの「Policy Package Distribution 送信時に信頼されるツリーで発生するエラーの回避」を参照してください。

特定のポリシーの作成については、4 章 197 ページの「Server Policies（サーバポリシー）」を参照してください。

次のフィールドとボタンを使用して、Distribution を設定します。

- 408 ページの「Up/Down」
- 409 ページの「Add」
- 409 ページの「削除」
- 409 ページの「プロパティ」
- 409 ページの「The Following Policy Packages Will Be Distributed」

Up/Down

ポリシーパッケージのインストール順序を並べ替えます。

Add

ポリシーパッケージを Distribution に追加します。

削除

ポリシーパッケージをリストから削除します。

プロパティ

選択されたポリシーパッケージのプロパティが表示されます。表示されたプロパティは編集できます。

The Following Policy Packages Will Be Distributed

配布されるポリシーパッケージと配布順序が表示されます。

RPM

Tiered Electronic Distribution を使用して Linux または Solaris サーバ向けに作成した Red Hat Package Manager (RPM) パッケージを配布できます。

次のフィールドとボタンを使用して、Distribution を設定します。

- 409 ページの「Up/Down」
- 409 ページの「Add From Distributor」
- 409 ページの「Add From FTP Site」
- 409 ページの「削除」
- 410 ページの「Selected Packages」
- 410 ページの「Installation Parameters」

Up/Down

RPM パッケージのインストール順序を並べ替えます。

Add From Distributor

Distributor のファイルシステムを参照して、RPM パッケージを選択します。

Add From FTP Site

FTP サイトを参照して RPM パッケージを選択します。

削除

選択した RPM パッケージをリストから削除します。

Selected Packages

追加した RPM パッケージが表示されます。

Installation Parameters

追加した RPM インストールパラメータが表示されます。

パラメータを入力する際の重要事項

- テキストフィールドにパラメータを入力したときは、(Enter) キーを押す必要があります。押さない場合、その入力は保存されません。
- いったん入力した 1 つのパラメータは削除できません。削除する必要がある部分を除外したそのパラメータ文字列全体を再入力する必要があります。
- パラメータの大文字と小文字を変更してその変更を認識させることはできません。代わりに、パラメータをいったん別の文字に変更したうえで、目的の大文字または小文字を使って元の文字に戻します。

Software Package

このオプションを使用すると、Distribution が、ConsoleOne の Server Software Package ネームスペースで作成された 1 つまたは複数のソフトウェアパッケージから構成されるようにできます。

旧バージョンの .spk および .cpk ファイルを ZENworks 6.5 Server Management に変換する方法については、275 ページの「古いバージョンの Server Software Package の ZENworks 6.5 Server Management への変換」を参照してください。

次のフィールドとボタンを使用して、Distribution を設定します。

- 410 ページの「Up/Down」
- 410 ページの「Add」
- 410 ページの「削除」
- 410 ページの「Selected Software Packages」

Up/Down

ソフトウェアパッケージのインストール順序を並べ替えます。

Add

ソフトウェアパッケージを Distribution に追加します。

削除

ソフトウェアパッケージをリストから削除します。

Selected Software Packages

配布されるソフトウェアパッケージと配布順序が表示されます。

B スケジュールタイプ

次の表では、各スケジュールタイプの説明とそれぞれの設定手順へのリンクを示します。

スケジュールタイプ	説明
Daily	スケジュールされた項目を毎日実行します。[Daily] には、実行時間帯の指定、時間帯内でのランダムな実行、および *xxx* 時間または分ごとの反復実行が含まれます。すべての Policy and Distribution Services コンポーネントによって使用されます。
Event	スケジュールされたポリシーを指定されたイベントに従って実行します。たとえば、システムの起動やシャットダウン、サードパーティアプリケーションで定義されたイベントなどです。ポリシーでのみ使用されます。
Interval	スケジュールされた項目を *xxx* 日、時間、分、および秒ごとに繰り返します。Distributor の場合のみ、間隔は Distributor が eDirectory を再読み込みしたときから開始されます。数秒から数日間までの任意の頻度を指定できます。ポリシー、Distributor、Distribution、Channel、および Subscriber で使用されます。
Monthly	スケジュールされた項目を月の選択した日に実行します。[Monthly] には、実行時間帯の指定および時間帯内でのランダムな実行が含まれます。すべての Policy and Distribution Services コンポーネントによって使用されます。
Never	Distribution が自動的に実行されないようにします。Tiered Electronic Distribution でのみ使用されます。 Distributor は eDirectory を読み込みますが、Subscriber は読み込まないため、環境設定が Distributor から送信されるまで、Subscriber は Distribution の作業ディレクトリを認識しません。したがって、すべてのスケジュールでデフォルトの [Never] を使用しないでください。[Never] を使用すると、Subscriber の作業ディレクトリが不明であるというエラーが表示される場合があります。
Package Schedule	スケジュールされた項目をデフォルトのスケジュールに従って実行します。デフォルトのスケジュールは [Policies] タブで変更できます。ポリシーでのみ使用されます。
Relative	スケジュールされたポリシーを、ポリシーパッケージが抽出された時点から指定した日数、時間、分および秒だけ経過したときに 1 回実行します。 たとえば、時間を 1 時間に設定して Distributor を更新した場合、新しいポリシーパッケージが Subscriber に送信され、抽出の 1 時間後に実行されます。ポリシーでのみ使用されます。 数秒から数日間までの任意の時間の範囲を指定できます。

スケジュールタイプ	説明
Run Immediately	スケジュールされた項目を、Distributor が eDirectory を再読み込みした後、ポリシーが更新されたときにすぐに実行します。*xxx* 日、時間、分、および秒ごとのアクションの繰り返しも含みます。数秒から数日間までの任意の頻度を指定できます。ポリシー、Distribution、Channel、および Subscriber で使用されます。
Time	スケジュールされた項目を指定された日時に 1 回実行します。すべての Policy and Distribution Services コンポーネントによって使用されます。
Weekly	スケジュールされた項目を週の選択した曜日に実行します。[Weekly] には、実行時間帯の指定および時間帯内でのランダムな実行が含まれます。ポリシーでのみ使用されます。
Yearly	スケジュールされた項目を年の選択した日に実行します。[Yearly] には、実行時間帯の指定および時間帯内でのランダムな実行が含まれます。すべての Policy and Distribution Services コンポーネントによって使用されます。

曜日

毎日実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Daily] を選択し、週の曜日を 1 つ以上選択します。

2 [Start Time] で、その日のスケジュールの開始時刻を選択します。

3 [End Time] で、スケジュールを実行できるその日の最終時刻を選択します。

4 選択した時間帯にスケジュールをランダムに開始するには、[Randomly Dispatch] チェックボックスをオンにします。

5 スケジュールでアクションを繰り返すには、[Repeat the Action Every] フィールドのチェックボックスをオンにして、アクションを繰り返す頻度を選択します。

どのオプションも 0 にすることができますが、最低 1 つの時間の増分値を設定する必要があります。

イベント

イベントが発生したときに実行されるようにポリシーをスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Event] を選択し、スケジュールをアクティブにするイベントを選択します。

イベント	説明
System Startup	システムが起動されたときにアクションを実行します。
System Shutdown	システムがシャットダウンする前にアクションを実行します。
Custom Event ID	サードパーティアプリケーションで定義されたイベント。

間隔 (Interval)

時間の間隔を置いて実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Interval] を選択し、アクションを繰り返す時間の間隔を選択します。

どのオプションも 0 にすることができますが、最低 1 つの時間の増分値を設定する必要があります。

月

毎月実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Monthly] を選択し、オプションを選択して、月の日付を選択します。

または

月の末日 (28、29、30、または 31 日) のオプションを選択します。

2 [Start Time] で、その日のスケジュールの開始時刻を選択します。

3 [End Time] で、スケジュールを実行できるその日の最終時刻を選択します。

4 選択した時間帯にスケジュールをランダムに開始するには、[Randomly Dispatch] チェックボックスをオンにします。

Never

このタイプは Tiered Electronic Distribution でのみ使用されます。このタイプのスケジュールを使用して、Distribution が自動的に実行されないようにすることができます。

Tiered Electronic Distribution の項目が自動的に実行されないようにスケジュールするには

1 [Schedule Type] の下向きの矢印を選択します。

2 [Never] を選択します。

Distribution が実行されないように指定できますが、Novell iManager で ZENworks Server Management の役割を使用すると、手動でこの設定を上書きすることができます (82 ページの「Policy and Distribution Services エージェントの強制実行」を参照してください)。

パッケージスケジュール

各ポリシーパッケージでは、そのパッケージに含まれるすべてのポリシーのデフォルトのスケジュールが設定されています。

現在の [Default Package Schedule] に従って実行されるようにポリシーをスケジュールする場合、何も操作する必要はありません。

[Package Schedule] を変更するには

1 ConsoleOne で、サーバポリシーを含む OU を選択し、右側のペインにある [Distributed Server Package] を右クリックし、[Properties] をクリックします。

2 [Edit] をクリックします。

3 [Package Schedule] を次のいずれかに変更します。

曜日
週
月
年
相対 (Relative)
すぐに実行 (Run Immediately)
イベント
間隔 (Interval)
Time

相対 (Relative)

ポリシーパッケージが抽出された時点から相対的に実行されるようにポリシーをスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Relative] を選択し、時間を選択します。

どのオプションも 0 にすることができますが、最低 1 つの時間の増分値を設定する必要があります。

すぐに実行 (Run Immediately)

すぐに実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Run Immediately] を選択します。

2 アクションを繰り返す場合は、[Repeat] チェックボックスをオンにします。

3 時間の長さを選択します。

どのオプションも 0 にすることができますが、最低 1 つの時間の増分値を設定する必要があります。

Time

特定の時刻に実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Time] を選択し、カレンダーのアイコンを選択します。

2 [Select Date and Time] ダイアログボックスで、

2a 月を選択します。

2b 年を選択します。

2c 月の日付を選択します。

2d 1 日の時刻を選択し、[OK] をクリックします。

週

毎週実行されるようにポリシーをスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Weekly] を選択し、週の曜日を選択します。

2 [Start Time] で、その日のスケジュールの開始時刻を選択します。

3 [End Time] で、スケジュールを実行できるその日の最終時刻を選択します。

4 選択した時間帯にスケジュールをランダムに開始するには、[Randomly Dispatch] チェックボックスをオンにします。

年

毎年実行されるように項目をスケジュールするには

1 [Schedule Type] の下向きの矢印をクリックし、[Yearly] を選択し、カレンダーのアイコンを選択します。

2 [Select Date] ダイアログボックスで、

2a 月を選択します。

2b 月の日付を選択します。

3 [Start Time] で、その日のスケジュールの開始時刻を選択します。

4 [End Time] で、スケジュールを実行できるその日の最終時刻を選択します。

5 選択した時間帯にスケジュールをランダムに開始するには、[Randomly Dispatch] チェックボックスをオンにします。

C サーバコンソールコマンド

Novell® ZENworks® Server Management の一部の機能は、NetWare® サーバコンソールでのコマンドライン入力を使用して実行できます。ここで説明するサーバコマンドは、ZENworks Server Management Server Policies および Tiered Electronic Distribution に適用されるコマンドです。

Novell iManager で ZENworks Server Management の役割を使用して、Web ブラウザでサーバコンソールコマンドを実行する方法については、2 章 69 ページの「Novell iManager」を参照してください。

サーバコンソールで入力した ZENworks Server Management コンソールコマンドは、そのサーバでのみ実行されます。詳細については、次の節を参照してください。

- 417 ページの「ZENworks Server Management コンソールコマンド」
- 420 ページの「Java コンソールコマンド」

ZENworks Server Management コンソールコマンド

次の表に、Server Management サーバコンソールコマンドと各コマンドの簡単な説明を示します。この表には、どのサーバコンソールプロンプトからコマンドを実行できるかも示されています。

「M」という見出しの列はサーバのメインコンソールプロンプトを示し、「Z」は ZENworks Server Management のプロンプトを示します。コンソールプロンプトの列で、「Y」はそのプロンプトでコマンドを実行できることを示します。「ミ」はそのプロンプトでコマンドを実行できないことを示します。

コマンド	M	Z	説明
HELP	Y	Y	実行できるコマンドのリストを表示します。コンポーネントで適用可能なコマンドだけが表示されます。
HELP *command*	Y	Y	指定したコマンドのヘルプを表示します。
CLS	Y	Y	画面をクリアします。コマンドを実行するときに、どの情報が新しい情報であるかをすばやく識別できます。

コマンド	M	Z	説明
DOWN *option*	Y	Y	サーバのメインコンソールプロンプトで使用されるコマンドと似ています。ただし、ZENworks Server Management プロンプトで Down を使用する場合、サーバを停止するためのサーバポリシーの設定が使用されます。 ZENworks Server Management プロンプトの場合、このコマンドにはいくつかのオプションがあります。 ◆ **DOWN SERVER:** サーバの停止だけを実行します。再起動しません。 ◆ **DOWN STATUS:** 現在の停止のステータスを表示します。 ◆ **DOWN RESTART:** サーバを停止し、再起動します。 ◆ **DOWN RESET:** サーバを停止し、リセットします。 ◆ **DOWN CANCEL:** サーバが実際に停止されるまでに、サーバの停止をキャンセルすることができます。この場合、サーバは使用不可能な状態にはなりません。 ◆ **DOWN !:** 有効な Down Server Process ポリシーを無視して、停止プロセスを直ちに実行します。
EVENTS *option*	ミ	Y	このコマンドには 3 つのオプションがあります。 ◆ **EVENTS LIST:** サードパーティのイベントを含め、登録されているすべてのイベントをリストします。 ◆ **EVENTS STATUS:** 各イベントのステータスを表示します。 ◆ **EVENTS FIRE *event_ID*:** 手動でイベントを実行できます。
EXIT	ミ	Y	現在のコマンドプロンプトの Java ソフトウェアを終了します。たとえば、Subscriber のプロンプトで実行した場合、Subscriber の Java ソフトウェアが終了されます。
LISTPLUGINS	ミ	Y	現在の Server Management プラグインをリストします。
PACKAGE *option*	ミ	Y	サーバにインストールされているソフトウェアパッケージについて次の操作を実行できます。 ◆ **PACKAGE LIST:** 現在インストールされているソフトウェアパッケージをリストします。このコマンドは、ロールバックするパッケージ、およびパッケージをロールバックする順序を調べるのに便利です。パッケージをロールバックする順序は、インストールを開始した順序ではなく、インストールが終了した順序の逆の順序です。 ◆ **PACKAGE PROCESS *full_package_path*:** ソフトウェアパッケージを手動でインストールするにはこのコマンドを使用します。 ◆ **PACKAGE ROLLBACK:** 最後にインストールされたソフトウェアパッケージを手動でロールバック（アンインストール）します。たとえば、サーバに 3 つのソフトウェアパッケージ（パッケージ 1、パッケージ 2、パッケージ 3) をインストールし、最初にパッケージ 1 が、2 番目にパッケージ 2 が、最後にパッケージ 3 がインストールされたとします。パッケージ 2 をロールバックする場合、まずパッケージ 3 をロールバックする必要があります。そのためには、サーバコンソールで「**package rollback**」を実行してパッケージ 3 をロールバックし、もう一度実行してパッケージ 2 をロールバックします。 ソフトウェアパッケージのインストールの順序はパッケージの処理が終了した時点によって決定されるので、インストールの順序を保証できません。したがって、Package Rollback コマンドを実行したときに、インストールの順序がパッケージ 2、パッケージ 1、パッケージ 3 となっている可能性があります。この順序は Package List コマンドで表示されます。
POLICY または POLICY LIST	ミ	Y	有効なサーバポリシーをリストします。リストされる各ポリシーには、POLICY ENFORCE コマンドを使用するときに参照するために対応するポリシー番号があります。

コマンド	M	Z	説明
POLICY ENFORCE *policy_number*	ミ	Y	特定のポリシーを手動で適用するために使用します。*policy_number* は、POLICY LIST コマンドを使用して見つけることができます。 このコマンドは、スケジュールよりも前にポリシーを適用する場合に便利です。ただし、通常は、POLICY REFRESH を最初に実行して、最新の変更を適用していることを確認します。
POLICY ENFORCE ALL	ミ	Y	POLICY REFRESH を実行した後などに、有効なすべてのポリシーを手動で適用するために使用します。
POLICY EVENTBASED	ミ	Y	イベントベースのポリシーをリストします。
POLICY PLUGINS	ミ	Y	現在の Policy Enforcer と現在のイベントハンドラをリストします。
POLICY REFRESH	ミ	Y	必要に応じて、サーバのポリシーおよびスケジュールだけを更新します。ポリシーを更新し、プロンプトで行った変更を元に戻す REFRESH コマンドとは異なります。 このコマンドを実行した後、POLICY ENFORCE を実行する必要があります。
POLICY REFRESHONLY	ミ	Y	サーバのポリシーを更新しますが、有効なポリシーをスケジュールしません。
POLICY RESCHEDULEONLY	ミ	Y	スケジュールに従って現在のすべてのポリシーを再スケジュールします。有効なポリシーは更新しません。
POLICY SCHEDULES	ミ	Y	有効であるすべてのポリシーのスケジュールをリストします。
PROMPT	ミ	Y	現在のプロンプトを一時的にリセットします。Java プロセスが終了または再起動された場合や、REFRESH コマンドが実行された場合、コンソールプロンプトの Novell eDirectory™ オブジェクトで指定された状態に戻ります。
REFRESH	ミ	Y	手動で、強制的にポリシーを更新します。ポリシーの更新には、現在サーバのサービスの場所に対する保留中の変更や、ZENworks Server Management プロンプトに対する一時的な変更などが含まれます。 単独で使用した場合、ZENworks Server Management ポリシーだけを更新します。すべてのポリシーを更新するには、POLICY REFRESH を使用します。
SETCONSOLELEVEL *number*	ミ	ミ	コンソールのメッセージレベルを設定します。 **0:** メッセージなし **1:** エラー **2:** 成功とレベル 1 のメッセージ **3:** 警告とレベル 2 のメッセージ **4:** 情報とレベル 3 のメッセージ **5:** トレース情報とレベル 4 のメッセージ **6:** 開発者用トレース情報とレベル 5 のメッセージ

コマンド	M	Z	説明
SETFILELEVEL *number*	ミ	Y	ファイルのメッセージレベルを設定します。 **0:** メッセージなし **1:** エラー **2:** 成功とレベル 1 のメッセージ **3:** 警告とレベル 2 のメッセージ **4:** 情報とレベル 3 のメッセージ **5:** トレース情報とレベル 4 のメッセージ **6:** 開発者用トレース情報とレベル 5 のメッセージ
SHOWSCHEDULE	ミ	Y	現在のスケジュールをリストします。
SHOWVARS	ミ	Y	定義済みの変数とその値をリストします。これらの変数は Server Software Packages で使用できます。
STATUS	ミ	Y	Policy and Distribution Services の現在のステータスをリストします。次の情報が含まれます。 ベースパス ロードされているプラグイン 登録されているイベント スケジュールされている項目 コンソールレベル
TIME	Y	Y	サーバに設定されている現在の日付と時刻を返します。
VERSION	Y	Y	ZENworks Server Management プロンプトの場合は Server Management のバージョンを、コンソールのメインプロンプトの場合は NetWare のバージョンを返します。

Java コンソールコマンド

次の表では、便利な Java Virtual Machine (JVM*) コマンドをいくつか示します。

コマンド	説明
java -show	ロードされているすべての Java プロセスをリストします。
java -kill*nnn*	指定された Java プロセスを終了します。(*nnn* は、java -show のリストで得られる Java プロセス番号を表します。
java -killzfsexit	すべての Server Management Java プロセスを強制終了します。
java -killall	ロードされているすべての Java プロセスを停止しますが、Java はロードしたままにします。
java -version	JVM のバージョンを表示します。
java -exit または unload java	JVM を含めて、すべての Java プロセスをアンロードしようとします。Java -exit コマンドを使用することをお勧めします。 zenfile.nlm など、Java から呼び出されたネイティブ NLM™ ファイルをアンロードするには、このコマンドが必要です。

D ロード / アンロードアクション

この情報は、Server Polices(4 章 197 ページの「Server Policies（サーバポリシー）」を参照）または Server Software Packages(5 章 241 ページの「Server Software Package に関する問題」を参照）コンポーネントを設定する手順の中で使用されます。

- 421 ページの「Load NLM/Process」
- 422 ページの「Load Java Class」
- 422 ページの「Unload Process」
- 422 ページの「Start Service」
- 422 ページの「Stop Service」

Load NLM/Process

サポートされているすべてのプラットフォームに該当します。

ソフトウェアパッケージによって NLM™ をロードすることを選択し、その NLM がターゲットサーバ上ですでに実行されている場合、パッケージのインストールは失敗し、ロールバックされます（ロールバックが有効になっている場合）。

ソフトウェアパッケージに NLM を含めている場合に、NLM がまだロードされていないことを保証するには、ロードオプションを追加する前に、その NLM のアンロードオプションを追加します。ただし、この方法を使用できるのは、その NLM をアンロードするときにユーザによるキーボードからの入力を必要としない場合だけです。

[Filename]：ファイルへのパスがシステムパス変数である場合を除き、実行可能ファイルへのフルパスを含む正確な名前を指定する必要があります。NLM ファイルの場合は、拡張子 .nlm を含めます。

[Parameters]：NLM またはプロセスの実行を開始するためのコマンドラインパラメータを含めます。

[Wait for this Process to Terminate before Continuing]：NLM やプロセスがそれ自体を終了する場合は、このチェックボックスを選択できます。NLM やプロセスは 10 分以内に終了する必要があります。終了しない場合、ロード処理全体が失敗します。デフォルトでは、このオプションは淡色表示されています。

Load Java Class

NetWare のみ。

[Filename] : これは正確な名前である必要があります。拡張子 .class は必要ありません。

[Parameters] : Java アプリケーションの実行を開始するためのコマンドラインパラメータを含めます。

[JVM Parameters] : Java 仮想コンピュータのパラメータを含めます。

[Wait for this Process to Terminate before Continuing] : Java アプリケーションがそれ自体を終了する場合は、このオプションを選択できます。時間制限はありません。アプリケーションが実行されている間、待機します。デフォルトでは、このオプションは淡色表示されています。

Unload Process

サポートされているすべてのプラットフォームに該当します。

この NLM をアンロードするのにユーザの操作が必要な場合は、ソフトウェアパッケージをインストールする前に、手動で NLM をアンロードする必要があります。

[Filename] : これは正確な名前である必要があります。パスは必要ありません。多くの NLM ファイルはアンロードするときにユーザの入力を必要とするため、アンロードを自動化することはできません。

[Wait for this Process to Unload before Continuing] : プロセスがそれ自体を終了する場合は、このオプションを選択できます。デフォルトでは、このオプションは淡色表示されています。

Start Service

Windows にのみ該当します。

[Service Name] : これは正確な名前である必要があります。

[Wait For This Service to Finish Running Before Continuing] : サービスがそれ自体を開始する場合は、このオプションを選択できます。デフォルトでは、このオプションは淡色表示されています。

Stop Service

Windows にのみ該当します。

[Service Name] : これは正確な名前である必要があります。

[Wait For This Service to Stop Before Continuing] : サービスがそれ自体を終了する場合は、このオプションを選択できます。デフォルトでは、このオプションは選択されません。

E Server Software Packages の要件

この情報は、ソフトウェアパッケージを設定する手順の中で使用されます。詳細については、5 章 241 ページの「Server Software Package に関する問題」を参照してください。

重要： 要件を選択することによって、ソフトウェアパッケージやパッケージコンポーネントをインストールするためにその要件が満たされている必要があることを指定します。

要件	説明
Operating System	ソフトウェアパッケージのファイルを実行するためのオペレーティングシステム (OS) の要件です。ファイルを実行するために必要な OS とターゲットサーバがその OS を実行しているかどうかの両方を含みます。
Memory (RAM)	ソフトウェアパッケージのファイルを実行するために必要な最小限の RAM です。ターゲットサーバがこの最小値を満たしていない場合、ソフトウェアパッケージはサーバに配布されません。
Disk Space	ターゲットサーバにファイルをインストールするために必要な最小限の空きディスク容量です。ターゲットサーバがこの最小空き容量を満たしていない場合、ソフトウェアパッケージはサーバに配布されません。
SET Commands	ソフトウェアパッケージ用にターゲットサーバで設定する NetWare® の SET コマンドです。
Registry	ソフトウェアパッケージのファイルのために、ターゲットサーバで必要になる可能性のあるレジストリの変更です。個々のレジストリエントリの設定については、429 ページの付録 F 、「Server Software Package コンポーネントのレジストリエントリ」を参照してください。
File	ターゲットサーバ上のファイルが存在しているかどうかや、特定の日付になっているかどうかを指定します。
Products.dat	ソフトウェアパッケージが必要とする products.dat に対する変更です。通常、この変更は、ソフトウェアパッケージの内容から、サーバ上のソフトウェアのバージョンを更新するために行います。products.dat ファイルは、サーバ上に存在するソフトウェアとそのバージョンを調べるために使用されます。

オペレーティングシステム

ソフトウェアパッケージをインストールする前に、サーバで特定のオペレーティングシステムが実行されていることを要求できます。

サーバのオペレーティングシステムの要件を設定するには

1 オペレーティングシステムの要件を選択した状態で、サーバのプラットフォームを選択します。

選択可能なプラットフォームは、NetWare、Windows、Linux、および Solaris です。

2 バージョンの関係を選択します。

Any
Less Than
Less Than or Equal To
Equal To
Greater Than
Greater Than or Equal To

3 [Version] フィールドで [Any] 以外のオプションを選択した場合は、次の表の情報に従って [Major]、[Minor]、および [Revision] フィールドに入力します。

Windows サーバの場合、バージョン情報は指定できません。したがって、Windows は次の表には含まれていません。

[Major] および [Minor] フィールドは、上位のバージョンを制限するために使用します。Netware および Windows の場合、[Revision] フィールドは、必要なサービスパックのリビジョンを指定するために使用します。Linux の場合、[Revision] フィールドは、必要な配布の更新バージョンを指定するために使用します。

OS のバージョン (Operating System Version)	Subscriber のバージョン [1]	メジャー	マイナー	Revision
NetWare 5.1 + SP5	ZfS 3.0.2 のみ	5	10	5
NetWare 5.1 + SP6	ZENworks 6.5 または ZfS 3.0.2	5	10	6
NetWare 5.1 + SP7	ZENworks 6.5 のみ	5	10	7
NetWare 6 + SP2	ZfS 3.0.2 のみ	6	0	2
NetWare 6 + SP3	ZfS 3.0.2 のみ (JVM 1.4.1 を使用)	6	0	3
NetWare 6 + SP4	ZENworks 6.5 または ZfS 3.0.2	6	0	4
NetWare 6 + SP5	ZENworks 6.5 のみ	6	0	5
NetWare 6.5	ZfS 3.0.2 のみ	6	5	0
NetWare 6.5 + SP1a	ZENworks 6.5 または ZfS 3.0.2	6	5	1
NetWare 6.5 + SP2	ZENworks 6.5 のみ	6	5	2
Red Hat Linux 7.1、7.2、7.3、8	ZfS 3.0.2 のみ	2	4	*変数* [2]
Red Hat Linux 9	ZENworks 6.5 のみ	2	4	*変数* [2]
Red Hat Advanced Server 2.1	ZENworks 6.5 または ZfS 3.0.2	2	4	*変数* [2]
Red Hat Enterprise Server 2.1	ZENworks 6.5 または ZfS 3.0.2	2	4	*変数* [2]
Red Hat Enterprise Linux AS 3	ZENworks 6.5 のみ	2	4	*変数* [2]
Red Hat Enterprise Linux ES 3	ZENworks 6.5 のみ	2	4	*変数* [2]

OS のバージョン (Operating System Version)	Subscriber のバージョン [1]	メジャー	マイナー	Revision
Solaris 8	ZfS 3.0.2 のみ	5	8	該当なし
Solaris 9	ZENworks 6.5 のみ	5	9	該当なし
SUSE® LINUX 8.1 [3]	ZfS 3.0.2 のみ	2	4	*変数* [2]
SUSE LINUX 8.2	ZfS 3.0.2 のみ	2	4	*変数* [2]
SUSE LINUX Enterprise Server 8	ZENworks 6.5 のみ	2	4	*変数* [2]
SUSE LINUX Standard Server 8	ZENworks 6.5 のみ	2	4	*変数* [2]
SUSE LINUX Enterprise Server 9	ZENworks 6.5 のみ	2	6	*変数* [2]
SUSE LINUX Standard Server 9	ZENworks 6.5 のみ	2	6	*変数* [2]

[1] [Subscriber] 列には、サーバプラットフォームでソフトウェアパッケージを処理するために必要な Subscriber のバージョンが示されます。ここで Subscriber のバージョンを指定する必要はありません。ただし、これらのネットワークオペレーティングシステムのいずれかを使用するサーバで正しいバージョンの Subscriber ソフトウェアを実行しない限り、そのサーバでソフトウェアパッケージを正常に送信および抽出できません。

段階的にアップグレードしている場合など、ネットワークで ZENworks 6.5 Server Management と ZENworks for Servers 3.0.2 の両方を実行することができます。この表は、両方の ZENworks 製品のバージョン情報を示しています。段階的なアップグレードの詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「アップグレードの概念と問題点」を参照にしてください。

[2] この表で Linux プラットフォームに対して変数と表示されている場合、[Revision] フィールドに入力する数値は、インストールされている Linux オペレーティングシステムに最初に同梱されていたカーネル、または Linux サーバの更新後のカーネルのリビジョンです。uname -a コマンドを使用して、正確なリビジョン番号を判断することができます。

また、入力する必要があるリビジョン番号は、[Version] フィールドで指定する条件 ([Equal To]、[Greater Than] など) によっても異なります。たとえば、[Revision] フィールドに「0」と入力し、[Version] フィールドで [Greater Than] を選択すると、すべてのカーネルリビジョンが含まれます。

[3] Linux のバージョンは Red Hat および SUSE について同じであるため、[Platform] フィールドでは Linux を選択すれば済みます。これら 2 つの Linux の配布をそれぞれ区別するために、Red Hat または SUSE のいずれかに属する特定のファイルがサーバ上に存在するよう、ソフトウェアパッケージ内の他の領域で要求することができます。たとえば、/etc/SuSE-release ファイルをサーバ上で要求すると、SUSE LINUX バージョンを使用するサーバだけがソフトウェアパッケージの受信を受け入れるようになります。

Memory (RAM)

サーバのメモリの要件を設定するには

1 メモリの要件を選択した状態で、条件を選択します。

Less Than
Less Than or Equal To
Greater Than
Greater Than or Equal To

2 選択した条件について、RAM のサイズをメガバイト単位で指定します。

ディスク領域

ディスク容量の要件を設定するには

1 ディスク容量の要件を選択した状態で、ルートの場所を選択します。

[SYS Volume] と [Volume] の 2 つのオプションがあります。NetWare サーバ上で使用するディスク容量を節約するために、他に利用可能なディスク容量のあるボリュームがある場合は、sys: ボリュームを選択しないでください。

重要： 複数のプラットフォームに送信する場合は、スラッシュ (/) 記号などのリテラル文字によるボリューム / ドライブ名を使用しないでください。たとえば、ソフトウェアパッケージで Linux に対して「/」記号を使用し、その Software Package Distribution が Windows サーバにも送信される場合、Windows は「/」をルートの場所として認識し、Linux サーバ専用のファイルが Windows サーバにインストールされます。この問題に対処するには、次のいずれかの操作を行います。

a. ディスク容量の場所について、複数のプラットフォームへの送信を可能にする変数を使用します。

または

b. オペレーティングシステムの要件とディスク容量の要件を組み合わせて使用し、リテラル文字によるディスク容量の場所があるサーバプラットフォームだけに Distribution の送信先を制限します。

リテラル文字による指定可能な場所の例：

[NetWare] :
sys:
data:

[Windows] :
C:¥
¥¥myserver¥data¥*shared_folder*

Linux または Solaris:
/
/usr
/usr/data
/usr/data
/etc
/mnt/files

Linux および Solaris サーバの場合は、ディスクパーティションを認識する任意のパスです。

2 [Volume] を選択した場合は、ボリューム名を指定します。

3 条件を選択します。

Less Than
Less Than or Equal To
Greater Than
Greater Than or Equal To

4 選択した条件について、必要な空きディスク容量をメガバイト単位で指定します。

指定する空きディスク容量がステップ 1 で指定した場所に存在することが重要です。

SET Commands

SET コマンドを追加する場合は、SET Commands ウィザードが自動的に実行されます。

SET コマンドの要件を設定するには

1 SET コマンドの要件を選択した状態で、SET コマンドの名前を指定します。

2 SET コマンドの値を指定します。

レジストリ

ソフトウェアパッケージをインストールする前に、レジストリ内に特定のエントリが存在していることを要求できます。

レジストリの要件を設定するには

1 レジストリの要件を選択した状態で、[Entry Type] を選択します。

Key
Name
Data

2 エントリのタイプが [Key] および [Name] の場合は、[Exists] または [Does Not Exist] のいずれかを選択します。

または

エントリのタイプが [Data] の場合は、[Equals] または [Does Not Equal] のいずれかを選択します。

3 ステップ 1 で選択したタイプに応じて、[Key]、[Name]、または [Data] のテキストを入力します。

キーの先頭にはバックスラッシュを 2 つ追加してください。たとえば、「¥¥HKEY_LOCAL_MACHINE¥software¥...」のように入力します。

重要： % 記号は、NetWare のレジストリ名では有効ではありません。

この [Registry] フィールドでは、[Registry Settings] フィールド (272 ページの「レジストリの設定」を参照) の場合とは異なり、HKEY_LOCAL_MACHINE は "My Server" に変換されません。

File

ファイルの要件を設定するには

1 ファイルの要件を選択した状態で、名前を指定します。

ファイルのフルパスを含めます。

2 必要なファイルのステータスを選択します。

File Exists
File Does Not Exist
Date Is

Products.dat

警告： products.dat ファイルを変更すると、NetWare サーバ上で実行やインストールが妨げられる場合があります。Novell® から提供されたすべてのエントリを変更しないでください。

products.dat の要件を設定するには

1 products.dat の要件を選択した状態で、.dat ファイル内の項目の名前を指定します。

重要： 名前は大文字と小文字が区別されます。

この項目は、.dat ファイル内の製品の ID です。

2 ステップ 1 で選択した項目に対応するバージョンテキストを指定します。

3 ステップ 2 で指定したバージョンについて、[Contains]、[Begins With]、[Matches] のいずれかの条件を選択します。

4 ステップ 1 で選択した項目に対応する説明のテキストを指定します。

5 ステップ 4 で指定した説明について、[Contains]、[Begins With]、[Matches] のいずれかの条件を選択します。

F Server Software Package コンポーネントのレジストリエントリ

次の情報は、ソフトウェアパッケージを設定する手順の中で使用されます。詳細については、272 ページの「レジストリの設定」を参照してください。

NetWare® または Windows のレジストリエントリで変更できるのは、キー、値名、および値データです。変更する場合はキーと値データのタイプを選択することができ、いずれかのタイプを選択した場合に対応する値名を指定できます。

いずれの場合も、レジストリで想定されている正確なキー名または値名、および正確なデータ値を入力する必要があります。

ソフトウェアパッケージを使用して設定できるのは、HKEY_LOCAL_MACHINE の下のレジストリ設定だけです。

ソフトウェアパッケージをインストールするときに、次のレジストリエントリを変更できます。

- 429 ページの「Key」
- 430 ページの「Binary」
- 430 ページの「Expand String」
- 431 ページの「(Default)」
- 431 ページの「DWord」
- 431 ページの「Multi-Value String」
- 432 ページの「String」

Key

キーはさまざまなレジストリエントリへのパスを作成します。たとえば、HKEY_LOCAL_MACHINE はルートレベルのレジストリキーで、HARDWARE はそのすぐ下にあるキーです。キーはツリー形式でフォルダのアイコンで表示されます。プラス記号またはマイナス記号をクリックして、ツリー構造を展開または縮小できます。

HKEY_LOCAL_MACHINE キーが表示されているボックスで、レジストリの変更を配置するパスを作成するには、[Key] レジストリエントリを使用する必要があります。

[Key] エントリを設定するには

1 キーツリーが表示されているボックスで、キーを挿入する場所を選択します。

2 ドロップダウンボックスから [Key] を選択し、[Add] をクリックします。

[New Key #1] が表示されます。

3 デフォルトのキー名を必要なキー名に変更します。

このフィールドに情報を入力するときは、(Enter) キーを押して変更を保存する必要があります。

4 レジストリの変更の条件を選択します。

Create
Delete

5 すべての従属キーに設定を適用するには、[Apply To All] をクリックします。

Binary

16 進数値のリストである値データのタイプです。たとえば、次のようなものです。

```
d0 04 72 6e
```

最初に、[Key] レジストリ設定オプションを使用して、[Binary] エントリを保持するキーへのパスを作成します。

[Binary] エントリを設定するには

1 キーツリーが表示されているボックスで、バイナリデータを挿入する場所を選択します。

2 ドロップダウンボックスから [Binary] を選択し、[Add] をクリックします。

[New Value #1] が表示されます。

3 デフォルトのバイナリ名を必要な名前に変更します。

4 レジストリの変更の条件を選択します。

Create
Delete

5 バイナリデータを指定します。

[Data] ボックスは 16 進エディタです。ラベルのない列が 3 つあります。

最初の列： 16 進文字の数のバイナリカウンタで、0000 から始まります。

2 番目の列： 16 進データで、1 行に 8 つのエントリがあります。

3 番目の列： 16 進データに対応するプレーンテキストの ASCII 文字です。

2 番目の列または 3 番目の列にデータを入力できます。2 番目の (16 進の) 列にデータを入力すると、3 番目の (テキストの) 列に対応する文字が表示されます。逆の場合も同じです。

Expand String

NetWare のみ。現在サポートされていません。

(Default)

通常、キーの最初のデータエントリです。

最初に、[Key] レジストリ設定オプションを使用して、[(Default)] エントリを保持するキーへのパスを作成します。

[(Default)] エントリを設定するには

1 キーツリーが表示されているボックスで、[(Default)] エントリを作成する場所を選択します。

2 ドロップダウンボックスから [(Default)] を選択し、[Add] をクリックします。

[(Default)] が表示されます。

3 [(Default)] エントリを選択した状態で、レジストリ変更の条件を選択します。

Create
Delete

4 [Data] で文字列を入力します。

DWord

DWord は、Double WORD 形式で表現された 16 進コードに基づいています。たとえば、次のように入力します。

0x00100022

最初に、[Key] レジストリ設定オプションを使用して、[DWord] エントリを保持するキーへのパスを作成します。

[DWord] エントリを設定するには

1 キーツリーが表示されているボックスで、[DWord] エントリを作成する場所を選択します。

2 ドロップダウンボックスから [DWord] を選択し、[Add] をクリックします。

[New Value #1] が表示されます。

3 デフォルトの DWord 名を必要な名前に変更します。

4 レジストリの変更の条件を選択します。

Create
Delete

5 [Data] で DWord 文字列を入力します。

Multi-Value String

NetWare のみ。現在サポートされていません。

String

文字列値は、引用符で囲まれた単語または数字のわかりやすい並びです。

最初に、[Key] レジストリ設定オプションを使用して、[String] エントリを保持するキーへのパスを作成します。

[String] エントリを設定するには

1 キーツリーが表示されているボックスで、文字列データを挿入する場所を選択します。

2 ドロップダウンボックスから [String] を選択し、[Add] をクリックします。

[New Value #1] が表示されます。

3 デフォルトの文字列名を必要な名前に変更します。

4 レジストリの変更の条件を選択します。

Create
Delete

5 [Data] で文字列を入力します。

G ドキュメントの更新

この節では、Novell® ZENworks® 6.5 Server Management の初回リリース後に、『*管理ガイド*』の Policy and Distribution Services に関する項で変更された内容について説明します。お使いのドキュメントを最新の状態に更新するために、この情報を役立ててください。

この節で列挙する変更はすべてドキュメントにも反映されているものです。マニュアルは、Web 上で HTML と PDF の 2 つの形式で提供されています。HTML および PDF ドキュメントは、ここに示すドキュメントの変更に基づいて最新の状態になっています。

ドキュメントの更新が発行された日付ごとに、更新情報をグループ化しています。日付の付いた節の中では、Policy and Distribution Services の目次に記載されている節名に基づいて、アルファベット順に変更を示しています。

使用している PDF ドキュメントのコピーが最新の内容であるかどうかを確認するには、PDF ドキュメントのタイトルページ、またはタイトルページのすぐ後ろの法的通知の欄で、発行された日付を参照してください。

ドキュメントは次に示す日付で更新されました。

- 433 ページの「2004 年 2 月 11 日」
- 435 ページの「2004 年 11 月 10 日」
- 436 ページの「2004 年 9 月 2 日」
- 436 ページの「2004 年 7 月 28 日」

2004 年 2 月 11 日

次の節が更新されました。変更内容は次のとおりです。

- インストール後の設定
- Tiered Electronic Distribution
- Tiered Electronic Distribution
- Desktop Application Distribution
- レポート機能
- Distribution のタイプ

インストール後の設定

各節に次の変更が加えられました。

場所	変更
25 ページの「インストール後の設定」	この節はサブセクションと同じタイトルのため、混乱を避けるために、名前が「配布システムの設定」から変更されました。
46 ページの「配布システムの設定」	「混在ネットワークオペレーティングシステム環境での Distributor のセットアップ」は、適用されなくなったため削除されました。ZENworks 6.5 SP1 Distributor は、eDirectory 8.*x* が実行されているサーバにしかインストールできないため、Distributor サーバで eDirectory 8.*x* に対する認証を実行できないという問題はなくなります。

Novell iManager

各節に次の変更が加えられました。

場所	変更
70 ページの「iManager の ZENworks Server Management の役割へのアクセス」	iManager 2.5 を含むログイン手順が更新されました。この節を機能別に 3 つの節に分けて、新しい節の情報を更新しました。

Tiered Electronic Distribution

各節に次の変更が加えられました。

場所	変更
114 ページの「既存の Distribution の新しいバージョンを作成および配布する方法」 および 117 ページの「最大リビジョン数」 および 301 ページの「Distribution の作成」	次の文が［Maximum Revisions］フィールドの説明に追加されました。 リビジョンの最大数に近づくと、SMTP 電子メール通知が送信されます。
118 ページの「MSI Distribution の抽出エラー」	Windows 2000 サーバで抽出エラーを回避する方法を説明する新しい節が追加されました。
122 ページの「MSI」	次の文が［MSI］タイプの説明に追加されました。 MSI 3 は、配布可能なバージョンとしてサポートされます。ただし、ZENworks 6.5 SP1 は、MSI 3 の新機能を個別にはサポートしていません。
180 ページの「File Distribution のディレクトリ同期の細分性」	わかりやすくするために、この節に新しい例が追加されました。

Desktop Application Distribution

各節に次の変更が加えられました。

場所	変更
6 章 283 ページの「Desktop Application Distribution」	新しい節（特に概念に関する節）が追加され、既存の節が更新されました。

レポート機能

各節に次の変更が加えられました。

場所	変更
380 ページの「レポートへのアクセス」	Policy and Distribution Services レポートにアクセスするには、オブジェクト経由とメニューオプション経由の 2 つの方法があります。

Distribution のタイプ

各節に次の変更が加えられました。

場所	変更
405 ページの「MSI」	MSI Distribution 情報が更新されました。

2004 年 11 月 10 日

次の節が更新されました。変更内容は次のとおりです。

- Desktop Application Distribution

Desktop Application Distribution

各節に次の変更が加えられました。

場所	変更
283 ページの「Desktop Application Distribution の理解」	この新しい節が追加され、6 章 283 ページの「Desktop Application Distribution」の他の節が再編成および更新されました。
300 ページの「Desktop Application Distribution の作成」	次の段落が、この節とダイジェストを説明する他の節に追加されました。 ダイジェストは、Distribution のパッケージの破損も検出します。破損があると、Subscriber は distfile.ted Distribution ファイルの名前を distfile.corrupt に変更し、次回に Channel のスケジュールが開始されたときに Distribution を再構築して送信します。

2004 年 9 月 2 日

ガイド全体を通して、グラフィックのフォントを変更し、新しいアイコンを使用しました。グラフィックの内容には、目立った変更はありません。

2004 年 7 月 28 日

次の節が更新されました。変更内容は次のとおりです。

- Tiered Electronic Distribution
- Server Policies（サーバポリシー）

Tiered Electronic Distribution

各節に次の変更が加えられました。

場所	変更
143 ページの「手動による Distribution のインポートとエクスポート」	この節が更新されました。これには、Distribution を抽出し、そのステータスを iManager で表示できるように Distribution のインポートを開始する新しい手順の追加が含まれています。

Server Policies（サーバポリシー）

各節に次の変更が加えられました。

場所	変更
215 ページの「Tiered Electronic Distribution ポリシーの設定」	手順 4 で、[Filename] フィールドの文が書き直され、Tiered Electronic Distribution 情報を記録するエージェントが明記されました。
223 ページの「Prohibited File」	次の説明が、Prohibited File ポリシーでのワイルドカード使用に関する手順 5 に追加されました。 **重要：**？ワイルドカードは、ZENworks と DOS では機能が異なります。たとえば、検索文字列 *.htm? は、.html で終わるファイルのみを検索しますが、DOS は、.htm と .html の両方で終わるファイルを検索します。つまり、ZENworks で？ワイルドカードを使用すると、文字の位置にファイル名を指定できます。
234 ページの「ZENworks Server Management」	手順 4 で、[Filename] フィールドの文が書き直され、ポリシー情報とソフトウェアパッケージ情報を記録するエージェントが明記されました。
235 ページの「ポリシーを使用したカスタムログファイルの作成」	情報レポートのカスタムログ作成方法に関して、この新しい節が追加されました。

II Server Inventory

Novell® ZENworks® 6.5 Server Management の Server Inventory コンポーネントを使用すると、企業のローカルサーバおよびリモートサーバからハードウェアおよびソフトウェアのインベントリ情報を収集できます。このインベントリ情報は、ZENworks 管理者がアクセスできるデータベースでスキャンおよび保存されます。

Novell ConsoleOne® から、サーバのハードウェア およびソフトウェアに関する詳しいインベントリ情報を参照できます。サーバの一元管理されたデータベースを照会することもできます。

次の節では、Server Inventory の機能とタスクについて説明します。

- 12 章 439 ページの「Server Inventory の理解」
- 13 章 453 ページの「Server Inventory のセットアップ」
- 14 章 517 ページの「Server Inventory コンポーネントの理解」
- 15 章 537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」
- 16 章 571 ページの「インベントリ情報の管理」
- 17 章 625 ページの「インベントリ情報の表示」
- 18 章 685 ページの「ステータスログによる Server Inventory の監視」
- 691 ページの付録 H、「パフォーマンスに関するヒント」
- 699 ページの付録 I、「Inventory Scanner で収集されるハードウェア情報」
- 715 ページの付録 J、「ZENworks 6.5 Server Management の Inventory 属性」
- 733 ページの付録 K、「列挙値」
- 743 ページの付録 L、「ドキュメントの更新」

12 Server Inventory の理解

Novell® ZENworks® 6.5 Server Management の Server Inventory コンポーネントは、企業の Novell NetWare® サーバおよび Windows* サーバからハードウェアおよびソフトウェアのインベントリ情報を収集し、一元化されたデータベースに保存します。ネットワーク管理者は、このデータベースを使用して企業の詳しいインベントリ情報を参照および照会することができます。

インベントリ情報は、サーバの管理方法について業務上の決定を行う場合に役立ちます。インベントリ情報を取得することで、次のようなサーバを特定することができます。

- 新しいアプリケーションが必要なサーバ
- ハードウェアやドライバの更新が必要なサーバ
- 企業のハードウェアおよびソフトウェア規格に準拠しているサーバ

この章では、Server Inventory の基本的な概要について説明します。この章は次の項目で構成されています。

- 439 ページの「Server Inventory 用語」
- 441 ページの「Server Inventory のコンポーネントの概要」
- 442 ページの「インベントリスキャンサイクルの理解」
- 443 ページの「インベントリサーバの役割の理解」

Server Inventory 用語

次の簡単な用語集では、Server Inventory で使用する用語の基本的な定義について説明します。

インベントリ対象サーバ： スキャンの対象になるサーバ。そのハードウェアおよびソフトウェアの情報がスキャンされた後、中央リポジトリに情報が保存されます。サーバの全ハードウェア / ソフトウェアインベントリを収集するには、対象になるサーバに Inventory Agent をインストールする必要があります。

インベントリサーバ： Inventory Service を実行するサーバ。このサーバでは、ZENworks 6.5 Server Management の他のサービスも実行できます。インベントリサーバは、インベントリ対象サーバのグループからインベントリ情報を収集し、その情報をインベントリデータベースに保存します。インベントリサーバのインベントリを収集する場合は、インベントリサーバに Inventory Agent をインストールする必要があります。

インベントリデータベース： 全インベントリ対象サーバのインベントリ情報のリポジトリ。

データベースサーバ： インベントリデータベースがマウントされている Sybase*、Oracle*、または MS SQL を実行するサーバ。このデータベースは、インベントリサーバでも、他のサーバでも実行できます。

管理コンソール：Server Inventory ConsoleOne スナップインがインストールされた Novell ConsoleOne® を実行する Windows ワークステーションまたはサーバ。管理コンソールは、インベントリシステムを管理するためのインタフェースを提供します。

eDirectory ツリー： Novell eDirectory™ ツリーは、部門、ユーザ、グループ、およびその他のネットワークリソースなどの複数レベルの eDirectory オブジェクトから構成されます。このガイドでは、この階層構造を eDirectory ツリーと呼びます。詳細については、Novell eDirectory Documentation Web サイト (http://www.novell.com/documentation) を参照してください。

インベントリツリー： インベントリ対象サーバおよびインベントリサーバから企業の一元管理されているインベントリデータベースへのインベントリ情報の転送を示す論理ツリー。

スタンドアロンサーバ： インベントリデータベースが搭載され、インベントリ対象サーバが接続されているインベントリサーバ。

リーフサーバ： インベントリツリー階層内で最下位のインベントリサーバ。1 台以上のインベントリ対象サーバが接続されており、インベントリデータベースを接続できます。このインベントリサーバは、接続されているインベントリ対象サーバからインベントリ情報を収集し、次のレベルのインベントリサーバにその情報を転送します。

中間サーバ： 階層内の下位インベントリサーバから上位インベントリサーバにインベントリ情報を転送するインベントリサーバ。インベントリ対象サーバかインベントリデータベースのいずれか一方、または両方を接続できます。

ルートサーバ： インベントリツリー階層内で最上位のインベントリサーバ。このサーバには、インベントリデータベースが搭載されており、そのデータベースには下位インベントリサーバのインベントリ情報がすべて保存されます。ルートサーバレベルでは、企業全体の完全なインベントリ情報を参照することができます。このサーバには、インベントリ対象サーバを接続できます。

サイト：通常、1 つの地理的な場所が 1 つのサイトとして設定されます。企業内に複数のサイトを設定できます。

ソフトウェアディクショナリまたはディクショナリ： ソフトウェアディクショナリには、ソフトウェア識別情報とルールのリストが含まれています。各ソフトウェア識別情報は、インベントリ対象サーバにインストールされている特定の製品を識別します。

ソフトウェア識別情報： ソフトウェア製品を識別するエントリのことをソフトウェア識別情報と呼びます。各ソフトウェア識別情報には、ファイル照合属性および対応するソフトウェア情報属性のセットが含まれています。インベントリスキャンで、Inventory Scanner によってファイルのヘッダから読み取られた属性がディクショナリ内に設定された属性と一致した場合、対応するソフトウェア情報属性の情報がインベントリデータベースに保存されます。

ソフトウェアディクショナリルール： ソフトウェアディクショナリルールは、スキャンプロセスの範囲を制御する条件セットを表します。

不明なソフトウェア： ソフトウェアディクショナリを使用しても、ネットワーク内にインストールされたすべてのソフトウェアを識別できない場合があります。ソフトウェアディクショナリに含まれていないソフトウェアのことを不明なソフトウェアといいます。

Server Inventory のコンポーネントの概要

ZENworks 6.5 Server Inventory をセットアップする前に、インベントリ機能を実行するときに相互に作用するインベントリコンポーネントについて理解しておく必要があります。

Server Inventory では、次のコンポーネントを使用しています。

- 441 ページの「Inventory Scanner」
- 441 ページの「インベントリサーバ上のインベントリコンポーネント」
- 442 ページの「Inventory Database」
- 442 ページの「管理コンソール」

Inventory Scanner

プラットフォームに依存する Scanner によって、インベントリ対象サーバのハードウェアおよびソフトウェアの構成が判断されます。Scanner はインベントリ対象サーバに配置します。インベントリ対象サーバに対してこの Scanner を実行すると、インベントリ情報が収集されます。そして、インベントリ情報はインベントリサーバに転送された後、処理されます。

Server Inventory ポリシーを使って、インベントリ対象サーバのスキャンスケジュールを設定し、ハードウェアスキャンをカスタマイズすることができます。Inventory Service オブジェクト (Inventory Service_*server_name*) から、インベントリ情報の場所を指定することができるほか、ソフトウェアディクショナリスナップインを使ってソフトウェアスキャンをカスタマイズすることもできます。

Inventory Scanner に関する詳細については、520 ページの「Inventory Scanner の理解」を参照してください。

インベントリサーバ上のインベントリコンポーネント

インベントリサーバコンポーネントによって、インベントリ情報が処理されます。次のコンポーネントは、NetWare および Windodws を搭載したインベントリサーバ上で同じ動作をする Java* プログラムです。

- Scan Collector

  Scan Collector は、Inventory agent からインベントリ情報を収集し、この情報をインベントリサーバの適切なディレクトリに保存します。このインベントリ情報は、XML-RPC プロトコルを使って転送されます。

- Selector

  Selector は、インベントリ情報を処理し、その情報を適切なディレクトリに配置します。詳細については、532 ページの「Selector の理解」を参照してください。

- Sender および Receiver

  インベントリサーバ上の Sender はインベントリ情報を圧縮した後、その情報を下位レベルのインベントリサーバから上位レベルのインベントリサーバ上の Receiver に転送します。ロールアップポリシーを使用すると、ロールアップ先の次のレベルのインベントリサーバを設定したり、ロールアップを行う時間をスケジュールしたりすることができます。詳細については、527 ページの「Sender-Receiver の理解」を参照してください。

- Storer

  Storer は、収集されたインベントリ情報をインベントリデータベースに格納します。データベースの場所ポリシーを使用すると、インベントリデータベースオブジェクト (Inventory database_*server_name*) のプロパティを設定したり、データベースオブジェクトをインベントリサーバに関連付けたりすることができます。詳細については、534 ページの「Storer の理解」を参照してください。

- Dictionary Provider および Dictionary Consumer

  すべてのインベントリサーバで、Dictionary Provider サービスと Dictionary Consumer サービスが実行されます。Dictionary Consumer サービスは、Dictionary Provider サービスからディクショナリ更新をダウンロードします。詳細については、534 ページの「Dictionary Provider と Dictionary Consumer について」を参照してください。

Inventory Database

インベントリデータベースは、インベントリ対象サーバのインベントリ情報のリポジトリです。Server Management では、データベースは CIM (Common Information Model) ベースのデータベースであり、リレーショナルデータベース管理システム (RDBMS) に実装されます。データベースは Sybase、Oracle、または MS SQL で管理されます。詳細については、487 ページの「インベントリデータベースのセットアップ」を参照してください。

管理コンソール

管理コンソールには、Novell の管理ツールである ConsoleOne を使用します。これは Java ベースのコンソールで、Server Inventory 管理用のスナップインが用意されています。

インベントリスキャンサイクルの理解

インベントリスキャンサイクルは次のとおりです。

1. Inventory Scanner は、更新されたディクショナリがインベントリサーバで利用可能かどうかをチェックし、更新されたディクショナリをダウンロードします。
2. Inventory Scanner は、スキャンスケジュールに従ってインベントリ対象サーバから収集したハードウェアおよびソフトウェア情報をインベントリサーバに送信します。
3. インベントリサーバは、そのインベントリ情報をインベントリデータベースに保存します。
4. 管理コンソールで、[Reporting] > [Summary] などのインベントリツールを使用してインベントリデータベースのインベントリ情報を参照および取得することができます。

インベントリサーバの役割の理解

この節では、インベントリサーバに割り当てることができる、次のような役割について説明します。

- 443 ページの「ルートサーバ」
- 444 ページの「Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）」
- 445 ページの「中間サーバ」
- 446 ページの「データベースが接続されている中間サーバ」
- 448 ページの「Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）」
- 449 ページの「リーフサーバ」
- 450 ページの「データベースが接続されているリーフサーバ」
- 451 ページの「スタンドアロンサーバ」

インベントリサーバの役割の早見表は、452 ページの「インベントリサーバの役割の早見表」を参照してください。

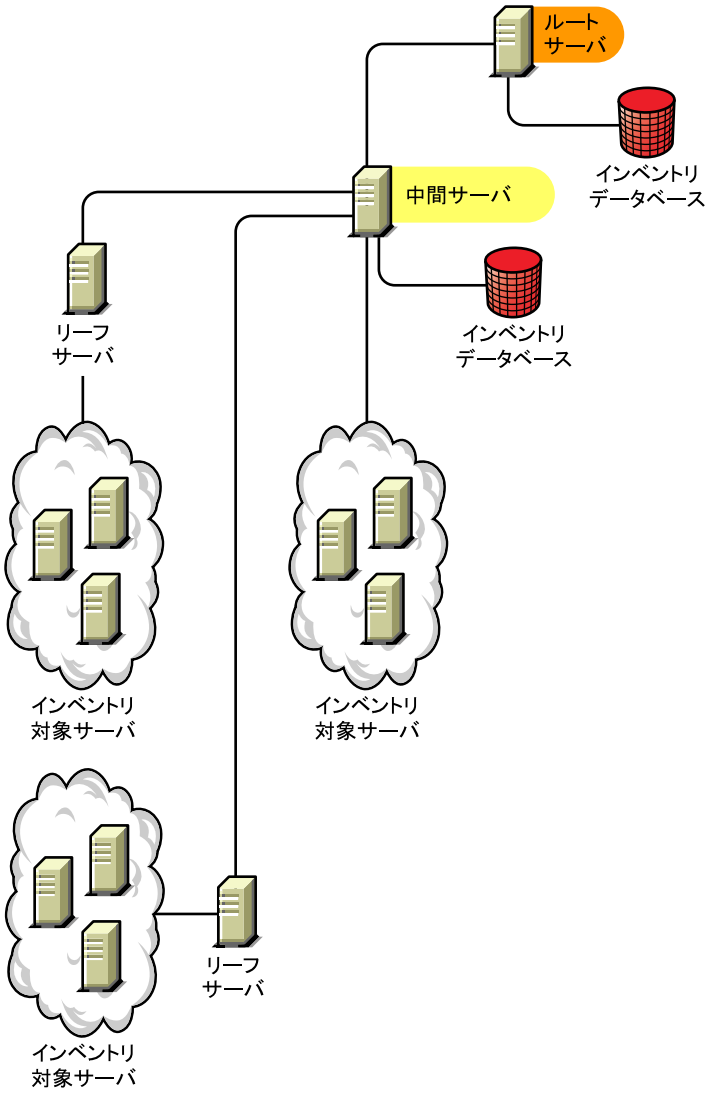
ルートサーバ

ルートサーバには次のような特徴があります。

- このサーバは、インベントリツリー階層の中で、最上位に配置されるインベントリサーバです。
- インベントリデータベースが接続されています。

ルートサーバを選択して企業のインベントリ情報を一元化されたデータベースに保存します。ルートサーバのインベントリデータベースには、すべての下位インベントリサーバのインベントリ情報が保存されます。

次の図は、データベースを搭載した中間サーバに接続されているリーフサーバを示しています。中間サーバはルートサーバに接続されています。



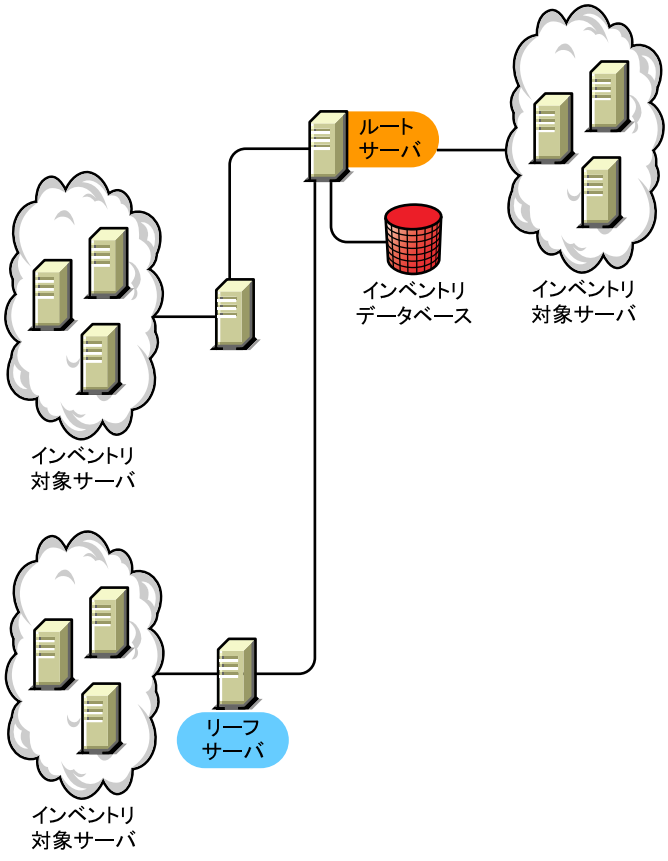
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）

インベントリ対象サーバが接続されているルートサーバには、次のような特徴があります。

- このサーバは、インベントリツリー階層の中で、最上位に配置されるインベントリサーバです。
- このサーバは、インベントリデータベースを含み、インベントリ対象サーバに接続しています。これらのインベントリ対象サーバを LAN 内に展開することをお勧めします。

企業のインベントリ情報を一元化されたデータベースに保存する場合、およびルートサーバと同じサイトにインベントリ対象サーバを配置する場合は、インベントリ対象サーバと接続されたルートサーバを選択します。インベントリ対象サーバからはルートサーバへインベントリ情報を直接送信できます。インベントリ対象サーバが接続されているルートサーバのインベントリデータベースは、すべてのインベントリ対象サーバのインベントリ情報に加え、すべての下位インベントリサーバの情報も保存します。

次の図は、インベントリ対象サーバとインベントリデータベースが接続されているルートサーバを示しています。ルートサーバには、リーフサーバも接続されています。



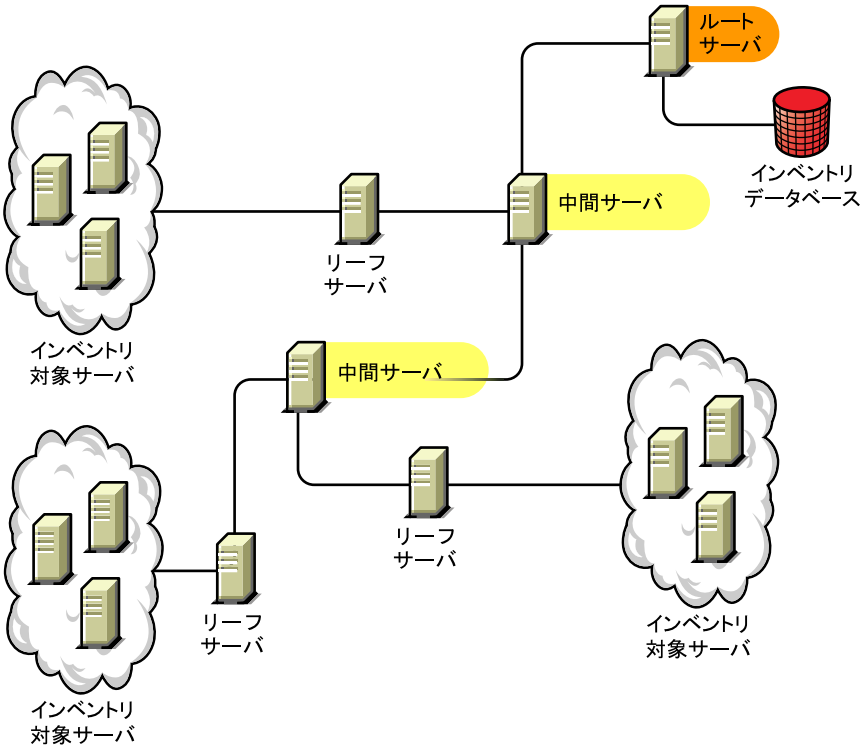
中間サーバ

中間サーバには次のような特徴があります。

- このインベントリサーバは、下位のリーフサーバにとっての中継サーバとして機能します。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- インベントリ対象サーバまたはインベントリデータベースは接続されません。
- 企業内に複数の中間サーバが存在する場合があります。

リンクのパラメータが頻繁に変更されるサイトには中間サーバを設置します。中間サーバのディスクにスキャンファイルを保存することで、帯域幅と信頼性の差をカバーします。

次の図は、ルートサーバに接続されている中間サーバを示しています。2 つのリーフサーバがインベントリ情報を中間サーバにロールアップします。この中間サーバは、インベントリ情報をルートサーバに接続された別の中間サーバにロールアップします。



この図では、多数のリーフサーバと中間サーバが異なるレベルにあります。中間サーバは、スキャン情報を次のレベルのサーバにアップロードするための中継サーバです。最後の中間サーバは、最上位のルートサーバに接続されています。リーフサーバが地理的に分散している場合は、この構成例が一般的です。すべてのリーフサーバはインベントリ情報を中間サーバに転送します。

リーフサーバが WAN 経由で中間サーバに接続される場合もあります。

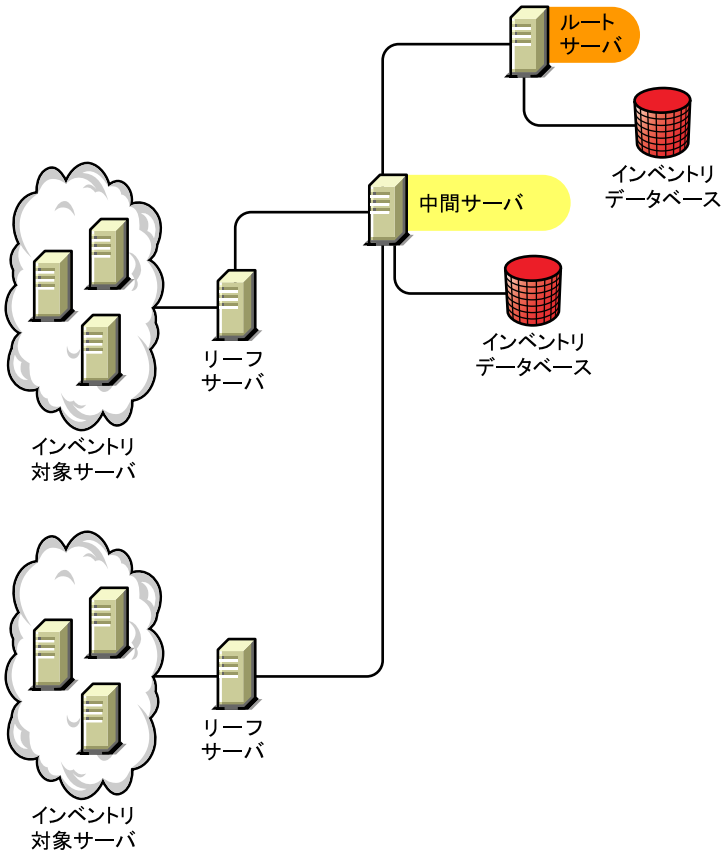
データベースが接続されている中間サーバ

データベースが接続されている中間サーバには次のような特徴があります。

- このインベントリサーバは、下位のリーフサーバにとっての中継サーバとして機能します。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- インベントリデータベースが接続されています。
- 企業内に、データベースが設定された中間サーバが複数存在する場合があります。

インベントリレポートを生成して中間サイトを管理するには、データベースが接続された中間サーバを選択します。このインベントリサーバにロールアップされたインベントリ情報は、ローカルのインベントリデータベースに保存され、さらに次のレベルのインベントリサーバにロールアップされます。

次の図は、2 つのリーフサーバが接続されている中間サーバを示しています。すべてのリーフサーバの統合されたインベントリ情報は、中間サーバレベルに配置されています。



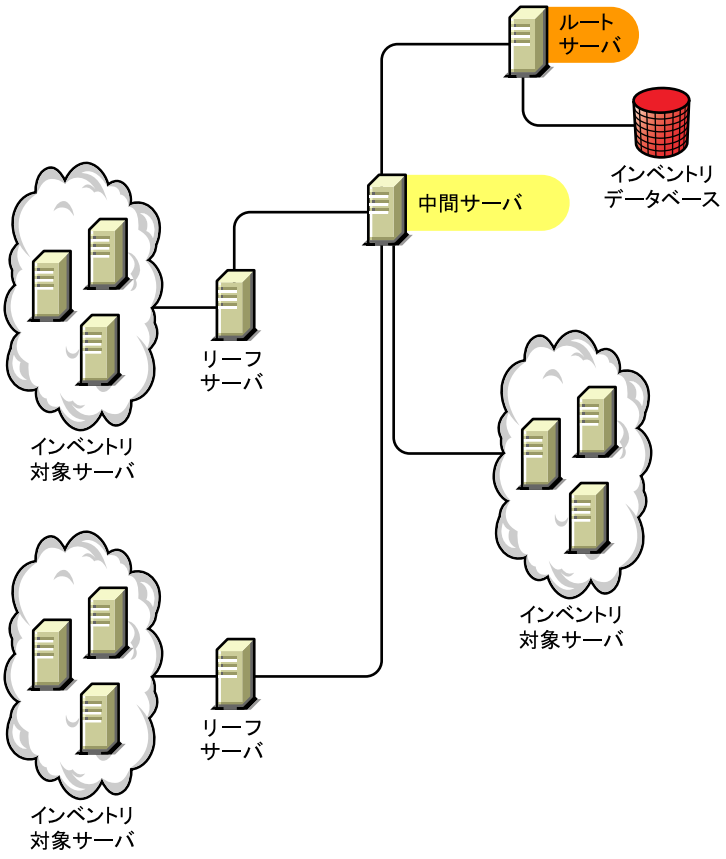
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）

インベントリ対象サーバが接続されている中間サーバには次のような特徴があります。

- 下位のリーフサーバにとっての中間サーバとして機能します。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- インベントリ対象サーバが接続されています。
- インベントリデータベースは接続されていません。
- 企業内に、インベントリ対象サーバに接続する中間サーバが複数存在する場合があります。

中間サーバおよび中間サーバに接続されたサイトにインベントリ対象サーバを接続し、そのインベントリ情報をルートサーバに保存する場合、インベントリ対象サーバに接続された中間サーバを選択します。

次の図は、2 つのリーフサーバが接続されている中間サーバを示しています。この中間サーバには、インベントリ対象サーバも接続されています。



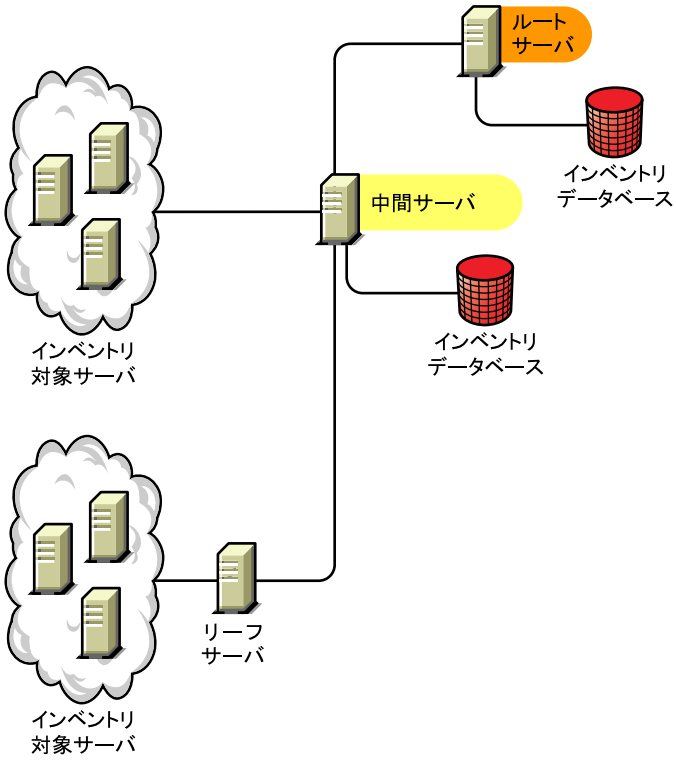
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）

データベースとインベントリ対象サーバが接続されている中間サーバには次のような特徴があります。

- 下位のリーフサーバの中継サーバとして機能します。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- インベントリ対象サーバが接続されています。
- インベントリデータベースが接続されています。
- 企業内に、データベースとインベントリ対象サーバに接続された中間サーバが複数存在する場合があります。

サイトでデータベースが接続されている中間サーバおよび Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）の機能を使用する場合、データベースおよびインベントリ対象サーバに接続された中間サーバを選択します。

次の図は、2 つのリーフサーバが接続されている中間サーバを示しています。中間サーバにインベントリ対象サーバが接続されています。中間サーバに直接接続されたすべてのリーフサーバとインベントリ対象サーバの統合インベントリデータベースは、中間サーバレベルに配置されています。



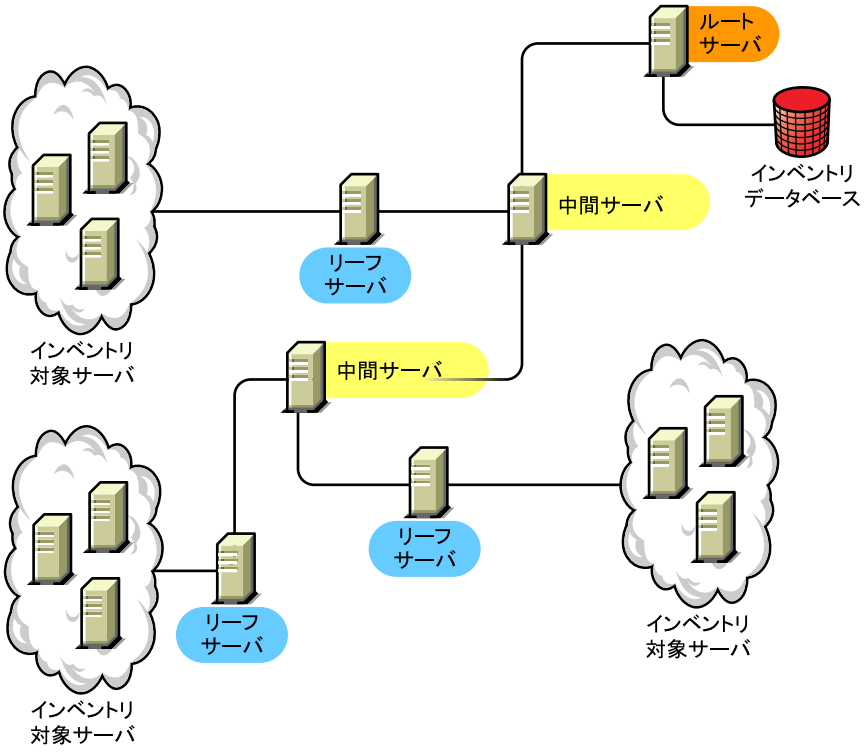
リーフサーバ

リーフサーバには次のような特徴があります。

- インベントリツリー階層内で最下位に配置されるインベントリサーバです。
- インベントリ対象サーバが接続されています。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- シンプルなリーフサーバには、インベントリデータベースが接続されていません。リーフサーバに接続されるインベントリ対象サーバは少ないので、インベントリデータベースは必要ありません。

リモートサイトにインベントリ対象サーバを配置し、かつ一元化されたデータベースのインベントリ対象サーバからインベントリ情報を取得および保存する場合、リーフサーバを選択します。

次の図は、中間サーバに接続されている多数のリーフサーバを示しています。中間サーバはルートサーバに接続されています。すべてのリーフサーバの統合されたインベントリデータベースは、ルートサーバレベルに配置されています。



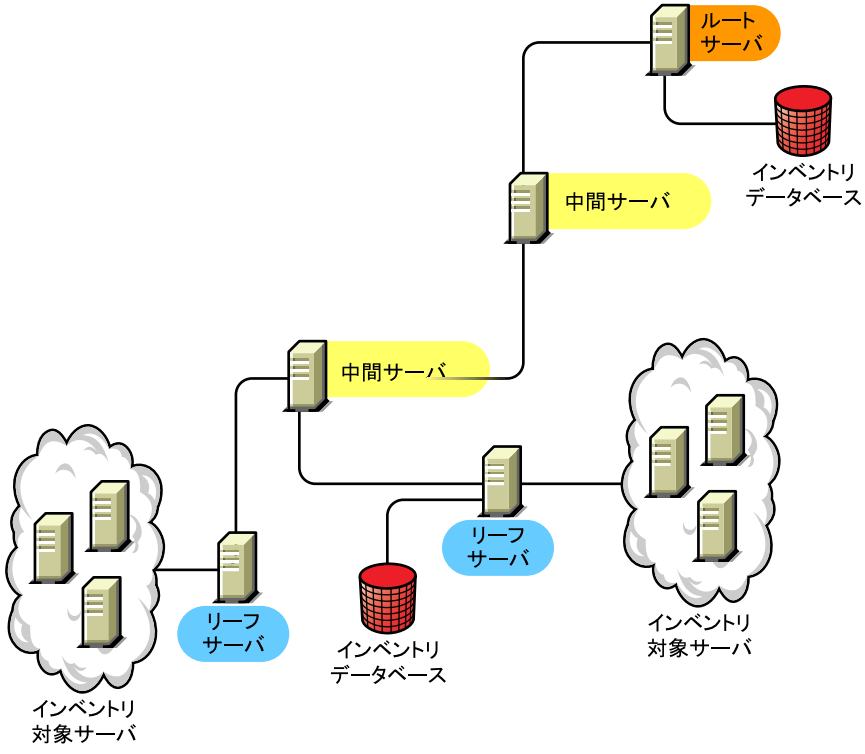
データベースが接続されているリーフサーバ

データベースが接続されているリーフサーバには次のような特徴があります。

- インベントリツリー階層内で最下位に配置されるインベントリサーバです。
- インベントリ対象サーバが接続されています。
- インベントリ情報を次のレベルのインベントリサーバに転送します。
- このサーバには、インベントリデータベースが接続されています。サーバに、データベースが接続されているリーフサーバとしての役割を割り当てて、サイト内にあるインベントリ対象サーバのインベントリ情報を管理できます。

リーフサーバの機能を使用し、かつインベントリレポートを生成してサイトを管理する場合、データベースに接続されているリーフサーバを選択します。

次の図は、2 つのリーフサーバが接続されている中間サーバを示しています。1 つのリーフサーバにインベントリデータベースが接続されています。このデータベースには、このリーフサーバに接続されているすべてのインベントリ対象サーバの統合されたインベントリ情報が格納されています。



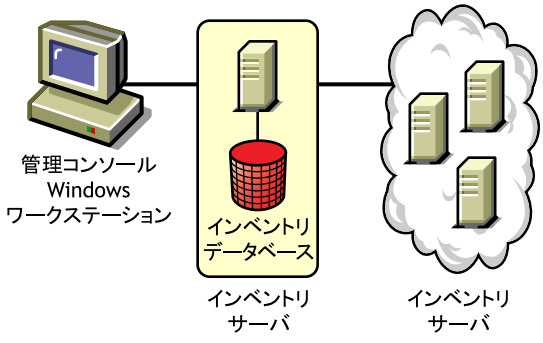
スタンドアロンサーバ

スタンドアロンサーバには次のような特徴があります。

- インベントリ対象サーバが接続されています。
- インベントリデータベースが接続されています。
- スキャン情報のロールアップは実行されず、中間サーバとルートサーバに接続する必要もありません。

ネットワークが 1 つのサイトで構成されているときに、そのサイトを管理する場合には、スタンドアロンサーバを使用します。

次の図は、スタンドアロンサーバを示しています。



インベントリサーバの役割の早見表

Inventory Server	インベントリデータベースの接続の有無	インベントリ対象サーバの接続の有無
ルートサーバ	Yes	No
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	Yes	Yes
中間サーバ	No	No
データベースが接続されている中間サーバ	Yes	No
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	No	Yes
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	Yes	Yes
リーフサーバ	No	Yes
データベースが接続されているリーフサーバ	Yes	Yes
スタンドアロンサーバ	Yes	Yes

13 Server Inventory のセットアップ

作業環境に Novell® ZENworks® 6.5 Server Inventory をインストールする前に、企業のインベントリサーバのツリー構造を計画し、決定しておきます。ネットワークの制約および情報の要件に基づいて、インベントリの展開を決定しておく必要があります。

次の節では、企業内の Server Inventory を展開するために役立つ情報を紹介します。

- 453 ページの「Server Inventory の展開」
- 487 ページの「インベントリデータベースのセットアップ」
- 507 ページの「Inventory Service オブジェクトの設定」
- 508 ページの「データベース場所ポリシーの設定」
- 509 ページの「Server Inventory ポリシーの設定」
- 511 ページの「ロールアップポリシーの設定」
- 513 ページの「ディクショナリ更新ポリシーの設定」
- 514 ページの「ディクショナリの配布の設定」

Server Inventory の展開

次の節は、Server Inventory を展開する際に役立ちます。

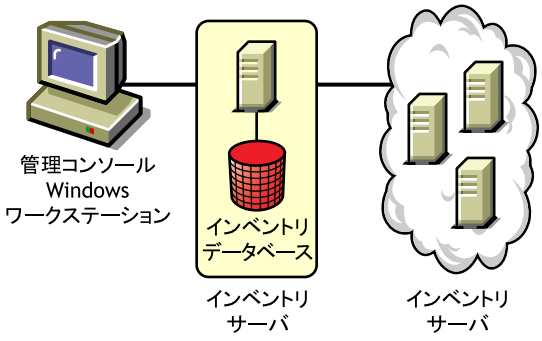
- 453 ページの「単純な展開」
- 457 ページの「高度な展開」

重要： 次の構成は一般的に推奨されるものです。企業内のトポロジに基づいて、さらに調整が必要になる場合があります。

単純な展開

シナリオ例では、ネットワークが単一サイトおよび最大 5000 台のインベントリ対象サーバで構成されています。インベントリサーバのコンポーネントおよびデータベースはスタンドアロンサーバ上に配置され、インベントリ対象サーバはスキャン情報をスタンドアロンサーバに送信します。

次の図は、この場合の構成例を示しています。



次の節では、単一サイト内の Server Inventory を展開するために役立つ情報を紹介します。

1. 454 ページの「展開に関する推奨事項」
2. 455 ページの「Server Inventory のインストール」
3. 455 ページの「Server Inventory のインストールの効果の理解」
4. 455 ページの「必要なポリシーの設定」
5. 455 ページの「Inventory Service の開始」
6. 455 ページの「ソフトウェアディクショナリの更新」
7. 455 ページの「スタンドアロン構成でのインベントリスキャンサイクルの理解」

展開に関する推奨事項

- インベントリサーバの最低要件は、512MB の RAM および 128MB のデータベースキャッシュを搭載していることです。
- インベントリサーバへのインベントリ情報の転送と、インベントリデータベースへのインベントリ情報の保存は、継続されるバックエンドプロセスであり、このプロセスには数時間または 1 日以上かかる場合があります。
- 1台のインベントリサーバに多数のインベントリ対象サーバが接続されている場合、すべてのインベントリ対象サーバのスキャンを一度に実行するようなスケジュールを設定しないことをお勧めします。一度に集中してスキャンを実行すると、Novell eDirectory™ および Inventory Service に負荷がかかります。
- eDirectory の時刻の同期間隔を 2 秒以内に設定します。
- サーバに搭載する最適なデータベースキャッシュサイズの要件は、サーバ環境によって異なる場合があります。ランタイム環境でさまざまなキャッシュサイズを試してみたうえで、必要なデータベースキャッシュサイズを決定してください。デフォルトでは、Sybase データベースのキャッシュサイズは 128MB です。データベースのパフォーマンス向上に関する詳細については、691 ページの付録 H、「パフォーマンスに関するヒント」を参照してください。

Server Inventory のインストール

Server Inventory のインストール時には、[Inventory Standalone Configuration] の設定を設定します。Server Inventory インストールの詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」にある「NetWare および Windows へのインストール」を参照してください。

Server Inventory のインストールの効果の理解

Server Inventory のインストールの効果に関する詳細については、474 ページの「Server Inventory のインストールの効果の理解」を参照してください。

必要なポリシーの設定

Server Inventory ポリシーを設定します。

Inventory Service の開始

ZENworks 6.5 Server Management のインストール後、Inventory Service が自動的に開始されます。

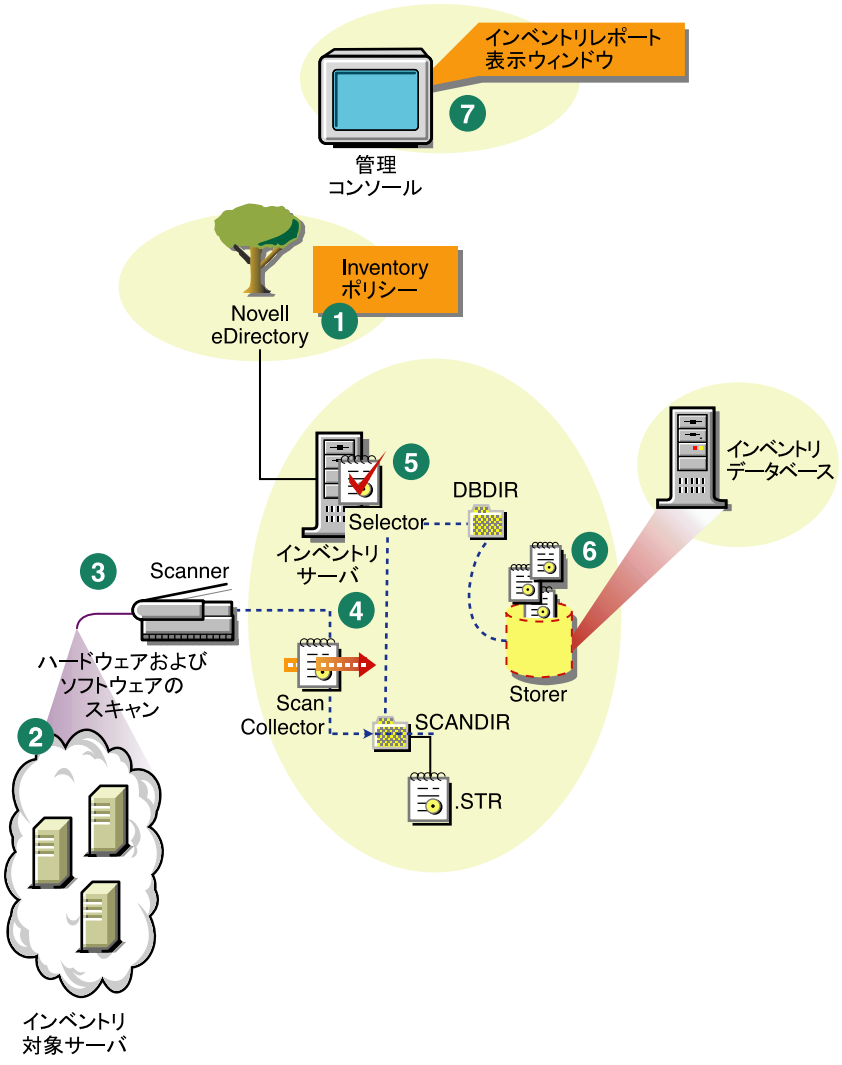
ソフトウェアディクショナリの更新

Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) から最新バージョンのディクショナリを手動でダウンロードし、ソフトウェアディクショナリを更新する必要があります。

注： Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) では、3ヶ月に 1 度ディクショナリが更新され、TID として発行されます。

スタンドアロン構成でのインベントリスキャンサイクルの理解

次の図は、スタンドアロン構成のスキャンコンポーネントとインベントリスキャンサイクルを示しています。これらについては以下で説明します。



インベントリスキャンサイクルは次のとおりです。

1. eDirectory の Inventory ポリシーによってインベントリの設定が定義されます。こうした設定には、インベントリ情報の送信先になるインベントリサーバの Inventory Service オブジェクト名、スキャン時間などが含まれます。これらの設定はカスタマイズできます。
2. Scanner は Policy and Distribution Services を使用して、Inventory ポリシーを読み取り、ポリシー設定に基づいてインベントリ情報を収集します。Inventory Scanner は、インベントリサーバでのディクショナリの更新を確認し、更新されたディクショナリをダウンロードします。
3. Scanner は、インベントリ対象サーバにローカルでインベントリ情報を保存します。この情報は、XML-RPC プロトコルを使用してインベントリサーバに転送されます。
4. Scan Collector は、XML-RPC プロトコルを使ってインベントリ情報を受信し、この情報をインベントリサーバのスキャンディレクトリに保存します。Scan Collector は、ZEN Web Server を使用して XML-RPC 要求を処理します。
5. Selector は、インベントリ情報を検証し、インベントリデータベースにその情報を保存します。
6. Storer は、インベントリ情報でデータベースを更新します。
7. ZENworks 管理者はインベントリ情報の照会を実行できます。

高度な展開

- 457 ページの「5000 台より多いインベントリ対象サーバを配置する単一サイトでのインベントリ展開」
- 460 ページの「複数サイトまたは企業サイトにおけるインベントリの展開」

5000 台より多いインベントリ対象サーバを配置する単一サイトでのインベントリ展開

このシナリオ例では、ネットワークは単一サイトおよび 5000 台より多いインベントリ対象サーバで構成されています。インベントリ設定は 2 台以上のスタンドアロンサーバで構成され、各サーバが最大 5000 台のインベントリ対象サーバからスキャン情報を受信します。すべてのスタンドアロンサーバはインベントリデータを単一データベースに保存します。

次の節では、単一サイト内の Server Inventory を展開するために役立つ情報を紹介します。

1. 457 ページの「展開に関する推奨事項」
2. 458 ページの「Server Inventory のインストール」
3. 458 ページの「Server Inventory のインストールの効果の理解」
4. 458 ページの「必要なポリシーの設定」
5. 458 ページの「Inventory Service の開始」
6. 458 ページの「ソフトウェアディクショナリの更新」
7. 458 ページの「スタンドアロン構成でのインベントリスキャンサイクルの理解」

展開に関する推奨事項

- インベントリサーバの最低要件は、512MB の RAM および 128MB のデータベースキャッシュを搭載していることです。
- すべてのインベントリ対象サーバは、LAN 上の最も近いインベントリサーバにインベントリ情報を送信します。ポリシーは、この情報に基づいて作成する必要があります。
- インベントリサーバへのインベントリ情報の転送と、インベントリデータベースへのインベントリ情報の保存は、継続されるバックエンドプロセスであり、このプロセスには数時間または 1 日以上かかる場合があります。
- 1台のインベントリサーバに多数のインベントリ対象サーバが接続されている場合、すべてのインベントリ対象サーバのスキャンを一度に実行するようなスケジュールを設定しないことをお勧めします。一度に集中してスキャンを実行すると、Novell eDirectory™ および Inventory Service に負荷がかかります。
- eDirectory の時刻の同期間隔を 2 秒以内に設定します。
- サーバに搭載する最適なデータベースキャッシュサイズの要件は、サーバ環境によって異なる場合があります。ランタイム環境でさまざまなキャッシュサイズを試してみたうえで、必要なデータベースキャッシュサイズを決定してください。デフォルトでは、Sybase データベースのキャッシュサイズは 128MB です。データベースのパフォーマンス向上に関する詳細については、691 ページの付録 H 、「パフォーマンスに関するヒント」を参照してください。

Server Inventory のインストール

Server Inventory のインストールに関する詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」にある「NetWare および Windows へのインストール」を参照してください。

Server Inventory のインストールの効果の理解

Server Inventory のインストールの効果に関する詳細については、474 ページの「Server Inventory のインストールの効果の理解」を参照してください。

必要なポリシーの設定

Server Inventory ポリシーを設定します。

Inventory Service の開始

ZENworks 6.5 Server Management のインストール後、Inventory Service が自動的に開始されます。

ソフトウェアディクショナリの更新

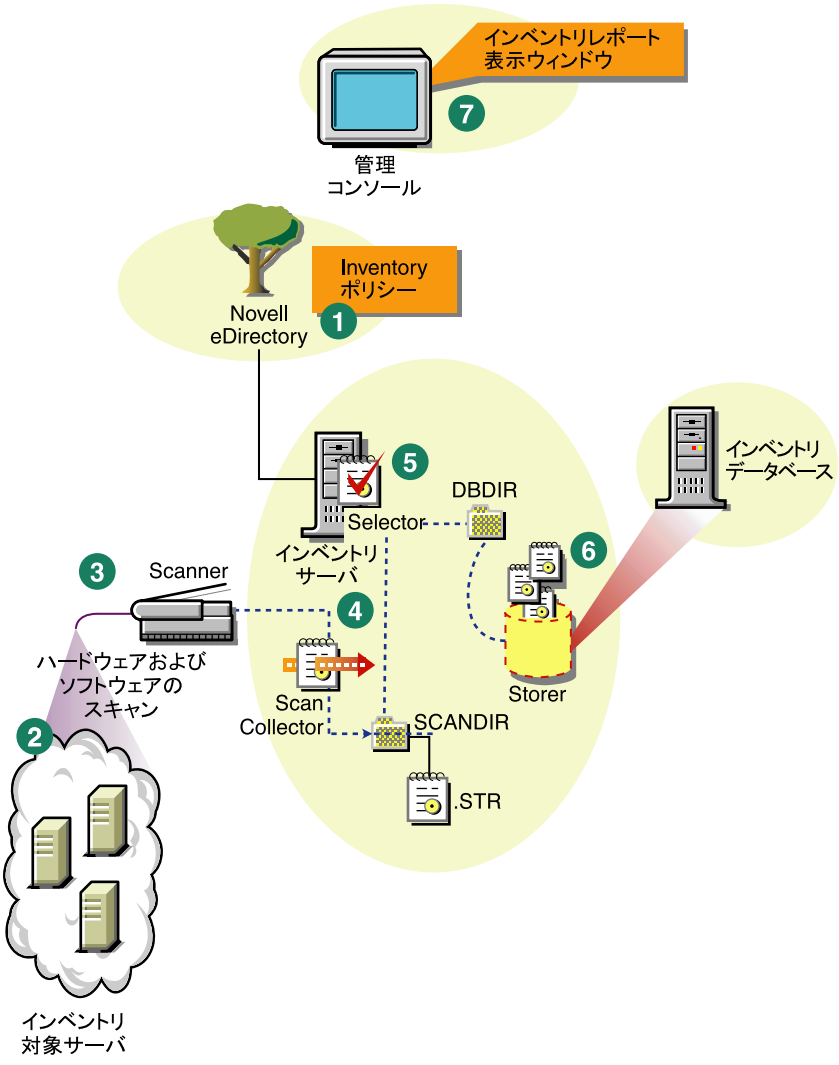
次のいずれかの方法で、ソフトウェアディクショナリを更新できます。

- 各インベントリサーバで、Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) から最新バージョンのディクショナリを手動でダウンロードし、ソフトウェアディクショナリを更新します。
- Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) からスタンドアローンサーバのいずれかに最新バージョンのディクショナリを手動でダウンロードし、513 ページの「ディクショナリ更新ポリシーの設定」を設定する手順でこのサーバから他のすべてのスタンドアロンサーバにディクショナリを自動的に配布します。詳細については、514 ページの「ディクショナリの配布の設定」を参照してください。

注： Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) では、3ヶ月に 1 度ディクショナリが更新され、TID として発行されます。

スタンドアロン構成でのインベントリスキャンサイクルの理解

次の図は、スタンドアロン構成のスキャンコンポーネントとインベントリスキャンサイクルを示しています。これらについては以下で説明します。



インベントリスキャンサイクルは次のとおりです。

1. eDirectory の Inventory ポリシーによってインベントリの設定が定義されます。こうした設定には、インベントリ情報の送信先になるインベントリサーバの Inventory Service オブジェクト名、スキャン時間などが含まれます。これらの設定はカスタマイズできます。
2. Scanner は Policy and Distribution Services を使用して、Inventory ポリシーを読み取り、ポリシー設定に基づいてインベントリ情報を収集します。Inventory Scanner は、インベントリサーバでのディクショナリの更新を確認し、更新されたディクショナリをダウンロードします。
3. Scanner は、インベントリ対象サーバにローカルでインベントリ情報を保存します。この情報は、XML-RPC プロトコルを使用してインベントリサーバに転送されます。
4. Scan Collector は、XML-RPC プロトコルを使ってインベントリ情報を受信し、この情報をインベントリサーバのスキャンディレクトリに保存します。Scan Collector は、ZEN Web Server を使用して XML-RPC 要求を処理します。
5. Selector は、インベントリ情報を検証し、インベントリデータベースにその情報を保存します。
6. Storer は、インベントリ情報でデータベースを更新します。
7. ZENworks 管理者はインベントリ情報の照会を実行できます。

複数サイトまたは企業サイトにおけるインベントリの展開

次の節では、複数または企業内のサイトで Server Inventory を展開するために役立つ情報を紹介します。

1. 460 ページの「インベントリツリーの構築」
2. 465 ページの「インベントリサーバおよびインベントリデータベースの展開オプション」
3. 470 ページの「展開に関する推奨事項」
4. 471 ページの「Server Inventory のインストール」
5. 471 ページの「Server Inventory のインストールの効果の理解」
6. 471 ページの「必要なポリシーの設定」
7. 472 ページの「Inventory Service の開始」
8. 472 ページの「ソフトウェアディクショナリの更新」
9. 473 ページの「サーバ間でのインベントリ情報のロールアップの理解」

インベントリツリーの構築

企業または複数サイトで、次の作業を順番に実行して、インベントリツリーを構築します。

- 460 ページの「1. 企業内のサイトリストの作成」
- 461 ページの「2. ルートサーバを配備する最適な場所」
- 462 ページの「3. その他に必要なデータベースの特定」

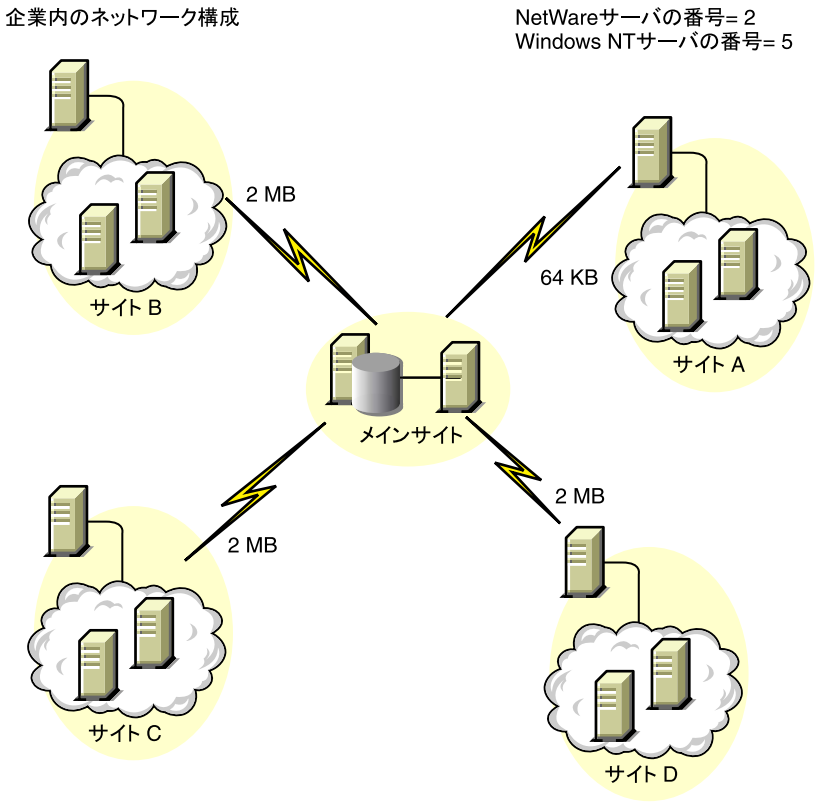
  462 ページの「オプションの手順：別のデータベースが必要な場合」
- 462 ページの「4. インベントリ情報のルートの特定」
- 463 ページの「5. 各サイトでインベントリサーバおよびデータベースサーバとして機能するサーバの特定」
- 464 ページの「6. 企業のインベントリデータを収集するためのサーバツリーの作成」
- 464 ページの「7. 実装計画の作成」
- 464 ページの「8. 実際の展開の開始」

1. 企業内のサイトリストの作成

企業全体のネットワークについて把握します。

- 企業内のサイトのリストを作成します。
- サイト間の物理リンクのリストを作成します。
- 帯域幅と信頼性の観点からリンクの種類を判断します。

次の図は、サーバが複数の場所に分散している企業内ネットワークの編成を示しています。



この図は、4 つのサイト (サイト A、サイト B、サイト C、サイト D) が中央のサイトに接続されていることを示しています。サイト間の物理リンクと、帯域幅から見たリンクの種類を示しています。

2. ルートサーバを配備する最適な場所

インベントリツリーのルートサーバは、最上位のサーバです。したがって、インベントリデータベースはルートサーバに接続する必要があります。

ルートサーバのインベントリデータベースには、ネットワーク上の下位にあるすべてのサイトとルートサーバサイトのインベントリ情報が保存されます。

次の点を考慮する必要があります。

- ルートサーバと管理コンソール間は高速リンクにする必要があります。
- ルートサーバが配置されているサイトと下位のインベントリサーバが配置されているサイト間は高速リンクにすることをお勧めします。
- 管理コンソールを使用すると、管理者は高速リンクでルートサーバに接続されているサイト、またはルートサーバレベルのサイトからインベントリ情報を収集できます。
- ネットワーク構成に適したデータベースサーバをインベントリサーバ用に準備する必要があります。

3. その他に必要なデータベースの特定

ルートサーバのデータベースに加え、サイト別にデータベースサーバを管理することができます。

異なる場所のインベントリを管理するために複数のサイトやサブツリーがあり、それらのサイトからネットワークへの接続リンクが低速である場合は、追加のデータベースを配置することができます。

また、単一サイトおよびサイトグループに個別のデータベースを用意すべきかどうかを判断する必要があります。製品を展開するだけなら他のデータベースを使用する必要がなくても、企業によってはさまざまなサイトにデータベースを配置する必要がある場合もあります。

注： ほとんどの企業では、企業全体で 1 つのデータベースを配置する以外に他のデータベースは必要ありません。

オプションの手順：別のデータベースが必要な場合

- データベースサーバを追加する場合は、データベースを必要としているサイトを特定します。また、データベースを必要としているサイトが、ローカルサイトなのか、多数のサブサイトから構成されるサイトなのかを確認する必要があります。各インベントリデータベースに情報を保存する必要があるサイトの特定もします。
- 単一のデータベースを使用するすべてのサイトでは、通常、ルートサーバのデータベースではなく、単一のデータベースにアクセスしてインベントリ管理を実行します。これにより、ルートサーバに搭載されているデータベースへの負荷が軽減されます。
- これらのサイトには、データベース管理者が必要です。

4. インベントリ情報のルートの特定

すべてのインベントリサーバのインベントリ情報を最も近くにあるデータベースに転送するルートを決定します。

ルートを決定するには

- 各ルートの中継サイトには、中間サーバを配置することができます。中間サーバは、情報を受信して次のサーバに転送します。これらは、インベントリ情報を転送するためのアプリケーション層レベルのルートです。隣接する 2 つのサーバ間には、ネットワーク層レベルのルートが複数存在する場合があります。これらのルートの決定および管理は、ネットワーク上のルータによって実行されます。
- ルートには、特定のサイトから最終目的地であるルートサーバのデータベースにインベントリ情報を転送する方法を示す情報が含まれています。
- 複数のルートが存在する場合があります。最も高速で信頼性の高いルートを選択してください。ルートを決定するには、物理ネットワークリンクを考慮する必要があります。
- ルートを決定して稼動した場合でも、後からそのルートを変更することができます。ただし、管理機能が損なわれたり、トラフィックが発生したりする場合があります。中間データベースがない場合は、eDirectory ベースのポリシーを変更することによりルートを変更できます。
- リンクのパラメータが頻繁に変更されるサイトには中間サーバを配置します。リンクの帯域幅や信頼性の違い、インベントリ情報のロールアップの必要性などを考慮する必要があります。

- 中間サーバを配置するサイトを決定するときには、インベントリ情報を中継するために中間サイトのインベントリサーバを使用できるかどうかを考慮する必要があります。Sender がインベントリ情報を次のサーバに送るまで、これらのサーバにはすべてのデータを格納しておけるだけのディスク容量が必要です。

5. 各サイトでインベントリサーバおよびデータベースサーバとして機能するサーバの特定

ZENworks 6.5 Server Management では、インベントリサーバごとに役割を選択します。詳細については、443 ページの「インベントリサーバの役割の理解」を参照してください。

インベントリサーバに接続されているインベントリ対象サーバの数によって、サーバの負荷が決まります。次の表は、各サーバに必要なディスク容量を示しています。

サーバタイプ	必要なディスク容量
リーフサーバ	*(n1 x s)* + *(n1 x z)*
データベースが接続されているリーフサーバ	*(n1 x s* x 2) + {*(n1 x dbg)*}
中間サーバ	*n2 x z*
データベースが接続されている中間サーバ	*(n2 x z)* + *(n2 x s)* + {*(n2 x dbg)*}
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	*(n1 x s x 2)* + *(n2 x z)*
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	*(n1 x s x 2)* + *(n2 x z)* + *(n2 x s)* + {*(n1 x dbg)* + *(n2 x dbg)*}
ルートサーバ	*(n2 x z)* + *(n2 x s)* + {*(n2 x dbg)*}
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	*(n1 x s x 2)* + *(n2 x z)* + *(n2 x s)* + {*(n1 x dbg)* + *(n2 x dbg)*}
スタンドアロンサーバ	*(n1 x s x 1)* + {*(n1 x dbg)*}

この表では、*n1* はサーバに接続されたインベントリ対象サーバの数を示します。

s はスキャンデータファイルのサイズです。このファイルサイズは、収集される情報によって異なります。インベントリ対象サーバ 1 台あたりのスキャン情報を 400KB として負荷を計算してください。

dbg は、データベース内のインベントリ情報の保存容量を示します。

n2 は、インベントリサーバにロールアップされているインベントリ対象サーバ数を示します。

z は、インベントリ対象サーバ 1 台あたりの圧縮スキャンデータファイルのサイズです。平均的な圧縮率は STR ファイルサイズの 80 ～ 90% です。

{ } は、データベースサーバのディスク容量を示します。この容量は、データベースが同一インベントリサーバ上にあるのか、インベントリサーバに接続されているのかによって異なります。データベースが同一インベントリサーバ上にある場合、データベースの容量を含めたインベントリサーバの合計ディスク容量を計算してください。たとえば、データベースが接続されたリーフサーバという役割のサーバ上に、インベントリデータベースが搭載されている場合は、インベントリ情報の保存に必要な容量を計算し、データベースのディスク容量も加えます。

6. 企業のインベントリデータを収集するためのサーバツリーの作成

設計するインベントリツリーが次のガイドラインに沿っていることを確認してください。

- ツリーのルートはルートサーバにします。
- 少なくともサイトごとに1台のインベントリサーバを配置することをお勧めします。
- 各サイトに、スキャンするインベントリ対象サーバを配置します。
- オプションとして、データベースサーバと中間サーバを別々のサイトに配置することもできます。

7. 実装計画の作成

インベントリツリーの設計後、ネットワークを段階的に展開していくための実装計画を立てる必要があります。Server Inventory をインストールする際には、上位から下位へと展開します。最上位のサーバ（ルートサーバ）からインストールを開始して、次の下位レベルのサーバのインストールに進みます。

8. 実際の展開の開始

実装計画を作成したら、その計画に従って実際の展開を開始します。

次の手順を実行します。

1. サイトにインベントリサーバを配置します。詳細については、471 ページの「Server Inventory のインストール」を参照してください。
2. インベントリサーバとインベントリ対象サーバに適用可能なポリシーを作成および設定します。詳細については、471 ページの「必要なポリシーの設定」を参照してください。

インベントリをセットアップするためのデータベースサーバの追加

インベントリをセットアップするためにサーバがすでに設定されているが、別のデータベースサーバを追加したい場合は、次の手順に従ってください。

1 インストールプログラムを実行して、サーバにインベントリデータベースをインストールします。

インストールプログラムにより、Sybase データベースがインストールされます。Oracle でデータベースを管理する場合は、Oracle データベースが存在することを確認します。詳細については、494 ページの「Oracle 8i インベントリデータベースの設定」および498 ページの「Oracle 9i インベントリデータベースのセットアップ」を参照してください。MS SQL でデータベースを管理する場合は、MS SQL データベースが存在することを確認します。詳細については、502 ページの「MS SQL Server 2000 インベントリデータベースのセットアップ」を参照してください。

2 Inventory Service をシャットダウンします。詳細については、477 ページの「NetWare インベントリサーバでの Inventory Service の停止」を参照してください。

3 選択したデータベースに基づいて、データベースの設定を確認します。詳細については、508 ページの「データベース場所ポリシーの設定」を参照してください。

4 データベースが接続されていない既存のインベントリサーバに新しいデータベースを接続するには、Inventory Service オブジェクト (Inventory Service_*server_name*) でインベントリサーバの役割を変更する必要があります。たとえば、既存のリーフサーバにインベントリデータベースを接続する場合、リーフサーバの Inventory Service オブジェクトでサーバの役割をリーフサーバからデータベースが接続されたリーフサーバに変更します。

新しく設置したインベントリサーバにインベントリデータベースを接続する場合は、そのインベントリサーバに適したサーバの役割を選択します。

インベントリサーバの役割を変更するには

4a ConsoleOne で、Inventory Service オブジェクトを右クリックし、[Properties]、[Inventory Service Object Properties] タブの順にクリックします。

4b Inventory Service オブジェクトの新しい役割を選択してから、[Apply] をクリックします。

役割を変更するために必要なアクションを実行します。詳細については、478 ページの「インベントリサーバの役割変更」を参照してください。

5 Inventory Service オブジェクトのフルスキャンを指定していることを確認します。

5a ConsoleOne で、Inventory Service オブジェクトを右クリックし、[Properties]、[Inventory Service Object Properties] タブの順にクリックします。

5b [Enable Scan] オプションを選択し、[OK] をクリックします。

6 Inventory Service を開始します。詳細については、476 ページの「NetWare インベントリサーバでの Inventory Service の起動」を参照してください。

インベントリサーバおよびインベントリデータベースの展開オプション

以下の節では、構成例をいくつか紹介します。

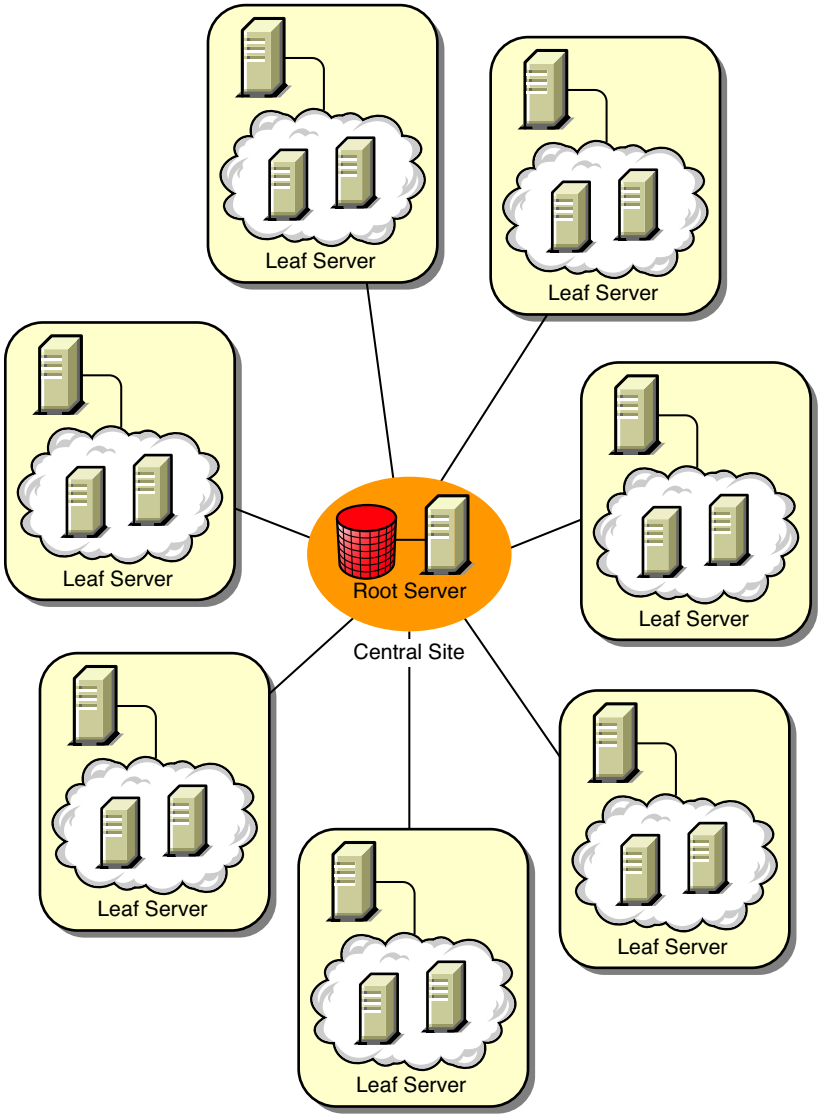
- 465 ページの「シナリオ 1:WAN における中間サーバを使用しないインベントリの展開」
- 466 ページの「シナリオ 2:WAN における中間サーバを使用したインベントリの展開」
- 468 ページの「シナリオ 3:eDirectory ツリー間のインベントリ情報のロールアップ」
- 469 ページの「シナリオ 4:eDirectory ツリーの統合」
- 469 ページの「シナリオ 5: ファイアウォール間のインベントリサーバの展開」

シナリオ 1:WAN における中間サーバを使用しないインベントリの展開

この構成では、WAN 経由で多くのリモートサイトが中央サイトに接続されたネットワークが構成されています。各リモートサイトにはリーフサーバがあります。リーフサーバは同じサイトのインベントリ対象サーバからインベントリ情報を収集し、そのインベントリ情報を中央のサイトにあるルートサーバにロールアップします。リーフサーバ自体にインベントリデータベースが接続されているため、リモートサイトは中央サイトから管理されます。

ヒント： リモートサイトをローカルで管理するには、リーフサーバにインベントリデータベースを接続し、インベントリサーバの役割をデータベースに接続されたリーフサーバに変更する必要があります。インベントリサーバの役割の変更方法の詳細については、478 ページの「インベントリサーバの役割変更」を参照してください。

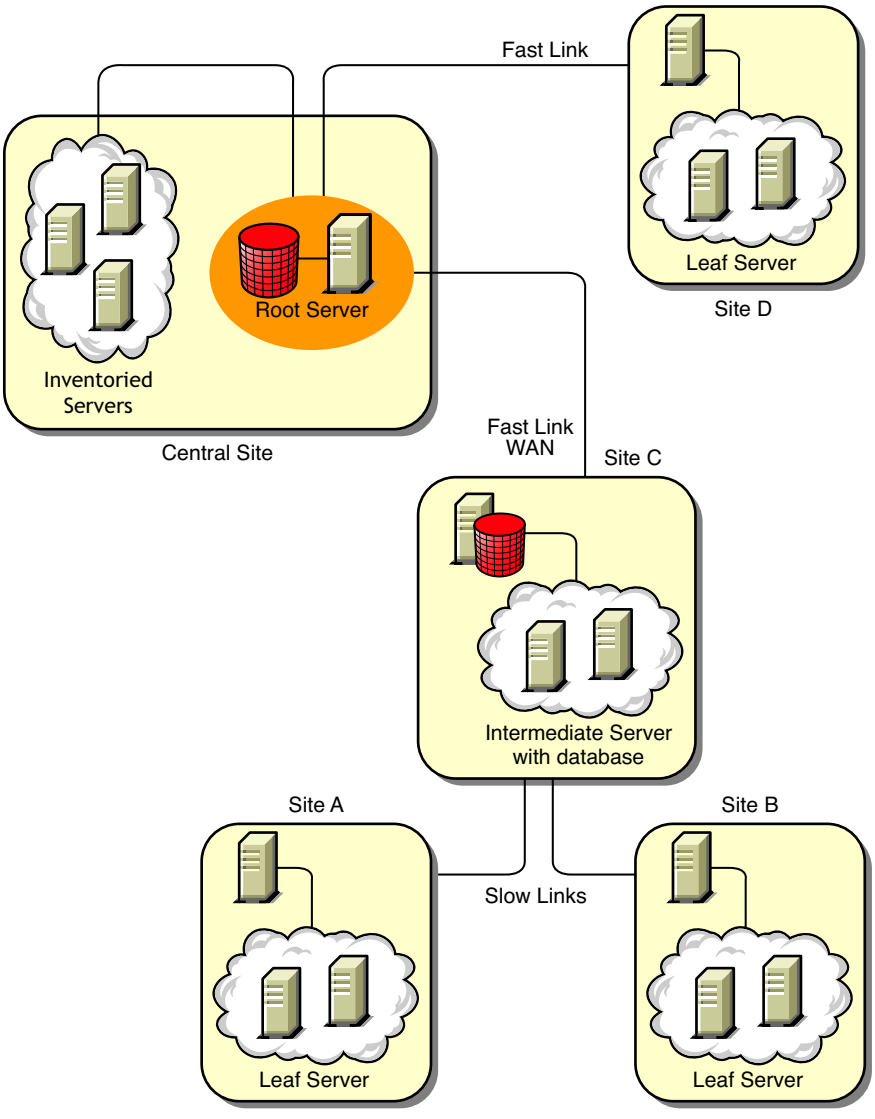
次の図は、この場合の構成例を示しています。



シナリオ 2:WAN における中間サーバを使用したインベントリの展開

この構成では、4 つのリモートサイト（A、B、C、および D）と中央サイトでネットワークが構成されています。サイト A およびサイト B は低速リンクでサイト C に接続され、中央サイトには直接接続されていません。サイト C は高速 WAN リンクで中央サイトに接続されています。サイト D は高速リンクで中央サイトに直接接続されています。サイト A、B、C は、サイト C で管理されます。

このシナリオを図で表すと次のようになります。



中央サイトから企業ネットワークを管理し、さらにサイト C からサイト A およびサイト B を管理するには、次のようにします。

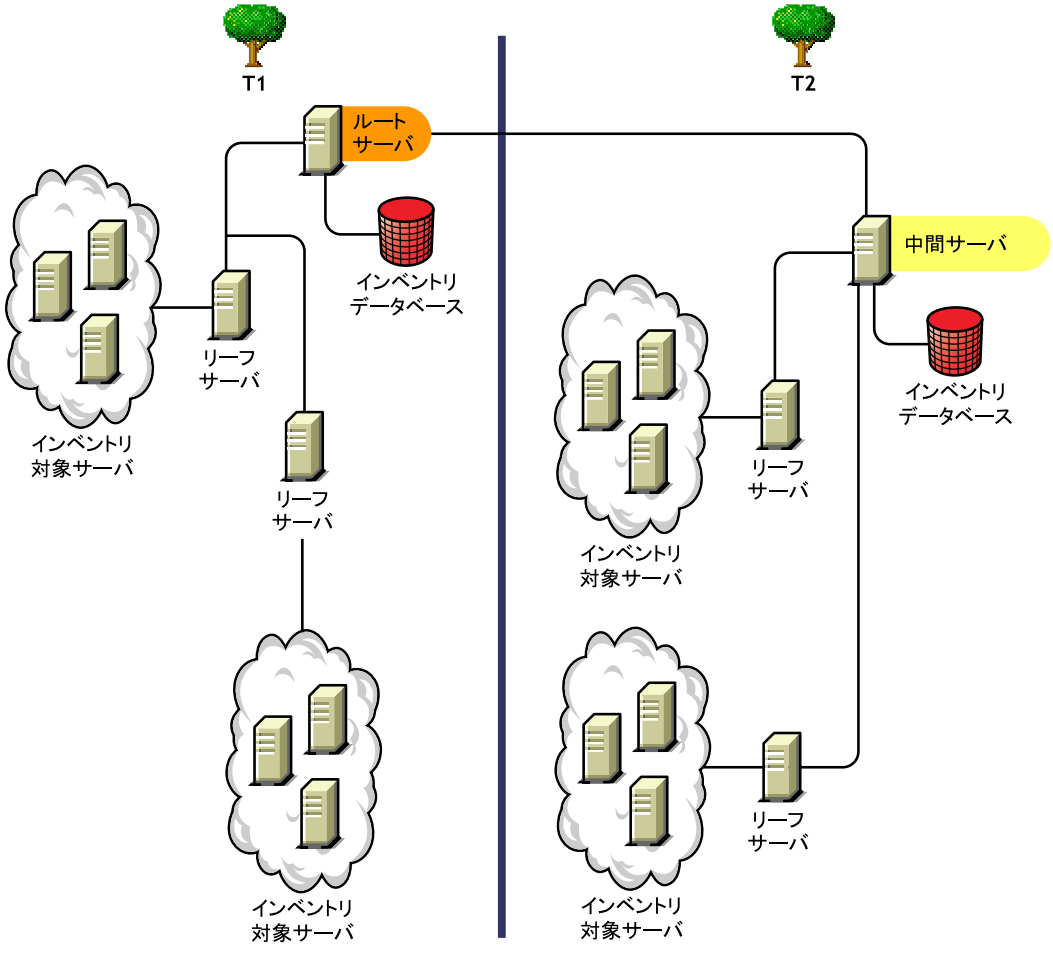
1. サイト A、サイト B、およびサイト D にリーフサーバを設置します。
2. サイト C に、データベースが接続された中間サーバを設置します。
3. サイト A およびサイト B のリーフサーバを設定し、サイト C にあるデータベースが接続された中間サーバにインベントリ情報がロールアップされるようにします。
4. サイト C にあるデータベースが接続された中間サーバを設定し、インベントリ情報が中央サイトのルートサーバにロールアップされるようにします。
5. サイト D のリーフサーバを設定し、インベントリ情報が中央サイトのルートサーバにロールアップされるようにします。

シナリオ 3:eDirectory ツリー間のインベントリ情報のロールアップ

この構成では、これまでに紹介したいずれの構成でも展開できます。一方の eDirectory ツリー内の最上位のインベントリサーバは、他方の eDirectory ツリーに配置されているインベントリサーバにインベントリ情報をロールアップします。

この構成では、ポリシーを配布するために、各 eDirectory ツリーに Distributor をインストールする必要があります。

次の図は、このインベントリ環境設定を展開できる構成例を示しています。



A と B の 2 つの組織があります。各組織には、eDirectory ツリーとインベントリツリーがあります。組織 A のインベントリツリーには 2 台のリーフサーバと 1 台のルートサーバが配置されています。組織 B のインベントリツリーにも 2 台のリーフサーバと 1 台のルートサーバが配置されています。両方の組織とインベントリツリーを統合し、それぞれの eDirectory ツリーは残すことが決定されました。統合すると、eDirectory ツリー T2 のルートサーバの役割は、データベースが接続されている中間サーバに変更され、インベントリ情報は中間サーバから eDirectory ツリー T1 にあるルートサーバにロールアップされます。

シナリオ 4:eDirectory ツリーの統合

この構成では、インベントリツリーおよび eDirectory ツリーの統合が可能です。eDirectory ツリーを統合すると、Inventory Service を起動する前に、*inventory_server_installation_drive* または *volume*¥zenworks¥inv¥server¥wminv¥properties¥config.properties ファイルで eDirectory ツリー名および Inventory Service の DN（オプション）を手動で変更する必要があります。eDirectory ツリーの統合の詳細については、Novell eDirectory Documentation Web サイト (http://www.novell.com/documentation) を参照してください。

インベントリツリーを統合するには、一方のインベントリツリーのルートサーバの役割を、他方のインベントリツリーのインベントリサーバにロールアップするように変更する必要があります。

eDirectory ツリー名とインベントリサーバの DN を変更するには、config.properties ファイルの次のエントリを編集します。

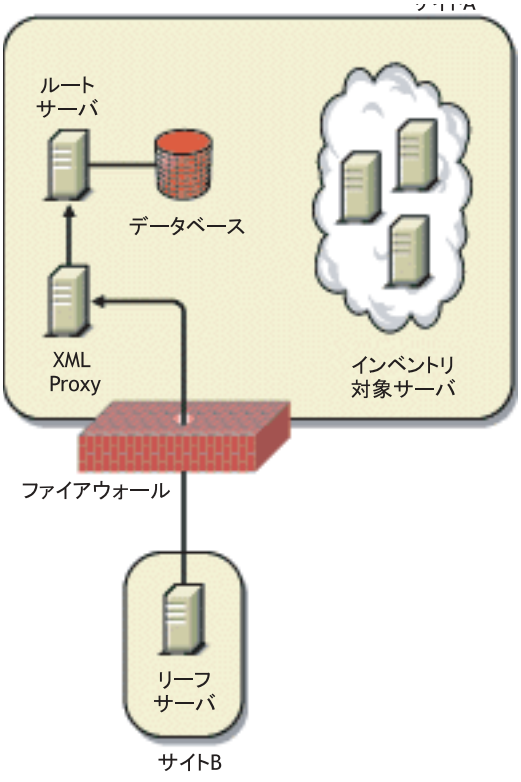
```
NDSTree=Target_eDirectory_tree_name

InventoryServiceDN=New_DN_of_the_Inventory_server
```

シナリオ 5: ファイアウォール間のインベントリサーバの展開

WAN リンクで接続されているサイト A およびサイト B の 2 つのサイトがあります。サイト A のインベントリサーバはサイト B のインベントリサーバにロールアップします。サイト A からサイト B への通信は、すべてサイト B のファイアウォールを経由します。

次の図は、このインベントリ環境設定を展開できる構成例を示しています。



ロールアップを有効にするには

- サイトAにXMLプロキシをインストールします。プロキシのインストールの詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」にある「NetWare および Windows へのインストール」を参照してください。
- サイトごとに少なくとも1つのXMLプロキシをインストールする必要があります。プロキシサーバ1台で、複数のインベントリサーバの要求に対処できます。
- ZENworks 6.5 Server Management のインストール中に、プロキシがリッスンするポートを設定できます。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」にある「NetWare および Windows へのインストール」を参照してください。

  ファイアウォールでこのポート上のプロキシサーバへの要求を許可する必要があります。XML プロキシサーバがファイアウォールによって許可されている標準ポートをリッスンするように設定できます。

  XML プロキシは商用 Web サーバをサポートしていません。XML プロキシに割り当てられたポート番号が同じサーバ上で実行される他のサービスで使用されていないことを確認しておく必要があります。

  XML プロキシサーバのアドレスとポート番号を使用して、ロールアップポリシーを設定する必要もあります。

展開に関する推奨事項

- インベントリ対象サーバのインベントリスキャンを設定する場合、インベントリスキャンの時間をずらすか、同時にスキャンするインベントリ対象サーバ数を制限することをお勧めします。
- 1台のインベントリサーバに多数のインベントリ対象サーバが接続されている場合、すべてのインベントリ対象サーバのスキャンを一度に実行するようなスケジュールを設定しないことをお勧めします。一度に集中してスキャンを実行すると、Novell eDirectory および Inventory Service に負荷がかかります。
- NetWareまたはWindowsサーバによってサポートされている接続の数によって決定される台数のインベントリ対象サーバをサーバに接続できます。最大 5000 台のインベントリ対象サーバが接続できます。
- Inventory ポリシーで情報のロールアップスケジュールを設定する場合は、ロールアップの頻度を最低でも 1 日に 1 回にしておくことをお勧めします。インベントリ情報のロールアップのスケジュール頻度を 1 時間に 1 度など、短く設定すると、インベントリサーバのパフォーマンスが低下する場合があります。
- インベントリをインストールする際には、上位から下位へと展開します。最上位のサーバからインストールを開始して、次の下位レベルのサーバのインストールに進みます。たとえば、ルートサーバとリーフサーバを含むインベントリセットアップの場合、ルートサーバに対するインベントリのインストールを完了してから、リーフサーバのインストールを実行します。
- インベントリサーバが Server Inventory のスキャンを、インベントリサーバから直接受け取るか、ロールアップを介して受け取る必要がある場合、このサーバに ZENworks 6.5 Server Management をインストールする必要があります。

- インベントリサーバおよびデータベースサーバに DNS を設定することをお勧めします。DNS を設定しなかった場合、ロールアップポリシーおよびデータベースロケーションポリシーで IP アドレスを選択します。情報収集とロールアップの頻度のスケジュール設定は、ルートサーバに応じて調整する必要があります。ルートサーバが .STR ファイルの負荷を処理できるか確認してください。

Server Inventory のインストール

Server Inventory のインストールに関する詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Policy-Enabled Server Management のインストール」にある「NetWare および Windows へのインストール」を参照してください。

Server Inventory のインストールの効果の理解

Server Inventory のインストールの効果に関する詳細については、474 ページの「Server Inventory のインストールの効果の理解」を参照してください。

必要なポリシーの設定

次の表は、Server Inventory のサーバをセットアップするために必要な作業を示しています。

セットアップするサーバタイプ	操作手順
スタンドアロンサーバ	1. 508 ページの「データベース場所ポリシーの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。
ルートサーバ	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 508 ページの「データベース場所ポリシーの設定」の手順に従います。
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。 3. 508 ページの「データベース場所ポリシーの設定」の手順に従います。
中間サーバ	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 511 ページの「ロールアップポリシーの設定」の手順に従います。
データベースが接続されている中間サーバ	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 511 ページの「ロールアップポリシーの設定」の手順に従います。 3. 508 ページの「データベース場所ポリシーの設定」の手順に従います。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。 3. 511 ページの「ロールアップポリシーの設定」の手順に従います。
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	1. 507 ページの「Inventory Service オブジェクトの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。 3. 511 ページの「ロールアップポリシーの設定」の手順に従います。 4. 508 ページの「データベース場所ポリシーの設定」の手順に従います。

セットアップするサーバタイプ	操作手順
リーフサーバ	1. 507 ページの「Inventory Serviceオブジェクトの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。 3. 511 ページの「ロールアップポリシーの設定」の手順に従います。
データベースが接続されているリーフサーバ	1. 507 ページの「Inventory Serviceオブジェクトの設定」の手順に従います。 2. 509 ページの「Server Inventory ポリシーの設定」の手順に従います。 3. 511 ページの「ロールアップポリシーの設定」の手順に従います。 4. 508 ページの「データベース場所ポリシーの設定」の手順に従います。

Inventory Service の開始

ZENworks 6.5 Server Management のインストール中に［Inventory Standalone Configuration］の設定を構成した場合にだけ、インストール後に Inventory Service が自動的に開始します。

Inventory Service を手動で開始するには、476 ページの「NetWare インベントリサーバでの Inventory Service の起動」を参照してください。

ソフトウェアディクショナリの更新

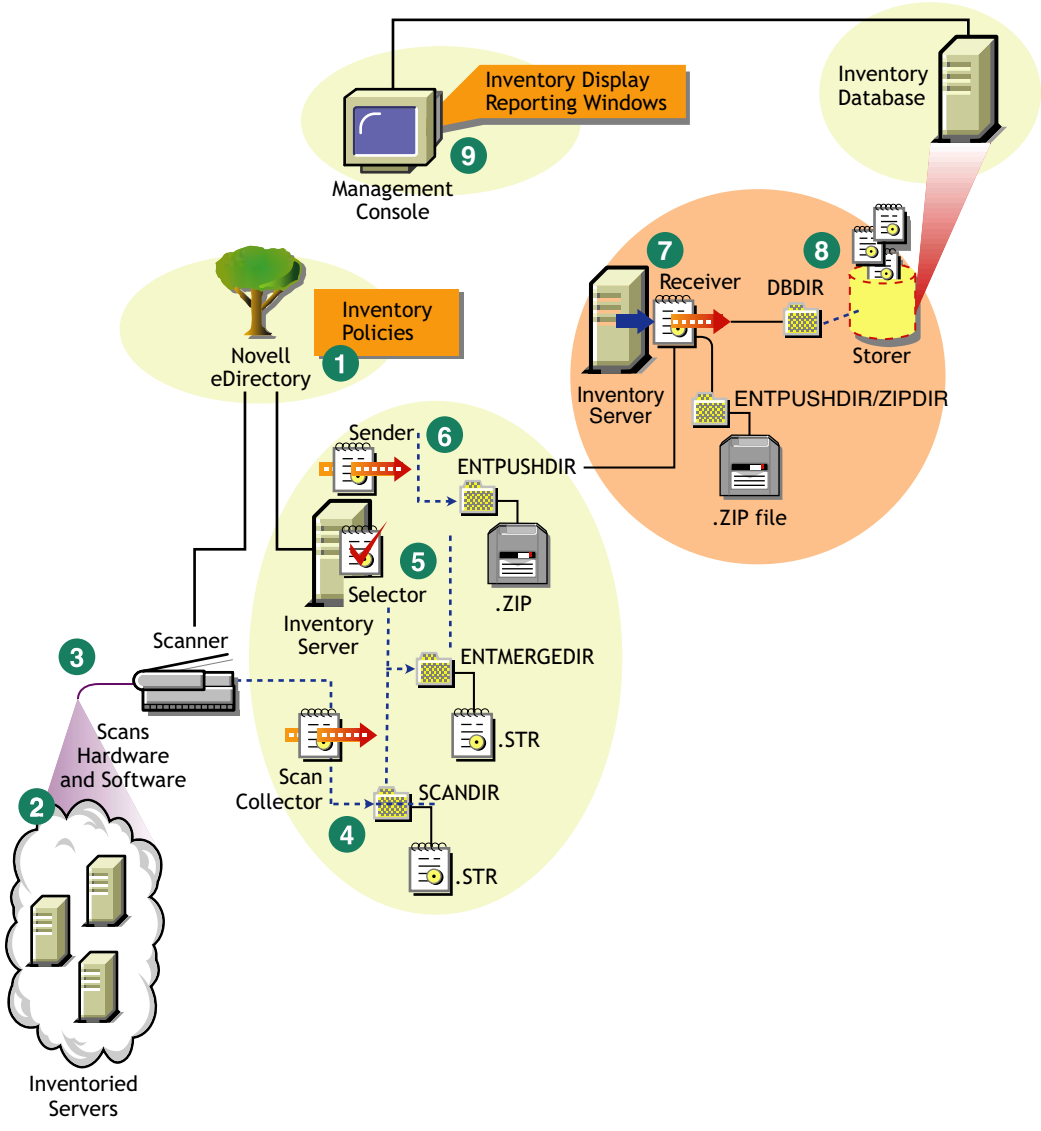
次のいずれかの方法で、ソフトウェアディクショナリを更新できます。

- 各インベントリサーバで、Novell Support Web サイト（http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm）から最新バージョンのディクショナリを手動でダウンロードし、ソフトウェアディクショナリを更新します。
- Novell Support Web サイト（http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm）からインベントリサーバ、できればルートサーバに最新バージョンのディクショナリを手動でダウンロードし、513 ページの「ディクショナリ更新ポリシーの設定」を設定する手順で他のすべてのサーバにディクショナリを自動的に配布します。詳細については、514 ページの「ディクショナリの配布の設定」を参照してください。

注： Novell Support Web サイト（http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm）では、3ヶ月に 1 度ディクショナリが更新され、TID として発行されます。

サーバ間でのインベントリ情報のロールアップの理解

次の図は、サーバ間でのインベントリ情報のロールアップを示しています。内容については以下で説明します。



インベントリ展開でインベントリ情報をサーバ間でロールアップする場合は、次のようなプロセスでスキャンが実行されます。

1. eDirectory の Inventory ポリシーによってインベントリの設定が定義されます。こうした設定には、インベントリ情報の送信先になるインベントリサーバの Inventory Service オブジェクト名、スキャン時間、およびソフトウェアスキャンのソフトウェアルールが含まれます。これらの設定はカスタマイズできます。
2. Scanner は Policy and Distribution Services を使って、Inventory ポリシーを読み取り、ポリシー設定に基づいてインベントリ情報を収集します。Inventory Scanner は、インベントリサーバでのディクショナリの更新を確認し、更新されたディクショナリをダウンロードします。
3. Scanner は、インベントリ対象サーバにローカルでインベントリ情報を保存します。この情報は、XML-RPC プロトコルを使用してインベントリサーバに転送されます。

4. Scan Collector は、XML-RPC プロトコルを使ってインベントリ情報を受信し、この情報をインベントリサーバにあるスキャンディレクトリの .str ファイルに保存します。Scan Collector は、ZEN Web Server を使用して XML-RPC 要求を処理します。
5. Selector は、インベントリ情報を検証し、インベントリ情報をロールアップするためにエンタープライズマージディレクトリにインベントリ情報を保存します。データベースが接続されている場合、Selector はファイルをデータベースディレクトリにも保存します。
6. インベントリサーバ上の Sender にはインベントリ情報の転送先インベントリサーバを識別するためのロールアップポリシーがあり、ロールアップスケジュールは情報をロールアップする時間を指定します。Sender は、.str ファイルを .zip ファイルに圧縮し、エンタープライズプッシュディレクトリにその .zip ファイルを保存します。Sender は次のレベルのインベントリサーバの Receiver に .zip ファイルを送信します。
7. 次のレベルのインベントリサーバ上の Receiver は、.zip ファイルを受信します。

   注： 次のレベルのインベントリサーバは、同じ eDirectory ツリーまたは別の eDirectory ツリーに配置することができます。

   中間サーバ上で、Receiver はエンタープライズプッシュディレクトリ (entpushdir) のファイルをコピーします。データベースが接続されている中間サーバ上、またはデータベースとインベントリ対象サーバが接続されている中間サーバ上で、Receiver はファイルを ¥entpushdir およびデータベースディレクトリ (dbdir) に保存します。

   ルートサーバ上またはインベントリ対象サーバが接続されているルートサーバ上では、Receiver はファイルを ¥dbdir にのみをコピーします。
8. Storer は、.str ファイルを圧縮した .zip ファイルを temp ディレクトリ (¥dbdir¥temp) に解凍し、インベントリ対象サーバの .str ファイルのインベントリ情報でデータベースを更新します。
9. ZENworks 管理者は、ConsoleOne でインベントリ情報の表示およびデータベースの照会を実行できます。

Server Inventory のインストールの効果の理解

ZENworks 6.5 Server Inventory のインストールプログラムは、インベントリサーバ上で次の作業を実行します。

- NetWare インベントリサーバ：
  - インベントリに関連するファイルを *installation_volume* にコピーします。
  - Server Inventory のスナップインを ConsoleOne ディレクトリにコピーします。
  - インベントリサーバをインストールするサーバごとに、eDirectory 内に Inventory Service オブジェクトを作成します。このオブジェクトには、属性 zeninvRole（サーバの役割）、zeninvScanFilePath (¥scandir ディレクトリへのパス)、zeninvHostServer（インベントリサーバがインストールされるサーバの DN)、および zeninvDictionarypath（ディクショナリディレクトリへのパス）が入力されます。
  - Inventory Service オブジェクトがすでに存在する場合は、オブジェクトが検証され、オブジェクトが無効な場合は再作成されます。
  - インストール中に、Inventory Service オブジェクトを NCP™ サーバのトラスティに設定して、比較権と読み込み権を割り当てます。

- Inventory Service オブジェクトをこのオブジェクトのトラスティとして割り当てます。
- インベントリサーバ上の指定ボリュームに、サブディレクトリを含むスキャンディレクトリを作成します。[Root] は、このディレクトリに対する作成権を持ちます。
- ディクショナリディレクトリ (dictdir) を作成し、一般ディクショナリとプライベートディクショナリのファイルをコピーします。[Root] は、このディレクトリに対して読み取りと書き込みを行う権利を持ちます。
- zenworks.properties ファイルを sys:¥system に作成します。このファイルには、インベントリサーバおよび ZENworks Web サーバのインストールパスが含まれています。
- Server Inventory をインストール中に[Inventory Standalone Configuration]の設定を設定した場合、Inventory Service Manager が自動的に起動します。
- インベントリサーバに ZENworks Web サーバがインストールされていない場合、ZENworks Web サーバをインストールします。
- Server Inventory を以前と同じインストールディレクトリに再インストールする場合、config.properties ファイルと directory.properties ファイルをバックアップして、これらのファイルを再作成します。

- Windows インベントリサーバ：
  - インベントリに関連するファイルを *installation_directory* にコピーします。
  - Server Inventory のスナップインコンポーネントを ConsoleOne ディレクトリにコピーします。
  - インベントリサーバの指定ボリュームにスキャンディレクトリとサブディレクトリを作成し、このディレクトリのすべてのユーザに対して共有と作成権を作成します。
  - ディクショナリディレクトリ (dictdir) を作成し、一般ディクショナリとプライベートディクショナリのファイルをコピーして、このディレクトリに対する読み取りと書き込みの権利をすべてのユーザに与えます。
  - インベントリサーバをインストールするサーバごとに、eDirectory 内に Inventory Service オブジェクトを作成します。属性 zeninvRole（サーバの役割）、zeninvScanFilePath (¥scandir へのパス)、zeninvHostServer（インベントリサーバがインストールされるサーバの DN)、および zeninvDictionarypath（ディクショナリディレクトリへのパス）が入力されます。
  - Inventory Service オブジェクトがすでに存在する場合は、オブジェクトが検証され、オブジェクトが無効な場合は再作成されます。
  - インストール中に、Inventory Service オブジェクトを NCP サーバのトラスティに設定して、比較権と読み込み権を割り当てます。
  - Inventory Service オブジェクトをこのオブジェクトのトラスティとして割り当てます。
  - Inventory Service Manager がサービスとして作成されます。
  - レジストリ設定を編集し、インベントリサーバおよび ZENworks Web サーバのインストールパスを追加します。
  - インベントリサーバに、ZENworks Service Manager がサービスとして作成されます。

- Server Inventory を以前と同じインストールディレクトリに再インストールする場合、config.properties ファイルと directory.properties ファイルをバックアップして、これらのファイルを再作成します。

データベースサーバ：

- 指定したサーバに Sybase データベースをインストールします。
- データベースサーバを以前のインストールディレクトリにインストールする場合、無効または存在しないデータベースファイルは再び作成されます。
- Sybase がすでにインストールされている場合は、データベースファイルのみがコピーされます。
- NetWare では、mgmtdb.db エントリは sys:¥system¥mgmtdbs.ncf ファイルに追加されます。Windows では、mgmtdb.db エントリはレジストリに追加されます。
- Sybase のデータベースオブジェクト (Inventory database_*server_name*) を作成し、オブジェクトのプロパティを設定します。
- サーバの起動時にデータベースがロードされます。

Inventory Service の開始と停止

この節では、次の内容について説明します。

- 476 ページの「NetWare インベントリサーバでの Inventory Service の起動」
- 477 ページの「NetWare インベントリサーバでの Inventory Service の停止」
- 477 ページの「Windows インベントリサーバでの Inventory Service の開始」
- 477 ページの「Windows インベントリサーバでの Inventory Service の停止」

各種 Inventory Service の詳細については、517 ページの「Inventory Service Manager の理解」を参照してください。

NetWare インベントリサーバでの Inventory Service の起動

Inventory Service を開始する前に、Inventory データベースが稼働していることを確認します。インベントリデータベースは、インストール後に自動的に起動します。

NetWare インベントリサーバ上で Inventory Service を起動するには、サーバコンソールのプロンプトで「**startinv**」と入力します。

Inventory Service を開始するには、サーバコンソールのプロンプトで、「**startser** ***inventory_service_name***」と入力します。

Inventory Service を起動した後に、Inventory Service が稼動していることを確認します。すべてのサービスを一覧表示するには、サーバコンソールのプロンプトで、「**listser ***」と入力します。Inventory Service を一覧表示するには、サーバコンソールのプロンプトで、「**listser** ***inventory_service_name***」と入力します。

Inventory Service が稼働していない場合、サーバステータスログを確認します。サーバステータスログの詳細については、686 ページの「インベントリサーバのインベントリコンポーネントのステータス表示」を参照してください。

NetWare インベントリサーバでの Inventory Service の停止

1 つの Inventory Service を停止するには、サーバコンソールのプロンプトで「**stopser** *Inventory_service_name*」と入力します。

すべての Inventory Service を停止するには、サーバコンソールのプロンプトで、「**stopser ***」と入力します。

Windows インベントリサーバでの Inventory Service の開始

Inventory Service を開始する前に、ZENworks Server Management コンポーネントとインベントリデータベースが稼働していることを確認してください。インベントリデータベースは、インストール後に自動的に起動します。

Windows 2000/2003 インベントリサーバ上で Inventory Service を開始するには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell Inventory Service］を選択し、［開始］をクリックします。

コンソールプロンプトから Inventory Service の一覧を開始するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2 プロンプトで「**startser** *inventory_service_name*」と入力します。

Inventory Service を起動した後に、Inventory Service が稼動していることを確認します。すべてのサービスを一覧表示するには、サーバコンソールのプロンプトで、「**listser "*"**」と入力します。コンソールプロンプトから Inventory Service の一覧を表示するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2 プロンプトで「**listser** *inventory_service_name*」と入力します。

Inventory Service が稼働していない場合、サーバステータスログを確認します。サーバステータスログの詳細については、686 ページの「インベントリサーバのインベントリコンポーネントのステータス表示」を参照してください。

Windows インベントリサーバでの Inventory Service の停止

Windows 2000/2003 インベントリサーバ上で Inventory Service を停止するには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell Inventory Service］を選択し、［停止］をクリックします。

コンソールプロンプトから Windows インベントリサーバのサービスを停止するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2「**stopser** *inventory_service_name*」と入力します。

インベントリサーバの役割変更

ZENworks 6.5 Server Management をインストールすると、インベントリサーバの役割はデフォルトでスタンドアロンに設定されます。Inventory Service オブジェクトを設定すると、インベントリの展開に基づいてインベントリサーバに特定の役割を割り当てることができます。

たとえば、展開計画で、ルートサーバ、データベースが接続されている中間サーバ、およびリーフサーバの 3 台のインベントリサーバがインベントリを展開するために指定されている場合、これらのサーバに Server Inventory をインストールし、インベントリサーバの役割を選択します。その後でインベントリ展開を変更する場合は、サーバの役割を変更する必要があります。たとえば、既存ルートサーバにインベントリ対象サーバを接続する場合、Inventory Service オブジェクトの役割をルートサーバからインベントリ対象サーバが接続されているルートサーバに変更します。新しい役割に応じて、設定する必要があるポリシーもあります。

インベントリサーバの役割を変更するには

1. 役割の変更は、既存のインベントリの展開に影響を及ぼす可能性があるため、注意して行ってください。また、必要なディスク容量を考慮し、インベントリに必要な環境が設定されていることを確認します。
2. ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックし、[Properties] をクリックし、[Inventory Service Object Properties] タブをクリックします。
3. Inventory Service オブジェクトの新しい役割を選択してから、[Apply] をクリックします。
4. 変更したインベントリサーバ上で実行されているサービスを停止し、役割を変更するために必要なアクションを実行した後、Inventory Service を開始します。

   すべての Inventory Service を停止するには

   - NetWare サーバでは、コンソールのプロンプトで次のコマンドを入力します。

     ```
     stopser *

     java -killZenWSInv
     ```

   - Windows 2000/2003 サーバでは、[サービス] ウィンドウで、[Novell Inventory Services]、[停止] の順にクリックします。

   すべての Inventory Service を再起動するには

   - NetWare サーバのコンソールプロンプトで、「**startinv**」と入力します。
   - Windows 2000/2003 サーバでは、[サービス] ウィンドウで、[Novell Inventory Services]、[開始] の順にクリックします。

次の節では、Inventory Service オブジェクトの役割を変更する際に役立つ情報を紹介します。

- 479 ページの「ルートサーバの役割変更」
- 480 ページの「インベントリ対象サーバが接続されているルートサーバの役割変更」
- 481 ページの「中間サーバの役割変更」
- 481 ページの「データベースが接続されている中間サーバの役割変更」

- 482 ページの「データベースとインベントリ対象サーバが接続されている中間サーバの役割変更」
- 483 ページの「インベントリ対象サーバが接続されている中間サーバの役割変更」
- 484 ページの「リーフサーバの役割変更」
- 485 ページの「データベースが接続されているリーフサーバの役割変更」
- 486 ページの「スタンドアロンサーバの役割変更」

ルートサーバの役割変更

ルートサーバの役割を別の役割に変更するには、次の表で指定されている操作を実行します。

ルートサーバの変更後の役割	作業
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	次の作業を実行します。 1. 役割を変更した後に、インベントリ対象サーバが接続されているルートサーバに接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、ルートサーバに関連付けられたデータベースの場所ポリシーを削除します。 2. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのサーバを指定します。
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのインベントリサーバを指定します。
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	役割を変更した後に次の作業を実行します。 1. 接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。 2. ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのサーバを指定します。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更する前に、ルートサーバに関連付けられたデータベースの場所ポリシーを削除します。 2. 役割を変更した後、接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。 3. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのインベントリサーバを指定します。
リーフサーバ、データベースが接続されたリーフサーバ、またはスタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、ルートサーバをこれらのインベントリサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

インベントリ対象サーバが接続されているルートサーバの役割変更

次の表の操作に従ってください。

インベントリ対象サーバが接続されているルートサーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、インベントリ対象サーバが接続されているルートサーバに関連付けられた Server Inventory ポリシーを削除します。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、データベースの場所ポリシーおよび Server Inventory ポリシーを削除します。 2. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのサーバを指定します。
データベースが接続されている中間サーバ	次の作業を実行します。 1. Server Inventory ポリシーがインベントリサーバに接続されているルートサーバに関連付けられている場合は、役割を変更する前に、このインベントリサーバに接続されている、またはこのインベントリサーバにロールアップする下位のインベントリサーバに接続されているルートサーバの Server Inventory ポリシーを削除します。 2. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのサーバを指定します。
Intermediate Server with Database and Inventoried Servers (データベースとインベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更した後、ロールアップポリシーを設定して、このインベントリサーバからの情報のロールアップ先である次のレベルのインベントリサーバを指定します。
Intermediate Server with Inventoried Servers (インベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更する前に、インベントリ対象サーバが接続されているルートサーバに関連付けられたデータベースの場所ポリシーを削除します。
リーフサーバ、データベースが接続されたリーフサーバ、またはスタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、ルートサーバをこれらのインベントリサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

中間サーバの役割変更

次の表の操作に従ってください。

中間サーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、ロールアップポリシーを削除します。 2. 役割を変更した後、データベースの場所ポリシーを設定します。
インベントリサーバが接続されているルートサーバ	次の作業を実行します。 1. 役割を変更する前に、ロールアップポリシーを削除します。 2. 役割を変更した後、ルートサーバに接続されているインベントリ対象サーバの Server Inventory ポリシーと、データベースの場所ポリシーを設定します。
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更した後、この Inventory Service オブジェクトに関連付けられたすべてのインベントリ対象サーバと、このインベントリサーバにロールアップする下位のインベントリサーバに関連付けられたインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。 2. 役割を変更した後、データベースの場所ポリシーを設定します。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更した後、接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。
リーフサーバ、データベースが接続されたリーフサーバ、またはスタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、中間サーバをこれらのインベントリサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

データベースが接続されている中間サーバの役割変更

次の表の操作に従ってください。

データベースが接続されている中間サーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。

データベースが接続されている中間サーバの変更後の役割	作業
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。 2. 役割を変更した後、接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されている中間サーバに関連付けられたデータベースの場所ポリシーを削除します。
Intermediate Server with Database and Inventoried Servers (データベースとインベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更した後、接続されたインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されている中間サーバに関連付けられたデータベースの場所ポリシーを削除します。 2. 役割を変更した後、接続したインベントリ対象サーバがスキャンされるように、Server Inventory ポリシーを設定します。
リーフサーバ、データベースが接続されたリーフサーバ、またはスタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、中間サーバをこれらのインベントリサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

データベースとインベントリ対象サーバが接続されている中間サーバの役割変更

次の表の操作に従ってください。

データベースとインベントリ対象サーバが接続されている中間サーバの変更後の役割	作業
ルートサーバ	役割を変更する前に、次の作業を実行します。 1. データベースおよびインベントリ対象サーバが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。 2. インベントリ対象サーバがこのサーバにスキャンファイルを送信しないように、インベントリ対象サーバに関連付けられた Server Inventory ポリシーを削除します。
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	次の作業を実行します。 1. 役割を変更する前に、データベースおよびインベントリ対象サーバが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。

データベースとインベントリ対象サーバが接続されている中間サーバの変更後の役割	作業
中間サーバ	役割を変更する前に、次の作業を実行します。 1. データベースおよびインベントリ対象サーバが接続されている中間サーバにロールアップする下位のサーバに関連付けられた Server Inventory ポリシーを削除します。 2. データベースおよびインベントリ対象サーバが接続されている中間サーバに関連付けられたデータベースの場所ポリシーを削除します。
データベースが接続されている中間サーバ	次の作業を実行します。 1. データベースおよびインベントリ対象サーバが接続されている中間サーバの Server Inventory ポリシーを削除するか、Server Inventory ポリシーを再設定します。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更する前に、データベースおよびインベントリ対象サーバが接続されている中間サーバに関連付けられたデータベースの場所ポリシーを削除します。
リーフサーバ、データベースが接続されたリーフサーバ、スタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、中間サーバをこれらのサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

インベントリ対象サーバが接続されている中間サーバの役割変更

次の表の操作に従ってください。

インベントリ対象サーバが接続されている中間サーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、インベントリ対象サーバが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。 2. 役割を変更する前に、接続されたインベントリ対象サーバがこのインベントリサーバにスキャンファイルを送信しないように、インベントリ対象サーバに関連付けられた Server Inventory ポリシーを削除します。 3. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	次の作業を実行します。 1. 役割を変更する前に、インベントリ対象サーバが接続されている中間サーバに関連付けられたロールアップポリシーを削除します。 2. 役割を変更した後、このインベントリサーバにロールアップする下位のインベントリサーバに接続されているインベントリ対象ワークステーションの Server Inventory ポリシーを設定します。 3. 役割を変更した後、データベースの場所ポリシーを設定します。

インベントリ対象サーバが接続されている中間サーバの変更後の役割	作業
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、Server Inventory ポリシーを削除します。
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更する前に、この Inventory Service オブジェクトに接続されているインベントリ対象サーバに関連付けられた Server Inventory ポリシーを削除します。 2. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
Intermediate Server with Database and Inventoried Servers (データベースとインベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
リーフサーバ、データベースが接続されたリーフサーバ、またはスタンドアロンサーバ	このような変更はインベントリシステム全体に影響するため、Server Inventory では、中間サーバをこれらのインベントリサーバに変更することはできません。これらの役割を割り当てる場合は、Server Inventory コンポーネントを再インストールし、設定を行ってください。

リーフサーバの役割変更

次の表の操作に従ってください。

リーフサーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、リーフサーバに関連付けられたロールアップポリシーを削除します。 2. 役割を変更する前に、インベントリ対象サーバに関連付けられた Server Inventory ポリシーを削除します。 3. 役割を変更した後、ルートサーバのデータベースの場所ポリシーを設定します。
Root Server with Inventoried Servers (インベントリ対象サーバが接続されているルートサーバ)	次の作業を実行します。 1. 役割を変更する前に、リーフサーバに関連付けられたロールアップポリシーを削除します。 2. 役割を変更した後、インベントリ対象サーバが接続されたルートサーバのデータベースの場所ポリシーを設定します。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、インベントリサーバに関連付けられたインベントリ対象サーバの Server Inventory ポリシーを削除するか、再設定します。

リーフサーバの変更後の役割	作業
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更する前に、このインベントリサーバにロールアップする下位のインベントリサーバに関連付けられたインベントリ対象ワークステーションの Server Inventory ポリシーを削除するか、または Server Inventory ポリシーを再設定します。 2. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
Intermediate Server with Database and Inventoried Servers (データベースとインベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
Intermediate Server with Inventoried Servers (インベントリ対象サーバが接続されている中間サーバ)	この役割の変更では、特定のポリシーを変更する必要はありません。
データベースが接続されているリーフサーバ	次の作業を実行します。 1. 役割を変更した後、このインベントリサーバのデータベースロケーションポリシーを設定します。
スタンドアロンサーバ	次の作業を実行します。 1. 役割を変更する前に、リーフサーバに関連付けられたロールアップポリシーを削除します。

データベースが接続されているリーフサーバの役割変更

次の表の操作に従ってください。

データベースが接続されているリーフサーバの変更後の役割	作業
ルートサーバ	役割を変更する前に、次の作業を実行します。 1. データベースが接続されているリーフサーバに関連付けられた Server Inventory ポリシーを削除します。 2. データベースが接続されているリーフサーバに関連付けられたロールアップポリシーを削除します。
Root Server with Inventoried Servers (インベントリ対象サーバが接続されているルートサーバ)	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられたロールアップポリシーを削除します。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられた Server Inventory ポリシーおよびデータベースの場所ポリシーを削除します。

データベースが接続されているリーフサーバの変更後の役割	作業
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられた Server Inventory ポリシーを削除します。
Intermediate Server with Database and Inventoried Servers (データベースとインベントリ対象サーバが接続されている中間サーバ)	この役割の変更では、特定のポリシーを変更する必要はありません。
Intermediate Server with Inventoried Servers (インベントリ対象サーバが接続されている中間サーバ)	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられたデータベースの場所ポリシーを削除します。
リーフサーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられたデータベースの場所ポリシーを削除します。
スタンドアロンサーバ	次の作業を実行します。 1. 役割を変更する前に、データベースが接続されているリーフサーバに関連付けられたロールアップポリシーを削除します。

スタンドアロンサーバの役割変更

次の表の操作に従ってください。

スタンドアロンサーバの変更後の役割	作業
ルートサーバ	次の作業を実行します。 1. 役割を変更する前に、スタンドアロンサーバに関連付けられた Server Inventory ポリシーを削除します。
Root Server with Inventoried Servers (インベントリ対象サーバが接続されているルートサーバ)	この役割の変更では、特定のポリシーを変更する必要はありません。
中間サーバ	次の作業を実行します。 1. 役割を変更する前に、スタンドアロンサーバに関連付けられた Server Inventory ポリシーおよびデータベースの場所ポリシーを削除します。 2. 役割を変更した後に、ロールアップポリシーを設定して、データベースが接続されている中間サーバからの情報のロールアップ先である次のレベルのインベントリサーバを指定します。

スタンドアロンサーバの変更後の役割	作業
データベースが接続されている中間サーバ	次の作業を実行します。 1. 役割を変更する前に、スタンドアロンサーバに関連付けられた Server Inventory ポリシーを削除します。 2. 役割を変更した後に、ロールアップポリシーを設定して、データベースが接続されている中間サーバからの情報のロールアップ先である次のレベルのインベントリサーバを指定します。
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更した後、ロールアップポリシーを設定して、データベースおよびインベントリ対象サーバが接続されている中間サーバからの情報のロールアップ先サーバを指定します。
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	次の作業を実行します。 1. 役割を変更する前に、スタンドアロンサーバに関連付けられたデータベースの場所ポリシーを削除します。 2. 役割を変更した後、ロールアップポリシーを設定して、インベントリ対象サーバが接続されている中間サーバからの情報のロールアップ先サーバを指定します。
リーフサーバ	次の作業を実行します。 1. 役割を変更する前に、スタンドアロンサーバに関連付けられたデータベースの場所ポリシーを削除します。 2. 役割を変更した後、ロールアップポリシーを設定して、リーフサーバからの情報のロールアップ先サーバを指定します。
データベースが接続されているリーフサーバ	次の作業を実行します。 1. 役割を変更した後、ロールアップポリシーを設定して、データベースが接続されているリーフサーバからの情報のロールアップ先サーバを指定します。

インベントリデータベースのセットアップ

次の節では、インベントリデータベースを設定するために役立つ情報を紹介します。

- 488 ページの「Sybase インベントリデータベースのセットアップ」
- 494 ページの「Oracle 8i インベントリデータベースの設定」
- 498 ページの「Oracle 9i インベントリデータベースのセットアップ」
- 502 ページの「MS SQL Server 2000 インベントリデータベースのセットアップ」

インベントリデータベースを置き換える場合は、Inventory Service を終了してからデータベースを置き換えます。データベースを置き換えてから、Inventory Service を再起動します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

Sybase インベントリデータベースのセットアップ

この節では、次のトピックについて説明します。

- 488 ページの「インベントリ属性に対する英語以外の列挙値のインベントリデータベースへの追加」
- 488 ページの「Sybase インベントリデータベースオブジェクトの手動作成」
- 490 ページの「NetWare または Windows サーバ上での Sybase データベース用データベーススペースの整理 (AlterDBSpace ツール)」
- 491 ページの「Sybase データベース起動パラメータの理解」
- 492 ページの「Sybase を実行するインベントリデータベースのバックアップ」

インベントリ属性に対する英語以外の列挙値のインベントリデータベースへの追加

英語以外の列挙値を追加して、国際バージョンでインベントリレポートにインベントリ属性の enum 値を表示できるようにする必要があります。英語以外の列挙値を英語バージョンの製品で有効にして、英語以外の言語のサイトからロールアップされたインベントリ情報が、英語バージョンのみがインストールされている上位のサーバで正しく取り込めるようにする必要があります。

列挙値を含む属性の一覧に関する詳細については、733 ページの付録 K、「列挙値」を参照してください。

英語以外の列挙値を追加するには

1 *zenworks_directory*¥inv¥server¥wminv¥properties¥connection.prop ファイルで JDBC 接続の設定を指定して、Sybase データベースに接続します。

これは、connection.prop ファイルのコメントセクションで指定された Sybase のテンプレートプロパティ設定をコピーして実行できます。Sybase サーバ設定と一致する JDBC URL 文字列で IP アドレス、ポート番号、およびデータベース SID を指定します。

2 サーバのプロンプトで、「**AddEnums** ***directory_name_containing_connection.prop***」と入力します。

インベントリサーバが Windows コンピュータで実行されている場合は、上述のコマンドを *zenworks_directory*¥inv¥server¥wminv¥bin から実行します。

コマンドの実行後、英語以外の列挙値の挿入に成功したことを示すメッセージが、コンソールプロンプトに表示されます。

Sybase インベントリデータベースオブジェクトの手動作成

Sybase インベントリデータベースオブジェクト (Inventory database_*server_name*) を手動で作成するには

1 ConsoleOne で、データベースオブジェクトを作成する eDirectory ツリーを右クリックし、[New] > [Object] > [ZENworks Database] > [OK] の順にクリックします。

2 データベースオブジェクトの名前を入力して、[OK] をクリックします。

3 データベースオブジェクトのデータベースサーバオプションを設定します。

3a ConsoleOne でデータベースオブジェクトを右クリックし、[Properties]、[ZENworks Database] タブの順にクリックします。

3b 次のいずれかの方法を使用して、データベースサーバオブジェクトを選択します。

- データベースサーバに eDirectory がインストールされている場合：[Server DN] フィールドで、データベースが物理的にインストールされ、実行されているサーバを表すサーバオブジェクトを参照して選択します。

  サーバの IP アドレスは、[Server IP Address] または [DNS Name] ドロップダウンリストに自動的に入力されます。選択したサーバオブジェクトが複数の IP アドレスを持つ場合は、適切な IP アドレスを選択します。

  [Server DN] フィールドに設定されている値をクリアするには、別のデータベースサーバの IP アドレスを入力するか、別のサーバオブジェクトを参照して選択します。

- データベースサーバに eDirectory がインストールされていない場合：サーバの IP アドレスまたは DNS 名を [Server IP Address] フィールドまたは [DNS Name] フィールドに入力します。

3c 次のオプションの値を入力します。

- **[Database (Read-Write) Username]：** *MW_DBA*
- **[Database (Read-Write) Password]：** *novell*
- **[Database (Read Only) Username]：** *MW_READER*
- **[Database (Read Only) Password]：** *novell*
- **[Database (Write Only) Username]：** *MW_UPDATER*
- **[Database (Write Only) Password]：** *novell*

3d [Apply] をクリックします。

3e JDBC ドライバのプロパティを設定するには、[JDBC Driver Information] タブをクリックします。

3f [Sybase] を選択し、[Default Settings] をクリックします。

これによって、デフォルトの JDBC ドライバ情報がフィールドに格納されます。

Sybase データベースの設定は次のとおりです。

- [Driver]：*com.sybase.jdbc.SybDriver*
- **[Protocol]：** *jdbc:*
- **[SubProtocol]：** *sybase*:
- [SubName]： *[Tds]：*
- **[Port]：** *2638*
- **[Flags]：** ?ServiceName=mgmtdb&JCONNECT_VERSION=4
- **[Database Service Name]：** *Sybase を起動している間に、-n Sybase 起動パラメータに対して指定されたデータベース名。*

  注： デフォルトでは、-n スイッチの値はデータベースサーバの IP アドレスです。このスイッチ値をそのまま使用する場合、同じ IP アドレスをデータベースサービス名として入力する必要があります。

3g [Apply]、[Close] の順にクリックします。

NetWare データベースサーバに SYS: 以外のボリュームがある場合、または Windows データベースサーバに追加のハードドライブがある場合は、Sybase データベーススペースファイルを異なるボリュームまたはドライブに置くと、データベースへのアクセス時のパフォーマンスが向上します。

ZENworks 6.5 Server Management の Sybase データベースコンポーネントをインストールする場合、システムのデータベースファイルとデータベーススペースファイルは指定したデータベースサーバ上の場所にインストールします。インベントリデータベースサーバのロード時に、システムデータベースファイル (mgmtdb.db) がロードされます。この mgmtdb.db ファイルは、データベーススペースファイルのインベントリ情報を参照します。データベーススペースファイル (mgmtdb1.db、mgmtdb2.db、mgmtdb3.db、mgmtdb4.db、mgmtdb5.db、mgmtdb6.db、mgmtdb7.db、mgmtdb8.db、mgmtdb9.db、mgmtdb10.db、および mgmtdb11.db) にはインベントリ情報が含まれます。

alterdb.props ファイルは、*inventory_server_installation_directory*¥wminv¥properties ディレクトリのデータベースサーバにインストールされます。ファイル内のセクションを変更して、ボリュームまたはディスク上のデータベーススペースの場所を指定できます。

alterdb.props ファイルの内容は次のとおりです。

```
#Database Space Properties

count=11

mgmtdb1=location_of_mgmtdb1

mgmtdb2=location_of_mgmtdb2

mgmtdb3=location_of_mgmtdb3

mgmtdb4=location_of_mgmtdb4

mgmtdb5=location_of_mgmtdb5

mgmtdb6=location_of_mgmtdb6

mgmtdb7=location_of_mgmtdb7

mgmtdb8=location_of_mgmtdb8

mgmtdb9=location_of_mgmtdb9

mgmtdb10=location_of_mgmtdb10

mgmtdb11=location_of_mgmtdb11

.....
```

データベーススペースを整理するには

1. データベースがロードされていないことを確認します。
2. インベントリサーバ上で Inventory Service Manager が実行されていないことを確認します。
3. インベントリサーバ上のデータベーススペースファイルを手動で移動します。

   パフォーマンスを向上させるために、次のようにデータベーススペースファイルを配置します。

   - MGMTDB1 と MGMTDB2 を同じ場所に配置

- MGMTDB3 と MGMTDB6 を同じ場所に配置
- MGMTDB5 と MGMTDB7 を同じ場所に配置
- MGMTDB8 と MGMTDB4 を同じ場所に配置
- MGMTDB9 と MGMTDB10 を同じ場所に配置
- MGMTDB11 を任意の場所に配置

重要： mgmtdb.db を NetWare サーバ上の他のディレクトリまたはボリュームに移動する場合は、mgmtdb.db の新しい場所を反映するよう sys:¥system¥mgmtdbs.ncf ファイルを更新します。

mgmtdb.db を、Windows サーバ上の他のディレクトリまたはボリュームに移動する場合、zenworks¥database¥dbengine ディレクトリに存在する ntdbconfig.exe を実行します。[NTDBCONFIG] ダイアログボックスで、mgmtdb.db の新しいパスを入力します。

4 alterdb.props ファイルで、11 個のデータベーススペースファイルの場所を変更します。

たとえば、NetWare の場合、次のように入力します。

```
mgmtdb3=sys:\\zenworks\\inv\\db
```

Windows の場合は、次のように入力します。

```
mgmtdb3=c:\\zenworks\\inv\\db
```

5 データベースをロードし、NetWare サーバ上または Windows サーバ上で「**mgmtdbs**」と入力して、データベースサービスを実行します。

コンソールに表示されるエラーメッセージは無視します。エラーメッセージが表示されるのは、データベーススペースファイルがロードされていないためです。

6 データベースの場所ポリシーが設定されていることを確認します。

7 インベントリサーバコンソールで、AlterDBSpace サービスを実行し、「**StartSer AlterDBSpace**」と入力します。

インベントリサーバ上で、AlterDBSpace ツールはサービスとして実行されます。

データベースが調整されたことを示すメッセージが表示されます。

8 データベースを終了してから、データベースをロードします。

データベースをロードしている間にエラーが発生していないことを確認します。エラーは、データベーススペースファイルの指定された場所が間違っているか、存在しないことを示します。alterdb.props ファイルでデータベーススペースファイルのパスが正しいことを確認し、データベーススペースファイルを整理する手順を繰り返します。

重要： データベーススペースファイルを別のボリュームまたはドライブに配置する場合は、ログファイルをシステムのデータベースファイル (mgmtdb.db) と同じボリュームまたはドライブに配置する必要があります。

Sybase データベース起動パラメータの理解

Sybase データベースの起動パラメータは次のとおりです。

- **-c：** データベースページおよびその他のサーバ情報をキャッシュするための初期メモリ予約を設定します。たとえば、-c 32M は 32MB のキャッシュサイズを予約します。
- **-gc：** 各データベースでチェックポイントを実行しないでデータベースサーバが実行される最長時間を分単位で設定します。デフォルト値は 60 分間です。たとえば、-gc 120 はチェックポイント時間を 120 分間に設定します。

- **-gn**: データベースサーバで使用される実行スレッドの数を設定します。
- **-m**: シャットダウンまたはサーバでスケジュールされているチェックポイントの結果としてチェックポイントが実行されたときに、トランザクションログを削除します。
- **-n**: データベースサーバのホスト名を指定します。たとえば、-n *IP_address* となります。
- **-ti**: 一定時間(分単位)要求を出さなかった場合に接続を切断します。デフォルトは240(4 時間) です。データベーストランザクションの中間にあるクライアントコンピュータは、トランザクションが終了するか接続が切断されるまでロックされます。?ti オプションは、停止している接続を切断し、ロックを解除します。たとえば、-ti 400 と指定します。
- **-x**: 通信リンクを指定します。たとえば、-x tcpip は TCP/IP リンクを示します。
- **-ct**: 同じ文字を表すが、異なる値を持つ文字セット間で文字列を変換することにより、文字セット変換を有効にします。これは、クライアントコンピュータとデータベースが異なる文字セットを使用している場合に役立ちます。
- **-gss**: サーバの各内部実行スレッドのスタックサイズを設定します。
- ***database_installation_path***: インベントリデータベースのインストールパスを指定します。たとえば、c:¥zenworks¥inv¥db¥mgmtdb.db となります。

Sybase を実行するインベントリデータベースのバックアップ

Server Inventory には、サーバから Sybase インベントリデータベースをバックアップするオプションが用意されています。データベースのバックアップを週ごとに実行することをお勧めします。ただし、サーバのインベントリを頻繁に追跡している場合は、バックアップの回数を増やします。

データベースファイルとトランザクションのログは、¥scandir の相対パスにバックアップできます。

ここでは、次の内容について説明します。

- 492 ページの「前提条件」
- 493 ページの「NetWare または Windows サーバに対するバックアップツールの実行」
- 494 ページの「インベントリデータベースの復元」

前提条件

このツールを使用するには

1. バックアップツールは、データベースサーバを関連付けたインベントリサーバに対してのみ実行できます。複数のデータベースサーバを展開した場合は、各データベースサーバに対してバックアップツールを実行する必要があります。
2. バックアップする必要があるデータベースがデータベースの場所ポリシーで設定されていることを確認します。データベースロケーションポリシーへのアクセス方法に関する詳細については、508 ページの「データベース場所ポリシーの設定」を参照してください。

3 サーバプロパティファイルの［DBBackup Service］セクションで、ARGUMENTS パラメータのバックアップ先を変更します。バックアップファイルは、¥scandir の相対パスで指定します。たとえば、¥scandir パスが sys:¥zenworks¥inv¥scandir の場合、データベースは sys:¥zenworks¥inv¥database¥*directory_you_specify* にバックアップされます。バックアップツールを実行するサーバに存在するサーバプロパティファイルを変更する必要があります。サーバの役割に応じたサーバプロパティファイルを変更します。たとえば、データベースが接続されたリーフサーバに対してバックアップツールを実行する場合、サーバプロパティファイル leaf_db_wks.properties を変更します。

4 バックアップツールの実行時に Service Manager がロードされていることを確認します。

NetWare または Windows サーバに対するバックアップツールの実行

次に示すいずれかの方法でバックアップツールを実行できます。

- サーバコンソールからバックアップツールを実行する：

  1. インベントリサーバコンソールで、「**StartSer DBBACKUP**」と入力します。
  2. バックアップログファイルでバックアップのステータスを参照します。データベースは、*zenworks_installation_path*¥zenworks¥inv¥db¥*directory_you_specify* にコピーされます。

  バックアップツールによってログファイル bacstatus.txt が作成され、NetWare サーバおよび Windows 2000 サーバの zenworks¥inv¥database ディレクトリに配置されます。ログにはバックアップ操作のステータスが記録されます。このテキストファイルを開くと、バックアップのステータスを参照できます。このファイルのサイズはバックアップ操作を行うたびに増加します。詳細が不要になったら、ファイルの内容を削除します。

- ConsoleOne からバックアップツールを実行する：

  1. ConsoleOne で、［Tools］＞［ZENworks Inventory］＞［Database Backup］＞の順にクリックします。

  インベントリデータベースに最新の情報をバックアップしたい場合は、データベースオブジェクトを右クリックし、［ZENworks Inventory］、［Database Backup］の順にクリックします。

  2. データベースのバックアップを保存するディレクトリのパスを入力します。

  警告： ディレクトリ名に 2 バイト文字を使用しないでください。2 バイト文字を使用すると、Sybase ではこの文字が別の名前として解釈され、別の名前のディレクトリにデータベースがバックアップされます。

  インベントリデータベースが NetWare サーバで実行している場合、パスを入力するか、［Browse］をクリックして、ディレクトリの参照および選択を実行できます。完全なパスを指定しないでデータベースのバックアップディレクトリ名を入力すると、バックアップディレクトリは sys: ディレクトリに作成されます。

  インベントリデータベースが Windows コンピュータで稼働している場合、バックアップディレクトリパスを手動で入力する必要があります。フルパスを指定せずにデータベースバックアップディレクトリ名を入力した場合、¥winnt¥system32 ディレクトリにバックアップディレクトリが作成されます。

注： データベースを新しいディレクトリにバックアップする場合、1 つのレベルだけを含むディレクトリが新たに作成されます。データベースをサブディレクトリにバックアップするには、プライマリディレクトリがすでに存在している必要があります。たとえば、データベースを新しい c:¥backup ディレクトリにバックアップする場合、¥backup ディレクトリが作成された後、このディレクトリにデータベースのバックアップが実行されます。ただしこのデータベースを、c:¥backup の直下に位置する新しい ¥database ディレクトリにバックアップしたい場合、¥backup ディレクトリがすでに存在している必要があります。

3. ［Start Backup］をクリックします。

これにより、データベースを実行しているサーバ上の指定されたディレクトリにデータベースのバックアップが実行され、既存ファイルを上書きする必要がある場合でも確認メッセージを表示することなく上書きが実行されます。

バックアップツールは、NetWare サーバおよび Windows 2000 サーバの *ConsoleOne_installation_directory*¥1.2¥bin ディレクトリにログファイルの bacstatus.txt を作成します。ログにはバックアップ操作のステータスが記録されます。このテキストファイルを開くと、バックアップのステータスを参照できます。このファイルのサイズはバックアップ操作を行うたびに増加します。詳細が不要になったら、ファイルの内容を削除します。

インベントリデータベースの復元

1 インベントリデータベースサーバが起動している場合は、Storer サービスを停止します。データベースサーバのコンソールで、「**StopSer Storer**」と入力します。

2 Sybase データベースを終了します。

- NetWare サーバ：データベースサーバのプロンプトで、「**q**」と入力して、Sybase データベースを終了します。
- Windows 2000/2003 の場合 :Windows のコントロールパネルで［Administrative Tools］、［Services］の順にダブルクリックします。次に、［Novell Database - Sybase］を選択し、［Stop］をクリックします。

3 バックアップファイルをコピーし、作業データベースファイルを上書きします。

4 データベースサーバを再起動します。

Oracle 8i インベントリデータベースの設定

次の節では、Oracle 8i インベントリデータベースの設定方法について説明します。

- 494 ページの「Windows サーバでの Oracle 8i インベントリデータベースの作成」
- 496 ページの「Oracle インベントリデータベースオブジェクトの手動作成」
- 498 ページの「Windows サーバでの複数の Oracle データベースインスタンスの設定および実行」

重要： この設定では、Oracle データベースのその他のバージョンまたはインスタンスのインベントリデータベースはマウントされません。

Windows サーバでの Oracle 8i インベントリデータベースの作成

次の前提条件が満たされていることを確認します。

- ❑ Oracle 8.1.7 がサーバにインストールされている必要があります。
- ❑ Server Inventory では、Oracle でインベントリデータベースを管理するために、最低 25 個のユーザライセンスが必要です。

次の手順に従って、Windows サーバ上に Oracle インベントリデータベースを手動で作成する必要があります。

1 c:¥schema ディレクトリを作成し、*ZENworks 6.5 Companion CD* の次のディレクトリにあるすべてのファイルを ¥schema ディレクトリにコピーします。

database¥oracle8i¥common

database¥oracle8i¥winntspecific

2 次のディレクトリ構造を作成します。
user_specified_path¥zenworks¥inventory¥oracle¥database¥trace

3 c:¥schema¥_create.sql で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

4 c:¥schema¥init.ora で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

5 c:¥schema¥_start.sql で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

d: が見つからない場合、データベースディレクトリ内の INIT.ORA のパスをチェックして、修正します。

6 c:¥schema¥init.ora ファイルを
user_specified_path¥zenworks¥inventory¥oracle¥ database にコピーします。

7 c:¥schema¥_start.sql ファイルを user_specified_*path*¥zenworks にコピーします。

8 Oracle サービスが正しくロードされていることと、データベースがマウントされていないことを確認します。

9 サーバのプロンプトで、「**svrmgrl**」と入力して、Oracle Server Manager をロードします。

10 Oracle Server Manager のプロンプト (svrmgrl プロンプト) で、「**@c:\schema\schema.sql**」と入力します。

データベースが正しく作成されたことを確認するために、schema/inv.log ファイルを調べます。データベースが正しく作成されていない場合、schema/inv.log には次のエラーメッセージが含まれます。Oracle not available, Out of space, Compilation error.

11 一部のインベントリ属性に対する英語以外の列挙 (enum) 値をインベントリデータベースに追加します。

英語以外の列挙値を追加して、国際バージョンでインベントリレポートにインベントリ属性の enum 値を表示できるようにする必要があります。英語以外の列挙値を英語バージョンの製品で有効にして、英語以外の言語のサイトからロールアップされたインベントリ情報が、英語バージョンのみがインストールされている上位のサーバで正しく取り込めるようにする必要があります。

列挙値を含む属性の一覧に関する詳細については、733 ページの付録 K 、「列挙値」を参照してください。

英語以外の列挙値を追加するには

11a *zenworks_directory*¥inv¥server¥wminv¥properties¥connection.prop ファイルで JDBC 接続の設定を指定して、Oracle データベースに接続します。

これは、connection.prop ファイルのコメントセクションで指定された Oracle のテンプレートプロパティ設定をコピーして実行できます。Oracle サーバ設定と一致する JDBC URL 文字列で IP アドレス、ポート番号、およびデータベース SID を指定します。

11b サーバのプロンプトで、「**AddEnums** *directory_name_containing_connection.prop*」と入力します。

インベントリサーバが Windows コンピュータで実行されている場合は、上述のコマンドを *zenworks_directory*¥inv¥server¥wminv¥bin から実行します。

11c svrmgrl プロンプトで次の SQL 文を実行して、ローカライズされた列挙値が正しく追加されていることを確認します。

- 列挙値をフランス語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_fr**
- 列挙値をスペイン語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_es;**
- 列挙値をドイツ語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_de;**
- 列挙値をポルトガル語(ブラジル)で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_pt_BR;**

12 svrmgrl プロンプトで、「**@c:\schema\schema1.sql**」と入力します。

データベースが正しく作成されたことを確認するために、schema/inv1.log ファイルを調べます。データベースが正しく作成されていない場合、schema/inv1.log には次のエラーメッセージが含まれます。Oracle not available, Out of space, Compilation error.

13 svrmgrl プロンプトで、「**connect internal**」と入力し、DBA としてログインします。

14 svrmgrl プロンプトで、「**shutdown normal**」と入力します。

15 svrmgrl プロンプトで、「**@*path*\zenworks_start.sql**」と入力して、インベントリデータベースを起動します。

16 インベントリデータベースオブジェクトを手動で生成します。

Oracle インベントリデータベースオブジェクトの手動作成

Oracle インベントリデータベースオブジェクト (Inventory database_*server_name*) を手動で作成するには

1 ConsoleOne で、データベースオブジェクトを作成する場所を eDirectory ツリー内で右クリックし、[New] > [Object] > [ZENworks Database] > [OK] の順にクリックします。

2 データベースオブジェクトの名前を入力して、[OK] をクリックします。

3 データベースオブジェクトのデータベースサーバオプションを設定します。

3a ConsoleOne でデータベースオブジェクトを右クリックし、[Properties]、[ZENworks Database] タブの順にクリックします。

3b 次のいずれかの方法を使用して、データベースサーバオブジェクトを選択します。

- データベースサーバに eDirectory がインストールされている場合：[Server DN] フィールドで、データベースが物理的にインストールされ、実行されているサーバのサーバオブジェクトを参照して選択します。

  サーバの IP アドレスは、[Server IP Address] または [DNS Name] ドロップダウンリストに自動的に入力されます。選択したサーバオブジェクトが複数の IP アドレスを持つ場合は、適切な IP アドレスを選択します。

  重要： データベースオブジェクトに設定されたデータベースサーバの DNS 名が有効であることを確認します。DNS 名が無効である場合、データベースオブジェクトの [Property] ページで適切なデータベースサーバの IP アドレスを選択する必要があります。

  [Server DN] フィールドに設定されている値をクリアするには、別のデータベースサーバの IP アドレスを入力するか、別のサーバオブジェクトを参照して選択します。

- データベースサーバに eDirectory がインストールされていない場合：サーバの IP アドレスまたは DNS 名を [Server IP Address] フィールドまたは [DNS Name] フィールドに入力します。

3c 次のオプションの値を入力します。

- **[Database (Read-Write) Username]：** *MW_DBA*
- **[Database (Read-Write) Password]：** *novell*
- **[Database (Read Only) Username]：** *MWO_READER*
- **[Database (Read Only) Password]：** *novell*
- **[Database (Write Only) Username]：** *MWO_UPDATER*
- **[Database (Write Only) Password]：** *novell*

3d [Apply] をクリックします。

3e JDBC ドライバのプロパティを設定するには、[JDBC Driver Information] タブをクリックします。

3f [Oracle] を選択して、[Default Settings] をクリックします。

これによって、デフォルトの JDBC ドライバ情報がフィールドに格納されます。

Oracle データベースの設定は次のとおりです。

- [Driver]：*oracle.jdbc.driver.OracleDriver*
- **[Protocol]：** *jdbc:*
- **[SubProtocol]：** *oracle*:
- [SubName]：*thin:@*
- **[Port]：** *1521*
- **[Flags]：** Oracle では使用しません。
- **[Database Service Name]：** *orcl*.(SID の値はデータベースインスタンスに割り当てられた値と同じです。)

3g [Apply]、[Close] の順にクリックします。

Windows サーバでの複数の Oracle データベースインスタンスの設定および実行

Oracle インスタンスを設定して実行するには

1 データベースサーバで、Oracle Database Configuration Assistant を実行します。デスクトップの［スタート］メニューで、［プログラム］>［Oracle］>［Database Administration］>［Oracle Database Configuration Assistant］の順にクリックします。

2 ［Create a Database］>［Next］>［Typical］>［Next］>［Copy Existing Database Files from the CD］>［Next］の順にクリックします。

3 次の詳細を入力します。

- **［Global Database Alias］：** mgmtdb.*your_windows_name*
- **［SID］：** この値には自動的に *mgmtdb* と入力されます。

4 ［Finish］をクリックします。

これにより Oracle データベースを作成できます。このプロセスにはかなり時間がかかります。OracleServiceMGMTDB サービスが作成され、起動されていることを確認します。

5 インベントリデータベースをロードします。

Oracle Server Manager を実行します。デスクトップメニューで、［スタート］>［ファイル名を指定して実行］の順にクリックし、「SVRMGRL」と入力します。

次のコマンドを入力します。

set instance mgmtdb

connect internal/*password_for_administrator*

Oracle 9i インベントリデータベースのセットアップ

次の節では、Oracle* 9i インベントリデータベースの設定方法について説明します。

- 498 ページの「Windows サーバでの Oracle 9i インベントリデータベースの作成」
- 500 ページの「Oracle インベントリデータベースオブジェクトの手動作成」
- 501 ページの「Windows サーバでの複数の Oracle データベースインスタンスの設定および実行」

重要： この設定では、Oracle データベースのその他のバージョンまたはインスタンスのインベントリデータベースはマウントされません。

Windows サーバでの Oracle 9i インベントリデータベースの作成

次の前提条件が満たされていることを確認します。

- ❑ インベントリデータベースを設定する前に Oracle 9i リリース 2 がサーバにインストールされている必要があります。
- ❑ Server Inventory では、Oracle でインベントリデータベースを管理するために、最低 25 個のユーザライセンスが必要です。

次の手順に従って、Windows サーバ上に Oracle インベントリデータベースを手動で作成する必要があります。

1 c:¥schema ディレクトリを作成し、*ZENworks 6.5 Companion 2 CD* の次のディレクトリにあるすべてのファイルを ¥schema ディレクトリにコピーします。

database¥oracle9i¥common

database¥oracle9i¥winntspecific

2 次のディレクトリ構造を作成します。
user_specified_path¥zenworks¥inventory¥oracle¥database¥trace

3 c:¥schema¥_create.sql で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

4 c:¥schema¥init.ora で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

5 c:¥schema¥_start.sql で、d: のすべてのインスタンスを *user_specified_path* に置き換えます。

d: が見つからない場合、データベースディレクトリ内の init.ora のパスをチェックして、修正します。

6 c:¥schema¥init.ora ファイルを *user_specified_path*¥zenworks¥inventory¥oracle¥ database にコピーします。

7 c:¥schema¥_start.sql ファイルを user_specified_*path*¥zenworks にコピーします。

8 Oracle サービスが正しくロードされていることと、データベースがマウントされていないことを確認します。

9 サーバのプロンプトで、「**sqlplus /nolog**」と入力して、Oracle Server Manager をロードします。

10 Oracle Server Manager のプロンプト（sqlplus プロンプト）で、「**@c:\schema\schema.sql**」と入力します。

データベースが正しく作成されたことを確認するために、schema/inv.log ファイルを調べます。データベースが正しく作成されていない場合、schema/inv.log には次のエラーメッセージが含まれます。Oracle not available, Out of space, Compilation error.

11 一部のインベントリ属性に対する英語以外の列挙（enum）値をインベントリデータベースに追加します。

英語以外の列挙値を追加して、国際バージョンでインベントリレポートにインベントリ属性の enum 値を表示できるようにする必要があります。英語以外の列挙値を英語バージョンの製品で有効にして、英語以外の言語のサイトからロールアップされたインベントリ情報が、英語バージョンのみがインストールされている上位のサーバで正しく取り込めるようにする必要があります。

列挙値を含む属性の一覧に関する詳細については、733 ページの付録 K 、「列挙値」を参照してください。

英語以外の列挙値を追加するには

11a *zenworks_directory*¥inv¥server¥wminv¥properties¥connection.prop ファイルで JDBC 接続の設定を指定して、Oracle データベースに接続します。

これは、connection.prop ファイルのコメントセクションで指定された Oracle のテンプレートプロパティ設定をコピーして実行できます。Oracle サーバ設定と一致する JDBC URL 文字列で IP アドレス、ポート番号、およびデータベース SID を指定します。

11b サーバのプロンプトで、「**AddEnums** *directory_name_containing_connection.prop*」と入力します。

インベントリサーバが Windows コンピュータで実行されている場合は、上述のコマンドを *zenworks_directory*¥inv¥server¥wminv¥bin から実行します。

11c sqlplus プロンプトで次の SQL 文を実行して、ローカライズされた列挙値が正しく追加されていることを確認します。

- 列挙値をフランス語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_fr**
- 列挙値をスペイン語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_es;**
- 列挙値をドイツ語で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_de;**
- 列挙値をポルトガル語(ブラジル)で表示する：**connect mw_dba/*password*** および **SELECT * FROM cim.ostype_pt_BR;**

12 sqlplus プロンプトで、「**@c:\schema\schema1.sql**」と入力します。

データベースが正しく作成されたことを確認するために、schema/inv1.log ファイルを調べます。データベースが正しく作成されていない場合、schema/inv1.log には次のエラーメッセージが含まれます。Oracle not available, Out of space, Compilation error.

13 sqlplus プロンプトで、「**connect / as sysdba**」と入力し、DBA としてログインします。

14 sqlplus プロンプトで、「**shutdown normal**」と入力します。

15 sqlplus プロンプトで、「**@*path*\zenworks_start.sql**」と入力して、インベントリデータベースを起動します。

16 500 ページの「Oracle インベントリデータベースオブジェクトの手動作成」に進みます。

Oracle インベントリデータベースオブジェクトの手動作成

1 ConsoleOne で、Novell eDirectory ツリー内のデータベースオブジェクトを作成する場所を右クリックし、[New]、[Object]、[ZENworks Database]、[OK] の順にクリックします。

2 データベースオブジェクトの名前を入力して、[OK] をクリックします。

3 データベースオブジェクトのデータベースサーバオプションを設定します。

3a ConsoleOne で、データベースオブジェクト (Inventory database_*server_name*) を右クリックし、[Properties] > [ZENworks Database] タブの順にクリックします。

3b 次のいずれかの方法でデータベースサーバオブジェクトを選択します。

- eDirectory がデータベースサーバにインストールされている場合は、[Server DN] フィールドで、データベースが物理的にインストールされ、実行されているサーバのサーバオブジェクトを参照して選択します。

  サーバの IP アドレスは、[Server IP Address] または [DNS Name] ドロップダウンリストに自動的に入力されます。選択したサーバオブジェクトが複数の IP アドレスを持つ場合は、適切な IP アドレスを選択します。

重要： データベースオブジェクトに設定されたデータベースサーバの DNS 名が有効であることを確認します。DNS 名が無効である場合、データベースオブジェクトの［Property］ページで適切なデータベースサーバの IP アドレスを選択する必要があります。

［Server DN］フィールドに設定されている値をクリアするには、別のデータベースサーバの IP アドレスを入力するか、別のサーバオブジェクトを参照して選択します。

- データベースサーバに eDirectory がインストールされていない場合：サーバの IP アドレスまたは DNS 名を［Server IP Address］フィールドまたは［DNS Name］フィールドに指定します。

3c 次の値を指定します。

- **［Database (Read-Write) User Name］：** *MW_DBA*
- **［Database (Read-Write) Password］：** *novell*
- **［Database (Read Only) User Name］：** *MWO_READER*
- **［Database (Read Only) Password］：** *novell*
- **［Database (Write Only) User Name］：** *MWO_UPDATER*
- **［Database (Write Only) Password］：** *novell*

3d ［Apply］をクリックします。

3e JDBC ドライバのプロパティを設定するには、［JDBC Driver Information］タブをクリックします。

3f ［Oracle］を選択し、［Default Settings］ボタンをクリックします。

これによって、デフォルトの JDBC ドライバ情報がフィールドに格納されます。

Oracle データベースの設定は次のとおりです。

- ［Driver］：*oracle.jdbc.driver.OracleDriver*
- **［Protocol］：** *jdbc:*
- **［SubProtocol］：** *oracle*:
- ［SubName］：*thin:@*
- **［Port］：** *1521*
- **［Flags］：** このフィールドは、Oracle では使用しません。
- **［Database Service Name］：** *orcl*（SID の値はデータベースインスタンスに割り当てられた値と同じです。）

3g ［Apply］、［Close］の順にクリックします。

Windows サーバでの複数の Oracle データベースインスタンスの設定および実行

次の前提条件が満たされていることを確認します。

- ❑ Oracle 9i リリース 2 を Windows インベントリサーバにインストールする必要があります。
- ❑ Server Inventory では、Oracle でインベントリデータベースを管理するために、最低 25 個のユーザライセンスが必要です。
- ❑ インベントリデータベースがすでに設定済みである必要があります。

Oracle インスタンスを設定して実行するには

1 データベースサーバのデスクトップの［スタート］メニューで、［プログラム］>［Oracle］>［Database Administration］>［Oracle Database Configuration Assistant］の順にクリックします。

2 ［Create a Database］>［Next］>［Typical］>［Next］>［Copy Existing Database Files from the CD］>［Next］の順にクリックします。

3 次の詳細を入力します。

- **［Global Database Alias］：** mgmtdb.*your_windows_nt/2000_name*
- **［SID］：** デフォルト値は *mgmtdb* です。

4 ［Finish］をクリックします。

Oracle データベースが作成されるまでしばらく時間がかかります。

OracleServiceMGMTDB サービスが作成され、起動されていることを確認します。

5 インベントリデータベースをロードします。

デスクトップメニューで、［スタート］>［ファイル名を指定して実行］の順にクリックし、「SQLPLUS」と入力して、Oracle Server Manager を実行します。

次のコマンドを入力します。

set instance mgmtdb

connect internal/*password_for_administrator*

MS SQL Server 2000 インベントリデータベースのセットアップ

ここでは、次の内容について説明します。

- 502 ページの「MS SQL Server 2000 インベントリデータベースの設定」
- 505 ページの「MS SQL 2000を実行するインベントリデータベースへのインベントリサーバと ConsoleOne の接続」

MS SQL Server 2000 インベントリデータベースの設定

データベースを設定する前に行う作業：

- ❑ Microsoft* SQL Server 2000 を Windows サーバにインストールします。
- ❑ p1mssqlinvdb.zip ファイルを解凍するために、ディスクの空き領域が 50MB 以上必要です。
- ❑ インベントリデータベースがインストールされているサーバにインベントリ情報を保存できるディスクの空き領域があることを確認します。

MS SQL Server 2000 インベントリデータベースを設定するには

1 *ZENworks 6.5 Companion 2* CD の ¥database¥mssql ディレクトリにある p1mssqlinvdb.zip ファイルを *path_of_inventory_database_directory_on_the_database_server* にコピーします。

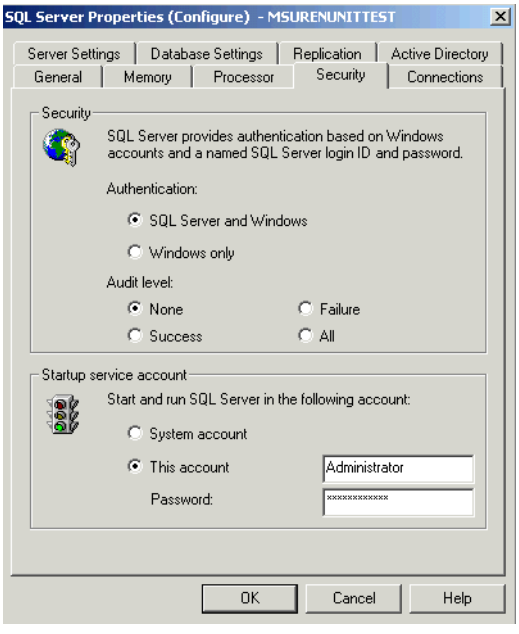
2 p1mssqlinvdb.zip を解凍します。

3 MS SQL サーバのデスクトップの［スタート］メニューから、［プログラム］>［Microsoft SQL Server(Microsoft SQL Server)］>［Enterprise Manager(Enterprise Manager)］の順にクリックします。

4 SQL Server Enterprise Manager で、Console Root/Microsoft SQL Servers/SQL Server Group/*machine_name_running_Inventory_database* を参照します。

5 *machine_name_running_Inventory_database* を右クリックし、［Properties］をクリックします。

6 ［SQL Server Properties］ダイアログボックスで、［Security］タブをクリックし、認証が SQL Server および Windows に設定されていることを確認します。



7 ［OK］をクリックします。

8 *machine_name_running_Inventory_database*/Databases を参照し、［Databases］を右クリックし、［All Tasks］をクリックして、［Attach Database］をダブルクリックします。

9 ［Attach Database］ダイアログボックスで、次の操作を行います。

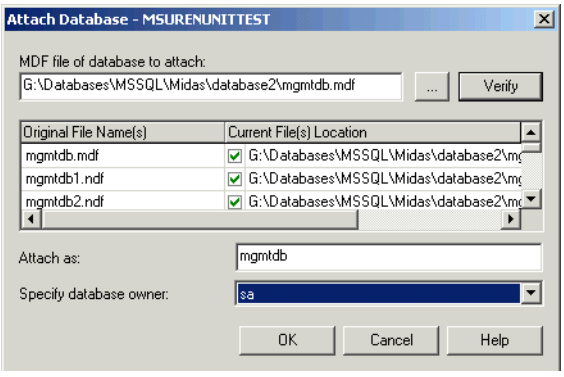
9a ［Browse］ボタンをクリックし、接続する .mdf データベースファイルとして mgmtdb.mdf を参照して選択します。

9b ［Attach As］フィールドの値が mgmtdb であることを確認します。

9c ［Specify database owner］ドロップダウンリストから sa を選択します。

9d ［OK］をクリックします。

ZENworks インベントリデータベース (mgmtdb) が Databases サーバグループに接続されます。



10 [mgmtdb] を選択し、[Tools] メニューの [SQL Query Analyzer] をクリックします。

11 SQL Query Analyzer で、次の作業を行います。

11a mgmtdb がドロップダウンリストで選択されていることを確認します。

11b [File] > [Open] の順にクリックします。

11c *ZENworks 6.5 Companion 2* CD の ¥database¥mssql ディレクトリから createloginnames.sql クエリファイルを選択します。

11d [Query] > [Execute] の順にクリックします。

正常に実行された場合は、次のメッセージが [Message] ペインに表示されます。

New Login Created

11e SQL Query Analyzer に MW_DBA としてログインし、次のドロップトリガ sql を実行します。

```
drop trigger cim.x$cim$component

go

drop trigger cim.x$cim$dependency

go

drop trigger managewise.x$managewise$designates

go

drop trigger managewise.x$managewise$currentloginuser

go

drop trigger managewise.x$managewise$lastloginuser

go

drop trigger cim.x$cim$installedsoftwareelement

go
```

12 （オプション）一部のインベントリ属性に対する英語以外の列挙（enum）値をインベントリデータベースに追加します。

英語以外の列挙値を追加して、国際バージョンでインベントリレポートにインベントリ属性の enum 値を表示できるようにする必要があります。英語以外の列挙値を英語バージョンの製品で有効にして、英語以外の言語のサイトからロールアップされたインベントリ情報が、英語バージョンのみがインストールされている上位のサーバで正しく取り込めるようにする必要があります。

列挙値を含む属性の一覧に関する詳細については、733 ページの付録 K 、「列挙値」を参照してください。

英語以外の列挙値を追加するには

12a *zenworks_directory*¥inv¥server¥wminv¥properties¥connection.prop ファイルで JDBC 接続の設定を指定して、MS SQL データベースに接続します。

これは、connection.prop ファイルのコメントセクションで指定された MS SQL のテンプレートプロパティ設定をコピーして実行できます。MS SQL サーバ設定と一致する JDBC URL 文字列で IP アドレス、ポート番号、およびデータベース SID を指定します。

12b サーバのプロンプトで、「**AddEnums** *directory_name_containing_connection.prop*」と入力します。

インベントリサーバが Windows コンピュータで実行されている場合は、上述のコマンドを *zenworks_directory*¥inv¥server¥wminv¥bin から実行します。

コマンドの実行後、英語以外の列挙値の挿入に成功したことを示すメッセージが、コンソールプロンプトに表示されます。

13 505 ページの「MS SQL 2000 を実行するインベントリデータベースへのインベントリサーバと ConsoleOne の接続」に進みます。

MS SQL 2000 を実行するインベントリデータベースへのインベントリサーバと ConsoleOne の接続

インベントリサーバコンポーネントと ConsoleOne は、Microsoft JDBC ドライバを使用して、MS SQL 2000 インベントリデータベースに接続します。インベントリシステムを使用するには、Microsoft SQL Server 2000 の JDBC ドライバをインストールし設定する必要があります。

JDBC の Microsoft SQL Server 2000 ドライバを設定して、MS SQL 2000 で実行されるインベントリデータベースにアクセスするには

1 Microsoft SQL Server の Web サイト（http://www.microsoft.com/downloads/details.aspx?FamilyID=9f1874b6-f8e1-4bd6-947c-0fc5bf05bf71&DisplayLang=en）から Windows 英語版の Microsoft JDBC ドライバをダウンロードします。

2 Windows コンピュータにドライバをインストールします。

3 msbase.jar、msutil.jar、および mssqlserver.jar ファイルを *inventory_server_installation_directory*¥inv¥server¥lib ディレクトリにコピーします。

4 インベントリスナップインがインストールされている ZENworks 6.5 Server Management ConsoleOne を実行しているコンピュータで、msbase.jar、msutil.jar、および mssqlserver.jar ファイルを *consoleone_installation_directory*¥lib¥zen ディレクトリにコピーします。

5 ConsoleOne で、インベントリサーバがインストールされているコンテナにデータベースオブジェクトを作成します。

5a コンテナを右クリックします。

5b [New] > [Object] の順にクリックし、オブジェクトのリストから [ZENworks Database] を選択して、[OK] をクリックします。

5c データベースオブジェクトの名前を入力して、[OK] をクリックします。

6 データベースオブジェクトのデータベースサーバオプションを設定します。

6a ConsoleOne でデータベースオブジェクトを右クリックし、[Properties]、[ZENworks Database] タブの順にクリックします。

6b 次のいずれかの方法を使用して、データベースサーバオブジェクトを選択します。

- eDirectory がデータベースサーバにインストールされている場合は、[Server DN] フィールドで、データベースが物理的にインストールされ、実行されているサーバのサーバオブジェクトを参照して選択します。

  サーバの IP アドレスは、[Server IP Address] または [DNS Name] ドロップダウンリストに自動的に入力されます。選択したサーバオブジェクトが複数の IP アドレスを持つ場合は、適切な IP アドレスを選択します。

  重要： データベースオブジェクトに設定されたデータベースサーバの DNS 名が有効であることを確認します。DNS 名が無効である場合、データベースオブジェクトの [Property] ページで適切なデータベースサーバの IP アドレスを選択する必要があります。

  [Server DN] フィールドに設定されている値をクリアするには、別のデータベースサーバの IP アドレスを入力するか、別のサーバオブジェクトを参照して選択します。

- データベースサーバに eDirectory がインストールされていない場合：サーバの IP アドレスまたは DNS 名を [Server IP Address] フィールドまたは [DNS Name] フィールドに指定します。

6c 次のオプションの値を入力します。

- **[Database (Read-Write) User Name]：** *MW_DBA*
- **[Database (Read-Write) Password]：** *novell*
- **[Database (Read Only) User Name]：** *MWM_READER*
- **[Database (Read Only) Password]：** *novell*
- **[Database (Write Only) User Name]：** *MWM_UPDATER*
- **[Database (Write Only) Password]：** *novell*

6d [Apply] をクリックします。

6e JDBC ドライバのプロパティを設定するには、[JDBC Driver Information] タブをクリックします。

6f [MS SQL] を選択し、[Default Settings] をクリックします。

これによって、デフォルトの JDBC ドライバ情報がフィールドに格納されます。

MS SQL Server の設定に基づいてデータベースの設定を変更します。MS SQL のデータベース設定は次のとおりです。

- [Driver] : *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **[Protocol] :** *jdbc:*
- **[SubProtocol] :** *microsoft:*
- [SubName] : *sqlserver://*
- **[Port] :** *1433*
- **[Flags] :** MS SQL では使用しません。
- **[Database Service Name] :** MS SQL では使用しません。

6g [Apply]、[Close] の順にクリックします。

Inventory Service オブジェクトの設定

Inventory Service オブジェクトの設定では、関連付けられたインベントリ対象サーバのスキャンを設定します。

Inventory Service オブジェクトを設定するには

1 ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックし、[Properties] をクリックして、[Inventory Service Object Properties] タブを表示します。

2 次の設定を変更します。

[Inventory Server Role] : インベントリをスキャンするために展開したインベントリサーバに基づいて、インベントリサーバの役割を指定する必要があります。443 ページの「インベントリサーバの役割の理解」を参照してください。

[Discard Scan Data Time] : [Inventory Service Object Property] ページで指定する [Discard Scan Data Time] の前に収集されたスキャン情報が格納されているスキャンデータファイルは破棄されます。スキャンデータファイルは、中間サーバ、データベースが接続されている中間サーバ、データベースとインベントリ対象サーバが接続されている中間サーバ、およびインベントリ対象サーバが接続されている中間サーバのいずれかの種類のインベントリサーバから削除されます。

[Scan Directory Path] インベントリ対象サーバから受信した、または他のインベントリサーバからロールアップされたスキャンが格納され、追加処理されるインベントリサーバ上にあるディレクトリ。NetWare インベントリサーバのスキャンディレクトリのパスは、*¥¥complete_DNS_name_of_the_server¥directory_path_of_scandir* です。たとえば、*¥¥complete_DNS_name_of_the_server*¥sys:¥zenworks¥inv¥scandir のようになります。Windows インベントリサーバのスキャンディレクトリのパスは、*¥¥complete_DNS_name_of_the_server*¥scandir です。

¥scandir パスに指定したインベントリサーバ名は変更できません。ただし、ディレクトリを変更する場合は、スキャンディレクトリパスを変更する前に新しいディレクトリがすでに存在していることを確認します。

パスを変更するには

- NetWare では、[Browse] をクリックしてパスを選択および追加するか、またはパスを入力します。
- Windows では、パスを手動で入力する必要があります。

[Enable Scan]：Inventory Service オブジェクトに関連付けられたインベントリ対象サーバをスキャンするには、Inventory Service オブジェクトのプロパティページに一覧表示されているスキャンオプションを有効にする必要があります。インベントリ対象サーバのスキャンを無効にするには、このオプションの選択を解除します。

3 [Dictionary Settings] タブをクリックして、必要なソフトウェアディクショナリのルールを設定します。詳細については、586 ページの「ソフトウェアディクショナリのルールの設定」を参照してください。

4 [OK] をクリックします。

注： Inventory ポリシーを変更するか、またはオブジェクトを設定する場合は、常に Inventory Service を停止します。オブジェクトのポリシーおよびプロパティを設定します。Inventory Service を再開します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

データベース場所ポリシーの設定

データベース場所ポリシーには、Inventory データベースの場所が含まれています。Database オブジェクトを、Service Location Package を使用して Inventory Service オブジェクトが置かれているコンテナに、または Server Package を使用してインベントリサーバに関連付けることができます。

注： SLP およびサーバパッケージを設定する場合は、サーバパッケージの設定が SLP の設定よりも優先されます。

Database オブジェクトを Inventory Service オブジェクトが置かれているコンテナに関連付けるには

1 ConsoleOne で、Service Location Package を右クリックし、[Properties] をクリックして [Policies] ページを表示します。

2 [Enabled] 列の下にある ZENworks データベースポリシーのチェックボックスをオンにします。

3 [Properties] をクリックして [Inventory Management] ページを表示します。

4 インベントリデータベースオブジェクトの DN (Inventory database_*server_name*) を参照して選択し、[OK] をクリックします。

Sybase データベースでは、eDirectory のインストールされた Windows サーバにインストールする場合を除いて、Server Inventory のインストール中にデータベースオブジェクトが自動的に作成されます。データベースオブジェクトを手動で作成する場合は、488 ページの「Sybase インベントリデータベースオブジェクトの手動作成」を参照してください。

Oracle データベースでは、データベースオブジェクトを作成した後、そのオブジェクトを設定する必要があります。詳細については、494 ページの「Oracle 8i インベントリデータベースの設定」を参照してください。

MS SQL データベースでは、データベースオブジェクトを設定する必要があります。詳細については、502 ページの「MS SQL Server 2000 インベントリデータベースのセットアップ」を参照してください。

5 [OK] をクリックします。

6 [Associations] タブをクリックし、[Add] をクリックします。

7 Inventory Service オブジェクトが置かれているコンテナを参照して選択し、[OK] をクリックします。

8 [Apply]、[Close] の順にクリックします。

Database オブジェクトをインベントリサーバに関連付けるには

1 ConsoleOne で、サーバパッケージを右クリックし、[Properties] をクリックして [Policies] ページを表示します。

2 [Enabled] 列の下にある ZENworks データベースポリシーのチェックボックスをオンにします。

3 [Properties] をクリックして [Inventory Management] ページを表示します。

4 インベントリデータベースオブジェクトの DN (Inventory database_*server_name*) を参照して選択し、[OK] をクリックします。

Sybase データベースでは、eDirectory のインストールされた Windows サーバにインストールする場合を除いて、Server Inventory のインストール中にデータベースオブジェクトが自動的に作成されます。データベースオブジェクトを手動で作成する場合は、488 ページの「Sybase インベントリデータベースオブジェクトの手動作成」を参照してください。

Oracle データベースでは、データベースオブジェクトを作成した後、そのオブジェクトを設定する必要があります。詳細については、494 ページの「Oracle 8i インベントリデータベースの設定」を参照してください。

Oracle データベースでは、データベースオブジェクトを作成した後、そのオブジェクトを設定する必要があります。詳細については、494 ページの「Oracle 8i インベントリデータベースの設定」を参照してください。

5 [OK] をクリックします。

6 [Associations] タブをクリックし、[Add] をクリックします。

7 インベントリサーバオブジェクトを参照して選択し、[OK] をクリックします。

8 [Apply]、[Close] の順にクリックします。

注： Inventory ポリシーを変更するか、またはオブジェクトを設定する場合は、常に Inventory Service を停止します。オブジェクトのポリシーおよびプロパティを設定します。Inventory Service を再開します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

Server Inventory ポリシーの設定

Server Inventory ポリシーには、インベントリ情報の送信先のインベントリサーバの IP アドレスまたは DNS 名が含まれています。このポリシーには、関連付けられたインベントリ対象サーバのインベントリスキャンのスケジュールも含まれています。各インベントリ対象サーバについて、Server Inventory ポリシーを設定する必要があります。

Server Inventory ポリシーパッケージを設定するには

1 ConsoleOne で、Distributed Server Package を右クリックし、[Properties] をクリックして [Policies] ページを表示します。

2 [Policies] タブをクリックし、インベントリ対象サーバのオペレーティングシステムに応じて、ドロップダウンリストから [NetWare] または [Windows] をクリックします。

3 [Enabled] 列の下にある Server Inventory ポリシーのチェックボックスを選択します。

4 [Properties] をクリックして [Server Inventory Policy] ページを表示します。

5 [General] タブで、次の項目を設定します。

5a Inventory Service オブジェクト (Inventory Service_*server_name*) の DN を参照して選択します。

この設定によって、Scanner がサーバのインベントリ情報をこのインベントリサーバに送信することを指定します。

5b インベントリサーバの DNS 名または IP アドレスを選択します。

5c ファイアウォール外にあるインベントリサーバにスキャンを実行する場合は、プロキシサーバの IP アドレスとポート番号を指定します。

6 (オプション) インベントリスキャンをカスタマイズします。

6a Windows インベントリ対象サーバのハードウェアスキャンをカスタマイズするには、[Hardware Scan] タブをクリックし、次のように設定します。

[Enable DMI Scan]：インベントリ対象 Windows サーバの DMI スキャンを含めます。

[Enable WMI Scan]：インベントリ対象 Windows サーバの WMI スキャンを含めます。

6b Novell ZENworks for Servers 3.0 または ZENworks for Servers 3.0.2 がインストールされている NetWare または Windows インベントリ対象サーバへのソフトウェアスキャンをカスタマイズするには、[Software Scan] タブをクリックして、次の設定を実行します。詳細については、621 ページの「ZENworks for Servers 3.X インベントリ対象サーバのスキャン対象ソフトウェアインベントリ情報のカスタマイズ」を参照してください。

重要：ZENworks 6.5 Server Management がインストールされているインベントリ対象サーバでは、こうした設定を行わないでください。

[Enable Software Scan]：Inventory ポリシーに関連付けられたインベントリ対象サーバに対するソフトウェアスキャンを有効にします。スキャンプログラムは、インベントリ対象サーバのソフトウェア情報を収集し、Inventory データベースに格納します。

[Custom Scan Editor]：インベントリ対象 Windows サーバでスキャンするアプリケーションの詳細のリストをカスタマイズできます。Inventory Scanner は、カスタムスキャンエディタに示されるアプリケーションの詳細情報をスキャンします。

たとえば、カスタムスキャンエディタで次の詳細を指定します。ベンダ名 =Microsoft; 製品名 =Microsoft Office; 製品バージョン =10.0; ファイル名 =winword.exe; ファイルサイズ =1 MB。Inventory Scanner は、インベントリ対象サーバでサイズが 1MB である winword.exe ファイルをスキャンします。このファイルが見つかった場合、Inventory データベースに "winword.exe;1 MB" について "Microsoft;Microsoft Office;10.0" が格納されます。

[Product Identification Number]：Windows インベントリ対象サーバのみにインストールされている Microsoft アプリケーションの製品 ID 番号をスキャンできます。

6c [Configuration Editor] タブをクリックし、必要に応じて、次の .ini ファイルの設定を変更します。

- **Asset Information:** DMI からベンダ固有の情報をスキャンします。資産の設定方法の詳細については、572 ページの「DMI を使ったベンダ固有の資産情報のスキャン」を参照してください。

- **Zipped Names:** Jaz* および Zip* ドライブのハードウェアスキャンをカスタマイズします。詳細については、574 ページの「Jaz および Zip ドライブベンダのハードウェアスキャン情報のカスタマイズ」を参照してください。
- **SWRules:** Novell ZENworks for Servers 3.0 または ZENworks for Servers 3.0.2 がインストールされたインベントリ対象 Windows サーバで SWRules ファイルを設定します。ZENworks 6.5 Server Management がインストールされているインベントリ対象サーバの設定は行わないでください。

  SWRules オプションは、ベンダおよび製品のソフトウェアスキャン情報をカスタマイズします。詳細については、621 ページの「ZENworks for Servers 3.X インベントリ対象サーバのスキャン対象ソフトウェアインベントリ情報のカスタマイズ」を参照してください。
- **HWRules:** モニタの公称サイズをカスタマイズします。HWRules の .ini ファイルの設定方法に関する詳細については、575 ページの「モニタのサイズに関するハードウェア情報のカスタマイズ」を参照してください。

7 [Policy Schedule] タブをクリックします。

8 スケジュールを変更し、[Apply]、[Close] の順にクリックします。

9 Distributed Server Package のプロパティページで、[Distribution] タブをクリックし、[Add] をクリックします。

10 Distribution オブジェクトを参照して追加し、[OK] をクリックします。

11 [Apply]、[Close] の順にクリックします。

12 ConsoleOne で、Inventory Service オブジェクトを右クリックし、[Properties]、[Inventory Service Object Properties] タブの順にクリックします。

13 [Enable Scan of Machines] チェックボックスがオンになっていることを確認し、[OK] をクリックします。

この設定によって、選択したインベントリサーバに関連付けられたインベントリ対象サーバについてスキャンが選択されます。

ロールアップポリシーの設定

ロールアップポリシーの設定では、スキャン情報をロールアップするために、選択したインベントリサーバを設定します。ロールアップポリシーの設定では、選択したインベントリサーバからのインベントリ情報を送信する次のレベルのインベントリサーバ (Inventory Service オブジェクトの DN) を特定します。この設定は eDirectory に保存され、インベントリサーバオブジェクトに関連付けられます。

ロールアップポリシーを設定するには

1 ConsoleOne で、サーバパッケージを右クリックし、[Properties]、[Policies] の順にクリックして、適切なサブオプションを選択します。このポリシーをすべてのサーバに適用する場合は、[General] サブオプションを選択します。

2 [Enabled] 列の下にある [Inventory Rollup Policy] チェックボックスをオンにします。

3 [Properties] をクリックし、[Roll-Up Policy] ページを表示します。

4 Inventory Service オブジェクト (Inventory Service_*server_name*) の DN を参照して選択します。

ロールアップ先のサーバオブジェクト： 選択したインベントリサーバからインベントリ情報を送信するために、次のレベルのインベントリサーバにある Inventory Service オブジェクトの DN を指定する必要があります。指定するサーバは、別の中間サーバ、データベースが接続されている中間サーバ、データベースとインベントリ対象サーバが接続されている中間サーバ、インベントリ対象サーバが接続されている中間サーバ、ルートサーバ、またはインベントリ対象サーバが接続されているルートサーバです。

注： 同じインベントリサーバ上では情報をロールアップできないため、指定したインベントリサーバが別のサーバであることを確認します。また、情報のロールアップを行うために、ロールアップ先の次のレベルのサーバとして、下位のインベントリサーバを指定することもできません。

5 デフォルトでは、次のレベルのサーバの DNS 名または IP アドレス (DNS 名が設定されていない場合) がフィールドに適用されます。次のレベルのサーバに複数の IP アドレスが設定されている場合、優先して使用するアドレスを選択します。

重要： 次のレベルのサーバで指定されている DNS 名が有効であることを確認します。DNS 名が無効の場合、適切なサーバ IP アドレスを選択する必要があります。

6 ファイアウォール外にあるインベントリサーバにロールアップする場合は、プロキシサーバの IP アドレス、DNS 名、およびポート番号を指定します。

7 [Apply] をクリックします。

8 [Roll-Up Policy] タブをクリックし、[Roll-Up Schedule] をクリックします。

9 ロールアップする時間のスケジュールに必要な設定を変更し、[Apply] をクリックします。

Inventory ポリシーで情報のロールアップスケジュールを設定する場合は、ロールアップの頻度を最低でも 1 日に 1 回にしておくことをお勧めします。インベントリ情報のロールアップのスケジュール頻度を 1 時間に 1 度など、短く設定すると、インベントリサーバのパフォーマンスが低下する場合があります。

10 (条件付き) サーバパッケージをまだ関連付けていない場合、インベントリサーバまたはコンテナに関連付けるように求めるメッセージが表示されます。以前に設定して有効にしたポリシーは、このポリシーパッケージをインベントリサーバまたはコンテナに関連付けなければ機能しません。

ポリシーパッケージを関連付けるには

10a [Associations] タブをクリックし、[Add] をクリックします。

10b ロールアップポリシーを関連付けるインベントリサーバまたはコンテナを参照し、選択します。

10c [OK] を 2 回クリックします。

11 [Apply]、[Close] の順にクリックします。

注： Inventory ポリシーを変更するか、または Roll-Up スケジュール以外のオブジェクトを設定する場合は、常に Inventory Service を停止します。オブジェクトのポリシーおよびプロパティを設定します。Inventory Service を再開します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

ディクショナリ更新ポリシーの設定

ディクショナリ更新ポリシーを使用して、他のインベントリサーバからのソフトウェアディクショナリ更新を受信するようにインベントリサーバを設定します。ネットワーク内の少なくとも 1 台のインベントリサーバに、ディクショナリ更新を手動でダウンロードする必要があります。このインベントリサーバを、他のインベントリサーバに対するディクショナリ更新の配布元として使用できます。

1 ConsoleOne で、サーバパッケージを右クリックし、[Properties]、[Policies] の順にクリックして、適切なサブオプションを選択します。このポリシーをすべてのサーバに適用する場合は、[General] サブオプションを選択します。

2 [Enabled] 列の下にあるディクショナリ更新ポリシーのチェックボックスを選択します。

3 [Properties] をクリックし、[Dictionary Update Policy] ページを表示します。

4 次の設定を指定します。

4a （推奨）ディクショナリ更新サービスで、ロールアップポリシーでディクショナリ更新の配布元に設定されているインベントリサーバを使用する場合には、[Use the Roll-Up Server as the Update Source] チェックボックスを選択してください。このオプションを選択しない場合、ディクショナリ更新サービスは次の設定を使用します。

このチェックボックスを選択する場合は、514 ページのステップ 9 に進んでください。このオプションを選択しなかった場合、ディクショナリ更新サービスは、このポリシー（ディクショナリ更新ポリシー）で設定された次の設定を使用します。513 ページのステップ 4b に進みます。

注： スタンドアロンサーバおよびルートサーバの場合、このオプションを選択しないでください。次のポリシー設定を手動で設定する必要があります。

4b [Source Service Object] フィールドで、ディクショナリ更新の配布元のインベントリサーバの DN を参照して選択します。

4c ディクショナリ更新を配布するインベントリサーバの IP アドレスまたは DNS 名を選択します。

4d 配布元のインベントリサーバがファイアウォールの向こう側にある場合には、XML プロキシサーバの DNS 名およびポート番号を指定します。

4e [Apply] をクリックします。

5 [Dictionary Update Policy] タブをクリックして、[Dictionary Update Schedule] をクリックします。

6 [Dictionary Update Schedule] ページを設定して、Dictionary Consumer を実行するスケジュールを決めます。

[Weekly] スケジュールを設定することをお勧めします。

7 [Apply] をクリックします。

8 （条件付き）サーバパッケージをまだ関連付けていない場合、インベントリサーバまたはコンテナに関連付けるように求めるメッセージが表示されます。以前に設定して有効にしたポリシーは、このポリシーパッケージをインベントリサーバまたはコンテナに関連付けなければ機能しません。

ポリシーパッケージを関連付けるには

8a [Associations] タブをクリックし、[Add] をクリックします。

8b ディクショナリアップデートポリシーを関連付けるインベントリサーバまたはコンテナを参照し、選択します。

8c [OK] を 2 回クリックします。

9 [Apply]、[Close] の順にクリックします。

注： ディクショナリアップデートポリシーの設定を変更するために、Inventory Service を停止する必要はありません。

ディクショナリの配布の設定

ソフトウェアディクショナリは、次の方法で更新できます。

- Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) から各インベントリサーバに手動でディクショナリをダウンロードします。

  注： Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) では、3ヶ月に 1 度ディクショナリが更新され、TID として発行されます。

- Novell Support Web サイトから 1 つのインベントリサーバ (通常はルートサーバ) に手動でディクショナリをダウンロードし、ディクショナリ更新ポリシーを設定してセットアップ内のすべてのサーバに自動的にディクショナリを配布します。

インベントリサーバでは、サーバの役割に関係なく、他の任意のインベントリサーバからディクショナリ更新を受信できます。インベントリサーバの役割とは、そのサーバがインベントリ情報を受信するかどうか、情報をローカルのインベントリデータベースに保存するかどうか、インベントリ情報をロールアップするかどうかを表します。

インベントリサーバ間でソフトウェアディクショナリを更新し、配布するには

1 Novell Support Web サイトから手動でディクショナリをダウンロードし、インベントリサーバ上の *zenworks_installation_directory*¥zenworks¥inv¥server¥dictdir ディレクトリに保存します。

2 ディクショナリ更新ポリシーを設定します。詳細については、513 ページの「ディクショナリ更新ポリシーの設定」を参照してください。

すべてのインベントリサーバには、Server Inventory のインストール時に、ディクショナリプロバイダサービス (Dictionary Provider service) とディクショナリコンシューマサービス (Dictionary Consumer service) が自動的にインストールされます。

インベントリサーバが起動すると、Dictionary Consumer はディクショナリ更新ポリシーを読み込み、そのポリシーで指定されている Dictionary Provider (別のインベントリサーバ上で実行されている) に問い合わせます。

次に、Dictionary Consumer は、ディクショナリ更新ポリシーで設定されているスケジュールに基づいてディクショナリ更新を確認します。Dictionary Consumer は、Dictionary Provider 上のディクショナリファイルの日付とローカルに保存されているファイルの日付を比較します。Dictionary Provider 上のファイルが最新である場合、Dictionary Consumer はスケジュールに従って XML-RPC を使用して Dictionary Provider からファイルをダウンロードします。

ダウンロードしたディクショナリファイルのユーザ定義ルールは、ローカルディクショナリ内のルールと統合されます。統合の結果、ローカルディクショナリに存在するルールと異なるルールのセットが生成された場合は、統合されたルールのセットがローカルディクショナリに書き込まれます。統合プロセスの実行中に競合が発生する場合があります。この場合、次の点を踏まえて競合が解決されます。

- ダウンロードされたディクショナリのルールは、常にローカルディクショナリのルールに優先します。
- ソフトウェア識別情報の間で競合が発生した場合、ローカルディクショナリで競合している識別情報が、最終的な（統合されたされた）ディクショナリから削除されます。
- ソフトウェアディクショナリルールでは、ダウンロードされたルール、ローカルルールの順に最終ディクショナリに書き込むことでプロセスの実行中に重複を削除し、最終結果を取得します。これにより、ダウンロードされたソフトウェアルールは常にローカルルールよりも優先されます。

次の構成では、インベントリサーバ間のソフトウェアディクショナリの配布について示しています。この構成のインベントリツリーには、1 台のルートサーバ (R1)、1 台のリーフサーバ (L1)、および 2 台のスタンドアロンサーバ (S1 と S2) が設定されています。L1 は、R1 にインベントリ情報をロールアップします。

次の手順を実行して、すべてのインベントリサーバのソフトウェアディクショナリを更新します。

1. Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) から R1 に手動でディクショナリをダウンロードします。
2. ディクショナリアップデートポリシーを作成し、設定で R1 をディクショナリプロバイダに指定して、そのポリシーを L1 に関連付けます。ディクショナリ更新ポリシーの設定方法の詳細については、513 ページの「ディクショナリ更新ポリシーの設定」を参照してください。
3. S1 と S2 については、Novell Support Web サイト (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093255.htm) から手動でディクショナリをダウンロードすることも、R1 から最新バージョンのディクショナリを自動的に受け取れるようインベントリサーバを設定することもできます。

   S1 と S2 が R1 から最新バージョンのディクショナリを自動的に受け取れるようにするには、R1 を Dictionary Provider に指定するディクショナリ更新ポリシーを作成および設定した後、このポリシーを S1 と S2 に関連付けます。ディクショナリ更新ポリシーの設定方法の詳細については、513 ページの「ディクショナリ更新ポリシーの設定」を参照してください。

14 Server Inventory コンポーネントの理解

次の節では、Novell® ZENworks® 6.5 Server Inventory のコンポーネントおよびプロセスについて説明します。

- 517 ページの「Inventory Service Manager の理解」
- 520 ページの「Server Configuration Service の理解」
- 520 ページの「Inventory Scanner の理解」
- 527 ページの「Sender-Receiver の理解」
- 532 ページの「Selector の理解」
- 534 ページの「Storer の理解」
- 534 ページの「Dictionary Provider と Dictionary Consumer について」
- 535 ページの「Upgrade Service の理解」
- 535 ページの「インベントリサーバ上のインベントリコンポーネントの概要」
- 536 ページの「インベントリデータベースの理解」

Inventory Service Manager の理解

Inventory Service Manager は、インベントリサーバプロパティファイルで指定されている環境設定パラメータに基づいて、インベントリサーバにインベントリコンポーネントをロードします。

この節では、次のトピックについて説明します。

- 517 ページの「サービスのリスト」
- 518 ページの「NetWare インベントリサーバ上のサービス」
- 519 ページの「Windows インベントリサーバ上のサービス」

サービスのリスト

Service Manager は、次の重要なサービスをロードします。Service Manager がプロパティファイルからロードするサービスのリストは、*inventory_server_installation_directory_or_volume*¥zenworks¥inv¥server¥wminv¥properties で得られます。

Server Configuration Service
Inventory Scheduler Service
Inventory Scheduler Service
Selector Service
Receiver Service

Sender Service
Storer Service
Scan Collector Service
Dictionary Consumer Service
Dictionary Provider Service

これらのサービス名を使用して、対応するサービスの表示、開始、停止を行えます。

Inventory Service Manager は、*inventory_server_installation_directory_or_volume*¥zenworks¥inv¥server¥wminv¥properties ディレクトリにあるサーバプロパティファイル (config.properties) と役割ベースのプロパティファイルを読み取って、必要なサービスとサーバコンポーネントをロードします。

重要： 更新でサービスや Service Manager のロードに失敗する場合があるため、プロパティファイルは変更しないでください。

NetWare インベントリサーバ上のサービス

NetWare® インベントリサーバでは、startinv.ncf をロードするために、インストールプログラムが sys:¥system ディレクトリにある autoexec.ncf ファイルを変更します。sys:¥system にある startinv.ncf ファイルにより、インベントリサーバの起動時に、Inventory Service Manager が起動されます。

Inventory Service Manager がすでにロードされている場合は、サービスを開始、停止、または表示できます。

- Inventory Service Manager がロードされているかどうかを確認するには、サーバのプロンプトで、「**java -show**」と入力します。

  次のメッセージが表示されます。

  com.novell.zenworks.inventory.servercommon.ZENWorksInventoryServiceManager

- Inventory Service を開始するには、インベントリサーバのプロンプトで「**StartSer** ***service_name***」と入力します。

  service_name はリスト表示されたサービスを示します。*service_name* を変更する場合は、サービスの命名構文に従います。

  たとえば、Storer を開始するには、「**StartSer** ***Storer***」と入力します。

- Inventory Service を停止するには、インベントリサーバのプロンプトで「**StopSer** ***service_name***」と入力します。

  service_name はリスト表示されたサービスを示します。*service_name* を変更する場合は、サービスの命名構文に従います。

  たとえば、Storer を停止するには、「**StopSer** ***Storer***」と入力します。

- Inventory Service をリスト表示するには、インベントリサーバのプロンプトで「**ListSer** ***service_name***」と入力します。

  service_name はリスト表示されたサービスを示します。*service_name* を変更する場合は、サービスの命名構文に従います。

- すべての Inventory Service を一覧表示するには、インベントリサーバのプロンプトで、「**ListSer ***」と入力します。

Windows インベントリサーバ上のサービス

Windows* インベントリサーバでは、インストールプログラムは Service Manager をサービスとして作成します。サーバの起動時に、この Inventory Service Manager がサービスとしてロードされます。

Inventory Service Manager (ZENworks Inventory Service) がすでにロードされている場合は、サービスを開始、停止、または表示することができます。

Windows 2000/2003 インベントリサーバ上で Inventory Service を開始するには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell Inventory Service］を選択し、［開始］をクリックします。

Windows 2000/2003 インベントリサーバ上で Inventory Service を停止するには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell Inventory Service］を選択し、［停止］をクリックします。

Inventory Service を開始するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2 プロンプトで、「**StartSer** *service_name*」と入力します。

service_name は、Inventory Service を示します。

Inventory Service を停止するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2 プロンプトで、「**StopSer** *service_name*」と入力します。

service_name は、Inventory Service を示します。

すべての Inventory Service (ZENworks Inventory Service) を停止するには、デスクトップメニューから Windows サービスを使用します。

Inventory Service を一覧表示するには

1 *installation_directory*¥inv¥server¥wminv¥bin ディレクトリに移動します。

2 プロンプトで、「**ListSer [-verbose]** *service_name*」と入力します。

service_name は、Inventory Service を示します。

service_name を変更する場合は、サービスの命名構文に従います。

すべてのサービスを示すには、「"*"」のようにアスタリスク (*) ワイルドカード文字を二重引用符で囲みます。このワイルドカード文字は、ListSer パラメータで使用できます。

Server Configuration Service の理解

Server Configuration Service は、次のタスクを実行します。

- Novell eDirectory™ からポリシー情報を読み込み、他のインベントリコンポーネントに渡します。
- ポリシーを検証して、ポリシーが正しく設定されていることを確認します。
- インベントリデータベースのバージョンを確認します。

Inventory Scanner の理解

ZENworks 6.5 Server Management は、Inventory Scanner を使用して、NetWare インベントリ対象サーバと Windows インベントリ対象サーバからハードウェアおよびソフトウェアに関する情報を収集します。

Scanner は、フロッピーディスクドライブ、ハードディスクドライブ、BIOS、バス、マウス、キーボード、ディスプレイアダプタ、ネットワークアダプタカード、モデム、Jaz* ドライブ、Zip* ドライブ、サウンドカード、メモリカード、シリアルポート、パラレルポート、およびプロセッサなどのハードウェアの詳細を収集します。ソフトウェアスキャンでは、インベントリ対象サーバのアプリケーションを確認し、ベンダ名、製品名、バージョンなどのスキャンするソフトウェアに関する情報をレポートします。

次の節では、Inventory Scanner に関する詳細について説明します。

- 520 ページの「インベントリスキャンプロセス」
- 521 ページの「NetWare インベントリ対象サーバに対するスキャン」
- 523 ページの「Windows インベントリ対象サーバに対するスキャン」

スキャンするハードウェア情報およびソフトウェア情報はカスタマイズすることができます。詳細については、572 ページの「スキャンするハードウェアインベントリ情報のカスタマイズ」および576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」を参照してください。

インベントリスキャンプロセス

1. Subscriber をインベントリ対象サーバにインストールして設定する必要があります。
2. Server Inventory ポリシーでは、スキャンスケジュールを設定できます。このスケジュールに基づいて、ポリシーエンジンがインベントリ対象サーバでのスキャンをスケジュールおよび実行します。
3. Inventory Scanner は、更新されたディクショナリがインベントリサーバで利用可能かどうかをチェックし、更新されたディクショナリをダウンロードします。
4. Policy Enforcer は、Inventory Service オブジェクトに設定されているインベントリ設定および Server Inventory ポリシーを最初に読み込み、次に Inventory Scanner を起動します。
5. Inventory Scanner は、ハードウェア情報とソフトウェア情報をスキャンします。
6. Scanner によって収集されたスキャン情報は、スキャンデータファイル (.str) として保存されます。このファイルは、インベントリサーバに送信されます。

NetWare インベントリ対象サーバに対するスキャン

Inventory Scanner は、NetWare インベントリ対象サーバ上のハードウェアインベントリ情報とソフトウェアインベントリ情報をスキャンします。詳細については、次の節を参照してください。

- 521 ページの「ハードウェアインベントリ情報のスキャン」
- 521 ページの「ソフトウェアインベントリ情報のスキャン」

ハードウェアインベントリ情報のスキャン

ハードウェアインベントリ情報がスキャンされる NetWare インベントリ対象サーバ上のソースは次のとおりです。

- 521 ページの「SNMP (Simple Network Management Protocol)」
- 521 ページの「SMBIOS」
- 521 ページの「プローブ」

Inventory Scanner によって収集されるハードウェア情報の詳細については、699 ページの付録 I、「Inventory Scanner で収集されるハードウェア情報」を参照してください。

SNMP (Simple Network Management Protocol)

Scanner は、SNMP に基づいて、特定のハードウェア (デバイス) およびネットワーク情報を収集します。Scanner は、SNMP を使用して、products.dat にインストールおよび登録されているソフトウェアについてのレポートも行います。Scanner は、SNMP v2.0、および hostmib.nlm、ipxrtr.nlm、ipxrtrnm.nlm のサービスを使用します。

SMBIOS

Inventory Scanner は、ほとんどのハードウェアの BIOS に組み込まれている SMBIOS 情報を使用して、BIOS のバージョン、BIOS のリリース日、製造元、備品タグ、製品名、シリアル番号、プロセッサ情報、キャッシュ情報、システムスロット情報、ポート情報、ビデオアダプタ名、サウンドカード名などをレポートします。Inventory Scanner は、invaid.nlm を使用して SMBIOS から情報を読み込みます。

プローブ

プローブは、Inventory Scanner に組み込まれている特別なアルゴリズムです。ハードウェア情報を収集するために使用されます。

ソフトウェアインベントリ情報のスキャン

Inventory Scanner は、NetWare インベントリ対象サーバ上の次のソフトウェアインベントリ情報をスキャンします。

- 522 ページの「インストールされたソフトウェアの情報」
- 523 ページの「ディスクの使用状況」
- 523 ページの「ファイル情報」
- 523 ページの「アンチウィルス製品のウィルス定義ファイル」

インストールされたソフトウェアの情報

Scanner は、インベントリ対象サーバの Microsoft* Installer (MSI)、プログラムの追加と削除、ディクショナリベースのスキャン、プローブなどのソースからソフトウェア情報を収集します。

Products.Dat： これには、NetWare インベントリ対象サーバにインストールされたソフトウェアが含まれます。

ディクショナリベースのスキャン： これには、ソフトウェアディクショナリルールに基づいて収集されるソフトウェアが含まれます。詳細については、576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」を参照してください。

プローブ： プローブは、Inventory Scanner に組み込まれている特別なアルゴリズムです。ZENworks スイートおよびインストールされた ZENworks スイートのコンポーネントに関するソフトウェア情報を収集するために使用されます。

次の表は、Scanner がそれぞれのソースから収集するソフトウェア情報を示します。

スキャン対象の属性	Product.Dat	ディクショナリベースのスキャン	プローブ
Product Name	Yes	Yes	Yes
Vendor Name	No	Yes	Yes
Product Version	Yes	Yes	Yes
Product Identifier	No	No	No
Product Install Location	No	Yes	Yes
Category	No	Yes	No
Description	No	Yes	No
Help Link	No	No	No
MSI Package GUID	No	No	Yes
Display/Internal Version	No	Yes	Yes
Language	No	No	Yes
UnInstall String	No	No	No
Installation Source	No	No	No
Display Name	No	No	Yes
Support Pack	No	No	Yes
Product Edition	No	No	Yes
Last Execution Time	No	No	No
Usage Count	No	No	No

ディスクの使用状況

Scanner は、ソフトウェアディクショナリエディタで設定されているファイル拡張子について、ディスクの使用状況に関する情報を収集します。詳細については、576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」を参照してください。

ファイル情報

Scanner は、ディクショナリエントリと一致するファイル、およびソフトウェアディクショナリルールを使用して設定された不明なソフトウェアのリストに含まれているファイルについて、次の情報をレポートします。詳細については、586 ページの「ソフトウェアディクショナリのルールの設定」を参照してください。

Scanner がレポートするファイル属性は、FileName、FileSize、LastModifiedTime、InternalName、FileVersion、ProductName、ProductVersion、CompanyName、Language、DirectoryPath、および SoftwareDictionaryID です。

アンチウィルス製品のウィルス定義ファイル

Scanner は、インベントリ対象サーバにインストールされている McAfee Netshield* 4.6.*x* について、最新のウィルス定義の日付とバージョンに関する情報を収集します。

Windows インベントリ対象サーバに対するスキャン

Inventory Scanner は、Windows インベントリ対象サーバ上のハードウェアインベントリ情報とソフトウェアインベントリ情報をスキャンします。詳細については、次の節を参照してください。

- 523 ページの「ハードウェアインベントリ情報のスキャン」
- 525 ページの「ソフトウェアインベントリ情報のスキャン」

ハードウェアインベントリ情報のスキャン

ハードウェアインベントリ情報がスキャンされる Windows インベントリ対象サーバ上のソースは次のとおりです。

- 523 ページの「DMI (Desktop Management Interface)」
- 524 ページの「WMI (Windows Management Instrumentation)」
- 525 ページの「プローブ」

Inventory Scanner によって収集されるハードウェア情報の詳細については、699 ページの付録 I、「Inventory Scanner で収集されるハードウェア情報」を参照してください。

DMI (Desktop Management Interface)

インベントリ対象サーバをスキャンする Scanner は、業界標準の DMI (Desktop Management Interface) 規格 2.0 に準拠するスキャンも実行します。これらのプログラムは、DMI の MI (Management Interface) を使用して、インベントリ対象サーバにインストールされているハードウェアコンポーネントを調べます。Scanner は、DMI によってインベントリ対象サーバに搭載されている特定のコンポーネントをスキャンします。Scanner は、DMI サービス層に照会して、この情報を取得します。

MI によって、DMI 準拠の Scanner はサービス層内のサービスプロバイダを探索できます。サービスプロバイダは、管理可能なコンポーネントから情報を収集し、管理情報フォーマットデータベースに保存します。CI (Component Interface) は、管理可能なコンポーネントおよびサービス層と通信します。次の図は、Scanner と DMI とのやり取りを示しています。

DMI 規格の詳細については、DMTF の Web サイト (http://www.dmtf.org) を参照してください。

注： インベントリ対象サーバが DMI に準拠している場合、および Server Inventory ポリシーで [Enable DMI Scan] チェックボックスが選択されている場合、Scanner は DMI サービス層を照会することによりハードウェア情報を収集します。それ以外の場合、Scanner はハードウェアを探索します。

DMI を搭載し、ベンダによって提供された DMI コンポーネントをインストールすることをお勧めします。

たとえば、Compaq Family Deskpro EN Model-SFF6500 で Windows 98 を実行している場合、Compaq の Web サイトから Management Product ソフトウェア (Windows 98 用 Compaq Insight Management Desktop Agents ソフトウェア) をダウンロードします。

Dell の場合は、Dell の Web サイトから DM/Desktop Management Utilities ソフトウェアをダウンロードします。

WMI (Windows Management Instrumentation)

Scanner は、Microsoft の WMI (Windows Management Instrumentation) 規格に基づいて、Windows インベントリ対象サーバからハードウェア情報を収集します。

WMI は、企業環境で管理情報へのアクセスを可能にする WBEM(Web-Based Enterprise Management) を Microsoft が実装したものです。WMI 1.5 は、業界標準である CIM (Common Information Model) スキーマに完全に準拠しています。詳細については、Microsoft WMI の Web サイト (http://www.microsoft.com/hwdev/driver/WMI) を参照してください。WMI は、DMI や SNMP など、既存の管理規格にも対応しています。

Scanner は、WMI を使用してインベントリ対象サーバにインストールされているハードウェアコンポーネントを調べます。また、WMI を使用してインベントリ対象サーバに搭載されている特定のコンポーネントもスキャンします。

WMI 準拠の scanner は、Windows インベントリ対象サーバでのみサポートされています。

Server Inventory で、インベントリ対象サーバの WMI 情報を表示できます。

インベントリ対象サーバから WMI 情報を取得するには、Microsoft WMI の Web サイト (http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/576/msdncompositedoc.xml) から Microsoft の Windows Management Instrumentation - Core Software Installation をダウンロードして、WMI Core Software を Windows 98 サーバにインストールする必要があります。

重要： インベントリ対象サーバに WMI をインストールするには、WMI Core Software Installation のみをダウンロードします。WMI に関連する問題は、ダウンロードした WMI SDK を使用してトラブルシューティングを行うことができます。Windows 2000 サーバには、すでに WMI Core Software がインストールされています。

デフォルトでは、DMI スキャンと WMI スキャンはいずれも有効です。DMI スキャンまたは WMI スキャンのいずれかを無効にするには、Inventory ポリシーのウィンドウで [Enable DMI] または [Enable WMI] のいずれかのチェックボックスの選択を解除します。

プローブ

プローブは、Inventory Scanner に組み込まれている特別なアルゴリズムです。ソフトウェア情報を収集するために使用されます。

ソフトウェアインベントリ情報のスキャン

Inventory Scanner は、Windows インベントリ対象サーバ上の次のソフトウェアインベントリ情報をスキャンします。

- 525 ページの「インストールされたソフトウェアの情報」
- 526 ページの「ディスクの使用状況」
- 526 ページの「ファイル情報」
- 526 ページの「アンチウィルス製品のウィルス定義ファイル」

インストールされたソフトウェアの情報

Scanner は、インベントリ対象ワークステーション上の Microsoft Installer (MSI)、プログラムの追加と削除、ディクショナリベースのスキャン、プローブなどのソースからソフトウェア情報を収集します。

MSI: これには、Microsoft Installer を使用してインベントリ対象サーバにインストールされたソフトウェアが含まれます。

プログラムの追加と削除： これには、[プログラムの追加と削除] ウィンドウに表示されるソフトウェアが含まれます。

ディクショナリベースのスキャン： これには、ソフトウェアディクショナリルールに基づいて収集されるソフトウェアが含まれます。詳細については、576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」を参照してください。

プローブ： プローブは、Inventory Scanner に組み込まれている特別なアルゴリズムです。Windows オペレーティングシステム、Internet Explorer、Media Player、Outlook Express、Microsoft Office とインストールされたそのコンポーネント、Novell Client とインストールされたそのコンポーネント、ZENworks スイートとインストールされたそのコンポーネントに関するソフトウェア情報を収集するために使用されます。

次の表は、Scanner がそれぞれのソースから収集するソフトウェア情報を示します。

スキャン対象の属性	MSI	プログラムの追加と削除	ディクショナリベースのスキャン	プローブ
Product Name	Yes	Yes	Yes	Yes
Vendor Name	Yes	No	Yes	Yes
Product Version	Yes	Yes	Yes	Yes
Product Identifier	Yes	Yes	No	No
Product Install Location	Yes	Yes	Yes	Yes
Category	No	No	Yes	No
Description	No	No	Yes	No

スキャン対象の属性	MSI	プログラムの追加と削除	ディクショナリベースのスキャン	プローブ
Help Link	Yes	Yes	No	No
MSI Package GUID	Yes	Yes	No	Yes
Display/Internal Version	Yes	Yes	Yes	Yes
Language	Yes	Yes	No	Yes
UnInstall String	Yes	Yes	No	No
Installation Source	Yes	Yes	No	No
Display Name	Yes	Yes	No	Yes
Support Pack	No	No	No	Yes
Product Edition	No	No	No	Yes
Last Execution Time	No	Yes	No	No
Usage Count	No	Yes	No	No

ディスクの使用状況

Scanner は、ソフトウェアディクショナリエディタで設定されているファイル拡張子について、ディスクの使用状況に関する情報を収集します。詳細については、576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」を参照してください。

ファイル情報

Scanner は、ディクショナリエントリと一致するファイル、およびソフトウェアディクショナリルールを使用して設定された不明なソフトウェアのリストに含まれているファイルについて、次の情報をレポートします。詳細については、586 ページの「ソフトウェアディクショナリのルールの設定」を参照してください。

Scanner がレポートするファイル属性は、FileName、FileSize、LastModifiedTime、InternalName、FileVersion、ProductName、ProductVersion、CompanyName、Language、DirectoryPath、および SoftwareDictionaryID です。

アンチウィルス製品のウィルス定義ファイル

Scanner は、次の製品バージョンについて、インベントリ対象サーバにインストールされている最新のウィルス定義の日付とバージョンに関する情報を収集します。

Symantec AntiVirus Corporate Edition 8.0
Norton AntiVirus Corporate Edition for Windows 7.0
Norton AntiVirus Corporate Edition 7.6.1.0000
Symantec Norton AntiVirus 2000
Symantec Norton Internet Security 2002
Symantec Norton AntiVirus 2003 (9.00)
Symantec Norton AntiVirus 2003 Professional Edition (9.00)
Symantec Norton AntiVirus 2004 (10.00)

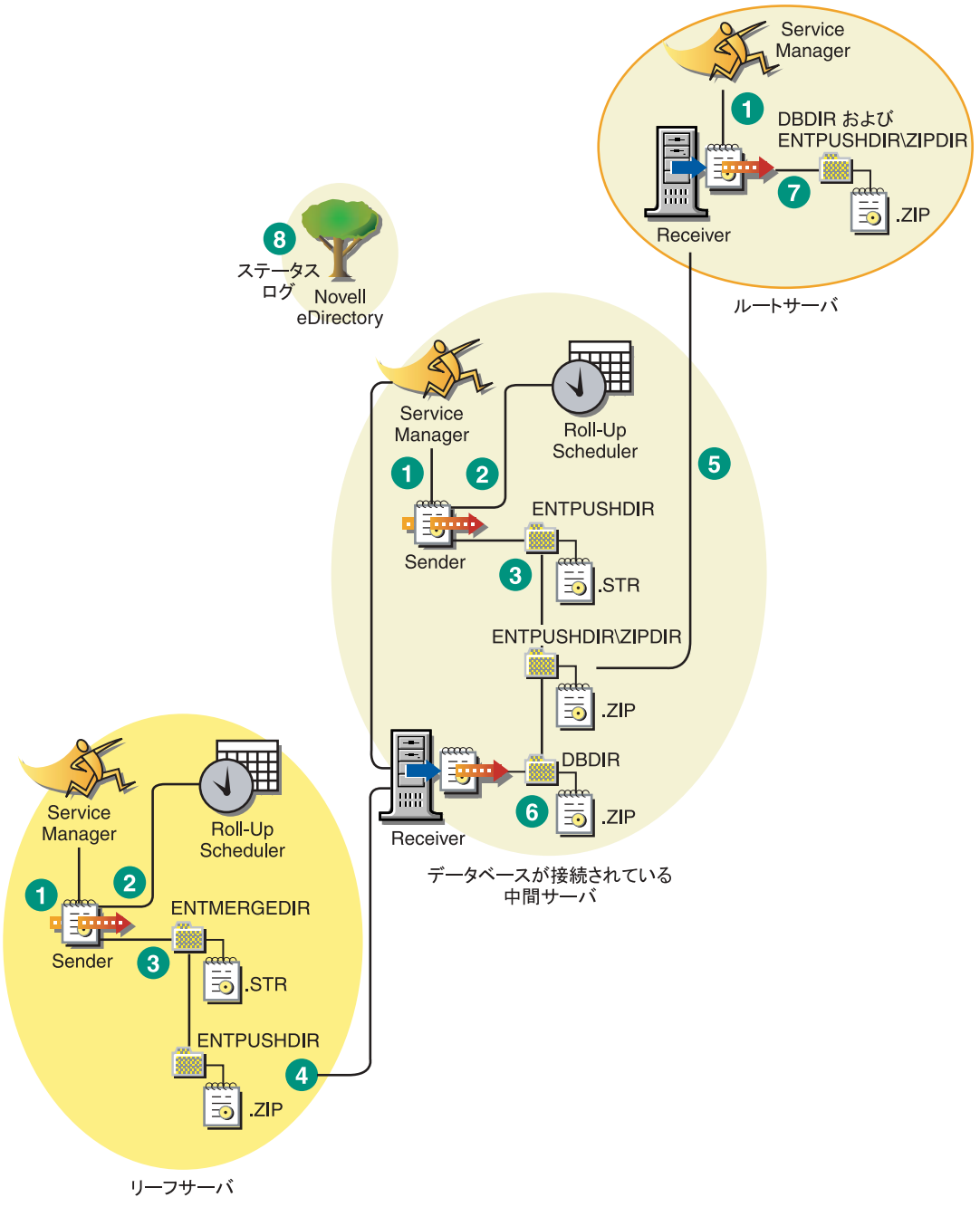
Symantec Norton Internet Security 2004 (10.00)
Symantec Norton AntiVirus 2004 Professional (10.00)
Symantec Norton Internet Security 2004 Professional (10.00)
Symantec Norton AntiVirus 2005 Professional (11.00)
Symantec Norton Internet Security 2005 Professional (11.00)
Network Associates McAfee VirusScan 4.0.3 (Windows 9*x*)
Network Associates McAfee VirusScan NT 4.0.3a (Windows NT)
Network Associates McAfee NetShield 4.5.0
Network Associates McAfee VirusScan 4.5.0
Network Associates McAfee VirusScan 4.5.1
Network Associates McAfee VirusScan (McAfee Security Center) 8.0
Network Associates McAfee VirusScan ASaP
Network Associates McAfee VirusScan Enterprise 7.1
Network Associates McAfee VirusScan Enterprise 8.0
Central Command Vexira AntiVirus Guard for Windows XP (2000 + NT) 2.10
Central Command Vexira AntiVirus Windows 95/98
Central Command Vexira AntiVirus NT/2000 Servers
Central Command Vexira AntiVirus Server Edition (6.26.*xx*.*xx*)
Sophos Anti-Virus - Windows NT/2000/XP/2003
Sophos Anti-Virus - Windows 95/98
Trend Micro PC-cillin 2002 (9.*x*)
Trend Micro PC-cillin 2003 (10.*x*)
Trend Micro Internet Security 11.*x* (PC-cillin)
Trend Micro Internet Security 2005 12.*x* (PC-cillin)
Trend Micro Server Protect 5.*xx*
Trend Micro OfficeScan 5.*xx* - Client for Windows NT/2000/XP
Trend Micro OfficeScan 5.*xx* - Client for Windows 9*x*

Sender-Receiver の理解

インベントリサーバ上の Sender と Receiver は、下位のインベントリサーバから上位のインベントリサーバにスキャンファイルを転送します。Sender-Receiver は、ZENworks Web Server を使用して XML-RPC 要求を処理します。詳細情報については、以下を参照してください。

- 529 ページの「Sender の理解」
- 530 ページの「Receiver の理解」
- 530 ページの「圧縮されたスキャンデータファイルの理解」
- 531 ページの「Sender-Receiver のディレクトリ」

次の図は、Sender と Receiver が実行するプロセスを示しています。



Sender と Receiver は次のプロセスを実行します。

1. Service Manager が、Sender-Receiver コンポーネントを起動します。
2. Roll-Up Scheduler が、指定されたロールアップ時刻に Sender をアクティブにします。
3. Sender は、エンタープライズマージディレクトリ (entmergedir) からエンタープライズプッシュディレクトリ (entpushdir) にスキャンデータファイル (.str) を移動し、そのファイルを .zip ファイルに圧縮します。

4. 各 .zip ファイルと .prp ファイルが再度 .zip ファイルに圧縮されます。.prp ファイルは、その .zip ファイルに関する情報を含む内部ファイルです。
5. Sender は、¥entpushdir ディレクトリから次のレベルのインベントリサーバの Receiver に .zip ファイルを送信します。
6. Receiver は、¥entpushdir¥zipdir ディレクトリに .zip ファイルを保存します。
7. Receiver は、.zip ファイルを ¥entpushdir ディレクトリにコピーし、¥entpushdir¥zipdir ディレクトリからその .zip ファイルを削除します。
8. データベースがサーバに接続されている場合、Receiver は、.zip ファイルをデータベースディレクトリ (dbdir) にコピーします。
9. Sender-Receiver はステータスを eDirectory に記録します。

Sender の理解

Sender は、リーフサーバまたは中間サーバ上で実行される Java* コンポーネントです。Service Manager によりロードされるサービスです。535 ページの「インベントリサーバ上のインベントリコンポーネントの概要」のインベントリサーバコンポーネントのクイックリファレンスの表を参照してください。

インベントリ情報をロールアップする際の Sender からの情報の流れは次のとおりです。

1. Service Manager が、インベントリサーバ上の Sender を起動します。Sender は、ロールアップスケジュールで指定されている時刻に、エンタープライズマージディレクトリ (entmergedir) からエンタープライズプッシュディレクトリ (entpushdir) にスキャンデータ (.str) を移動します。

   Sender は、インベントリサーバの ¥entpushdir ディレクトリにあるこの .str ファイルを .zip ファイルに圧縮した後、.str ファイルを削除します。この .zip ファイルは、.prp ファイルと共に .zip ファイルに再び圧縮されます。.prp ファイルは、その .zip ファイルに関する情報を含む内部ファイルです。詳細については、530 ページの「圧縮されたスキャンデータファイルの理解」を参照してください。
2. Sender は、eDirectory の Inventory Service オブジェクトの zeninvRollUpLog 属性に、新しいレコードを作成します。このレコードには、Sender が .str ファイルを圧縮したサーバおよび .zip ファイルの名前とサイズなどの詳細情報が含まれます。
3. Receiver の Inventory Service オブジェクトのプロパティの [Discard Scan Data Time] に基づいて、Sender は、指定されたスキャンデータ廃棄時刻より前に作成された .zip ファイルを ¥entpushdir ディレクトリから削除します。これにより、ロールアップで送信される不要なスキャン情報を削除できます。
4. Sender は、圧縮した .zip ファイルを Receiver に送信します。このとき、最も古い圧縮ファイルから送信します。
5. .zip ファイルの転送後、Sender は ¥entpushdir ディレクトリ内の圧縮ファイルを削除します。
6. 情報のロールアップ後、Sender は圧縮ファイルを作成したインベントリサーバの zeninvRollUpLog 属性を更新します。更新する内容は、Sender がファイルを転送した送信元のインベントリサーバ、.zip ファイル名、転送時刻、ファイルの転送に要した合計時間、送信先インベントリサーバなどの詳細情報です。

   ツリー間でインベントリ情報をロールアップする場合、ロールアップステータスメッセージは、ツリー内で .zip ファイルを受信する最初のインベントリサーバに記録されます。

Sender の全アクションのステータス情報は、ロールアップログとサーバステータスログに記録されます。詳細については、685 ページの「ステータスログによる Server Inventory の監視」を参照してください。

Sender は、Receiver に接続できない場合、10 秒後に接続を再試行します。再試行の間隔は、係数を 2 として指数的に増加します。Receiver への接続を 14 回再試行した後、再試行は中止されます。中止まで、Sender は約 23 時間再試行を継続します。接続が確立している間、他の情報は処理されません。

Receiver の理解

Receiver は、中間サーバまたはルートサーバ上で実行される Java コンポーネントであり、Service Manager によりロードされるサービスです。535 ページの「インベントリサーバ上のインベントリコンポーネントの概要」のインベントリサーバコンポーネントのクイックリファレンスの表を参照してください。

Receiver は次の処理を実行します。

1. Receiver は、Sender からスキャン .zip ファイルを受信し、¥entpushdir¥zipdir ディレクトリに保存します。
2. Receiver は、.zip ファイルを ¥entpushdir ディレクトリにコピーし、¥entpushdir¥zipdir ディレクトリからその .zip ファイルを削除します。

   中間サーバで、ファイルは ¥entpushdir に保存されます。データベースが接続されている中間サーバ、またはデータベースとインベントリ対象サーバが接続されている中間サーバで、ファイルは ¥entpushdir に保存されデータベースディレクトリ (dbdir) にコピーされます。
3. ルートサーバまたはインベントリ対象サーバが接続されているルートサーバ上の Receiver は、Sender から .zip ファイルを受信し、¥entpushdir¥zipdir ディレクトリに保存します。ファイルをインベントリサーバ上の ¥dbdir ディレクトリにコピーします。
4. Receiver は、ステータス情報をロールアップログに記録します。詳細については、685 ページの「ステータスログによる Server Inventory の監視」を参照してください。

圧縮されたスキャンデータファイルの理解

Sender はスキャンデータファイル (.str) を .zip ファイルに圧縮します。この .zip ファイルは、.prp ファイルと共に .zip ファイルに再び圧縮されます。.zip ファイル (.zip ファイルと .prp ファイルを含む) は、次の命名規則に従って名前が付けられます。

scheduledtime_inventoryservername_treename_storedstatus.zip

scheduledtime は .zip ファイルが作成された日時、*inventoryservername* は .zip ファイルが圧縮されたインベントリサーバ、*treename* は .zip ファイルが存在する一意のツリー名、*storedstatus* は .zip ファイルの保存ステータス、*ZIP* は圧縮されたファイルのファイル拡張子を示します。

storedstatus は、0、1、または 2 によって示されます。0 は、.zip ファイルがまだ保存されていないことを示します。1 は、.zip ファイルが初めてインベントリサーバに保存されることを示します。2 は、.zip ファイルが一度保存されたことがあることを示します。

.zip ファイル名は、データベースがインベントリサーバに接続されているかどうかによって異なります。

.zip ファイルには、.zip ファイルとプロパティファイルが含まれます。プロパティファイルは、次の命名規則に従って名前が付けられます。

scheduledtime_inventoryservername.prp

プロパティファイルには、スケジュール設定されている時間、インベントリサーバ名、および署名が含まれています。署名は .zip ファイルの認証に役立ちます。

各 .zip ファイルには最大 50 個の .str ファイルを含めることができます。

Sender-Receiver のディレクトリ

次の表は、Sender-Receiver が使用するディレクトリのクイックリファレンスです。

サーバ	Sender	Receiver	Entmergdir	Entpushdir ¥ Zipdir	Entpushdir	Dbdir
リーフサーバ、データベースが接続されているリーフサーバ	このインベントリサーバ上で実行	--	Sender は、.str ファイルを ¥entpushdir に移動します。	--	Sender は、.str ファイルを .zip ファイル形式に圧縮します。 Sender は .str ファイルを削除します。 .zip ファイルを次のレベルのインベントリサーバに送信します。	--
中間サーバ	このインベントリサーバ上で実行	このインベントリサーバ上で実行	--	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルを受信します。	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルをコピーします。 Sender は、次のレベルのインベントリサーバに .zip ファイルを送信します。	--
Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	このインベントリサーバ上で実行	このインベントリサーバ上で実行	Sender は、.str ファイルを ¥entpushdir に移動します。	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルを受信します。	Receiver は、¥zipdir からこのディレクトリに .zip ファイルをコピーします。 Sender は、次のレベルのインベントリサーバに .zip ファイルを送信します。 Sender は、.str ファイルを .zip ファイル形式に圧縮します。 Sender は .str ファイルを削除します。	--

サーバ	Sender	Receiver	Entmergdir	Entpushdir ¥ Zipdir	Entpushdir	Dbdir
データベースが接続されている中間サーバ	このインベントリサーバ上で実行	このインベントリサーバ上で実行	--	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルを受信します。	Receiver は、¥zipdir からこのディレクトリに .zip ファイルをコピーします。 Sender は、次のレベルのインベントリサーバに .zip ファイルを送信します。	Receiver は、このディレクトリ内にファイルをコピーします。
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	このインベントリサーバ上で実行	このインベントリサーバ上で実行	Sender は、.str ファイルを ¥entpushdir に移動します。	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルを受信します。	Receiver は、¥zipdir からこのディレクトリに .zip ファイルをコピーします。 Sender は、.str ファイルを .zip ファイル形式に圧縮します。 Sender は .str ファイルを削除します。 Sender は、次のレベルのインベントリサーバに .zip ファイルを送信します。	Receiver は、このディレクトリ内にファイルをコピーします。
ルートサーバ、 Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	--	このインベントリサーバ上で実行	--	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルを受信します。	--	Receiver は、このディレクトリ内で、下位のインベントリサーバから .zip ファイルをコピーします。

スタンドアロンサーバには Receiver はロードされません。

Selector の理解

Selector は、インベントリ対象サーバからインベントリ情報を受信するインベントリサーバ上の Java コンポーネントです。インベントリサーバは、リーフサーバ、データベースが接続されているリーフサーバ、データベースとインベントリ対象サーバが接続されている中間サーバ、インベントリ対象サーバが接続されている中間サーバ、インベントリ対象サーバが接続されているルートサーバ、およびスタンドアロンサーバのいずれかです。535 ページの「インベントリサーバ上のインベントリコンポーネントの概要」のインベントリサーバコンポーネントのクイックリファレンスの表を参照してください。

Selector は次の処理を実行します。

1. インベントリ対象サーバのスキャン中に、Scanner は、インベントリ対象サーバで実行される各スキャンについて、インベントリサーバのスキャンディレクトリ (scandir) にスキャンデータファイル (.str) を作成します。¥scandir の場所は Inventory Service オブジェクトから取得します。Selector は、Scan Collector が ¥scandir ディレクトリに保存した .str ファイルを処理します。
2. Selector は、次の条件をチェックして、Scanner によって生成された .str ファイルが有効であることを確認します。
   - .str ファイルを使用して生成され、Scanner によって .str ファイルに記録された整数値と、Selector によって .str ファイルを使用して生成された整数値は同じである必要があります。
   - .str ファイルの実サイズは、.str ファイルに記録されているサイズと同期している必要があります。

   Selector は有効な .str ファイルのみを処理します。ディレクトリに無効なファイルがある場合、Selector はそれらのファイルを削除します。
3. インベントリサーバの役割に基づき、Selector は、.str ファイルを ¥dbdir ディレクトリ（データベースが接続されている場合）と ¥entmerge ディレクトリにコピーします。.str ファイルがディレクトリにすでに存在する場合は、ファイルが上書きされます。

   次の表は、Selector がファイルをコピーするか、ファイル名を変更するディレクトリの一覧です。

サーバ	データベースディレクトリ (dbdir) に .str ファイルをコピー	データベースディレクトリ (dbdir) の .str ファイルの名前を変更	エンタープライズマージディレクトリ (entmergedir) の .str ファイルの名前を変更
データベースが接続されているリーフサーバ	Yes	--	Yes
リーフサーバ	--	--	Yes
Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	Yes	--	Yes
スタンドアロンサーバ	--	Yes	--
Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	--	Yes	--

4. Selector は、ステータス情報をサーバログに記録します。詳細については、685 ページの「ステータスログによる Server Inventory の監視」を参照してください。

Storer の理解

Storer は、データベースが接続されているインベントリサーバ上の Java コンポーネントです。インベントリサーバは、データベースが接続されているリーフサーバ、データベースが接続されている中間サーバ、データベースとインベントリ対象サーバが接続されている中間サーバ、ルートサーバ、インベントリ対象サーバが接続されているルートサーバのいずれかです。535 ページの「インベントリサーバ上のインベントリコンポーネントの概要」のインベントリサーバコンポーネントのクイックリファレンスの表を参照してください。

Storer は、Service Manager によってロードされるサービスとして実行され、¥dbdir ディレクトリ内のファイルを処理します。

Storer は次の処理を実行します。

1. Storer は、インベントリサーバの Configuration Service から起動設定パラメータを読み込みます。
2. Storer は、eDirectory に保存されているインベントリサーバの設定情報に基づいて、データベースディレクトリ (dbdir) でスキャンファイルを調べます。インベントリサーバの設定情報により、eDirectory ポリシーに基づいて、¥dbdir の場所やデータベースサーバが決定されます。Selector は .str ファイルを ¥dbdir ディレクトリに挿入し、Receiver は .zip ファイルを ¥dbdir ディレクトリに挿入します。
3. Storer は、.str ファイルと .zip ファイルを交互に処理します。
4. Storer は、圧縮された .str ファイルと .prp ファイルを含む .zip ファイルを temp ディレクトリ (¥dbdir¥temp) に解凍し、インベントリ対象サーバの .str ファイルのインベントリ情報でデータベースを更新します。
5. Storer はインベントリサーバのステータスログにあるステータスを更新し、ロールアップログを更新します。インベントリサーバのステータスログにあるインベントリサーバのステータス情報は表示できます。

   ツリー間でインベントリ情報をロールアップする場合、ロールアップステータスメッセージは、ツリー内で .zip ファイルを受信する最初のインベントリサーバに記録されます。詳細については、685 ページの「ステータスログによる Server Inventory の監視」を参照してください。

Dictionary Provider と Dictionary Consumer について

すべてのインベントリサーバおよびインベントリ対象サーバには、Server Inventory のインストール時に自動的にインストールされる Dictionary Provider サービスと Dictionary Consumer サービスがあります。

インベントリ対象サーバが起動すると、Dictionary Consumer はディクショナリ更新ポリシーを読み込み、そのポリシーで指定されている Dictionary Provider(インベントリサーバ上で実行されている) に問い合わせます。

次に、Dictionary Consumer は、ディクショナリ更新ポリシーで設定されているスケジュールに基づいてディクショナリ更新を確認します。Dictionary Consumer は、Dictionary Provider 上のディクショナリファイルの日付とローカルに保存されているファイルの日付を比較します。Dictionary Provider 上のファイルが最新である場合、Dictionary Consumer はスケジュールに従って XML-RPC を使用して Dictionary Provider からファイルをダウンロードします。

Upgrade Service の理解

Upgrade Service は、Service Manager によってロードされるサービスとして実行されます。

Upgrade Service は、ZENworks 6.5 Server Management および ZENworks 6.5 Desktop Management と互換性を持つようにインベントリデータベーススキーマと情報を修正します。Upgrade Service は、すべての機能をステートドリブン方式で実行します。これは、あるステップが正常に実行されたとき、Upgrade Service が同じステップを実行しないようにするためです。Upgrade Service は非割り込みサービスです。このため、Upgrade Service を手動で中止することはできません。Upgrade Service は、すべての機能を実行した後で自動的に終了します。

データベースの移行作業は、移行ログに記録されます。移行ログは、*installation_path*¥zenworks¥inv¥server¥wminv¥logs¥migrationlogs ディレクトリに作成されます。

インベントリサーバ上のインベントリコンポーネントの概要

インベントリサーバのタイプに応じて、インベントリサーバ上には次のインベントリコンポーネントが存在します。

サーバコンポーネント	ルートサーバ	Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	リーフサーバ	データベースが接続されているリーフサーバ	中間サーバ	Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	データベースが接続されている中間サーバ	Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	スタンドアロンサーバ
Service Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scan Collector	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Selector	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes
Storer	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes
Sender	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Receiver	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
データベース	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes
Inventory Removal Service	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Upgrade Service	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes

サーバコンポーネント	ルートサーバ	Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）	リーフサーバ	データベースが接続されているリーフサーバ	中間サーバ	Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）	データベースが接続されている中間サーバ	Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）	スタンドアロンサーバ
Dictionary Consumer と Dictionary Provider	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

インベントリデータベースの理解

Server Inventory では、CIM (Common Information Model) 準拠の Sybase データベースを一元管理できます。インベントリデータベースは、サーバのハードウェアおよびソフトウェアのリポジトリとして機能します。ネットワーク管理者は、ConsoleOne でインベントリ情報を表示したり、データベースを照会したり、インベントリレポートを作成したりできます。詳細については、15 章 537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。

15 ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解

この節では、DMTF (Distributed Management Task Force) の CIM (Common Information Model) を使用して実装される Novell® ZENworks® 6.5 Server Management インベントリデータベーススキーマの設計について説明します。この節をよく理解するには、CIM や DMI (Desktop Management Interface) などの用語を熟知している必要があります。RDBMS (Relational Database Based Managed Systems) とデータベースの概念についてもよく理解しておく必要があります。

次の各節で詳細について説明します。

- 537 ページの「概要」
- 538 ページの「CIM スキーマ」
- 545 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマ」

概要

DMTF は、デスクトップ環境、エンタープライズ環境、インターネット環境に対する管理基準およびイニシアチブの開発、採用、統一を推進する業界団体です。DMTF の詳細については、DMTF の Web サイト (http://www.dmtf.org) を参照してください。

DMTF の CIM は、システム管理およびネットワーク管理に対するアプローチであり、オブジェクト指向パラダイムの基本的な構造技術および概念化技術を利用しています。このアプローチでは、統一モデリング方式を採用しています。この方式は、基本的なオブジェクト指向構成要素と共に、複数の団体によるオブジェクト指向スキーマの共同開発をサポートしています。

管理スキーマは、分類と関連付け、および管理対象環境を記述するための共通のフレームワークを構築するための基本クラスセットの両方に対して、基本トポロジレベルで共通の概念的フレームワークを構築するためのものです。管理スキーマは次の概念層に分けられます。

- **コアモデル：** 全管理領域に適用できる概念を表す情報モデル。
- **共通モデル：** 特定の管理領域に共通し、特定のテクノロジや実装に依存しない概念を表す情報モデル。共通領域とは、システム、アプリケーション、データベース、ネットワーク、およびデバイスです。情報モデルは具体的で明確であるため、管理アプリケーションの開発の基礎になります。このモデルには、テクノロジに固有のスキーマ領域を拡張するための基本クラスセットがあります。コアモデルと共通モデルを併せて CIM スキーマと言います。
- **拡張スキーマ：** このスキーマは、共通モデルをテクノロジ固有に拡張したものです。このスキーマは、たとえば、NetWare®、Microsoft* Windows* といったオペレーティングシステムなどの環境に固有のものです。

CIM は仕様とスキーマで構成されています (DMTF の Web サイト (http://www.dmtf.org/standards/standard_cim.php) を参照してください)。仕様には、メタスキーマに加えて、MOF (Managed Object Format) と呼ばれる具象表記言語が定義されています。

CIM スキーマ

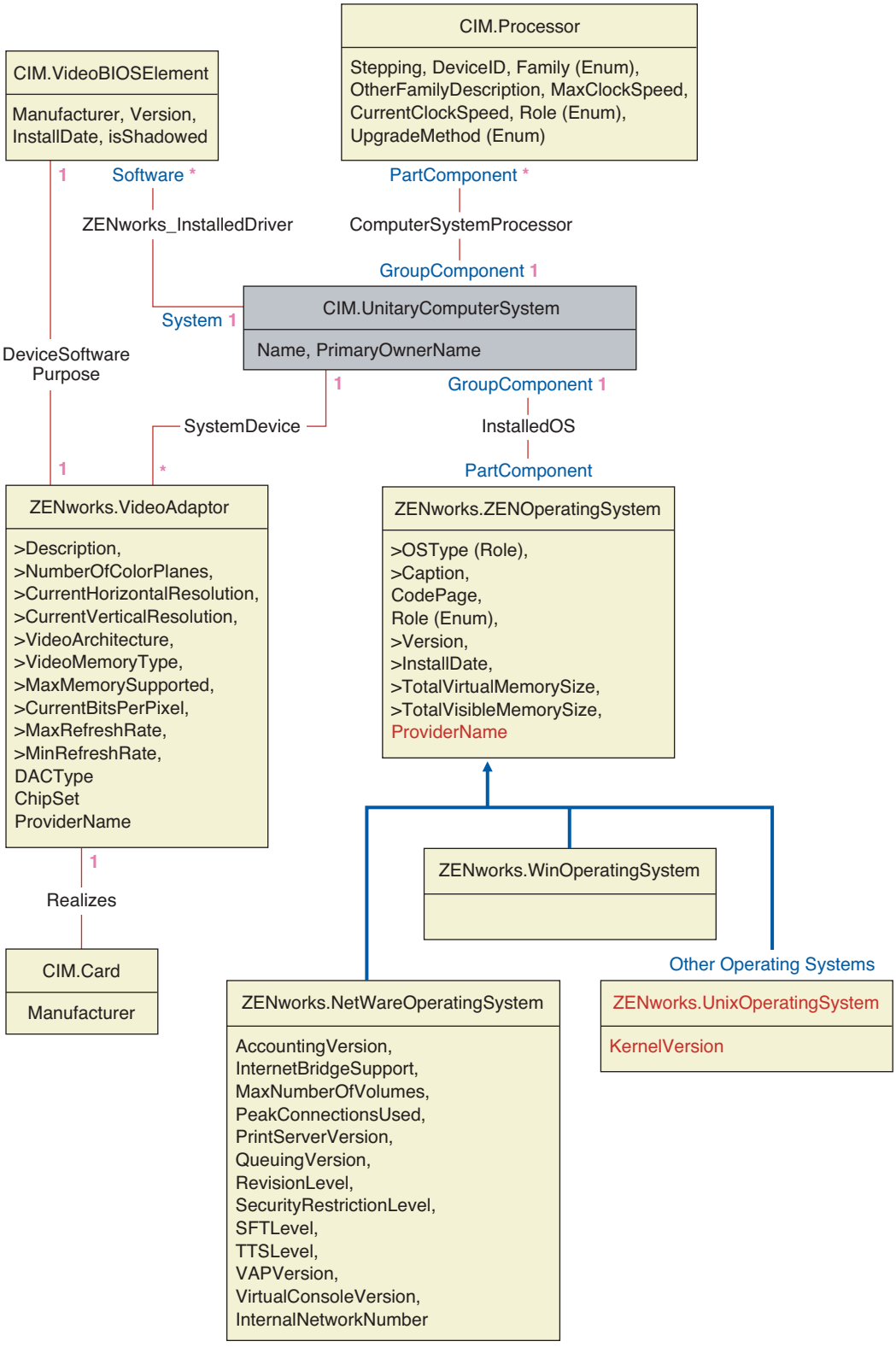
メタスキーマのエレメントは、クラス、プロパティ、およびメソッドです。メタスキーマは、クラスのタイプとして指示と関連付けをサポートし、プロパティのタイプとして参照をサポートします。

クラスは、クラス間のサブタイプの関係を表す汎化階層に配列できます。汎化階層は、ルート有向グラフであり、多重継承はサポートしていません。

通常のクラスには、ブール、整数、文字列などの組み込みタイプのスカラまたは配列のプロパティを含めることができます。組み込みクラスや他のクラスへの参照を含めることはできません。

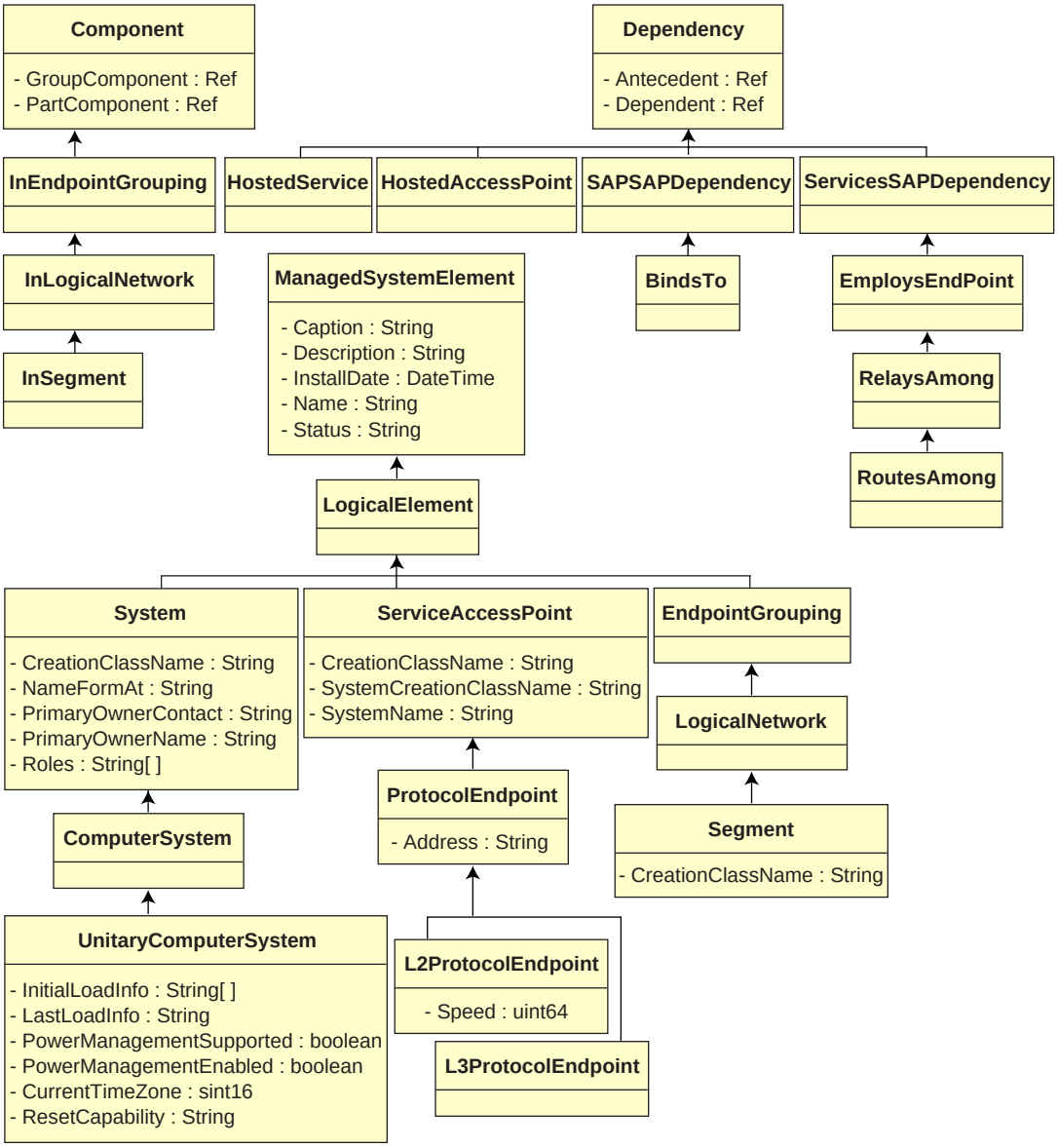
関連付けとは、複数の参照が含まれる特別なクラスです。複数のオブジェクトの関係を示します。関連付けを定義する方法によって、関連するクラスに影響を与えることなくクラス間の関係を確立できます。つまり、関連付けを追加しても、関連するクラスのインタフェースには影響を及ぼしません。関連付けのみが参照を持つことができます。

次の図のスキーマのフラグメントは、ZENworks 6.5 Server Management が使用する CIM オブジェクト間の関係を示しています。



この図は、CIM スキーマがリレーショナル DBMS スキーマにマッピングする方法を示しています。クラスはクラス名と共にボックスの見出しに示されています。関連付けは、2 つのクラスを結ぶ線の間に示されています。

このスキーマのフラグメントの継承階層は、次の CIM 2.2 スキーマの図に示されています。参照は Ref タイプとして太字で示され、参照のタイプを限定する各関連付けのサブタイプも示されています。



CIM 対リレーショナルマッピング

CIM は、クラス、継承、ポリモフィズムを備えたオブジェクトモデルです。生成されたリレーショナルスキーマへのマッピングは、こうした特徴を最大限に保持します。リレーショナルマッピングの一部として、次の 2 つの側面があります。

- **論理スキーマ：**論理スキーマは、API と同じように、アプリケーションに対して情報を表示する方法を定義します。その目的は、基になるデータベースに関係なく論理スキーマを同じにして、サポートされているデータベースでアプリケーションソフトウェアを変更しないで実行できるようにすることです。SQL(「シーケル」と発音します）は標準ですが、この目的を十分に達成することはできません。アプリケーションソフトウェアは、使用するデータベースについて詳細に認識する必要があり、この情報は、アプリケーションコードの小さな領域に抽出して分離しておくことができます。
- **物理スキーマ：** 物理スキーマは、データベースで情報を構築する方法を定義します。このスキーマは、SQL と RDBMS の特性によって、データベース固有のものになる傾向があります。このガイドでは、一般的な意味での物理スキーマについてのみ説明します。

データベースのテーブルは、CIM 階層の各クラスを表します。テーブル内の対応するタイプの列は、そのクラスの非継承プロパティを示します。各テーブルには、プライマリーキー id$ があります。このキーはインスタンスを一意に識別する 64 ビットの整数です。CIM クラスのインスタンスは、継承階層のクラスに対応するテーブルの行に示されます。各行には、id$ と同じ値が含まれています。

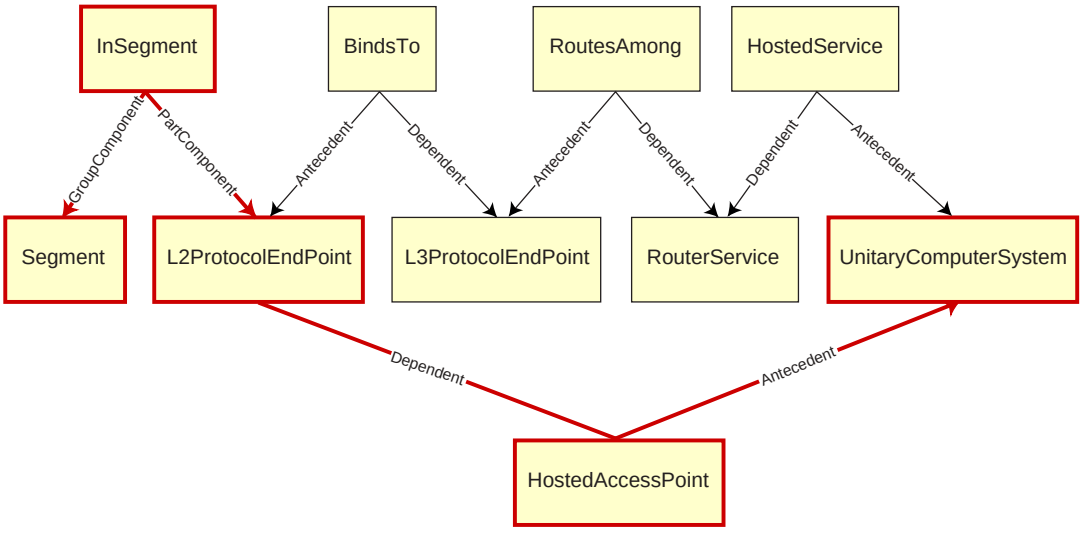
各 CIM クラスは、id$ を使用して継承階層内のテーブルの行を結合し、そのクラスのインスタンスに対して複合プロパティ（継承とローカル）を生成するビューによっても示されます。ビューには、インスタンスの実際の（終端の）クラスのタイプを表す整数タイプの列 class$ も含まれています。

関連付けは、通常のクラスと同じ方法でマッピングされ、参照プロパティは、参照するオブジェクトインスタンスの id$ フィールドがある列で示されます。このため、関連付けの参照フィールドと参照するテーブルの id$ フィールドを結合して、関連付けを確認できます。

次の図は、このマッピングを使用する一般的な照会を示しています。

```
Get Computers for Segment

SELECT CIM.UnitaryComputerSystem.*
FROM    CIM.UnitaryComputerSystem, CIM.Segment, CIM.L2ProtocolEndPoint,
        CIM.HostedAccessPoint, CIM.InSegment
WHERE  CIM.SegmentName = 'xxx'
AND     CIM.InSegment.GroupComponent = CIM.Segment.id$
AND     CIM.InSegment.PartComponent = CIM.L2ProtocolEndPoint.id$
AND     CIM.HostedAccessPoint.Dependent = CIM.L2ProtocolEndPoint.id$
AND     CIM.HostedAccessPoint.Antecedent = CIM.UnitaryComputerSystem.id$
```



この照会は、特定のネットワークセグメントに接続されている全コンピュータを検索します。関連するクラスと関係は、太枠で強調して示されています。

次のトピックでは、両方のスキーマタイプについて説明します。

- 542 ページの「論理スキーマ」
- 544 ページの「物理スキーマ」

論理スキーマ

論理スキーマは、データベースおよびアプリケーションプログラムのユーザが見ることができるデータベーススキーマです。このスキーマは、ストアドプロシージャとビューで構成されています。基になるテーブルは、アプリケーションから見えません。

インベントリコンポーネントは、JDBC を使用して RDBMS に SQL 文を発行し、RDBMS データタイプと Java* データタイプを変換します。JDBC にストアドプロシージャとビューを使用すると、基になるデータベーステクノロジから、また物理スキーマの変更からアプリケーションコードを隔離する一定の抽出を実行できます。

論理スキーマのエレメントの詳細については次の節で説明します。

- 543 ページの「スキーマエレメントの命名」
- 543 ページの「ユーザと役割」
- 544 ページの「データタイプ」
- 544 ページの「ビュー」

スキーマエレメントの命名

データベーススキーマでは CIM 名を変更しないで使用することをお勧めします。命名規則には次のような相違点があるため、問題が発生する場合があります。

- CIM と SQL の名前では、大文字と小文字が区別されません。
- すべてのデータベースには、それぞれ異なる予約語があります。この予約語は、スキーマエレメント名として使用する場合、引用符 (″ ″) で囲む必要があります。ただし、Oracle* では、引用符で囲むと大文字と小文字が区別されます。
- CIM クラスでは、SQL の予約語を名前として使用しないようにします。
- CIM 名の長さには制限はなく、通常は長い名前が付けられています。Sybase では 128 文字まで使用できますが、Oracle では 30 文字に制限されています。

これらの問題は、スキーマの生成中に、CIM 名の大文字小文字を維持する、30 文字より長い名前を短縮する、および予約語を結合した名前を引用符で囲むことで回避できます。

28 文字より長い名前は、28 文字以下のルート名に短縮されて 2 文字のプレフィックスを付けることができるため、SQL スキーマエレメントでそのルート名を使用できます。短縮アルゴリズムによって、名前は記憶しやすく認識可能で、その範囲内で固有の名前になるように短縮されます。短縮された名前には、他の名前との競合を避けるためにサフィックスとして # 文字が付けられます (CIM では # は無効な文字であることに注意してください)。同じ範囲内の複数の名前が同じ形に短縮された場合、他の名前と区別するために 1 桁追加されます。たとえば、AttributeCachingForRegularFilesMin は、AttCacForRegularFilesMin# に短縮されます。

このような短縮された名前はすべて、プログラムが本来の CIM 名を検索して短縮名を取得し、SQL で使用できるように、短縮名テーブルに書き込まれます。

ビューは、アプリケーションコードと照会によって最もよく操作されるスキーマエレメントです。ビューが表す CIM クラスと同じ名前を使用します。たとえば、CIM.UnitaryComputerSystem クラスは、CIM.UnitaryComputerSystem という名前のビューで表されます。

必要に応じて、クラス名とプロパティ名を結合して $ 文字で区切り、インデックスと補助テーブルを作成します。通常、これらの名前は短縮されます。たとえば、NetworkAdapter$NetworkAddresses は、NetAdapter$NetAddresses# に短縮されます。これは、ZENworks 6.5 Server Management スキーマユーザに悪影響を及ぼすことはありません。

ユーザと役割

SQL では、スキーマと同じ名前のユーザがスキーマの所有者です。たとえば、CIM、ManageWise®、ZENworks® などです。

また、データベース管理者特権と全スキーマオブジェクトへのアクセス権を持つ MW_DBA ユーザがいます。MW_Reader の役割には全スキーマオブジェクトへの読み込み専用アクセス権があり、MW_Updater の役割には全スキーマオブジェクトへの読み込みと書き込み、および実行のアクセス権があります。

アプリケーションプログラムは、要件に応じて、Sybase データベースには MW_Reader または MW_Updater のいずれかとして、Oracle データベースには MWO_Reader または MWO_Updater のいずれかとして、MS SQL Server データベースには MWM_Reader または MWM_Updater のいずれかとしてアクセスする必要があります。

データタイプ

CIM データタイプは、データベースが備えている最適なデータタイプにマッピングされます。通常、Java アプリケーションは、JDBC を使用してデータにアクセスするため、タイプを必要としません。

Java は本来符号なしのタイプをサポートしていないため、符号なしのタイプを表す次のサイズのクラスまたは整数タイプを使用する必要があります。また、データベースの読み書き中に問題が発生しないようにします。たとえば、データベースの符号なしフィールドに負の数を読み書きすると、エラーが発生することがあります。

CIM および Java の文字列は Unicode* であるため、データベースは UTF8 文字セットを使用して作成します。国際化対応によって問題が発生することはありませんが、照会における大文字と小文字の区別によって問題が発生することがあります。

すべてのデータベースでは、データベース内に保存されている文字列データの大文字と小文字が保持されますが、照会中は大文字と小文字が区別されるデータまたは区別されないデータのいずれかとしてデータにアクセスします。ZENworks 6.5 Server Management では、照会されるデータは照会前にデータベースから取得され、大文字と小文字は自動的に区別されるため、Inventory Query コンポーネントは影響を受けません。

CIM では、最大文字列サイズで、または最大文字列サイズなしで文字列を指定できます。多くの文字列には指定サイズはありません。つまり、文字列の長さは無制限です。効率性の観点から、この長さが無制限の文字列は、最大サイズが 254 文字の変数文字列にマッピングされます。最大サイズの CIM 文字列は、同じサイズの変数データベース文字列にマッピングされます。データベース内では、Unicode 文字の保存には複数バイトが必要なため、サイズは文字ではなくバイトで表します。

ビュー

CIM クラスは、そのクラスのローカルプロパティと継承した非配列プロパティをすべて含むビューによって、データベースに示されます。ビューには CIM クラスと同じ名前が付けられます。

ビューは SELECT 文を使用して照会でき、UPDATE 文を使用して更新できます。ビューには INSERT 文および DELETE 文を使用できないため、コンストラクタプロシージャとデストラクタプロシージャを使用します。

物理スキーマ

- テーブル定義 't$*xxx*' インデックス定義 'i$*xxx*'
- トリガ定義 'x$*xxx*'、'n$*xxx*'、および'u$*xxx*'
- シーケンス定義 (Oracle) 's$*xxx*'
- ストアドプロシージャと関数

論理スキーマは、物理スキーマの上に配置し、ユーザやアプリケーションが物理スキーマを認識する必要がないようにします。

ZENworks 6.5 Server Management のインベントリデータベーススキーマ

次の節では、データベーススキーマクラスおよび ZENworks 6.5 Server Management で使用するための CIM スキーマの拡張と関連付けについて説明します。これらの拡張では、そのスキーマ名として ZENworks または ManageWise を使用します。ZENworks.*classname* は ZENworks スキーマの拡張クラスを示し、ManageWise.*classname* は ManageWise スキーマの拡張クラスを示します。

次の節は、ZENworks 6.5 Server Management データベーススキーマの理解に役立ちます。

- 545 ページの「ZENworks 6.5 Server Management での CIM スキーマ実装のケーススタディ」
- 548 ページの「スキーマ図の凡例」
- 549 ページの「ZENworks 6.5 Server Management の CIM と拡張スキーマのスキーマ図」
- 556 ページの「ソフトウェアインベントリのスキーマ」
- 561 ページの「インベントリデータベースの照会例」

ZENworks 6.5 Server Management での CIM スキーマ実装のケーススタディ

次の構成は、特定の割り込み番号を持つ 2 つのパラレルポートを備えたインベントリ対象サーバを示しています。

次のスキーマ図で、CIM.UnitaryComputerSystem は管理対象のインベントリシステムを表します。

この図では、クラス CIM.PointingDevice は、CIM.UnitaryComputerSystem を参照する SystemDevice.GroupComponent と CIM.PointingDevice を参照する SystemDevice.PartComponent の関連付け CIM.SystemDevice によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、コンピュータシステムには複数のポインティングデバイスを接続できます。

クラス CIM.IRQ は、関連付け CIM.AllocatedResource によって CIM.PointingDevice に関連付けられています。Dependent は CIM.PointingDevice を参照し、Antecedent は CIM.IRQ を参照します。

クラス ZENworks.ZENKeyboard は、CIM.UnitaryComputerSystem を参照する SystemDevice.GroupComponent と ZENworks.ZENKeyboard を参照する SystemDevice.PartComponent の関連付け CIM.SystemDevice によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対 1 です。つまり、コンピュータシステムにはキーボードを 1 台だけ接続できます。

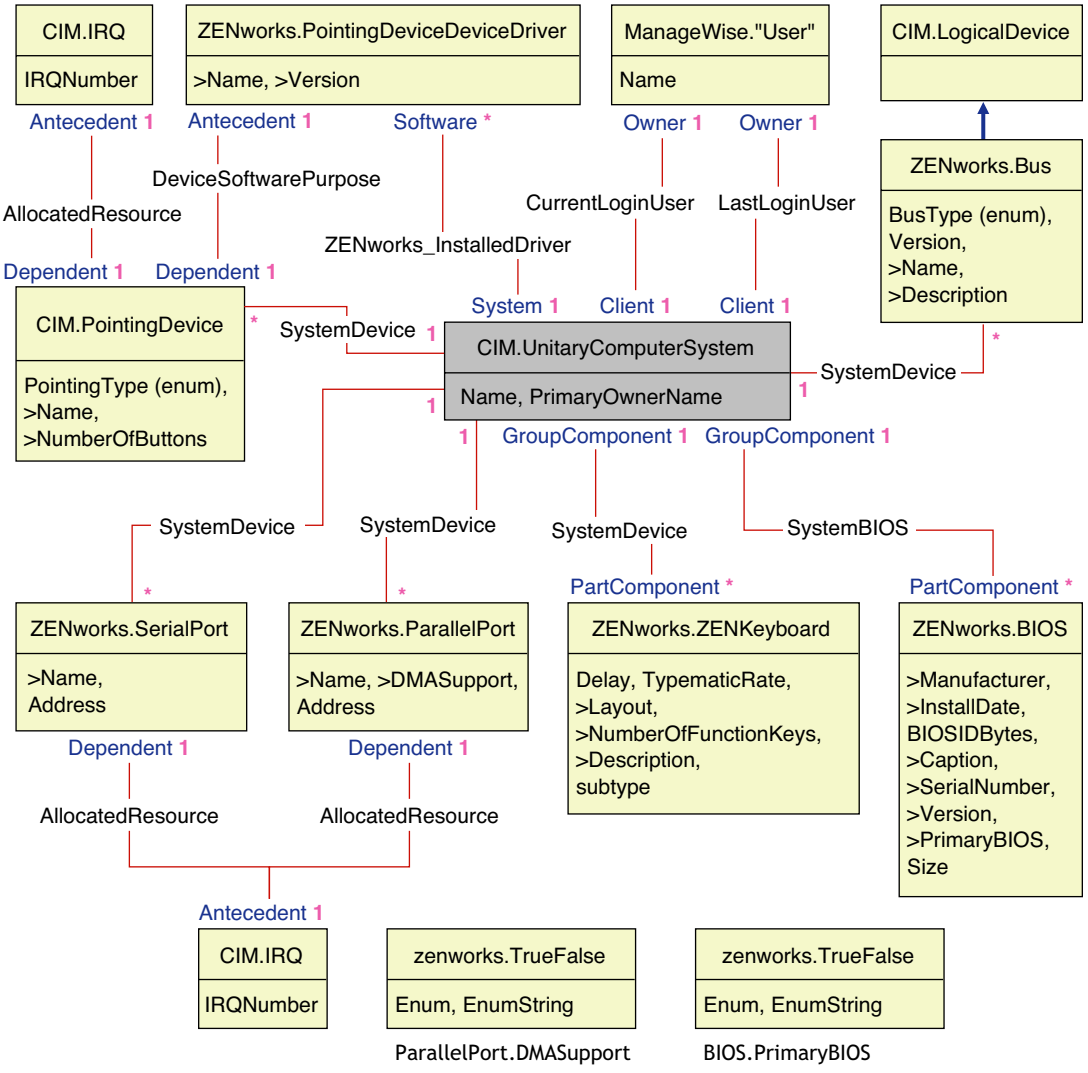
クラス ZENworks.BIOS は、CIM.UnitaryComputerSystem を参照する SystemDevice.GroupComponent と ZENworks.BIOS を参照する SystemBIOS.PartComponent の関連付け CIM.SystemBIOS によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対 1 です。つまり、コンピュータシステムは BIOS を 1 つだけ持つことができます。

クラス CIM.ZENworks.ParallelPort は、CIM.UnitaryComputerSystem を参照する SystemDevice.GroupComponent と CIM.ZENworks.ParallelPort を参照する SystemDevice.PartComponent の関連付け CIM.SystemDevice によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、コンピュータシステムは複数のパラレルポートを持つことができます。

クラス ZENworks.BUS は、CIM.UnitaryComputerSystem を参照する SystemDevice.GroupComponent と ZENworks.BUS を参照する SystemDevice.PartComponent の関連付け CIM.SystemDevice によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、コンピュータシステムはバスを複数持つことができます。

クラス ManageWise.User は、CurrentLoginUser と LastLoginUser によって CIM.UnitaryComputerSystem に関連付けられています。CurrentLoginUser では、User の特定のインスタンスは、インベントリ対象サーバに現在ログインしているユーザを表します。LastLoginUser では、User の特定のインスタンスは、インベントリ対象サーバに最後にログインしたユーザを表します。

クラス CIM.IRQ は、関連付け CIM.AllocatedResource によって CIM.ParallelPort に関連付けられています。Dependent は CIM.ParallelPort を参照し、Antecedent は CIM.IRQ を参照します。



スキーマ図は次の内容を示しています。

- コンピュータシステムが管理するすべてのコンポーネントは、UnitaryComputerSystem クラスからの関連付けとして示されています。2 つのクラス間の参照のタイプ (1..n, 1..1) が示されています。
- スキーマ名がない関連付けは、CIM スキーマと仮定されています。

  CIM.SystemDevice の関連付けのインスタンスを 3 つ使用する CIM.UnitaryComputerSystem の 1 つのインスタンスには、ZENworks.ParallelPort のインスタンスが 3 つ関連付けられています。CIM.SystemDevice.GroupComponent は UnitaryComputerSystem を参照し、CIM.SystemDevice.PartComponent は ParallelPort を参照します。

  これは、1 対 n オブジェクト参照関係と呼ばれ、図では「1..*」として示されています。同様に、ParallelPort のすべてのインスタンスには、ポートの irq を指定する CIM.IRQ に対応するインスタンスがあります。これは 1 対 1 の関係で、図では 1..1 として示されています。

その他のクラスもすべて同様の表記に従います。

その他のクラスのスキーマ図については、549 ページの「ZENworks 6.5 Server Management の CIM と拡張スキーマのスキーマ図」を参照してください。

スキーマ図の凡例

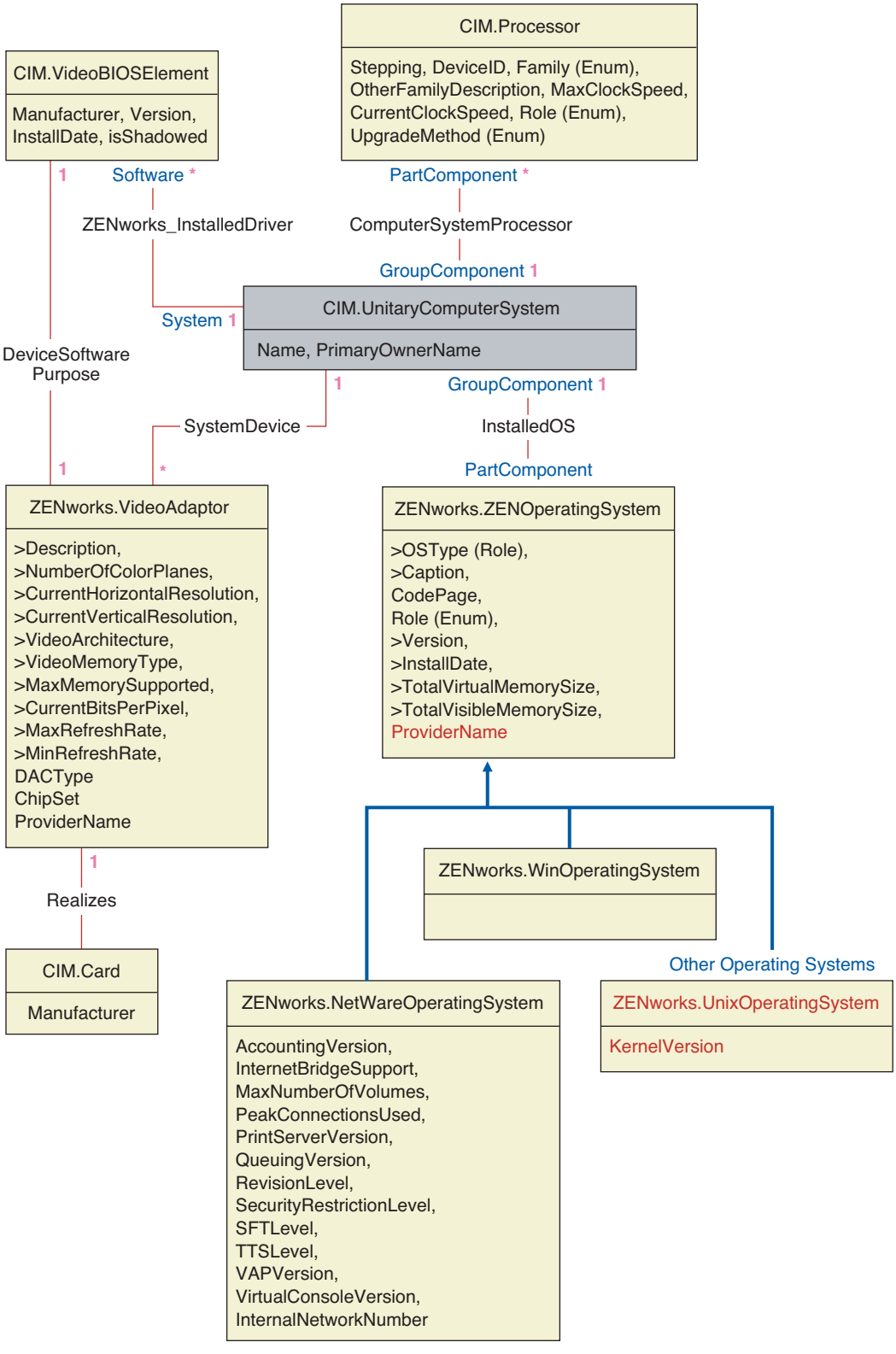
スキーマ図を読むための凡例は次のとおりです。

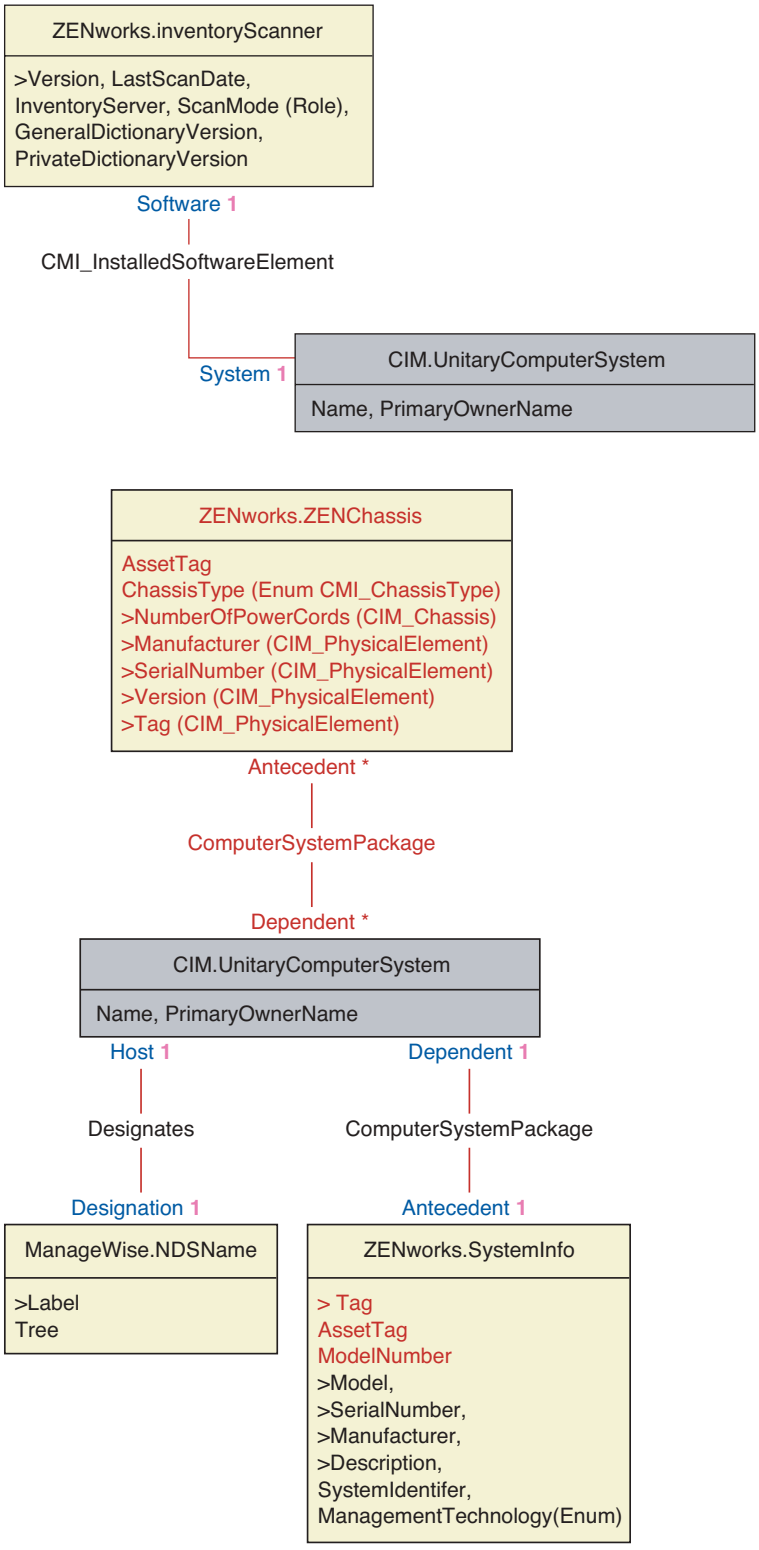
- クラス名は四角で囲まれ、見出しにクラス名、その中に属性名が示されます。
- 赤い線は、関連付けクラスを使用する 2 つのクラスを結合します。
- 青い線は、クラス継承階層を示します。矢印が示すクラスは継承元のクラスです。矢印が始まるクラスは継承クラスです。
- 関連付けクラス名は、2 つのクラスを結合する線内に示されます。
- 関連付けクラスの参照は、関連付けられたクラスの上下どちらかに示されます。

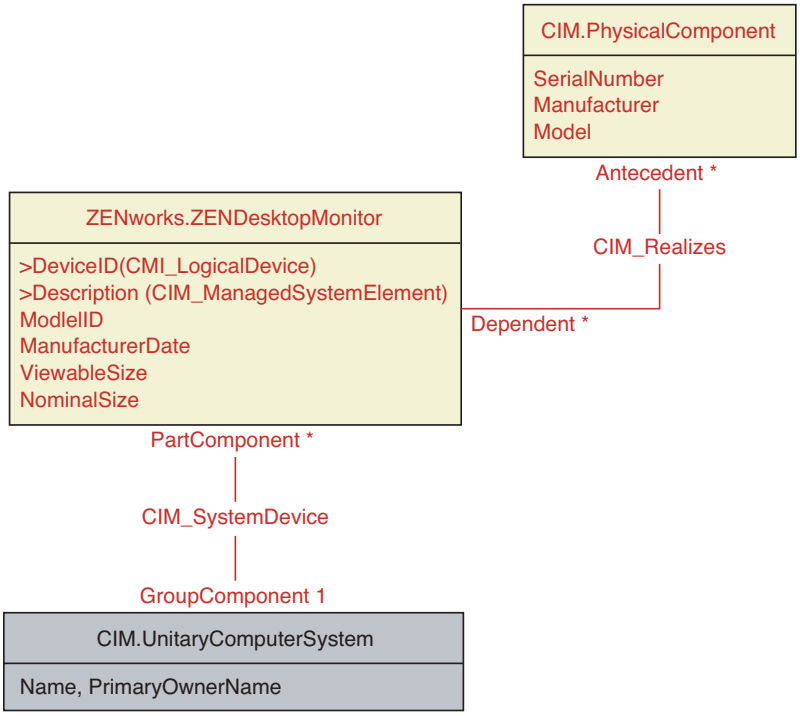
CIM スキーマについての詳細は、DMTF の Web サイト (http://www.dmtf.org) にある CIM 2.2 スキーマの仕様を参照してください。

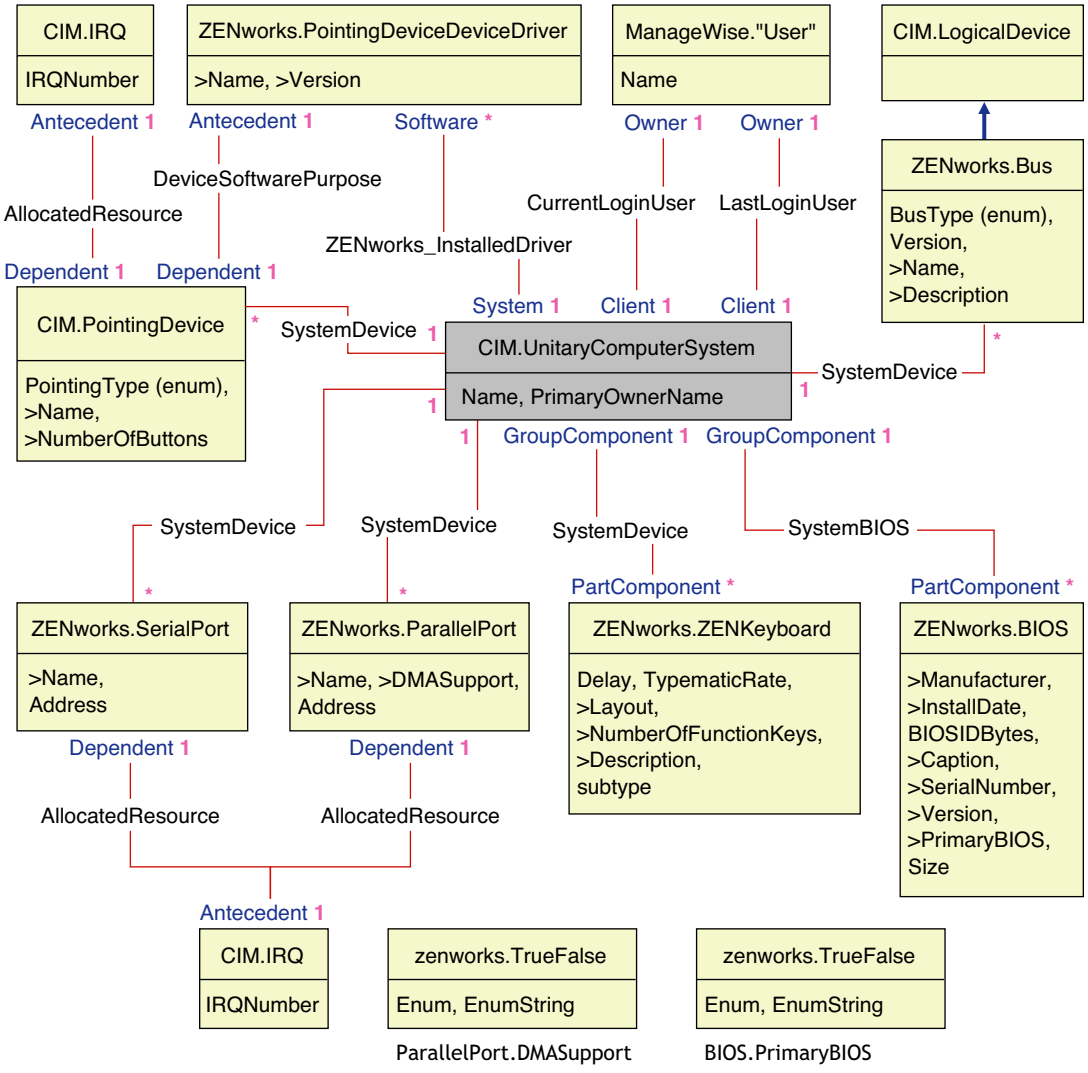
ZENworks 6.5 Server Management の CIM と拡張スキーマのスキーマ図

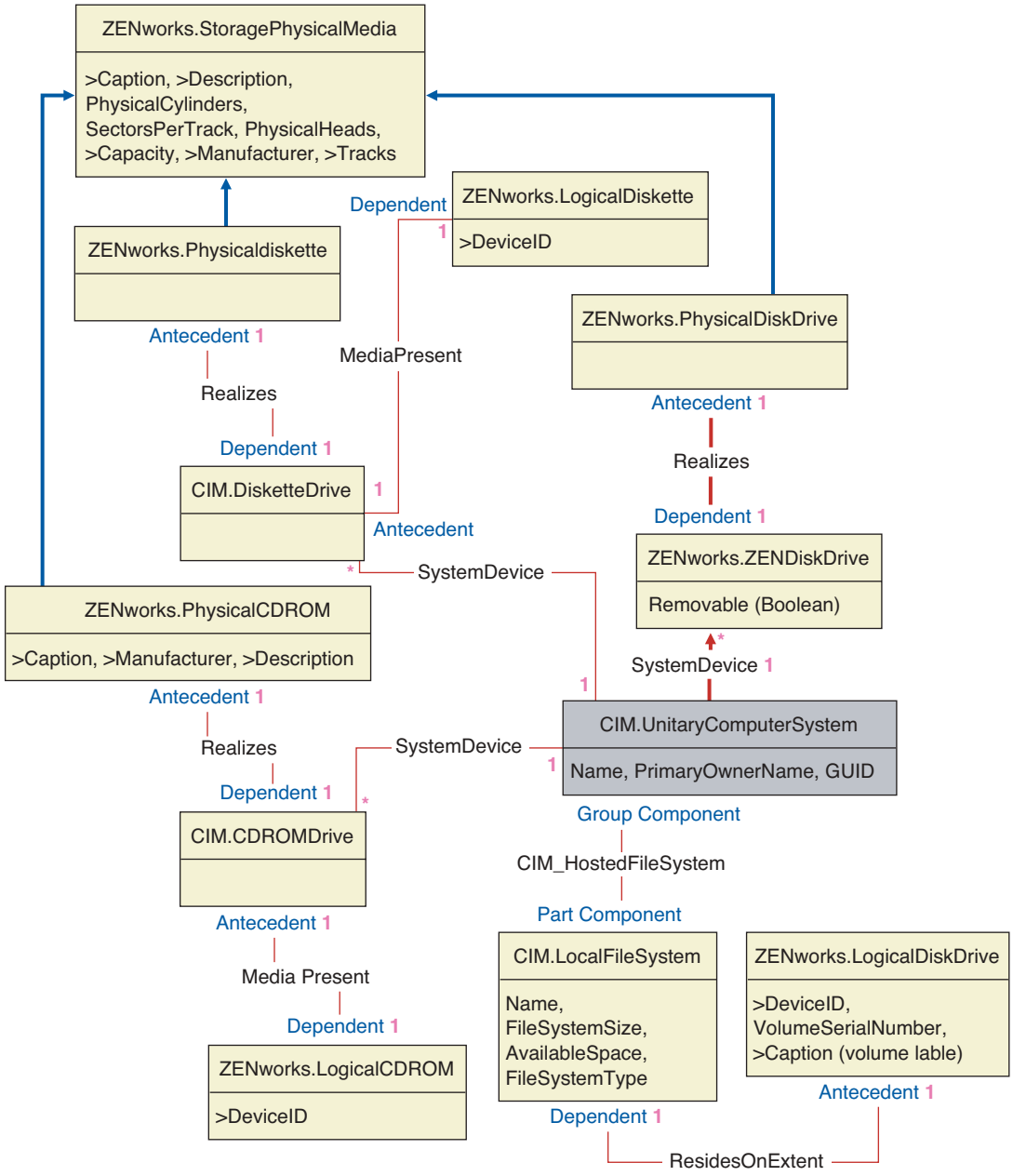
次の CIM と拡張スキーマのスキーマ図は、ZENworks 6.5 Server Management のインベントリデータベースをモデリングしたものです。

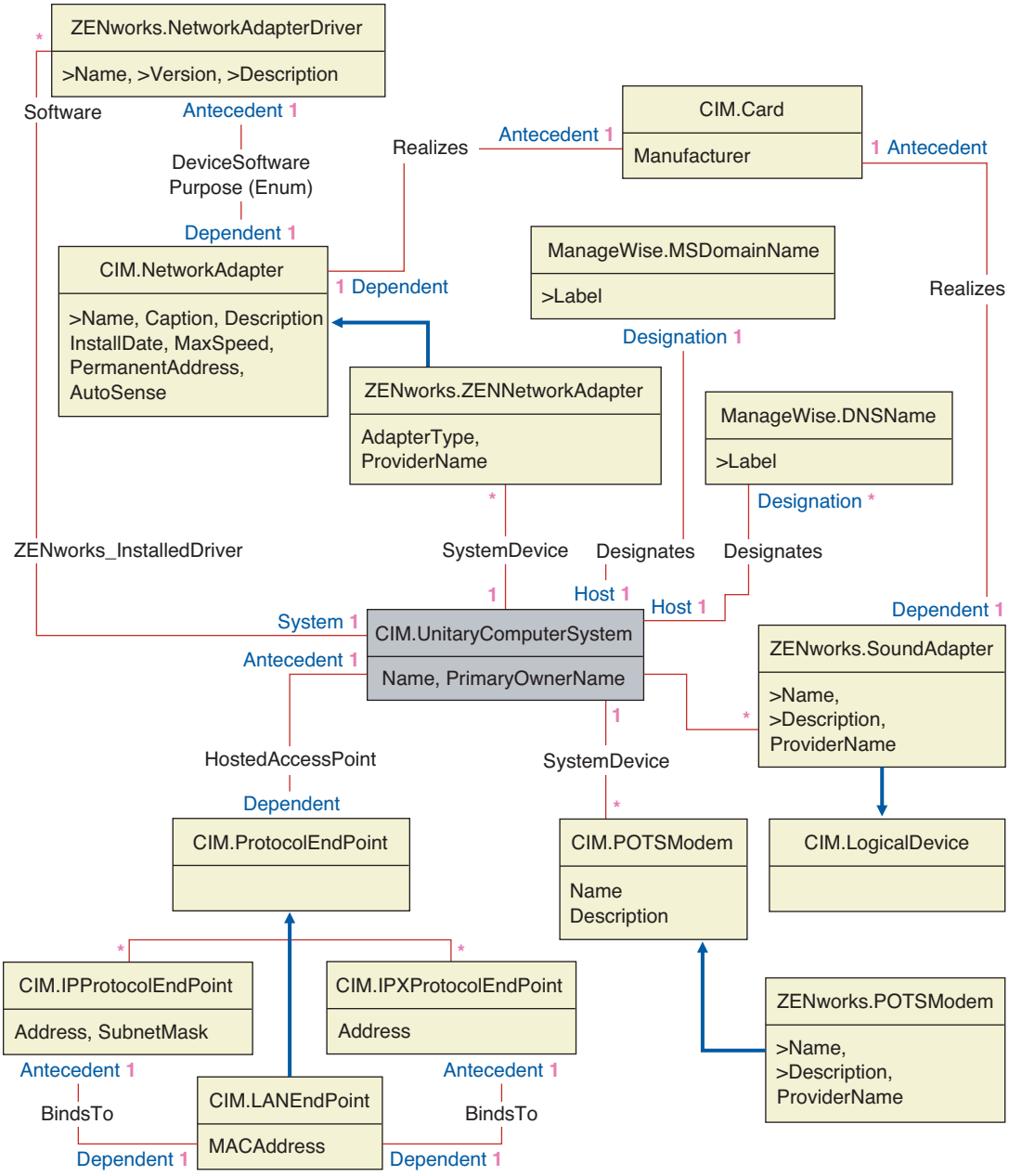


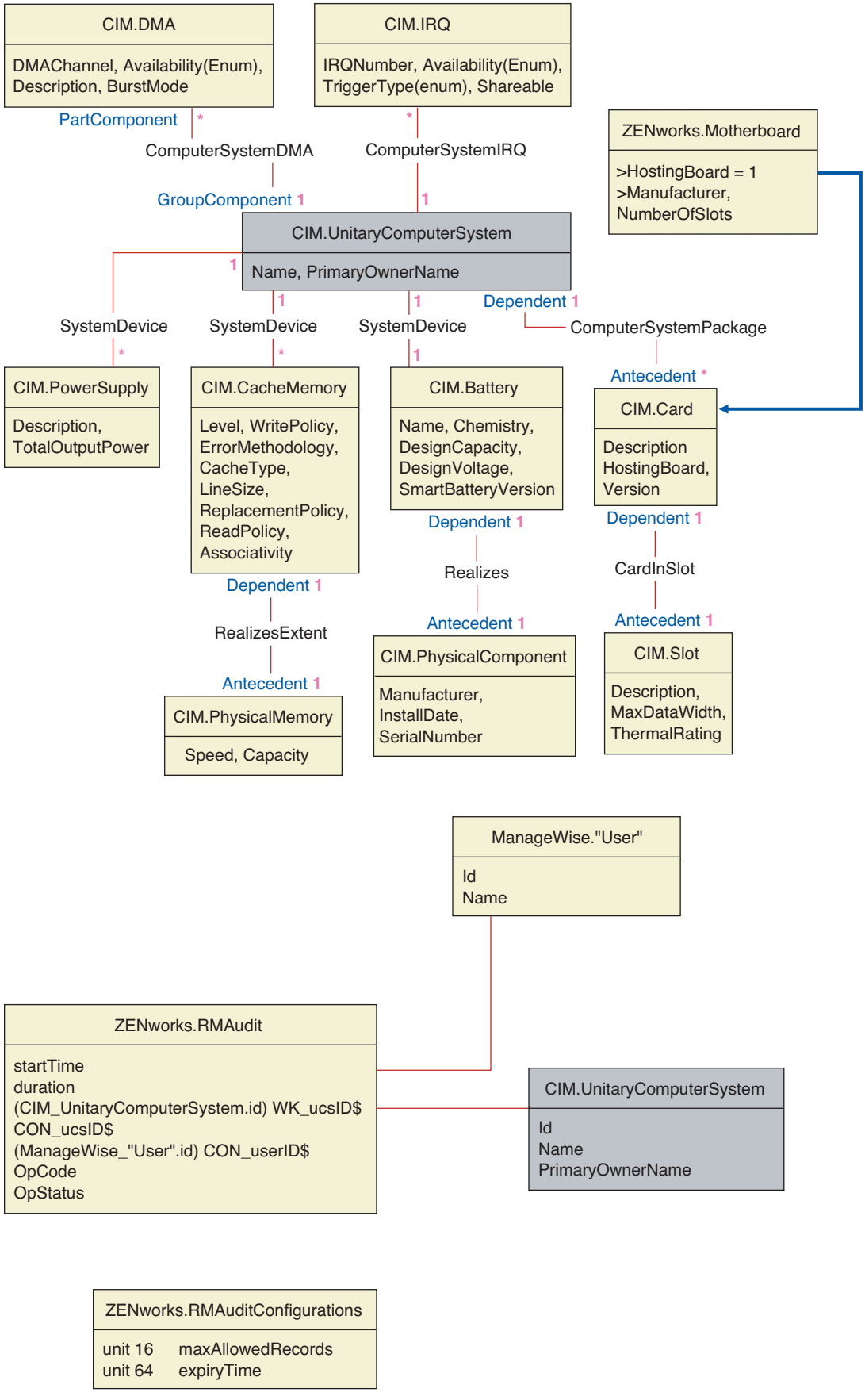

ZENworks.inventoryScanner
>Version, LastScanDate,
InventoryServer, ScanMode (Role),
GeneralDictionaryVersion,
PrivateDictionaryVersion
Software 1
CMI_InstalledSoftwareElement
System 1
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName
ZENworks.ZENChassis
AssetTag
ChassisType (Enum CMI_ChassisType)
>NumberOfPowerCords (CIM_Chassis)
>Manufacturer (CIM_PhysicalElement)
>SerialNumber (CIM_PhysicalElement)
>Version (CIM_PhysicalElement)
>Tag (CIM_PhysicalElement)
Antecedent *
ComputerSystemPackage
Dependent *
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName
Host 1
Dependent 1
Designates
ComputerSystemPackage
Designation 1
Antecedent 1
ManageWise.NDSName
>Label
Tree
ZENworks.SystemInfo
> Tag
AssetTag
ModelNumber
>Model,
>SerialNumber,
>Manufacturer,
>Description,
SystemIdentifer,
ManagementTechnology(Enum)


CIM.PhysicalComponent
SerialNumber
Manufacturer
Model
Antecedent *
CIM_Realizes
Dependent *
ZENworks.ZENDesktopMonitor
>DeviceID(CMI_LogicalDevice)
>Description (CIM_ManagedSystemElement)
ModleIID
ManufacturerDate
ViewableSize
NominalSize
PartComponent *
CIM_SystemDevice
GroupComponent 1
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName


CIM.IRQ
IRQNumber
ZENworks.PointingDeviceDeviceDriver
>Name, >Version
ManageWise."User"
Name
CIM.LogicalDevice
Antecedent 1
Antecedent 1
Software *
Owner 1
Owner 1
ZENworks.Bus
BusType (enum),
Version,
>Name,
>Description
DeviceSoftwarePurpose
AllocatedResource
CurrentLoginUser
LastLoginUser
ZENworks_InstalledDriver
Dependent 1
Dependent 1
System 1
Client 1
Client 1
CIM.PointingDevice
PointingType (enum),
>Name,
>NumberOfButtons
SystemDevice
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName
SystemDevice
GroupComponent 1
GroupComponent 1
SystemDevice
SystemDevice
SystemDevice
SystemBIOS
PartComponent *
PartComponent *
ZENworks.SerialPort
>Name,
Address
ZENworks.ParallelPort
>Name, >DMASupport,
Address
ZENworks.ZENKeyboard
Delay, TypematicRate,
>Layout,
>NumberOfFunctionKeys,
>Description,
subtype
ZENworks.BIOS
>Manufacturer,
>InstallDate,
BIOSIDBytes,
>Caption,
>SerialNumber,
>Version,
>PrimaryBIOS,
Size
Dependent 1
Dependent 1
AllocatedResource
AllocatedResource
Antecedent 1
CIM.IRQ
IRQNumber
zenworks.TrueFalse
Enum, EnumString
ParallelPort.DMASupport
zenworks.TrueFalse
Enum, EnumString
BIOS.PrimaryBIOS


ZENworks.StoragePhysicalMedia
>Caption, >Description, PhysicalCylinders, SectorsPerTrack, PhysicalHeads, >Capacity, >Manufacturer, >Tracks
Dependent
1
ZENworks.LogicalDiskette
>DeviceID
ZENworks.Physicaldiskette
Antecedent 1
Realizes
Dependent 1
MediaPresent
ZENworks.PhysicalDiskDrive
Antecedent 1
Realizes
Dependent 1
CIM.DisketteDrive
1
Antecedent
*
SystemDevice
ZENworks.ZENDiskDrive
Removable (Boolean)
*
SystemDevice 1
1
ZENworks.PhysicalCDROM
>Caption, >Manufacturer, >Description
Antecedent 1
Realizes
Dependent 1
SystemDevice
1
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName, GUID
*
Group Component
CIM_HostedFileSystem
Part Component
CIM.CDROMDrive
Antecedent 1
Media Present
Dependent 1
CIM.LocalFileSystem
Name, FileSystemSize, AvailableSpace, FileSystemType
ZENworks.LogicalDiskDrive
>DeviceID, VolumeSerialNumber, >Caption (volume lable)
Antecedent 1
Dependent 1
ZENworks.LogicalCDROM
>DeviceID
ResidesOnExtent

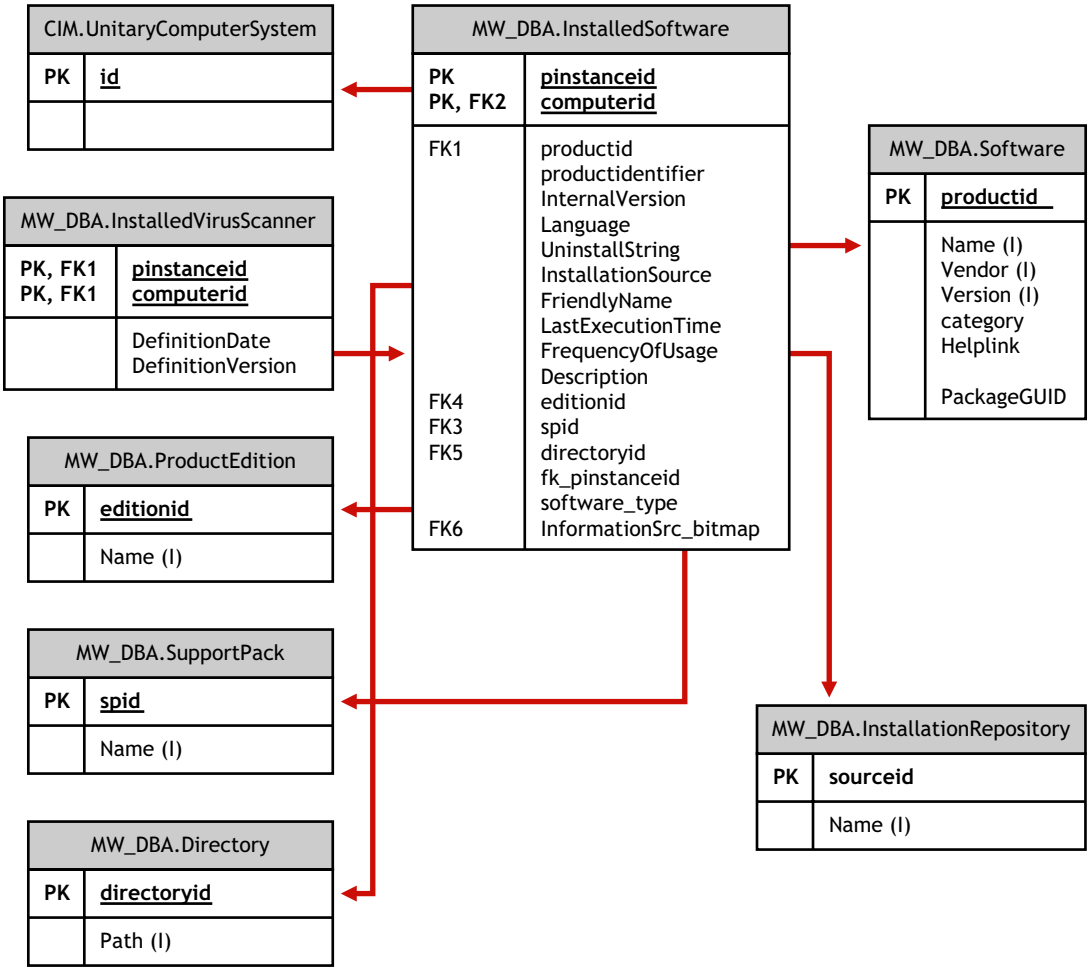

ZENworks.NetworkAdapterDriver
>Name, >Version, >Description
Software
Antecedent 1
DeviceSoftware
Purpose (Enum)
Dependent 1
CIM.NetworkAdapter
>Name, Caption, Description
InstallDate, MaxSpeed,
PermanentAddress,
AutoSense
Realizes
Antecedent 1
CIM.Card
Manufacturer
1 Antecedent
Realizes
1 Dependent
ManageWise.MSDomainName
>Label
Designation 1
ZENworks.ZENNetworkAdapter
AdapterType,
ProviderName
ManageWise.DNSName
>Label
Designation *
ZENworks_InstalledDriver
SystemDevice
Designates
Designates
1
Host 1
Host 1
System 1
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName
Antecedent 1
Dependent 1
ZENworks.SoundAdapter
>Name,
>Description,
ProviderName
HostedAccessPoint
Dependent
SystemDevice
CIM.ProtocolEndPoint
CIM.POTSModem
Name
Description
CIM.LogicalDevice
CIM.IPProtocolEndPoint
Address, SubnetMask
CIM.IPXProtocolEndPoint
Address
ZENworks.POTSModem
>Name,
>Description,
ProviderName
Antecedent 1
Antecedent 1
BindsTo
BindsTo
CIM.LANEndPoint
MACAddress
Dependent 1
Dependent 1


CIM.DMA
DMAChannel, Availability(Enum), Description, BurstMode
CIM.IRQ
IRQNumber, Availability(Enum), TriggerType(enum), Shareable
PartComponent
*
*
ComputerSystemDMA
ComputerSystemIRQ
GroupComponent 1
1
ZENworks.Motherboard
>HostingBoard = 1
>Manufacturer, NumberOfSlots
CIM.UnitaryComputerSystem
Name, PrimaryOwnerName
1
1
1
Dependent 1
SystemDevice
SystemDevice
SystemDevice
ComputerSystemPackage
*
*
1
Antecedent *
CIM.PowerSupply
Description, TotalOutputPower
CIM.CacheMemory
Level, WritePolicy, ErrorMethodology, CacheType, LineSize, ReplacementPolicy, ReadPolicy, Associativity
CIM.Battery
Name, Chemistry, DesignCapacity, DesignVoltage, SmartBatteryVersion
CIM.Card
Description HostingBoard, Version
Dependent 1
Dependent 1
Dependent 1
Realizes
CardInSlot
RealizesExtent
Antecedent 1
Antecedent 1
Antecedent 1
CIM.PhysicalComponent
Manufacturer, InstallDate, SerialNumber
CIM.Slot
Description, MaxDataWidth, ThermalRating
CIM.PhysicalMemory
Speed, Capacity
ManageWise."User"
Id
Name
ZENworks.RMAudit
startTime
duration
(CIM_UnitaryComputerSystem.id) WK_ucsID$
CON_ucsID$
(ManageWise_"User".id) CON_userID$
OpCode
OpStatus
CIM.UnitaryComputerSystem
Id
Name
PrimaryOwnerName
ZENworks.RMAuditConfigurations
unit 16 maxAllowedRecords
unit 64 expiryTime

ソフトウェアインベントリのスキーマ

次のソフトウェアスキーマ図は、ZENworks 6.5 Server Management のインベントリデータベースをモデリングしたものです。次のスキーマ図で、CIM.UnitaryComputerSystem は管理対象のインベントリシステムを表します。

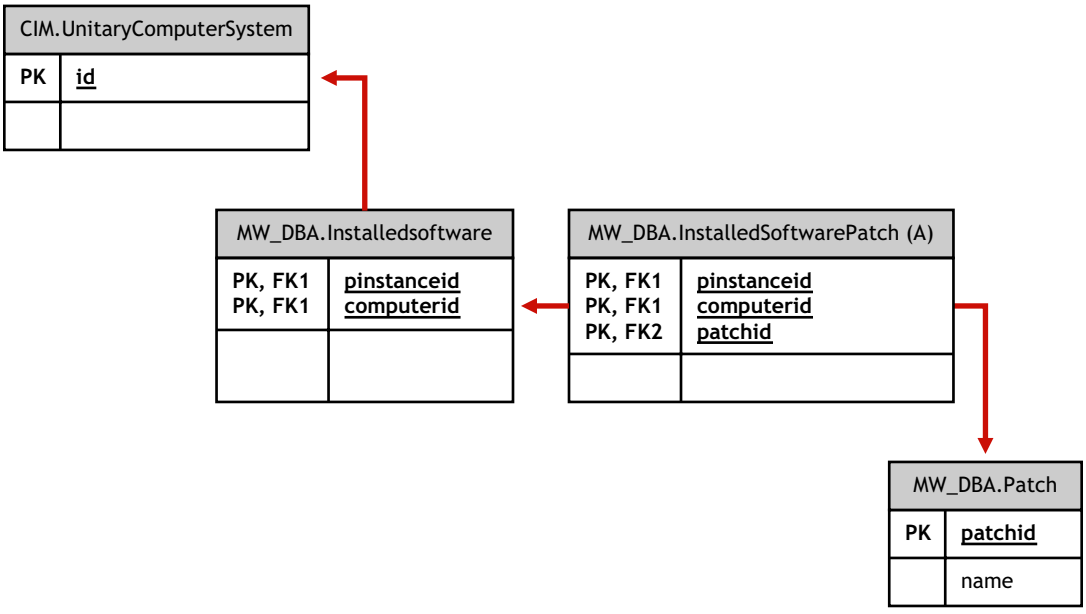
テーブルに関する詳細については、715 ページの付録 J、「ZENworks 6.5 Server Management の Inventory 属性」を参照してください。



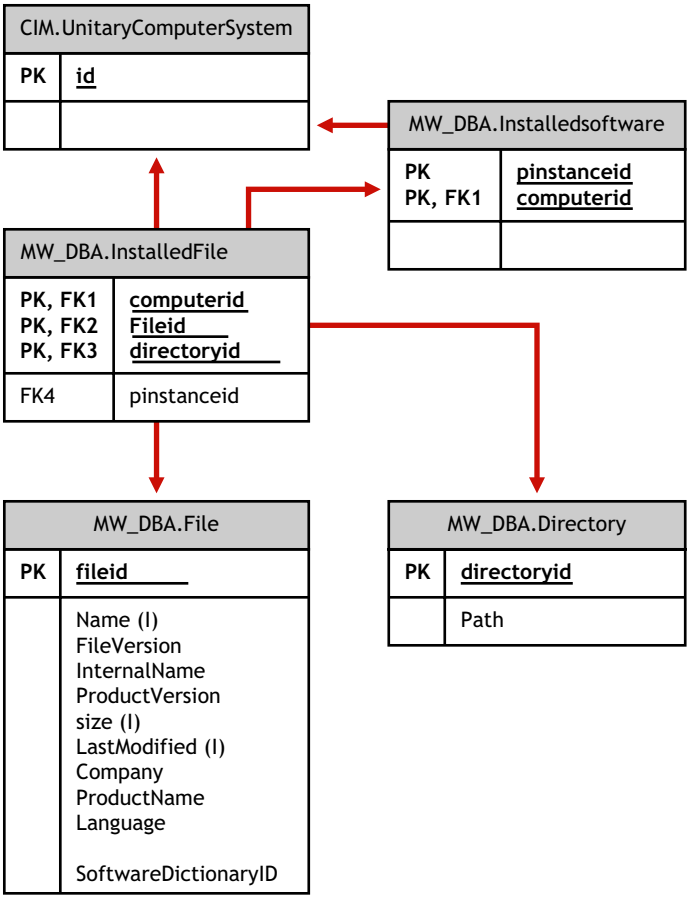
この図では、クラス MW_DBA.Software は、CIM.UnitaryComputerSystem を参照する MW_DBA.InstalledSoftware.ComputerSystem と MW_DBA.Software を参照する MW_DBA.InstalledSoftware.ProductID の関連付け MW_DBA.InstalledSoftware によって、CIM.UnitaryComputerSystem に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、コンピュータシステムは複数のソフトウェア情報を持つことができます。

関連付け MW_DBA.InstalledSoftware には、テーブル ProductEdition、SupportPack、Directory、および Installation Repository に対する外部キーリファレンスがあります。

MW_DBA.InstalledVirusScanner は、ウィルス定義の日付やバージョンなどのウィルス固有の情報と共にソフトウェア情報を MW_DBA.InstalledSoftware から継承します。

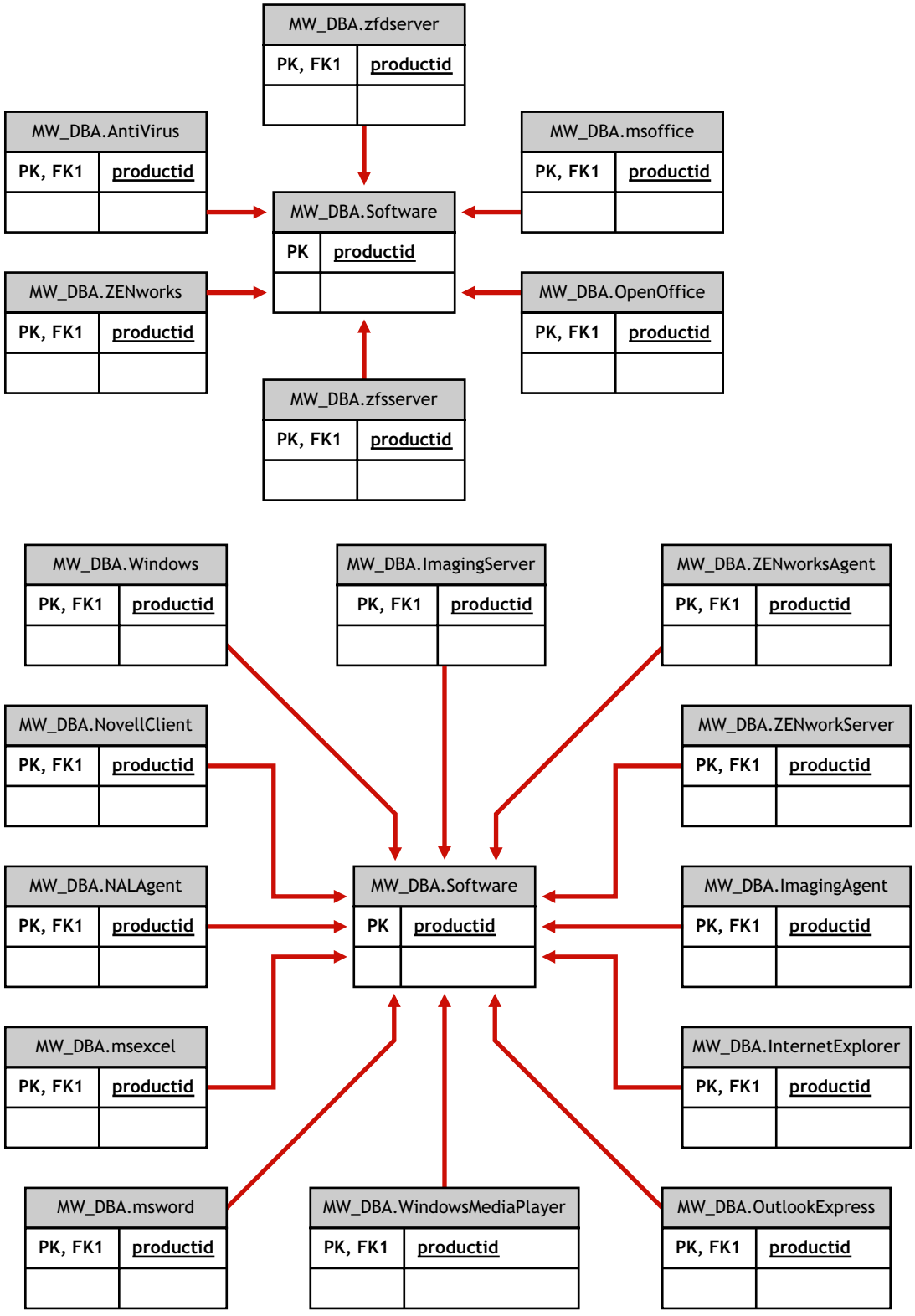


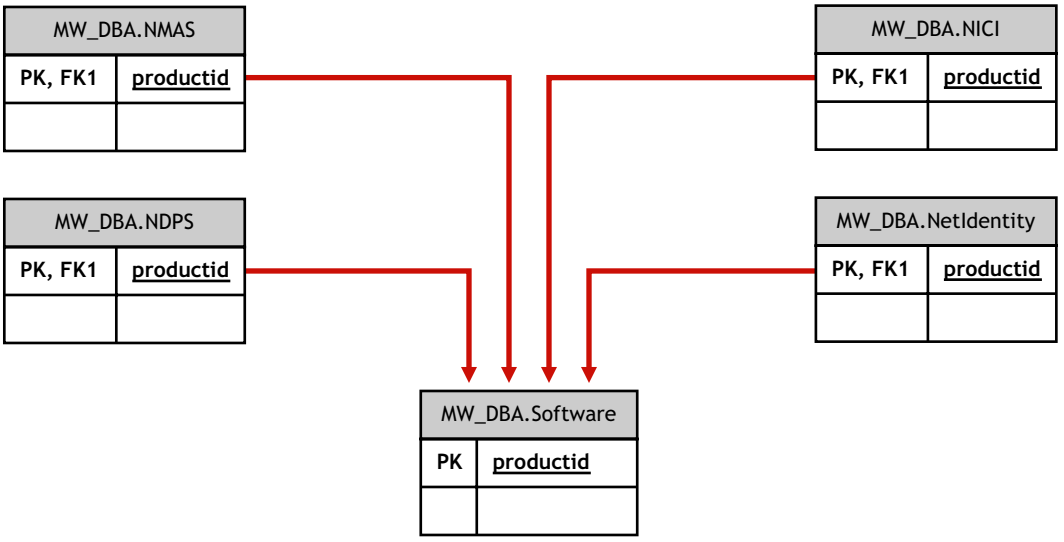
この図では、クラス MW_DBA.Patch は、MW_DBA.InstalledSoftware を参照する MW_DBA.InstalledSoftwarePatch.pinstanceID と MW_DBA.Patch を参照する MW_DBA.InstalledSoftwarePatch.PatchID の関連付け MW_DBA.InstalledSoftwarePatch によって、MW_DBA.InstalledSoftware に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、ソフトウェアはパッチ情報を持たないか、1 つ以上のパッチ情報を持つことができます。



この図では、クラス MW_DBA.File は、MW_DBA.InstalledSoftware を参照する MW_DBA.InstalledFile.pinstanceID と MW_DBA.File を参照する MW_DBA.InstalledFile.fileID の関連付け MW_DBA.InstalledFile によって、MW_DBA.InstalledSoftware に関連付けられています。この 2 つのクラスの関係は 1 対多です。つまり、ソフトウェアはパッチ情報を持たないか、1 つ以上のパッチ情報を持つことができます。

この図では、クラス MW_DBA.Directory は、MW_DBA.InstalledSoftware を参照する MW_DBA.InstalledFile.pinstanceID と MW_DBA.Directory を参照する MW_DBA.InstalledFile.DirectoryID の関連付け MW_DBA.InstalledFile によって、MW_DBA.InstalledSoftware に関連付けられています。

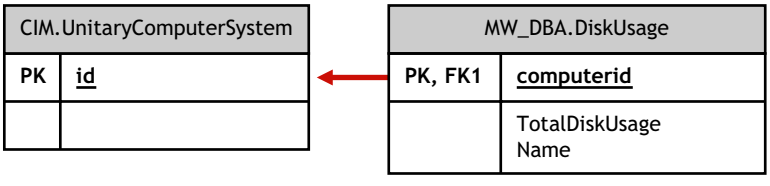




この図では、MW_DBA.MSoffice は MW_DBA.SOftware からソフトウェア情報を継承します。このサブクラスは、MS office 情報を直接取得します。

これは次の各クラスにも当てはまります。

mw_dba.zfdserver
mw_dba.zfsserver
mw_dba.zfsinventoryserver
mw_dba.zfsinventoryagent
mw_dba.zfsrmserver
mw_dba.zfsrmagent
mw_dba.zfdrmserver
mw_dba.zfdrmagent
mw_dba.zfsinvxmlproxyserver
mw_dba.zfdnalagent
mw_dba.middletier
mw_dba.zfspxeserver
mw_dba.zfsmmsadctrendingagent
mw_dba.zfhaccesspoin
mw_dba.zfdinventoryserver
mw_dba.zfdinventoryagent
mw_dba.mspowerpoint
mw_dba.msoutlook
mw_dba.msaccess
mw_dba.mspublisher
mw_dba.msfrontpage
mw_dba.msinfopath
mw_dba.zfdimagingagent
mw_dba.zfdnalserver
mw_dba.zfsmmsserver
mw_dba.zfsmmssrvmgmtagent
mw_dba.zfspdsdb
mw_dba.zfhdesktopsync
mw_dba.zfdagent
mw_dba.zfsagent
mw_dba.msphotodraw
mw_dba.zfdwsmanager
mw_dba.zfdwsimportserver
mw_dba.zfdinvdbserver
mw_dba.zfsinvdbserver
mw_dba.zfdinvxmlproxyserver
mw_dba.zfdimagingserver
mw_dba.zfdnaldb
mw_dba.zfspds
mw_dba.zfsmmstrafficanalysisagent
mw_dba.zfhserver



この図では、MW_DBA.DiskUsage には CIM.UnitaryComputerSystem.ID に対する computerID 列外部キー参照が含まれます。MW_DBA.DiskUsage テーブルには、ディスク使用の合計とファイル拡張子名が含まれます。

インベントリデータベースの照会例

次の照会例は、ZENworks 6.5 Server Management インベントリデータベースからインベントリ情報を取得するためのものです。

関連付けられているスキーマクラスと属性の詳細については、549 ページの「ZENworks 6.5 Server Management の CIM と拡張スキーマのスキーマ図」のスキーマ図を参照してください。

1. データベースからすべてのインベントリ対象サーバの名前と ID を取得し、これらのサーバが登録されている eDirectory ツリーも取得します。次に、この照会を示します。

```
SELECT
  u.id$, u.name, m.tree
FROM
  ManageWise.NDSName m,
  CIM.UnitaryComputerSystem u,
  ManageWise.Designates s
WHERE
  s.Designation=m.id$ AND s.Host=u.id$;
```

   この照会では、ツリー名はコンピュータシステム名の一部です。

2. データベース内のすべてのインベントリ対象サーバの備品タグ、メーカー、およびモデル番号を取得します。次に、この照会を示します。

```
SELECT
  m.AssetTag,
  m.Manufacturer,
  m.ModelNumber,
  m.SerialNumber
FROM
  CIM.UnitaryComputerSystem u,
  CIM.ComputerSystemPackage s,
  ZENworks.SystemInfo m
WHERE
  s.Antecedent=m.id$ AND s.Dependent=u.id$;
```

3. 'NOVELL_AUS' eDirectory ツリーに登録されているインベントリ対象サーバ 'SJOHN164_99_139_79' にインストールされているすべての Microsoft アプリケーションおよびそのバージョンと ID を取得します。次に、この照会を示します。

```
SELECT

  m.Name,

  m.Version,

  im.ProductIdentifier

FROM

  CIM.UnitaryComputerSystem u,

  MW_DBA.InstalledSoftware im,

  MW_DBA.Software m

WHERE

  u.Name='SJOHN164_99_139_79.Novell_AUS' AND

  (im.computerid=u.id$ and im.productid=m.productid)

  AND m.Vendor LIKE 'Microsoft%';
```

4. インベントリ対象サーバ 'SJOHN164_99_139_79.NOVELL_AUS' のプロセッサ情報を取得します。次に、この照会を示します。

```
SELECT

  procr.DeviceID,

  role.EnumString,

  family.EnumString,

  procr.OtherFamilyDescription,

  upg.EnumString,

  procr.MaxClockSpeed,

  procr.CurrentClockSpeed,

  procr.Stepping

FROM

  CIM.UnitaryComputerSystem ucs,

  CIM.ComputerSystemProcessor csp,

  CIM.Processor procr,

  CIM.Role_en_US role,

  CIM.Family_en_US family,

  CIM.UpgradeMethod_en_US upg
```

```
WHERE
 ucs.name='SJOHN164_99_139_79.Novell_AUS' AND
  csp.PartComponent=procr.id$ AND
(
  (
    ( procr.Role IS NOT NULL AND procr.Role=role.Enum ) OR
    ( procr.Role IS NULL AND role.Enum=1000 )
  )
  AND:
procr.Family=family.Enum
  AND:
  (
   ( procr.UpgradeMethod IS NOT NULL AND procr.UpgradeMethod=upg.Enum ) OR
    ( procr.UpgradeMethod IS NULL AND upg.Enum=1000 )
  )
);
```

5. インベントリ対象サーバ'SJOHN164_99_139_79.NOVELL_AUS'に使用する UnitaryComputerSystem の ID を取得します。次に、この照会を示します。

```
SELECT
  id$,
FROM
  CIM.UnitaryComputerSystem
WHERE
  Name='SJOHN164_99_139_79.Novell_AUS';
```

6. データベース内のインベントリ対象サーバの数を検索します。次に、この照会を示します。

```
SELECT
  count(u.id$)
FROM
  CIM.UnitaryComputerSystem u,
  CIM.InstalledSoftwareElement s,
  ZENworks.InventoryScanner m
WHERE
  m.id$=s.Software AND u.id$=s.System;
```

7. 照会例 5 に示されている照会によって、特定のインベントリ対象サーバに使用する UnitaryComputerSystem の ID が判明すると、照会例 4 を次のように変更できます。

```
SELECT
procr.DeviceID,
role.EnumString,
family.EnumString,
procr.OtherFamilyDescription,
upg.EnumString,
procr.MaxClockSpeed,
procr.CurrentClockSpeed,
procr.Stepping
FROM
CIM.UnitaryComputerSystem ucs,
CIM.ComputerSystemProcessor csp,
CIM.Processor procr,
CIM.Role_en_US role,
CIM.Family_en_US family,
CIM.UpgradeMethod_en_US upg
WHERE
ucs.id$ = ?AND
csp.PartComponent=procr.id$ AND
(
  (
    ( procr.Role IS NOT NULL AND procr.Role=role.Enum ) OR
    ( procr.Role IS NULL AND role.Enum=1000 )
  )
  AND:
procr.Family=family.Enum
  AND:
  (
   ( procr.UpgradeMethod IS NOT NULL AND procr.UpgradeMethod=upg.Enum ) OR
    ( procr.UpgradeMethod IS NULL AND upg.Enum=1000 )
  )
);
```

指定されたインベントリ対象サーバの ID を、照会の「ucs.id$」の値「?」と置き換えます。

8. データベース内のすべてのサーバの IP アドレス、IPX アドレス、および MAC アドレスを一覧表示します。次に、この照会を示します。

```
SELECT
  u.name,
  ip.Address,
  ipx.Address,
  mac.MACAddress
FROM
  CIM.UnitaryComputerSystem u,
  CIM.HostedAccessPoint s1,
  CIM.IPProtocolEndpoint ip,
  CIM.HostedAccessPoint s2,
  CIM.IPXProtocolEndpoint ipx,
  CIM.HostedAccessPoint s3,
  CIM.LANEndpoint mac
WHERE
  (s1.Dependent=ip.id$ and s1.Antecedent=u.id$) AND
  (s2.Dependent=ipx.id$ and s2.Antecedent=u.id$) AND
  (s3.Dependent=mac.id$ and s3.Antecedent=u.id$);
```

9. 指定されたインベントリ対象サーバのハードディスクのドライブの名前とその他のプロパティを取得します。次に、この照会を示します。

```
SELECT
  n.Name,
  m.DeviceID,
  n.FileSystemSize,
  n.AvailableSpace,
  n.FileSystemType,
  m.VolumeSerialNumber,
  m.caption as VolumeLabel
FROM
  CIM.HostedFileSystem s,
  CIM.LocalFileSystem n,
  CIM.ResidesOnExtent r,
  ZENworks.LogicalDiskDrive m
WHERE
  (s.GroupComponent=? and s.PartComponent=n.id$) AND
  (r.Dependent=n.id$ and r.Antecedent=m.id$);
```

10. データベースに保存されているすべてのカスタム属性情報を取得します。次に、この照会を示します。

```
SELECT * FROM ZENworks.CustomInformation;
```

11. クラス CIM.UnitaryComputerSystem に関連付けられているすべてのカスタム属性情報を取得します。次に、この照会を示します。

```
SELECT

  *

FROM

  ZENworks.CustomInformation

WHERE

  extractClass(id) IN

  (SELECT id FROM MW_DBA.t$Class WHERE
  ClassName='CIM.UnitaryComputerSystem')
```

12. 企業内のすべての Microsoft Office インストールを取得します。次に、この照会を示します。

```
SELECT

  u.name,

  m.FriendlyName,

  im.InternalVersion,

  im.ProductIdentifier

FROM

  CIM.UnitaryComputerSystem u,

  MW_DBA.InstalledSoftware im,

  MW_DBA.Software m,

  MW_DBA.MSOffice mso

WHERE

  mso.id$=m.productid AND

  m.productid=im.productid AND

  im.computerid=u.id$;
```

13. 企業内のすべての Internet Explorer インストールを取得します。次に、この照会を示します。

```
SELECT

  u.Name,

  m.Name,

  m.Version,

  im.InternalVersion,

  im.ProductIdentifier
```

```
FROM

  CIM.UnitaryComputerSystem u,

  MW_DBA.InstalledSoftware im,

  MW_DBA.Software m,

  MW_DBA.InternetExplorer ie

WHERE

  ie.id$=m.productid AND

  m.productid=im.productid AND

  im.computerid=u.id$;
```

注： 照会 12 および 13 では、コンポーネントに関連するテーブル以外は、ほとんど同じ構文に従います。類似するアプローチを、Windows Media Player、Outlook Express、Microsoft Word、Microsoft Excel などのコンポーネントにも使用できます。これらのテーブルはすべてスキーマで利用できます。

14. 企業内のすべてのアンチウィルス製品インストールを取得します。次に、この照会を示します。

```
SELECT

  u.Name,

  m.Name,

  m.Version,

  im.InternalVersion,

  ivs.DefinitionVersion,

  ivs.DefinitionDate

FROM

  CIM.UnitaryComputerSystem u,

  MW_DBA.InstalledSoftware im,

  MW_DBA.Software m,

  MW_DBA.InstalledVirusScanner ivs

WHERE

  ivs.pinstanceid=im.pinstanceid AND

  m.productid=im.productid AND

  im.computerid=u.id$;
```

15. インベントリ対象サーバ'SJOHN164_99_139_79.NOVELL_AUS'にインストールされているすべてのアプリケーション、およびアプリケーションに関連付けられているファイルのすべての詳細を取得します。次に、この照会を示します。

```
SELECT
  u.Name,
  m.Name,
  m.Version,
  m.Category,
  zfile.company,
  zfile.productname,
  zfile.productversion,
  zfile.name,
  dir.path,
  zfile.fileversion,
  zfile."size",
  zfile.lastmodified,
  zfile.internalname,
  zfile.softwaredictionaryid
FROM
  CIM.UnitaryComputerSystem u,
  MW_DBA.InstalledSoftware iso,
  MW_DBA.Software m,
  MW_DBA.InstalledFile ifile,
  MW_DBA."file" zfile,
  MW_DBA.Directory dir
WHERE
  u.Name='SJOHN164_99_139_79.Novell_AUS' AND
  iso.computerid=u.id$ AND
  iso.productid=m.productid AND
  iso.pinstanceid=ifile.pinstanceid AND
  ifile.directoryid=dir.id AND
  ifile.fileid=zfile.id;
```

16. 有効なソフトウェアに関連付けられていないインベントリ対象サーバ ’SJOHN164_99_139_79.NOVELL_AUS’ 上に存在するすべてのファイルを取得します。次に、この照会を示します。

```
SELECT
  u.Name,
  zfile.name,
  dir.path,
  zfile.fileversion,
  zfile."size",
  zfile.lastmodified,
  zfile.internalname,
  zfile.productversion,
  zfile.company,
  zfile.productname
FROM
  CIM.UnitaryComputerSystem u,
  MW_DBA.InstalledFile ifile,
  MW_DBA."file" zfile,
  MW_DBA.Directory dir
WHERE
  u.Name='SJOHN164_99_139_79.Novell_AUS' AND
  u.id$=ifile.computerid AND
  ifile.fileid=zfile.id AND
  ifile.directoryid=dir.id AND
  ifile.pinstanceid is null;
```

17. 企業内の各インベントリコンピュータ上で、既知の拡張子を持つファイルによるディスク使用状況の詳細を取得します。次に、この照会を示します。

```
SELECT
  u.Name,
  du.Name,
  du.TotalDiskUsage
FROM
  CIM.UnitaryComputerSystem u,
  MW_DBA.DiskUsage du
WHERE
  u.id$=du.Computerid AND
  du.Name is not null;
```

16 インベントリ情報の管理

次の節では、Novell® ZENworks® 6.5 Server Inventory での情報の表示方法をカスタマイズするための情報について説明します。

- 571 ページの「インベントリ用に配備されたインベントリサーバの表示」
- 572 ページの「スキャンするハードウェアインベントリ情報のカスタマイズ」
- 576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」
- 621 ページの「ZENworks for Servers 3.X インベントリ対象サーバのスキャン対象ソフトウェアインベントリ情報のカスタマイズ」
- 621 ページの「インベントリデータベースからの重複するインベントリ対象サーバの削除」

インベントリ用に配備されたインベントリサーバの表示

ConsoleOne® を使用して、インベントリ収集用に設定したインベントリサーバおよびデータベースを表示することができます。

すべてのインベントリツリービューを取得するには、自分のインベントリツリーに設定されたインベントリサーバを含んでいるすべての Novell eDirectory™ ツリーにログインする必要があります。ConsoleOne でコンテナを選択し、[View] メニューをクリックして [Complete Tree View] をクリックします。選択したコンテナに含まれるすべてのインベントリサーバが [Complete Tree View] に表示されます。

異なる Novell eDirectory ツリーのインベントリサーバ間で情報のロールアップを実行するインベントリ展開の場合にすべてのツリービューを表示するには

1. ConsoleOne で [NDS Tree] を選択します。
2. [View] > [Complete Tree View] の順にクリックします。
3. eDirectory ツリーを選択するか、またはインベントリサーバを含むツリー内のコンテナを選択します。
4. [OK] をクリックします。

選択したインベントリサーバから最上位のサーバに至るまでのすべてのインベントリサーバを表示するには、ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックして [View] をクリックし、[Up Tree View] をクリックするか、Inventory Service オブジェクトをダブルクリックします。

インベントリ配備が単一の eDirectory ツリーで構成されている場合、[Up Tree View] をクリックすると、選択したインベントリサーバから最上位レベル (ルートサーバ) までのすべてのインベントリサーバが表示されます。

異なる eDirectory ツリーのインベントリサーバ間でインベントリ情報のロールアップを実行するインベントリ配備の場合、[Up Tree View] をクリックすると、選択したインベントリサーバから最上位レベルのサーバまで、ログインしたすべてのインベントリサーバが表示されます。

注： ショートカットキーを使ってインベントリツリーを折りたたむことはできません。

スキャンするハードウェアインベントリ情報のカスタマイズ

ZENworks 6.5 Server Management を使って、デフォルトのハードウェアインベントリに含まれていない情報をインベントリ対象サーバから収集することができます。

- 572 ページの「DMI を使ったベンダ固有の資産情報のスキャン」
- 574 ページの「JazおよびZipドライブベンダのハードウェアスキャン情報のカスタマイズ」
- 575 ページの「モニタのサイズに関するハードウェア情報のカスタマイズ」

DMI を使ったベンダ固有の資産情報のスキャン

1 [Server Inventory Policy] で、[Configuration Editor] タブをクリックします。

詳細については、509 ページの「Server Inventory ポリシーの設定」を参照してください。

2 [Asset Information] サブオプションをクリックし、[Set Defaults] をクリックします。

次のエントリが適用されます。

```
[ASSETTAG]

DMI1_CLASSNAME=

DMI1_ATTRIBUTEID=

DMI2_CLASSNAME=

DMI2_ATTRIBUTEID=

[SERIALNUMBER]

DMI1_CLASSNAME=

DMI1_ATTRIBUTEID=

DMI2_CLASSNAME=

DMI2_ATTRIBUTEID=

[MODEL]

DMI1_CLASSNAME=

DMI1_ATTRIBUTEID=

DMI2_CLASSNAME=

DMI2_ATTRIBUTEID=

[COMPUTERTYPE]DMI1_CLASSNAME=DMI1_ATTRIBUTEID=

[MODELNUMBER]DMI1_CLASSNAME=DMI1_ATTRIBUTEID=
```

3 値を指定します。

[Asset Information] には、次のセクションが含まれます。

- [ASSETTAG] セクションには備品タグを指定します
- [SERIALNUMBER] セクションにはシリアル番号を指定します
- [MODEL] セクションにはコンピュータモデルを指定します
- [COMPUTERTYPE] にはコンピュータの種類を指定します
- [MODELNUMBER] にはコンピュータのモデル番号を指定します

各セクションには、特定の DMI クラス名および DMI クラス属性 ID が含まれます。

[Asset Information] の書式は次のとおりです。

```
[ASSETTAG]
DMI1_CLASSNAME=DMI_class_name_for_asset_tag
DMI1_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
[SERIALNUMBER]
DMI1_CLASSNAME=DMI_class_name_for_serial_number
DMI1_ATTRIBUTEID=DMI_attribute_ID_for_serial_number
[MODEL]
DMI1_CLASSNAME=DMI_class_name_for_computer_model
DMI1_ATTRIBUTEID=DMI_attribute_ID_for_computer_model
```

[Asset Information] の各セクションの値には、最大 64 文字長の文字列を設定できます。

DMI クラス名には、DMTF|COMPONENTID|00x 以外の任意の DMI クラスを設定できます。

異なるカスタム DMI クラスを実装している DMI ベンダが複数存在する場合、複数の DMI クラスを指定できます。前に示したセクションでは、最大 5 つのクラスを指定できます。たとえば、5 つのクラスを指定した場合の資産情報は次のようになります。

```
[ASSETTAG]
DMI1_CLASSNAME=DMI_class_name_for_asset_tag
DMI1_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
DMI2_CLASSNAME=DMI_class_name_for_asset_tag
DMI2_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
DMI3_CLASSNAME=DMI_class_name_for_asset_tag
DMI3_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
DMI4_CLASSNAME=DMI_class_name_for_asset_tag
DMI4_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
DMI5_CLASSNAME=DMI_class_name_for_asset_tag
DMI5_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
```

Scanner は DMI1 を処理し、DMI1 の値が有効な場合は、残りの DMI クラスを処理しません。

4 [OK] をクリックします。

5 インベントリ対象サーバでスキャンを実行します。

インベントリ情報が [Inventory Summary] ウィンドウに表示されるのを確認します。

Jaz および Zip ドライブベンダのハードウェアスキャン情報のカスタマイズ

インベントリ対象サーバでは、バックアップデバイスおよびフロッピーデバイスなどのデバイスベンダに関するスキャン情報は、通常利用できません。こうした情報が利用できる場合でも、ベンダ情報に詳細情報が含まれることはありません。[Server Inventory Policy] > [Configuration Editor] > [Zipped Names] の順に移動して、こうしたデバイスのベンダに関する情報をカスタマイズして更新することができます。Scanner は、これらのデバイスのハードウェアスキャンプロセスの実行中に、この情報を読み取ります。

表示用のベンダ情報をカスタマイズして更新するには

1 [Server Inventory Policy] で、[Configuration Editor] タブをクリックします。

詳細については、509 ページの「Server Inventory ポリシーの設定」を参照してください。

2 [ZIPPED NAMES] サブオプションをクリックし、[Set Defaults] をクリックします。

デフォルト値が表示されます。

```
[Identifier]

iomega ZIP 100=Iomega 100MB Backup Device

iomega jaz 1GB=Iomega 1GB Backup Device

IOMEGA  ZIP 100         D.13=Iomega Corporation

IOMEGA  ZIP 1GB         D.13=Iomega Corporation

...
```

セクション内の各エントリの形式は、次のとおりです。

```
[Identifier]

device_id=vendor_display_name_you_specify
```

device_id には、インベントリ対象サーバにデバイスをインストールするときにベンダによってレジストリ内に生成および更新される一意の ID が入ります。

たとえば、このセクションの内容は次のようになります。

```
[Identifier]

iomega ZIP 100=Iomega 100MB Backup Device
```

このエントリは、インベントリ対象サーバにインストールされた 100MB の Zip* ドライブを示しています。

3 エントリを追加または変更します。

デバイス ID エントリに間違った値を指定すると、そのデバイスはインベントリウィンドウに表示されません。

4 [OK] をクリックします。

モニタのサイズに関するハードウェア情報のカスタマイズ

モニタに対してスキャンされるインベントリ情報は次のとおりです。

Nominal Size: モニタの対角線上の長さを示す数値（画面の片隅から反対側の隅までの距離）。たとえば、17 インチ。

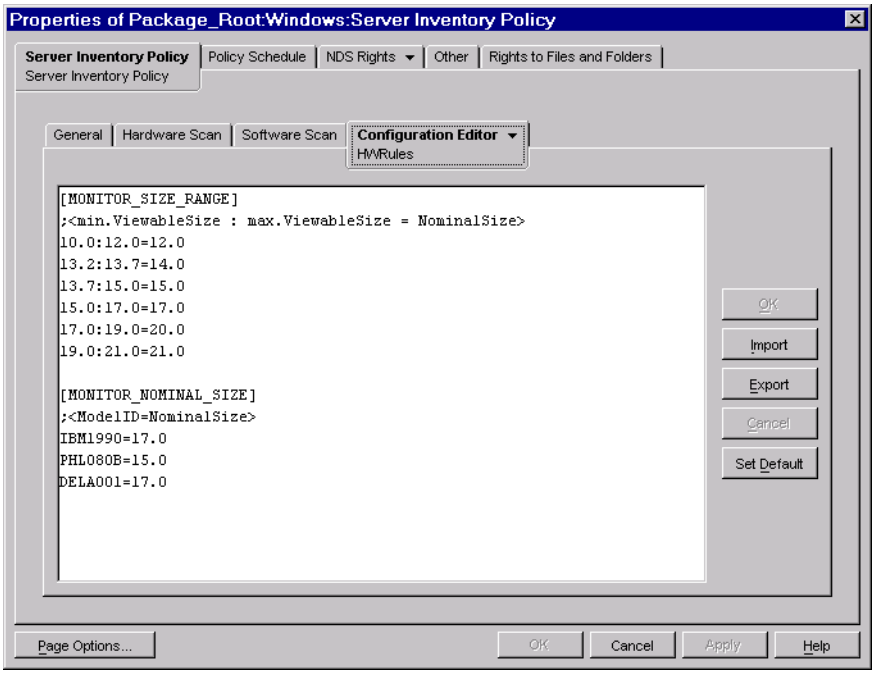
Viewable Size: イメージを縁取る黒い枠を除いて、画面イメージの対角線上の長さを示す数値。たとえば、15.8 インチ。

Inventory Scanner は、インベントリ対象 Windows* サーバのモニタの表示可能サイズを自動的にスキャンします。Server Inventory ポリシーを使用して、レポート対象のモニタの公称サイズをカスタマイズすることができます。

重要： Inventory Scanner は 1997 年以降に製造されたモニタのインベントリ情報のみレポートします。

モニタの公称サイズのスキャンをカスタマイズするには

1 [Server Inventory Policy] で、[Configuration Editor] タブをクリックして、[HWRules] をクリックします。



2 [Set Default] をクリックします。

デフォルトの値が [Configuration Editor] ボックスに表示されます。

3 エントリを追加または変更します。

HWRules.ini の書式は次のとおりです。

```
[MONITOR_SIZE_RANGE]

minimum_viewable_size_you_specify:maximum_viewable_size_you_specify =
nominal_size_you_specify

[MONITOR_NOMINAL_SIZE]

model_ID_reported_by_scanner = nominal_size_you_specify
```

[MONITOR_SIZE_RANGE] セクションに、表示可能サイズの最小と最大の範囲、およびモニタの対応する公称サイズを指定します。Inventory Scanner は、モニタのモデル ID をスキャンし、HWRules.ini ファイルの [MONITOR_NOMINAL_SIZE] セクションに設定されている公称サイズをレポートします。

[MONITOR_NOMINAL_SIZE] セクションで、モデル ID と Inventory Scanner からレポートされた対応する公称サイズを指定します。この情報は、[Hardware/Software Inventory] > [Hardware] > [Monitor] 属性の [Inventory Summary] ダイアログボックスに表示されます。

スキャンしたモデル ID が [MONITOR_NOMINAL_SIZE] に表示されていない場合、Scanner はモニタの表示可能サイズをスキャンします。表示可能サイズに基づいて、Scanner は HWRules.ini ファイルの [MONITOR_SIZE_RANGE] セクションに設定されている公称サイズをレポートします。

たとえば、HWRules.ini ファイルの内容が次のとおりであるとします。

```
[MONITOR_SIZE_RANGE]

10.0:12.0=12.0

13.2:13.7=14.0

[MONITOR_NOMINAL_SIZE]

IBM1990=17.0

PHL080B=15.0
```

4 [OK] をクリックすると、この内容が Server Inventory ポリシーに保存されます。

ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ

Inventory Scanner の次の拡張機能により、ZENworks 6.5 Server Inventory を使用するインベントリ対象サーバに対するスキャンプロセスをより効果的および効率的に制御できるようになりました。

- 次のソフトウェアインベントリ情報のスキャンをサポートします。
  - Windows* オペレーティングシステムおよびそのパッチ
  - Internet Explorer とその修正プログラム
  - Windows Media Player とその修正プログラム
  - Outlook Express とその修正プログラム
  - Novell Client32™ およびインストールされたコンポーネント
  - ZENworks スイートおよびインストールされたコンポーネント
  - Microsoft* Office およびそのインストールされたアプリケーション
  - Symantec* Antivirus Corporate Edition および McAfee* Antivirus などのウイルス対策製品
  - Symantec Antivirus Corporate Edition および McAfee Antivirus などのウイルス対策製品のウイルス定義日およびバージョン
- Windows の [アプリケーションの追加と削除] および MSI データベースで一覧表示される製品のスキャンをサポートします。

- ソフトウェアのタイトルのディクショナリを含んでおり、インストールされたソフトウェアに関する、より正確なレポートを提供します。
- ソフトウェアスキャンの範囲を制御するルールを提供します。
- 設定済みのファイル拡張子が使用する総ディスク容量のレポートを作成します。

ここでは、次の内容について説明します。

- 577 ページの「ZENworks ソフトウェアディクショナリとは」
- 578 ページの「ソフトウェアディクショナリルールとは」
- 578 ページの「ソフトウェア識別情報とは」
- 578 ページの「キー ID とは」
- 578 ページの「不明なソフトウェアとは」
- 578 ページの「継承されたルールとは」
- 579 ページの「優先されるルールとは」
- 579 ページの「ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解」
- 585 ページの「ソフトウェアディクショナリパターンタイプについて」
- 586 ページの「ソフトウェアディクショナリのルールの設定」
- 617 ページの「ソフトウェアディクショナリの展開に関する基準の設定」
- 619 ページの「[Inventory Summary] でのソフトウェアインベントリ情報の表示」
- 619 ページの「ソフトウェアインベントリレポートの生成」

ZENworks ソフトウェアディクショナリとは

ZENworks ソフトウェアディクショナリには、ソフトウェア識別情報とルールのリストが含まれています。各ソフトウェア識別情報は、インベントリ対象サーバにインストールされている特定の製品を識別します。ルールは、スキャンプロセスの範囲を制御します。

Server Inventory ソフトウェアをインストールすると、ZENworks ソフトウェアディクショナリは自動的にインベントリサーバとインベントリ対象サーバにインストールされます。必要なポリシーを設定して Inventory Service を開始すると、Inventory Scanner はソフトウェアディクショナリに基づいてソフトウェア情報をレポートします。

ZENworks ソフトウェアディクショナリには、一般ディクショナリとプライベートディクショナリの 2 種類があります。

一般ディクショナリ： 一般ディクショナリは、ソフトウェアディクショナリの一部であり、定義済みのソフトウェア識別情報が含まれています。Inventory Scanner は、このディクショナリに基づいて、特定の製品がインベントリ対象サーバにインストールされているかどうかをレポートします。

プライベートディクショナリ： プライベートディクショナリは、ソフトウェアディクショナリの一部であり、ユーザ定義のソフトウェア識別情報、およびインベントリスキャンの範囲の定義とソフトウェア情報のカスタマイズを可能にするルールが含まれています。ユーザは、ルールを設定することができます。ルールの設定方法の詳細については、586 ページの「ソフトウェアディクショナリのルールの設定」を参照してください。

重要： プライベートディクショナリで定義したルールは、一般ディクショナリの定義済みのルールよりも優先されます。

ソフトウェアディクショナリルールとは

ソフトウェアディクショナリルールは、スキャンプロセスの範囲を制御する条件セットを表します。

ソフトウェア識別情報とは

ソフトウェア製品を識別するエントリのことをソフトウェア識別情報と呼びます。各ソフトウェア識別情報には、ファイル照合属性および対応するソフトウェア情報属性のセットが含まれています。インベントリスキャンで、Inventory Scanner によってファイルのヘッダから読み取られた属性がディクショナリ内に設定された属性と一致した場合、対応するソフトウェア情報属性の情報がインベントリデータベースに保存されます。

キー ID とは

ソフトウェア製品は、ディクショナリ内の複数のソフトウェア識別情報で識別できます。このような場合、Inventory Scanner は、これらのソフトウェア識別情報の 1 つからソフトウェア情報を任意で選択できます。キー ID は、Inventory Scanner がソフトウェア情報を選択する元になるソフトウェア識別情報を識別します。キー ID は、異なるソフトウェア識別情報の属性値 (Description など) に若干の違いがあり、Inventory Scanner で特定のソフトウェア識別情報から情報を選択する必要がある場合に便利です。

不明なソフトウェアとは

不明なソフトウェアの特徴は次のとおりです。

- インベントリ対象サーバにインストールされます。
- ZENworks ソフトウェアディクショナリの [Report Files with These File Extensions As Unidentified Software] ルールで設定されます。
- ソフトウェアディクショナリ (Software Dictionary) テーブルでは設定されません。

継承されたルールとは

継承されたルールは、ディクショナリ配布によって別のインベントリサーバから取得されるソフトウェアディクショナリ内のエントリです。このルールを編集したり削除したりすることはできません。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

優先されるルールとは

一般ディクショナリ内のデフォルトのソフトウェア識別情報は変更できませんが、デフォルトのソフトウェア識別情報を変更する場合は、デフォルトの識別情報よりも優先される、新しいソフトウェア識別情報を作成する必要があります。Inventory Scanner は、優先されたエントリを採用して、デフォルトの識別情報を無視します。

デフォルトの識別情報よりも優先されるソフトウェア識別情報を作成するには、デフォルトの識別情報に定義されたすべての照合属性に同じ値を指定して、ソフトウェア情報属性に新しい値を指定する必要があります。

ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解

ZENworks ソフトウェアディクショナリルールは、優先順位に従って使用されます。すべてのソフトウェアディクショナリルールに適用されるガイドラインと、特定のカテゴリのソフトウェアディクショナリルールにのみ適用されるガイドラインがあります。詳細については、次の節を参照してください。

- 579 ページの「すべてのソフトウェアディクショナリルールに適用されるガイドライン」
- 580 ページの「Report Only Maximum Software Version と Report All Software Versions の間の優先順位」
- 580 ページの「Software Scanning カテゴリでグループ化されたソフトウェアディクショナリルールの優先順位」
- 582 ページの「Disk Usage Scanningカテゴリでグループ化されたソフトウェアディクショナリルールの優先順位」

すべてのソフトウェアディクショナリルールに適用されるガイドライン

次のガイドラインは、設定したすべてのソフトウェアディクショナリルールに適用されます。

- すべてのソフトウェアディクショナリルールは、Inventory Scanner によってインベントリ対象サーバで適用されます。
- ソフトウェアディクショナリルールの設定は、ソフトウェアディクショナリ ConsoleOne スナップインを使用して変更できます。ソフトウェアディクショナリルールの設定方法の詳細については、586 ページの「ソフトウェアディクショナリのルールの設定」を参照してください。
- それぞれのインベントリスキャンには、そのスキャンに使用されるディクショナリファイルのバージョンが含まれています。この情報は、インベントリデータベースに保存されます。
- ユーザ定義のソフトウェア識別情報は、ソフトウェアディクショナリに存在するデフォルトのソフトウェア識別情報よりも優先されますが、デフォルトのソフトウェア識別情報よりも優先されるのは、一度に 1 つのユーザ定義ソフトウェア識別情報のみです。

Report Only Maximum Software Version と Report All Software Versions の間の優先順位

デフォルトでは、scanner はインストールされているソフトウェアの最新バージョンのみをレポートします。[Report All Software Versions] のルールが [Report Only Maximum Software Version] のルールと競合する場合は、[Report Only Maximum Software Version] のルールが [Report All Software Versions] のルールよりも優先されます。

Software Scanning カテゴリでグループ化されたソフトウェアディクショナリルールの優先順位

Software Scanning カテゴリ内のソフトウェアディクショナリルールにより、ローカルファイルシステム上のファイルのスキャン範囲が制御されます。

Software Scanning カテゴリには、次のソフトウェアディクショナリルールがあります。

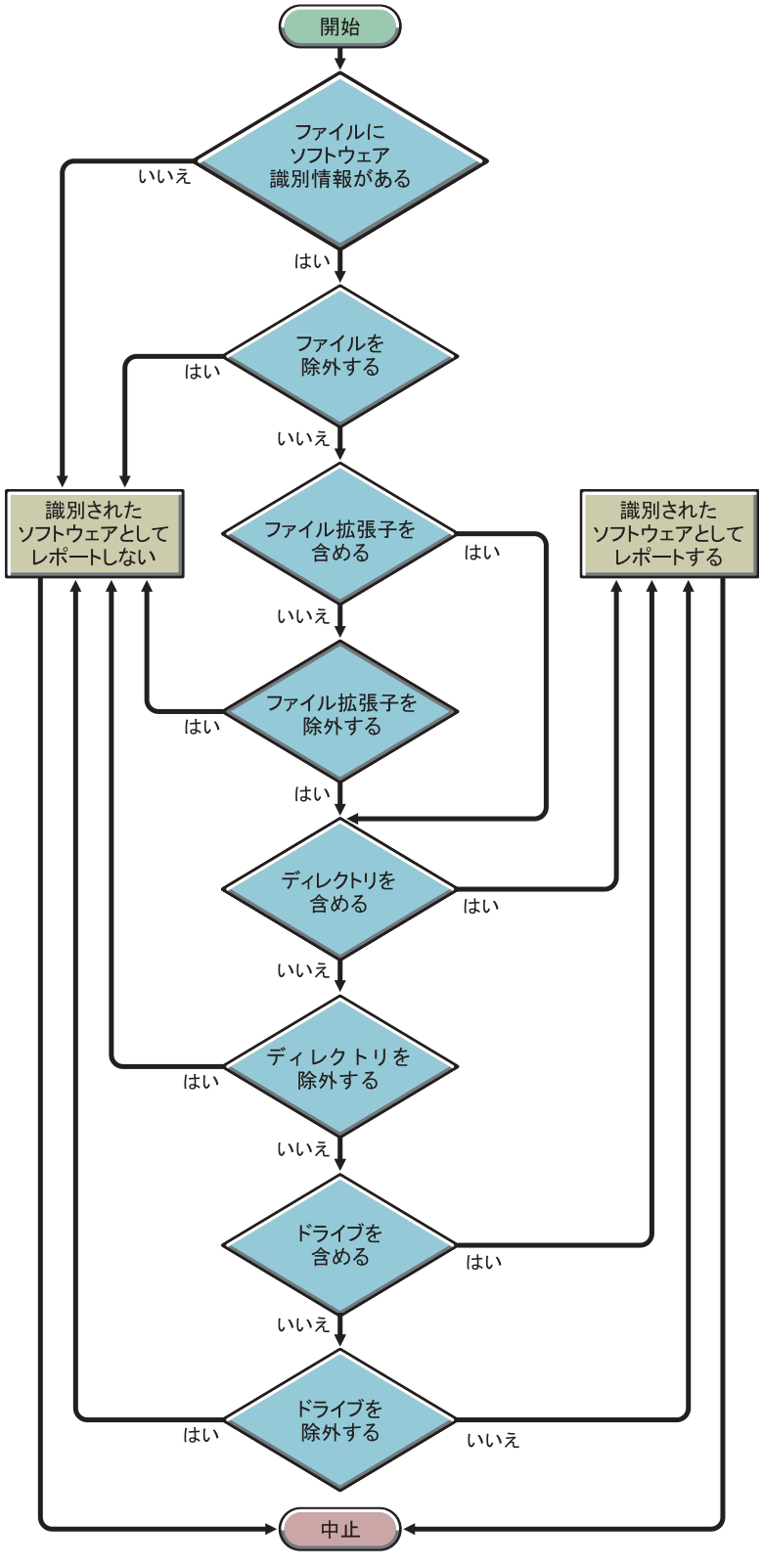
- 604 ページの「[Scan File Extensions]」
- 603 ページの「[Ignore File Extensions]」
- 602 ページの「[Scan Directories]」
- 601 ページの「[Ignore Directories]」
- 600 ページの「[Scan Drives]」
- 600 ページの「[Ignore Drives]」
- 606 ページの「ソフトウェアスキャンフィルタ - [Software]」
- 605 ページの「ソフトウェアスキャンフィルタ - [Files]」

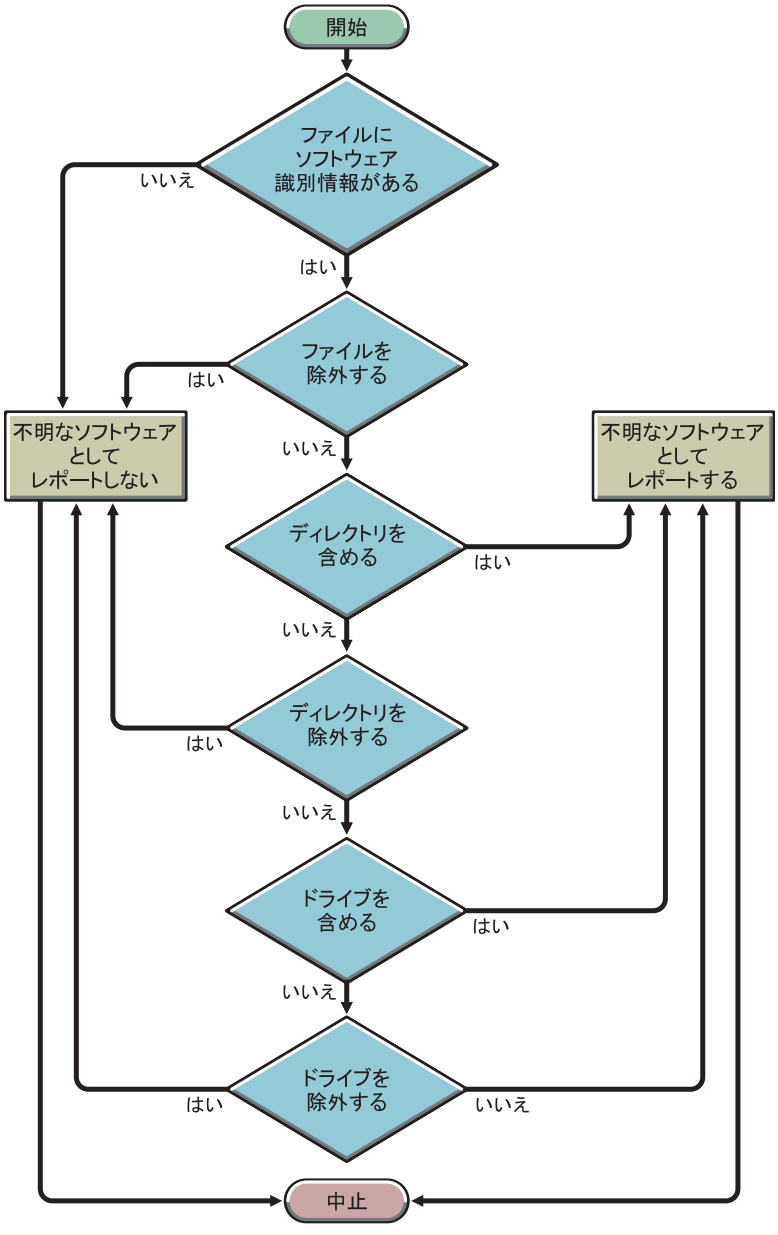
これらのルールを何も設定しない場合、Inventory Scanner はインベントリ対象サーバのハードディスクにあるすべてのファイルをスキャンします。ファイルのソフトウェアディクショナリに一致するソフトウェア識別情報がある場合、ファイルは識別済みのソフトウェアとしてレポートされます。それ以外の場合は、不明なソフトウェアとしてレポートされます。

これらのルールを設定した場合、各ルールは次に示す降順で適用されます。

- ソフトウェアスキャンフィルタ - [Files]
- ソフトウェアスキャンフィルタ - [Software]
- [Scan File Extensions]
- [Ignore File Extensions]
- [Scan Directories]
- [Ignore Directories]
- [Scan Drives]
- [Ignore Drives]

次のフローチャートは、これらのルールの優先順位を示しています。





Disk Usage Scanning カテゴリでグループ化されたソフトウェアディクショナリルールの優先順位

Disk Usage Scanning カテゴリ内のソフトウェアディクショナリルールにより、ファイルがディスク使用状況スキャンの対象になるかどうかが決まります。

Disk Usage Scanning カテゴリには、次のソフトウェアディクショナリルールがあります。

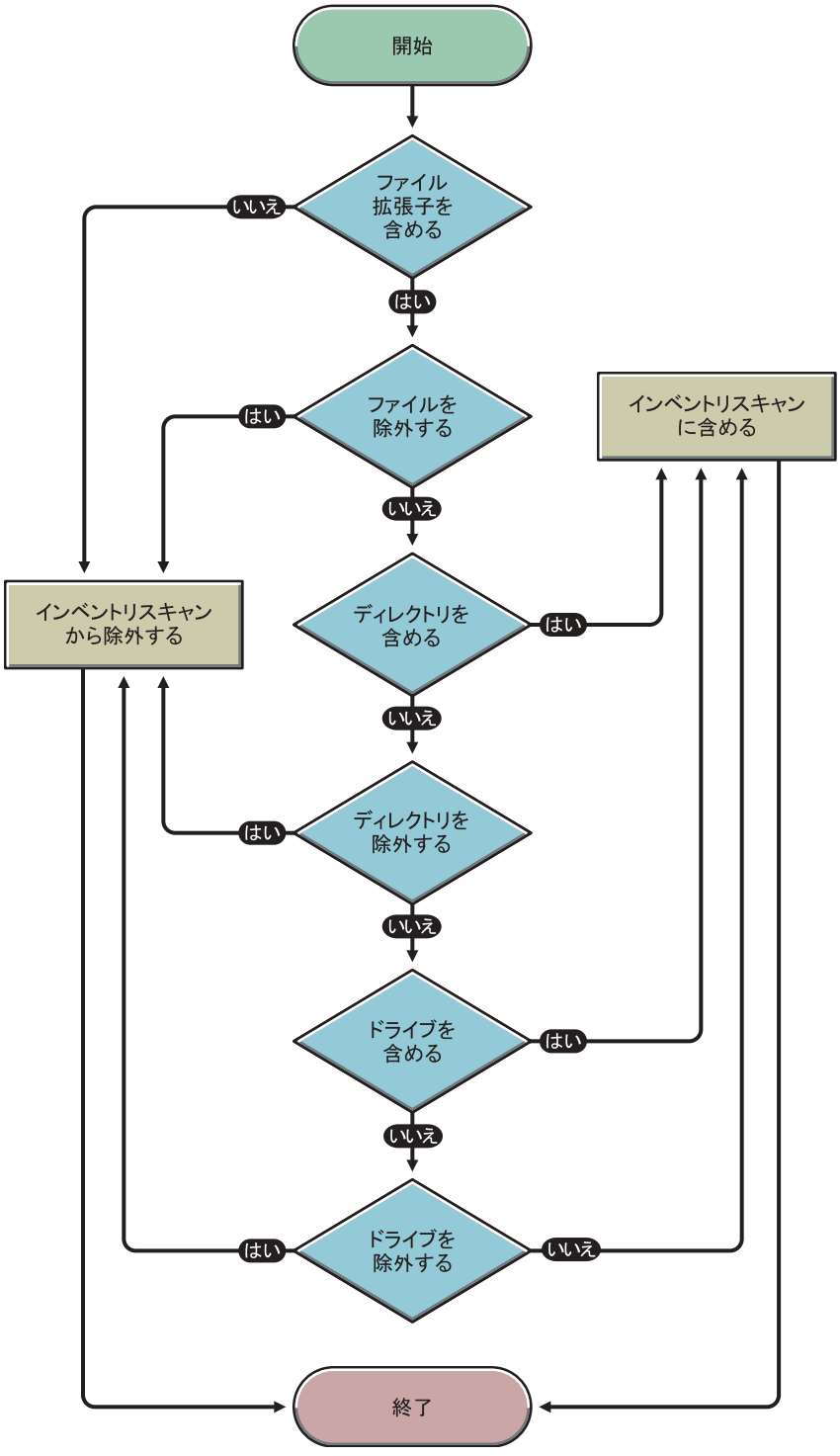
- 598 ページの「[Report Disk Space Used by File Extensions]」
- 611 ページの「ディスク使用状況スキャンフィルタ - [Files]」
- 611 ページの「[Scan Directories]」
- 610 ページの「[Ignore Directories]」
- 609 ページの「[Scan Drives]」
- 609 ページの「[Ignore Drives]」

ファイルをディスク使用状況スキャンの対象に含めるには、そのファイルの拡張子が Report Disk Space Used by File Extensions ルールに含まれている必要があり、他の Disk Usage Scanning ルールのインベントリスキャンから除外されないようにする必要があります。

次の各ルールが降順で適用されます。

- ディスク使用状況スキャンフィルタ - [Files]
- [Scan Directories]
- [Ignore Directories]
- [Scan Drives]
- [Ignore Drives]

次のフローチャートは、これらのルールの優先順位を示しています。



ソフトウェアディクショナリパターンタイプについて

ソフトウェアディクショナリルールを設定する前に、ZENworks 6.5 でサポートされる次のソフトウェアディクショナリパターンタイプに注意する必要があります。

- 585 ページの「Regular Expression(正規表現)」
- 585 ページの「Expandable Expression(展開可能な表現)」
- 585 ページの「System Expandable Expression(システムの展開可能な表現)」

Regular Expression(正規表現)

Regular Expression とは、POSIX 正規表現を表します。regexp (正規表現) の詳細については、The Open Group Base Specifications Issue 6 Web サイト (http://www.opengroup.org/onlinepubs/007904975/basedefs/xbd_chap09.html) を参照してください。

Regular Expression の使用例

- 「Novell」で始まるすべてのベンダ名を検索するには、「Novell.*」と指定します。
- 実行可能ファイルを検索するには、「[exe|EXE]」と指定します。
- 「r」で始まり「t」で終わる 6 文字の名前を持つファイルを検索するには、「[r....t]」と指定します。
- 「A」から「C」の間で始まり「E」で終わる名前を持つファイルを検索するには、「[A-C].*[E]」と指定します。
- 名前に大文字が含まれていないファイルを検索するには、「[^A-Z]+」と指定します。

注: [、¥、^、$、.、|、?、(、)、*、および + などのメタ文字を使用する場合は、文字の前にバックスラッシュ (¥) を挿入します。たとえば、正規表現で「c:¥windows」と指定するには、「c:¥¥windows」と指定します。

Expandable Expression(展開可能な表現)

Expandable Expression には、表示可能な文字とアスタリスク (*) ワイルドカード文字が含まれています。

「*」は 0 個以上の表示可能な文字と一致します。

Expandable Expression の使用例

- 「Microsoft」で始まるベンダ名のすべてのインスタンスを検索するには、「Microsoft*」と指定します。
- 拡張子が「.exe」のファイルを検索の対象に含めるには、「exe」と指定します。

System Expandable Expression(システムの展開可能な表現)

- **NetWare の場合:** システムの展開可能な表現には、表示可能な文字、環境変数への参照、またはワイルドカード文字のアスタリスク (*) を使用できます。

  重要: 「*」は、一意の文字として使用する場合を除いて、0 または 1 つ以上の表示可能文字に一致し、環境変数では区切り文字「¥」で区切りません。たとえば、「user*」環境変数では、「*」は一意の文字であり、scanner は名前が「user*」の環境変数を検索します。「user¥*」環境変数では、「*」は 0 または 1 つ以上の表示可能文字に一致します。

環境変数の例 :$sysdir

- **Windows の場合：** システムの展開可能な表現には、表示可能な文字、環境変数への参照、またはワイルドカード文字のアスタリスク (*) を使用できます。

  「*」は 0 個以上の表示可能な文字と一致します。

  環境変数の例 :%temp%

  重要： システムの拡張可能な表現には、表示可能な文字の組み合わせ、環境変数への参照、またはワイルドカード文字のアスタリスク (*) を使用できますが、環境変数を使用する場合には、環境変数を式の最初に指定する必要があります。たとえば、「%temp%/*」のように指定します。

  System Expandable Expression の使用例

  - C ドライブのディスク使用状況を検索するには、C と指定します。
  - c:¥program files ディレクトリ内のファイルを検索するには、「c:¥program files」と指定します。
  - 拡張子が「.com」のファイルを検索するには、「com」と指定します。

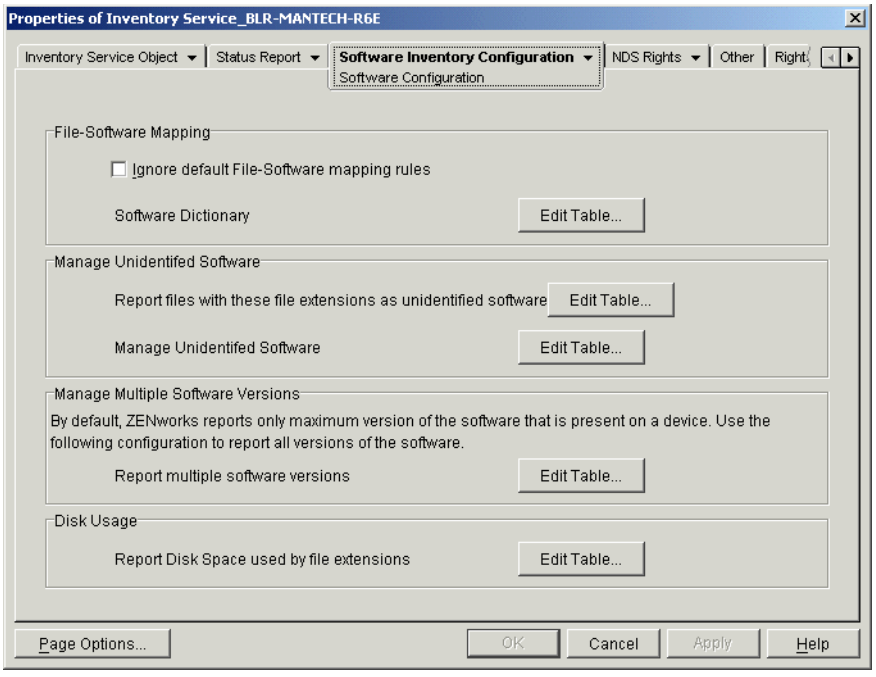
ソフトウェアディクショナリのルールの設定

1 ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックし、[Properties] をクリックします。

2 [Software Configuration] ページで次の設定を行うことで、ソフトウェアインベントリ情報をスキャンすることができます。

- **ファイルとソフトウェアのマッピング：** 次のルールを追加します。
  - 589 ページの「ファイルとソフトウェアのデフォルトマッピングルールの無視」
  - 589 ページの「ソフトウェアディクショナリ (Software Dictionary)」
- **不明なソフトウェアの管理：** 次のルールを追加します。
  - 593 ページの「[Report Files with These File Extensions As Unidentified Software]」
  - 594 ページの「[Manage Unidentified Software]」
- **複数のソフトウェアバージョンの管理：** 次のルールを追加します。
  - 595 ページの「複数のソフトウェアバージョンのレポート」
- **[Disk Usage]：** 次のルールを追加します。
  - 598 ページの「[Report Disk Space Used by File Extensions]」

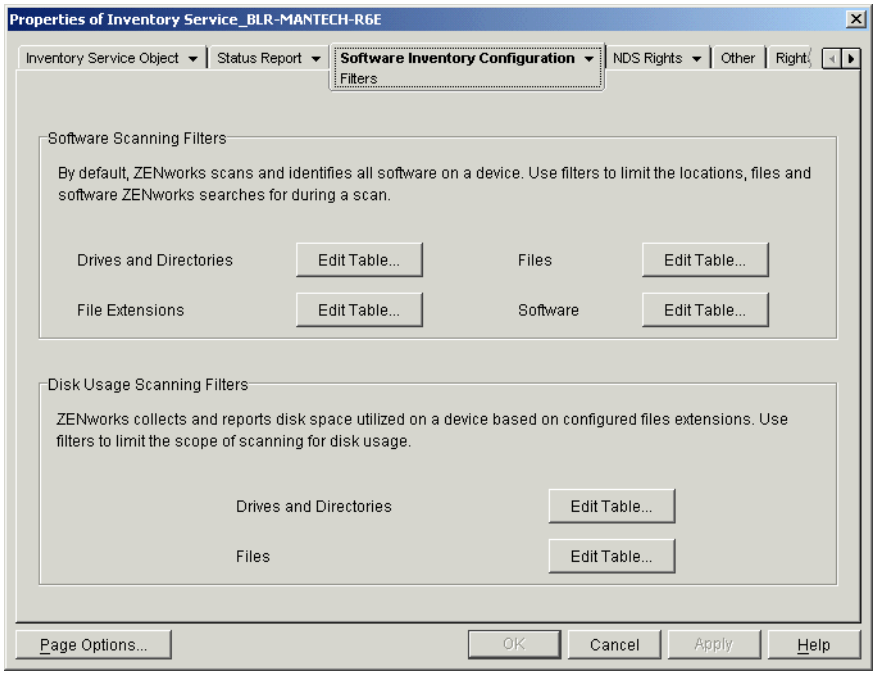
重要： ZENworks ソフトウェアディクショナリルールを設定する際には、これらのルールの使用方法に注意する必要があります。詳細については、579 ページの「ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解」を参照してください。



3 [Filters] ページでは、ファイルをスキャンするスコープを制御できます。

- **ソフトウェアスキャンフィルタ：** 次のルールを追加します。
  - 599 ページの「ソフトウェアスキャンフィルタ - [Drives and Directories]」
  - 603 ページの「ソフトウェアスキャンフィルタ - [File Extensions]」
  - 605 ページの「ソフトウェアスキャンフィルタ - [Files]」
  - 606 ページの「ソフトウェアスキャンフィルタ - [Software]」
- **ディスク使用状況のスキャンのフィルタ：** 次のルールを追加します。
  - 607 ページの「ディスク使用状況スキャンフィルタ - [Drives and Directories]」
  - 611 ページの「ディスク使用状況スキャンフィルタ - [Files]」

重要： ZENworks ソフトウェアディクショナリルールを設定する際には、これらのルールの使用方法に注意する必要があります。詳細については、579 ページの「ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解」を参照してください。



4 [Aliases] ページでは、次の設定を行えます。

- **別名の指定：** ベンダやソフトウェアの名前の別名を設定できます。

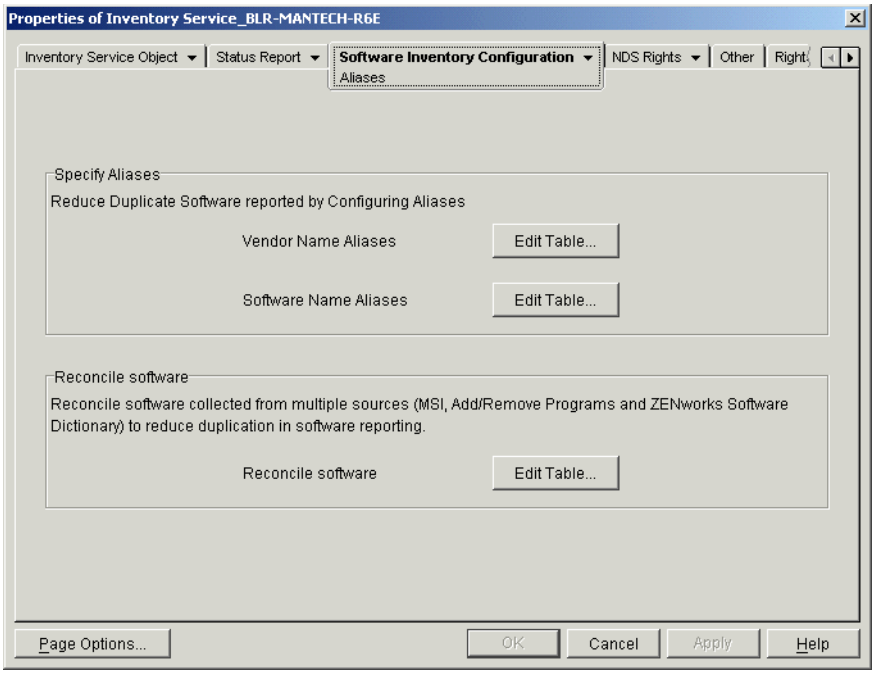
  Inventory ConsoleOne ユーティリティでは、デフォルトでソフトウェア情報は各ベンダ名で分類されます。同じベンダのソフトウェアに異なるベンダ名または製品名が使用されている場合があります。この場合、Inventory ConsoleOne ユーティリティでは、異なるセクションの下にソフトウェア情報が表示されます。

  しかし別名を指定することで、ソフトウェア情報をまとめることができます。これらの設定は、次のソフトウェアディクショナリルールでカスタマイズできます。

  - 613 ページの「[Vendor Name Aliases]」
  - 614 ページの「[Software Name Aliases]」

- **ソフトウェアの調停：**[プログラムの追加と削除] または MSI で認識されているソフトウェア、および ZENworks ソフトウェアディクショナリで認識されているソフトウェアを統合することができます。詳細については、615 ページの「[Reconcile Software]」を参照してください。

重要： ZENworks ソフトウェアディクショナリルールを設定する際には、これらのルールの使用方法に注意する必要があります。詳細については、579 ページの「ZENworks ソフトウェアディクショナリルールの使用と優先順位の理解」を参照してください。



5 [Apply]、[Close] の順にクリックします。

ファイルとソフトウェアのデフォルトマッピングルールの無視

ソフトウェアインベントリ情報をスキャンする際に、ZENworks ソフトウェアディクショナリに設定されているファイルとソフトウェアのデフォルトマッピングルールを Inventory Scanner で使用しない場合には、[Ignore Default File-Software Mapping Rules] チェックボックスを選択します。

重要： ソフトウェアディクショナリが別のインベントリサーバから更新される場合、このオプションは選択できません。

ソフトウェアディクショナリ (Software Dictionary)

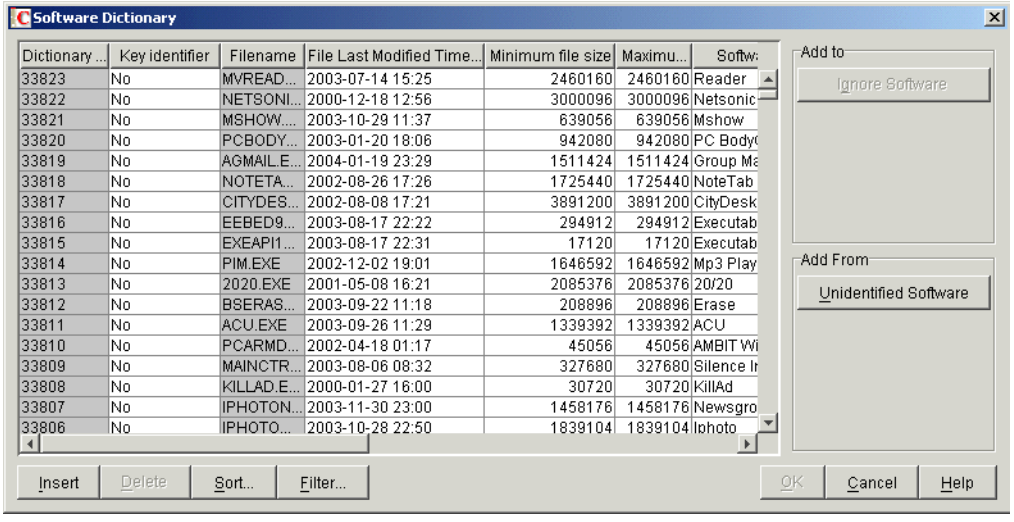
[Software Dictionary] オプションでは、ZENworks ソフトウェアディクショナリ内のソフトウェア識別情報を設定できます。

デフォルトでは、ZENworks ソフトウェアディクショナリには定義済みのソフトウェア識別情報が含まれています。ZENworks ソフトウェアディクショナリに新しいソフトウェア識別情報を作成する方法として、定義済みのソフトウェア識別情報を編集する方法と、ゼロから新しいソフトウェア識別情報を作成する方法があります。

ZENworks ソフトウェアディクショナリのルールを設定するには

1 [Edit Table] をクリックします。

[Software Dictionary] テーブルが表示されます。



[Software Dictionary] テーブルには、ZENworks ソフトウェアディクショナリに格納されているデータが表示されます。このテーブルに含まれるエントリには、次のものがあります。

- **薄い灰色：** テーブルにはこれらのエントリを上書きするエントリがすでに含まれているのでこれらのエントリはスキャン対象とならないことを示します。
- **濃い灰色：** これらは継承されたルールです。継承されたルールの詳細については、578 ページの「継承されたルールとは」を参照してください。

2 [Software Dictionary] テーブルでは、次の操作を実行できます。

- 591 ページの「ソフトウェアディクショナリへのエントリの手動による追加」
- 592 ページの「ソフトウェアディクショナリへのエントリの自動的な追加」
- 592 ページの「ソフトウェアディクショナリからのエントリの削除」
- 593 ページの「ソフトウェアディクショナリのエントリの値の変更」
- 593 ページの「ソフトウェアのスキャンからの除外」
- 616 ページの「テーブル内のエントリのソート」
- 616 ページの「テーブル内のエントリのフィルタ処理」
- 617 ページの「テーブル内のエントリの更新」

3 [OK] をクリックします。

ソフトウェアディクショナリへのエントリの手動による追加

1 [Software Dictionary] テーブルで、[Insert] をクリックして新しい行を追加します。

2 次の属性の値を指定します。

ファイル名、ファイルの最終更新時 (yyyy-dd-mm 時：分)、最小ファイルサイズ (バイト単位)、最大ファイルサイズ (バイト単位)、ソフトウェア名、サポートパック、ソフトウェアバージョン、内部バージョン、説明、ベンダ名、プラットフォーム、およびカテゴリ。

次の属性は「照合属性」とよばれます。ファイル名、ファイルの最終修正日時、最小ファイルサイズ、最大ファイルサイズ、内部バージョン。これらの一致する属性の値は、Inventory Scanner がインベントリ対象サーバ上のファイルヘッダからスキャンした値と比較されます。値が一致する場合、対応するソフトウェア情報属性 (ソフトウェア名、サポートパック、ソフトウェアバージョン、説明、ベンダ名、プラットフォーム、およびカテゴリ) の値がインベントリデータベースに保存されます。

[Software Dictionary] テーブルで、次の属性の値を指定する必要があります。ファイル名、ソフトウェア名、およびベンダ。他の属性値の指定はオプションです。

エントリを追加すると、ディクショナリ ID と呼ばれる一意の ID がこのエントリに自動的に割り当てられます。

たとえば、[Software Dictionary - Row Editor] テーブルで次のように設定します。

Filename= MSACCESS.EXE
ファイルの最終更新時 = 1998-30-01 05:30
Minimum File Size= 299854
Maximum File Size= 400000
ソフトウェア名 = Access
ソフトウェアバージョン = 7.0
Internal Version= 7.0
Description= Microsoft Access
Vendor= Microsoft
Category= Database

Inventory Scanner のスキャンで「ファイル名 = MSACCESS.EXE; ファイルの最終更新時 = 1998-30-01 05:30; ファイルサイズ = 300000」という値のファイルが見つかった場合は、次の情報がインベントリデータベースに保存されます。

ソフトウェア名 = Access
ソフトウェアバージョン = 7.0
Description= Microsoft Access
Vendor= Microsoft
Category= Database

属性の値を指定しなかった場合、この属性は上書きエントリを決定するものとはみなされません。また、照合属性だけが上書きエントリを決定するものとみなされます。たとえば、[Configure Dictionary] テーブルに、MS Word に関する次のエントリがあるとします。

ファイル名	ファイルの最小サイズ	ファイルの最大サイズ	ソフトウェア名 (Software Name)	ベンダ
winword.exe	10000	10000	Word	Microsoft
winword.exe	0	30000	Word	Microsoft

上書きエントリを判定する場合、最大ファイルサイズ値のみが考慮されます。したがって、最大ファイルサイズが 30000 の 2 番目のエントリによって 1 番目のエントリが上書きされます。

3 （省略可能）このエントリの［Key Identifier］チェックボックスを選択します。

たとえば、［ソフトウェアディクショナリ］テーブルに、MS Word に関する次のエントリがあるとします。

ファイル名	ファイルの最終更新時	ファイルの最小サイズ	ファイルの最大サイズ	ソフトウェア名 (Software Name)	ソフトウェアバージョン	内部バージョン	説明	ベンダ
winword.exe	2004-30-10 5:30	10000	10000	Word	2002	10.0.4219	Microsoft Word	Microsoft
osa.exe	2004-30-02 16:00	10000	10000	Word	2002	10.0.4300	Microsoft Office XP Component	Microsoft

キー ID が定義されていない場合、MS Word のソフトウェア情報は、これらのどのエントリからも選択される可能性があります。

「Winword.exe」に対応する識別情報から情報が選択されるようにするには、「Winword.exe」の［Key Identifier］を選択する必要があります。［Configure Software Dictionary］テーブルでキー ID として「Winword.exe」を選択すると、Inventory Scanner は winword.exe に関連する情報をインベントリデータベースに保存します。

ソフトウェアディクショナリへのエントリの自動的な追加

1 ［Add From］ペインの［Unidentified Software］をクリックします。

2 ［Manage Unidentified Software］テーブルで、次の手順を実行します。

2a ソフトウェアディクショナリに追加するエントリを選択します。

2b ［Add To］ペインの［Software Dictionary］をクリックします。

2c ［Close］をクリックします。

ソフトウェアディクショナリからのエントリの削除

1 削除するエントリを選択します。

2 ［Delete］をクリックします。

重要： 削除できるのは、非継承エントリのみです。

ソフトウェアディクショナリのエントリの値の変更

1 [Software Dictionary] テーブルで、値を変更するエントリをダブルクリックします。

一度に 1 つのエントリのみを変更できます。

ヒント： [Row Editor] ダイアログボックスは、変更するエントリを選択し、Enter キー、Spacebar キー、または F2 キーを押して起動することもできます。

2 値を変更します。

ディクショナリ ID 属性とファイル名属性の値を変更することはできません。

3 [OK] をクリックします。

重要： 継承されたルールの値を変更することはできません。また、デフォルトの定義済みルールを変更すると、新しいユーザ定義ルールが作成されます。

ソフトウェアのスキャンからの除外

1 [Software Dictionary] テーブルで、インベントリスキャンから除外するソフトウェアに対応するエントリを選択します。

2 [Add To] ペインの [Ignore Software] をクリックします。

ソフトウェアスキャンフィルタ - [Software] の [Ignore Software] テーブルにエントリが追加されます。

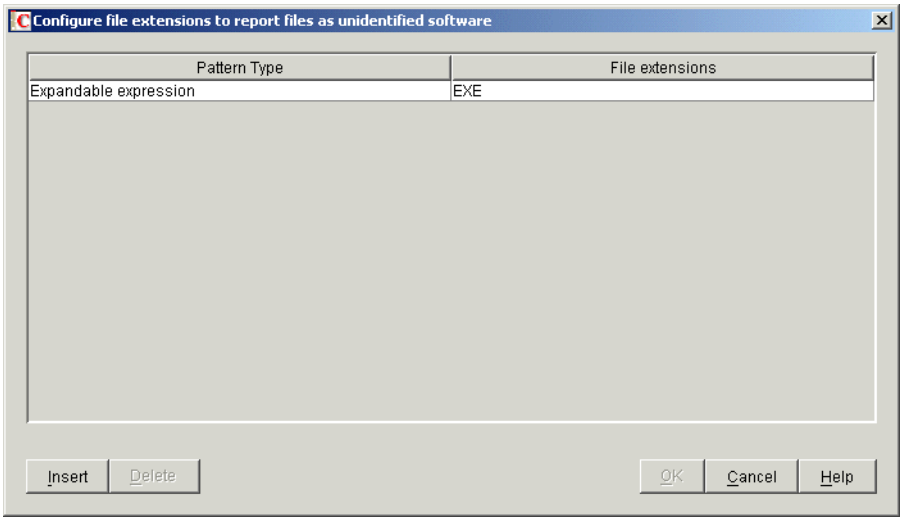
[Report Files with These File Extensions As Unidentified Software]

[Report Files with These File Extensions As Unidentified Software] ルールを使用すると、不明なソフトウェアとしてレポートする必要があるファイルのファイル拡張子を設定できます。

ルールを設定するには

1 [Edit Table] をクリックします。

[Configure File Extensions to Report Files as Unidentified Software]テーブルが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

4 ファイル拡張子を指定します。

5 [OK] をクリックします。

たとえば、拡張子が「exe」のソフトウェアを不明なソフトウェアとしてレポートするように Inventory Scanner を設定するには、テーブルで次のように設定します。

Pattern Type = Expandable expression

ファイル拡張子 = exe

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

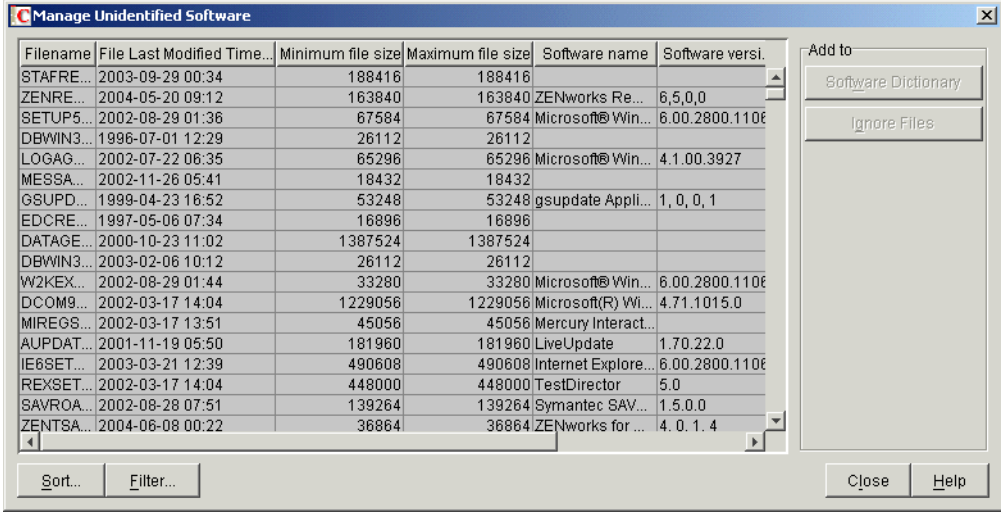
[Manage Unidentified Software]

[Manage Unidentified Software] ルールを使用すると、未定義のソフトウェアをインベントリスキャンの対象とするかどうかを設定できます。

このルールを設定するには

1 [Edit Table] をクリックします。

[Manage Unidentified Software] テーブルが表示されます。



重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

2 [Manage Unidentified Software] テーブルでは、次の操作を実行できます。

- 595 ページの「不明なソフトウェアをスキャンの対象とする」
- 595 ページの「不明なソフトウェアをスキャンから除外する」
- 616 ページの「テーブル内のエントリのソート」
- 616 ページの「テーブル内のエントリのフィルタ処理」
- 617 ページの「テーブル内のエントリの更新」

3 [OK] をクリックします。

不明なソフトウェアをスキャンの対象とする

後続のスキャンにおいて不明なソフトウェアが既知のソフトウェアとしてレポートされるようにするには、次の手順を実行します。

1 テーブル内のソフトウェアエントリを選択します。

2 [Add To] ペインの [Software Dictionary] をクリックします。

ソフトウェアディクショナリ (Software Dictionary) テーブルにエントリが自動的に追加されます。

不明なソフトウェアをスキャンから除外する

後続のスキャンにおいて不明なソフトウェアがレポートされないようにするには、次の手順を実行します。

1 テーブル内のソフトウェアエントリを選択します。

2 [Add To] ペインの [Ignore Files] をクリックします。

エントリがソフトウェアスキャンフィルタ - [Files] のテーブルに自動的に追加されます。

複数のソフトウェアバージョンのレポート

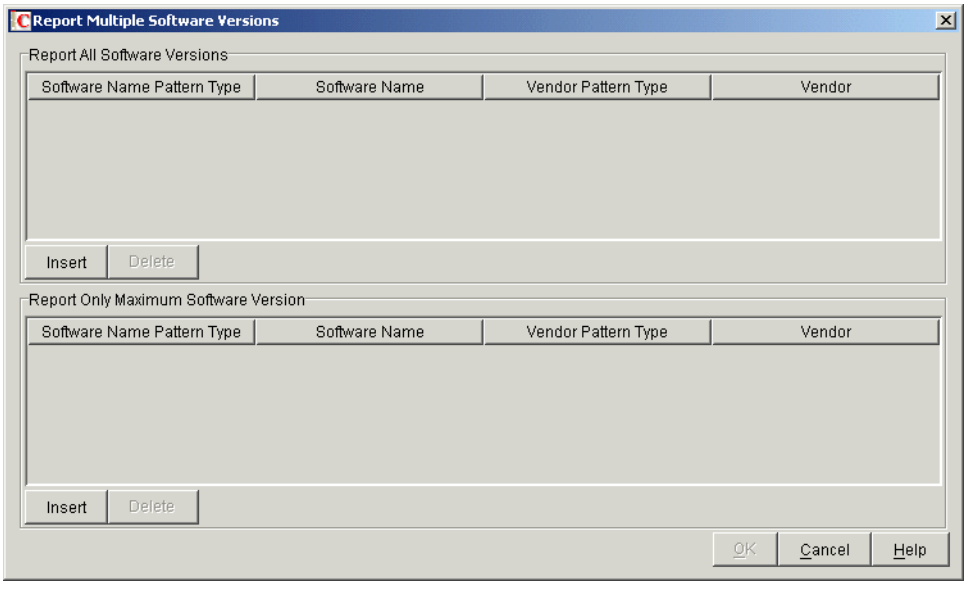
[Report Multiple Software Versions] ルールを使用すると、インベントリ対象サーバにインストールされている複数のバージョンを Inventory Scanner でレポートする対象にするソフトウェアを指定できます。

デフォルトでは、Inventory Scanner は、インベントリ対象サーバにインストールされている最新バージョンのソフトウェアをスキャンします。

このルールを設定するには

1 [Edit Table] をクリックします。

[Report Multiple Software Versions] ダイアログボックスが表示されます。



2 Inventory Scanner で、インベントリ対象サーバにインストールされているソフトウェアのすべてのバージョンをレポートするには、[Report All Software Versions] テーブルでルールを設定します。

2a [Report All Software Versions] テーブルで、[Insert] をクリックして新しい行を追加します。

2b [Software Name Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

2c ソフトウェア名を指定します。

2d （オプション）[Vendor Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

2e （オプション）ベンダ名を指定します。

たとえば、インベントリ対象サーバにインストールされている Adobe Acrobat Reader のすべてのバージョンが Inventory Scanner によってレポートされるようにするには、テーブルに次の設定を指定します。

ソフトウェア名パターンタイプ = 拡張可能な表現
ソフトウェア名 = Acrobat* Reader*
ベンダパターンタイプ = 拡張可能な表現
ベンダ名 = Adobe*

インベントリ対象サーバに Acrobat Reader 5.0 と 6.0 がインストールされている場合、Inventory Scanner は両方のバージョンの Acrobat Reader (5.0 と 6.0) をレポートします。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

3 Inventory Scanner で、インベントリ対象サーバにインストールされているソフトウェアの最新バージョンのみをレポートするには、[Report Only Maximum Software Version] テーブルでルールを設定します。

3a [Report Only Maximum Software Version] テーブルで、[Insert] をクリックして新しい行を追加します。

3b [Software Name Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

3c ソフトウェア名を指定します。

3d （オプション）[Vendor Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

3e （オプション）ベンダ名を指定します。

たとえば、インベントリ対象サーバにインストールされている Adobe Acrobat Reader の最新バージョンだけが Inventory Scanner によってレポートされるようにするには、テーブルに次の設定を指定します。

ソフトウェア名パターンタイプ = 拡張可能な表現
ソフトウェア名 = Acrobat* Reader*
ベンダパターンタイプ = 拡張可能な表現
ベンダ名 = Adobe*

インベントリ対象サーバに Adobe Acrobat Reader 4.0 と 5.0 がインストールされている場合、Inventory Scanner は Adobe Acrobat Reader 5.0 のみをレポートします。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

4 [OK] をクリックします。

デフォルトでは、scanner はインストールされているソフトウェアの最新バージョンのみをレポートします。[Report All Software Versions] のルールが [Report Only Maximum Software Version] のルールと競合する場合、[Report All Software Versions] のルールは [Report Only Maximum Software Version] のルールによって上書きされます。

たとえば、Microsoft Office を除く Microsoft ソフトウェアのすべてのバージョンが Inventory Scanner によりレポートされるように設定する一方で、インストールされている Microsoft Office の最新バージョンのみがレポートされるように設定する場合は、次のようにフィルタを設定します。

- **[Report All Software Versions]** 次の設定を指定します。

  ソフトウェア名パターンタイプ = 拡張可能な表現
  ソフトウェア名 = *
  ベンダパターンタイプ = 拡張可能な表現
  ベンダ名 = Microsoft*

- [Report Only Maximum Version] 次の設定を指定します。

  ソフトウェア名パターンタイプ = 拡張可能な表現
  ソフトウェア名 = *office*
  ベンダパターンタイプ = 拡張可能な表現
  ベンダ名 = Microsoft*

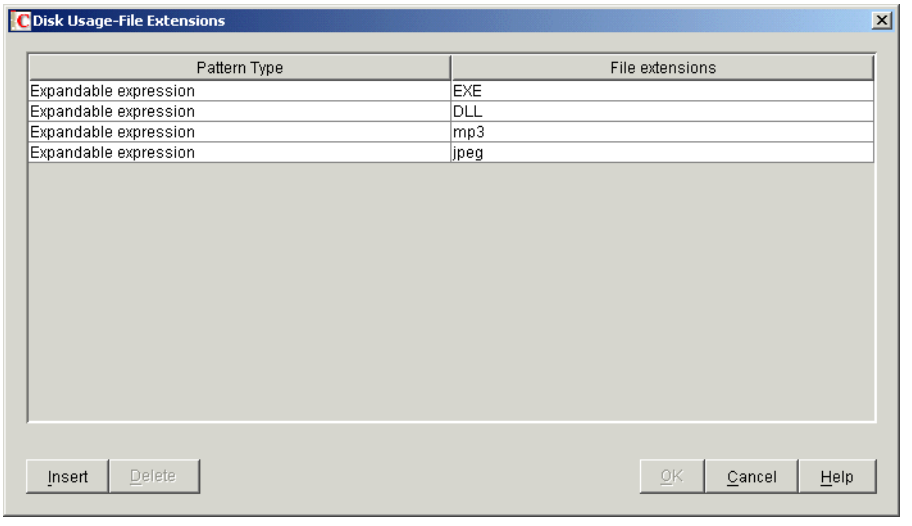
[Report Disk Space Used by File Extensions]

[Report Disk Space Used by File Extensions] ルールを使用すると、総ディスク使用量をスキャンするファイルのファイル拡張子を指定できます。

このルールを設定するには

1 [Edit Table] をクリックします。

[Disk Usage - File Extensions] テーブルが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

4 ファイル拡張子を指定します。

5 [OK] をクリックします。

たとえば、拡張子が ".pif" のすべてのファイルについて、Inventory Scanner でディスク使用状況をスキャンする場合は、[Disk Usage - File Extensions] テーブルで次のように設定します。

Pattern Type = Expandable expression
ファイル拡張子 = pif

Inventory Scanner は、拡張子が「.pif」のすべてのファイルについて総ディスク使用量をスキャンしてインベントリデータベースに保存します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Disk Usage - File Extensions] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

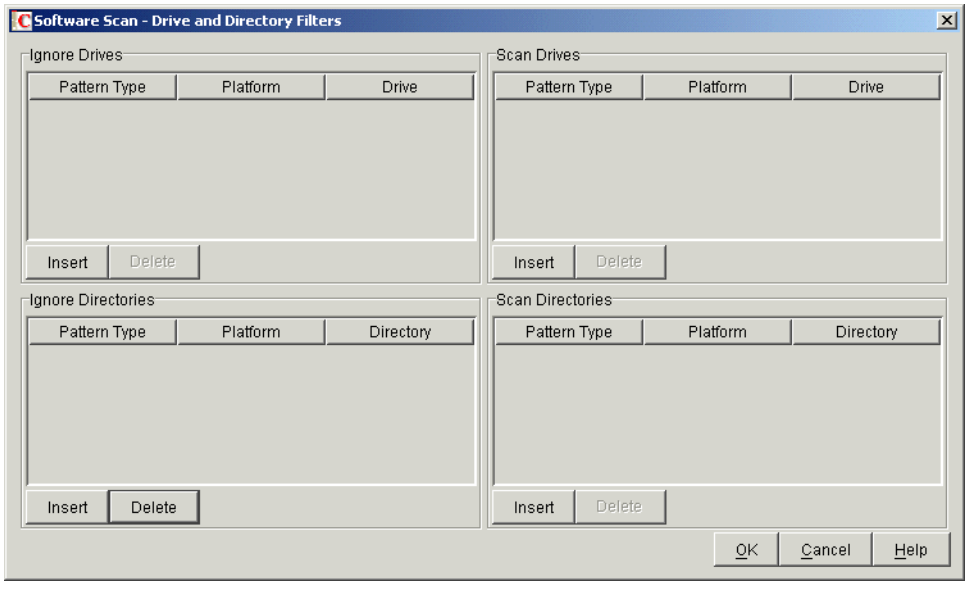
ソフトウェアスキャンフィルタ - [Drives and Directories]

[Drives and Directories] フィルタを使用すると、指定したドライブおよびディレクトリ内のソフトウェアファイルのスキャンを制御できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Software Scan - Drive and Directory Filters] ダイアログボックスが表示されます。



2 次のフィルタを設定します。

- 600 ページの「 [Ignore Drives] 」
- 600 ページの「 [Scan Drives] 」
- 601 ページの「 [Ignore Directories] 」
- 602 ページの「 [Scan Directories] 」

デフォルトでは、Inventory Scanner は、インベントリ対象サーバ上のすべてのディレクトリをスキャンします。[Ignore Directories] フィルタを使用してスキャン時にすべてのディレクトリを無視するルールを設定した一方で、特定のディレクトリをスキャン対象としたい場合は、[Scan Directories] フィルタを使用して特定のディレクトリを指定します。[Scan Directories] フィルタの設定は、[Ignore Directories] フィルタおよび [Ignore Drives] フィルタの設定を上書きします。

たとえば、Inventory Scanner で、Windows インベントリ対象サーバ上の c:¥program files ディレクトリを除く C: のすべてのファイルおよびディレクトリを無視する場合、次に示すフィルタを設定します。

- [Ignore Drives] 次の設定を指定します。

  Pattern Type = System expandable expression
  Platform = Windows
  ドライブ = C

- [Scan Directories] 次の設定を指定します。

  Pattern Type = System expandable expression
  Platform = Windows
  Drive = c:¥program files

3 [OK] をクリックします。

[Ignore Drives]

「Ignore Drives」フィルタを使用すると、インベントリ対象サーバ上でスキャンの対象としないドライブを指定できます。

デフォルトでは、Inventory Scanner はすべてのドライブをスキャンします。

このフィルタを設定するには

1 [Ignore Drives] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Any] に変更されます。この値は変更できません。

4 ドライブ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上の C ドライブにあるファイルを Inventory Scanner によるスキャンから除外する場合は、[Ignore Drives] テーブルに次の設定を指定します。

Pattern Type = System expandable expression
Platform = Windows
ドライブ = C

Inventory Scanner は、C ドライブのファイルをスキャンしません。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Ignore Drives] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

[Scan Drives]

「Scan Drives」フィルタを使用すると、インベントリ対象サーバでスキャンの対象とするドライブを指定できます。

このフィルタを設定するには

1 [Scan Drives] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。

4 ドライブ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上の C ドライブにあるファイルを Inventory Scanner でスキャンする場合は、[Scan Drives] テーブルに次の設定を指定します。

Pattern Type = System expandable expression
Platform = Windows
ドライブ = C

[Ignore Drives] テーブルに次の設定を指定する必要があります。

Pattern Type = System expandable expression
Platform = Windows
Drive = *

Inventory Scanner は、C ドライブのファイルのみをスキャンしてソフトウェア情報を確認します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Scan Drives] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

重要： デフォルトでは、Inventory Scanner は、インベントリ対象サーバ上のすべてのドライブをスキャンします。[Ignore Drives] フィルタを使用してスキャン時にすべてのドライブを無視するように設定した一方で、特定のドライブをスキャン対象としたい場合は、[Scan Drives] フィルタを使用して特定のドライブを指定します。[Scan Drives] フィルタは、[Ignore Drives] フィルタの設定を上書きします。

[Ignore Directories]

「Ignore Directories」フィルタを使用すると、インベントリ対象サーバでスキャンの対象としないディレクトリを指定できます。

デフォルトでは、Inventory Scanner はすべてのディレクトリをスキャンします。

このフィルタを設定するには

1 [Ignore Directories] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして［System expandable expression］を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、［Platform］ドロップダウンリストで［NetWare］または［Windows］を選択します。

重要： パターンタイプとして［Expandable expression］または［Regular expression］を選択すると、自動的に［Platform］列の対応する値が［Platform］に変更されます。この値は変更できません。

4 ディレクトリ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上の c:¥program files ディレクトリのファイルを Inventory Scanner によるスキャンから除外する場合は、［Ignore Directories］テーブルで次のように設定します。

Pattern Type = System expandable expression

Platform = Windows

Directory= C:¥Program Files

Inventory Scanner は、c:¥program files 内のファイルをスキャンしません。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

［Ignore Directories］テーブルからエントリを削除するには、エントリを選択し、［Delete］をクリックします。削除できるのは、非継承エントリのみです。

［Scan Directories］

「Scan Directories」フィルタを使用すると、インベントリ対象サーバでスキャンの対象とするディレクトリを指定できます。

このフィルタを設定するには

1 ［Scan Directories］テーブルで、［Insert］をクリックして新しい行を追加します。

2 ［Pattern Type］ドロップダウンリストで、［System expandable expression］、［Expandable expression］、または［Regular expression］を選択します。

3 （条件付き）パターンタイプとして［System expandable expression］を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、［Platform］ドロップダウンリストで［NetWare］または［Windows］を選択します。

重要： パターンタイプとして［Expandable expression］または［Regular expression］を選択すると、自動的に［Platform］列の対応する値が［Platform］に変更されます。この値は変更できません。

4 ディレクトリ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上で、c:¥program files ディレクトリのファイルを Inventory Scanner でスキャンする場合は、［Scan Directories］テーブルで次のように設定します。

Pattern Type = System expandable expression

Platform = Windows

Directory= C:¥Program Files

［Ignore Directories］テーブルに次の設定を指定する必要があります。

Pattern Type = System expandable expression

Platform = Windows

Directory = *

Inventory Scanner は、c:¥program files ディレクトリのファイルのみをスキャンしてソフトウェア情報を確認します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Scan Directories] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

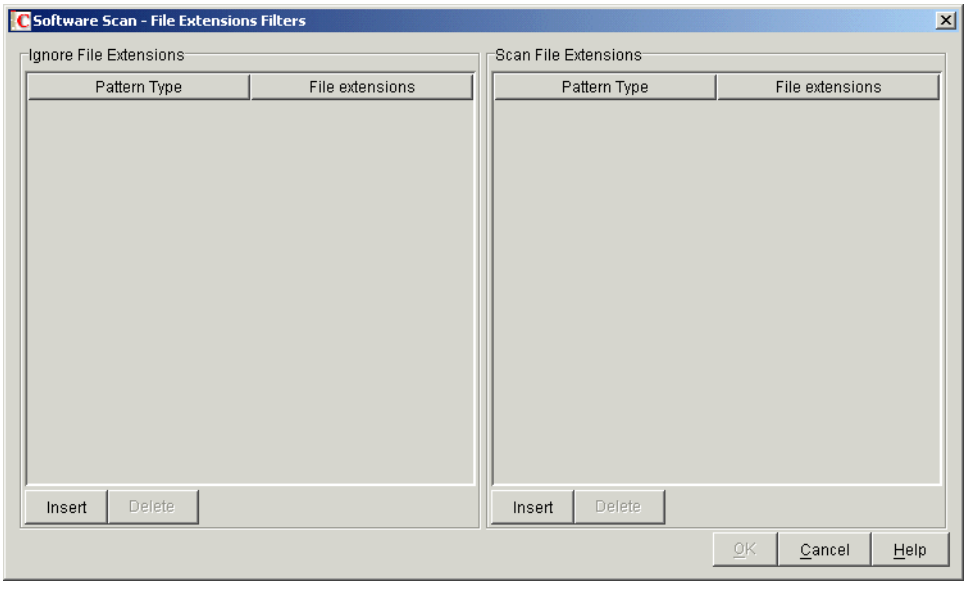
ソフトウェアスキャンフィルタ - [File Extensions]

[File Extensions] フィルタを使用すると、指定した拡張子を持つソフトウェアファイルのスキャンを制御できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Software Scan - File Extensions Filters]ダイアログボックスが表示されます。



2 次のフィルタを設定します。

- 603 ページの「[Ignore File Extensions]」
- 604 ページの「[Scan File Extensions]」

3 [OK] をクリックします。

[Ignore File Extensions]

「Ignore File Extensions」フィルタを使用すると、インベントリ対象サーバでスキャンの対象としないファイル拡張子を指定できます。

このフィルタを設定するには

1 [Ignore File Extensions] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

3 ファイル拡張子を指定します。

たとえば、拡張子が「.exe」で始まるファイルを Inventory Scanner でスキャンしない場合は、[Ignore File Extensions] テーブルに次の設定を指定します。

Pattern Type = Expandable expression
ファイル拡張子 = ex*

Inventory Scanner は、拡張子が「.ex」で始まるファイルをスキャンから除外します。たとえば、ex1、.ex2、.exe、および exec ファイルが該当します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Ignore File Extensions] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

[Scan File Extensions]

「Scan File Extensions」フィルタを使用すると、インベントリ対象サーバでスキャンの対象とするファイル拡張子を指定できます。

[Ignore File Extensions] フィルタを使用してファイル拡張子をスキャンから除外した一方で、特定のファイル拡張子をスキャン対象としたい場合は、[Scan File Extensions] フィルタを使用して特定のファイル拡張子を指定します。[Scan File Extensions] フィルタは、[Ignore File Extensions] フィルタの設定を上書きします。

このフィルタを設定するには

1 [Scan File Extensions] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

3 ファイル拡張子を指定します。

たとえば、拡張子が「.exe」のすべてのファイルを Inventory Scanner でスキャンする場合は、[Scan File Extensions] テーブルで次のように設定します。

Pattern Type = Regular expression
File Extension = [exe|EXE]

Inventory Scanner は、拡張子が「.exe」のファイルのみをスキャンしてインベントリデータベースに保存します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Scan File Extensions] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

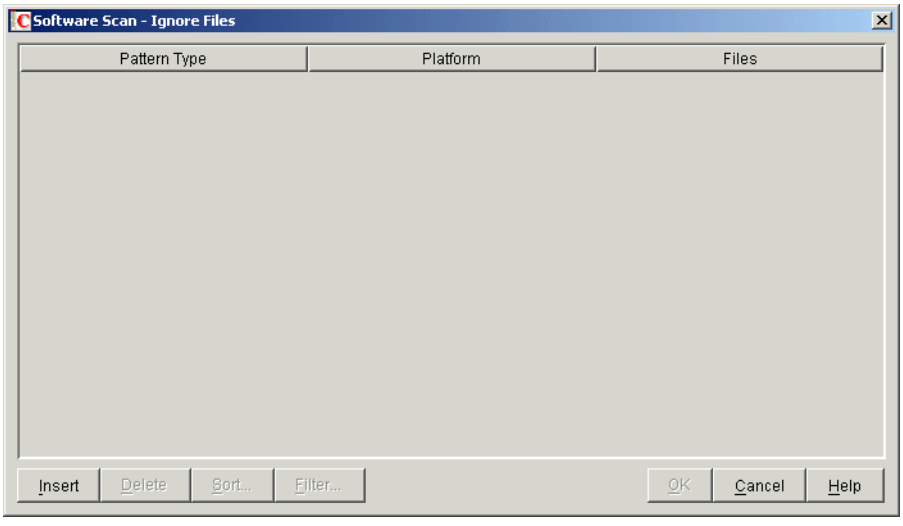
ソフトウェアスキャンフィルタ - [Files]

[Files] フィルタを使用すると、インベントリスキャン時に除外するソフトウェアを設定できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Software Scan - Ignore Files] テーブルが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

4 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Any] に変更されます。この値は変更できません。

5 ファイル名を指定します。

6 [OK] をクリックします。

たとえば、Inventory Scanner ですべての Windows インベントリ対象サーバ上にある notepad.exe をスキャンする場合は、次のように設定します。

Platform = Windows

Pattern Type = System expandable expression

ファイル =notepad.exe

このテーブルには、[Manage Unidentified Software] テーブルから追加されたファイルも表示されます。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Software Scan - File Filters] テーブルでは、次の操作を実行することもできます。

- 削除できるのは、非継承エントリのみです。
- テーブル内のエントリのソート .
- テーブル内のエントリのフィルタ処理 .
- テーブル内のエントリの更新 .

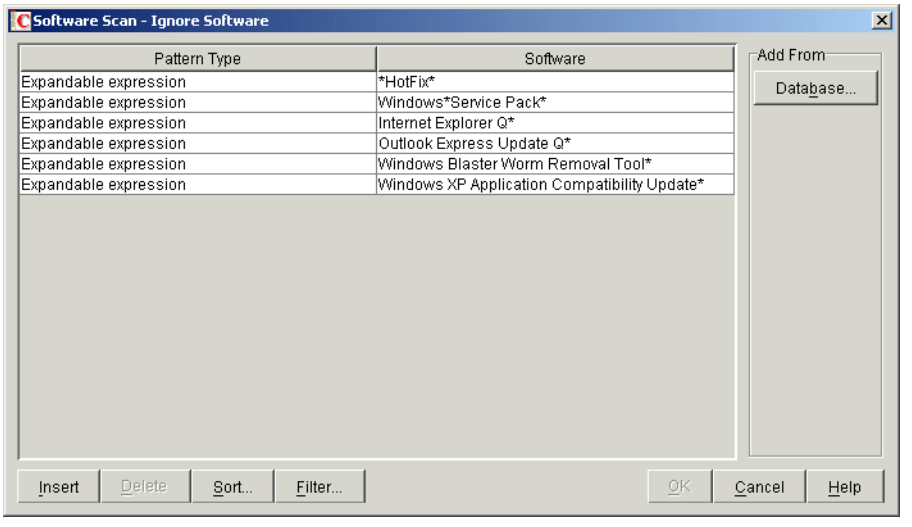
ソフトウェアスキャンフィルタ - [Software]

[Software] フィルタを使用すると、インベントリスキャン時にレポートされないソフトウェアを設定できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Software Scan - Ignore Software] テーブルが表示されます。



2 [Ignore Software] テーブルには、手動でまたは自動的にエントリを追加できます。

手動によるテーブルへのエントリの追加

1. [Insert] をクリックして新しい行を追加します。
2. [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。
3. ソフトウェア名を指定します。
4. [OK] をクリックします。

たとえば、Inventory Scanner で Adobe 製品をスキャンしないように設定するには、次のように設定します。

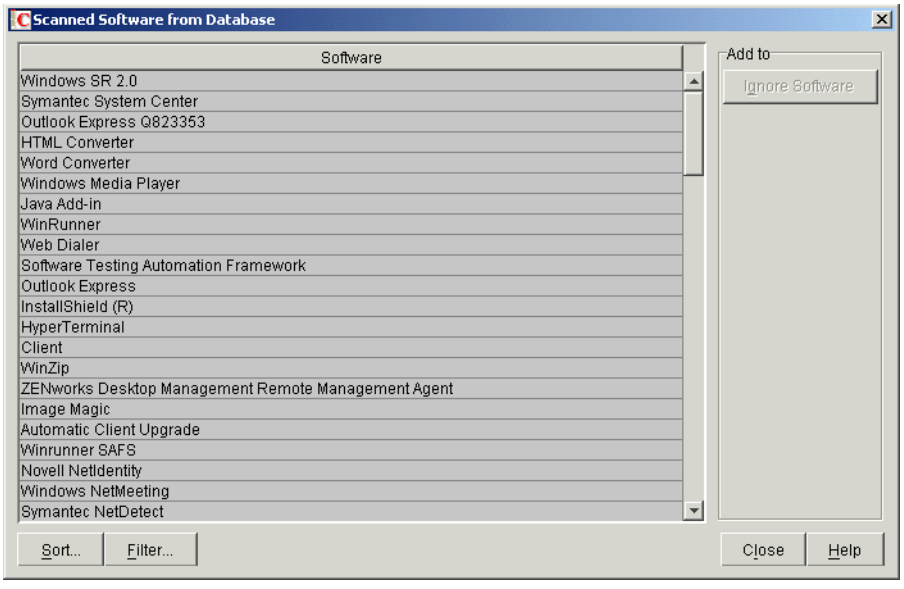
Pattern Type = Expandable expression

Software = Adobe*

Inventory Scanner は、名前が「Adobe」で始まるソフトウェアをレポートから除外します。

自動的なテーブルへのエントリの追加

1. [Add From] ペインの [Database] をクリックします。
   [Scanned Software from Database] ダイアログボックスが表示されます。



2. [Ignore Software] テーブルに追加するソフトウェアを選択します。
3. [Add to] ペインの [Ignore Software] ボタンをクリックします。
4. [Close] をクリックします。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Software Scan - Ignore Software] テーブルでは、次の操作を実行することもできます。

- 削除できるのは、非継承エントリのみです。
- テーブル内のエントリのソート .
- テーブル内のエントリのフィルタ処理 .
- テーブル内のエントリの更新 .

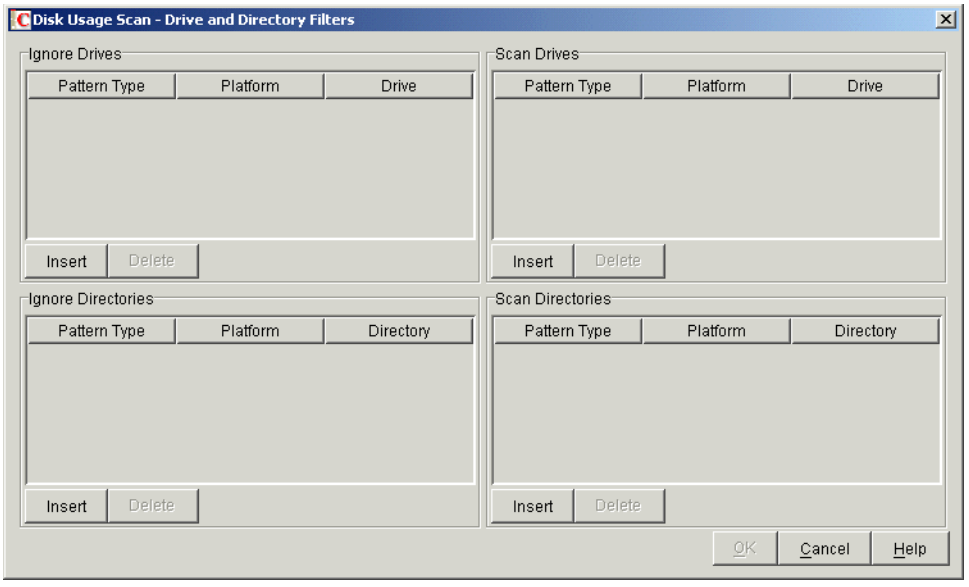
ディスク使用状況スキャンフィルタ - [Drives and Directories]

[Drives and Directories] フィルタを使用すると、インベントリディスク使用状況スキャン時に含めるまたは除外するドライブおよびディレクトリを指定できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Disk Usage Scan - Drive and Directory Filters] ダイアログボックスが表示されます。



2 次のフィルタを設定します。

- 609 ページの「[Ignore Drives]」
- 609 ページの「[Scan Drives]」
- 610 ページの「[Ignore Directories]」
- 611 ページの「[Scan Directories]」

デフォルトでは、Inventory Scanner は、インベントリ対象サーバ上のすべてのディレクトリのディスク使用状況をスキャンします。[Ignore Directories] フィルタを使用してディスク使用状況スキャン時にすべてのディレクトリを無視するように設定した一方で、特定のディレクトリをスキャン対象としたい場合は、[Scan Directories] フィルタを使用して特定のディレクトリを指定します。[Scan Directories] フィルタの設定は、[Ignore Directories] フィルタおよび [Ignore Drives] フィルタの設定を上書きします。

たとえば、Inventory Scanner で、Windows インベントリ対象サーバ上の c:¥program files ディレクトリを除く C: のすべてのファイルおよびディレクトリのディスク使用状況を無視する場合、次に示すフィルタを設定します。

- **[Ignore Drives]** 次の設定を指定します。

  Pattern Type = System expandable expression
  Platform = Windows
  ドライブ = C

- **[Scan Directories]** 次の設定を指定します。

  Pattern Type = System expandable expression
  Platform = Windows
  Drive=c:¥program files

3 [OK] をクリックします。

[Ignore Drives]

「Ignore Drives」フィルタを使用すると、インベントリ対象サーバ上でディスク使用状況をスキャンの対象としないドライブを指定できます。

デフォルトでは、Inventory Scanner はすべてのドライブをスキャンします。

[Ignore Drives] フィルタを設定するには

1 [Ignore Drives] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。

4 ドライブ名を指定します。

たとえば、すべての Windows* インベントリ対象サーバ上の C ドライブのディスク使用状況を Inventory Scanner によるスキャンから除外する場合は、[Ignore Drives] テーブルに次の設定を指定します。

Pattern Type = System expandable expression
Platform = Windows
ドライブ = C

Inventory Scanner は、C ドライブのファイルのディスク使用状況をスキャンから除外します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Ignore Drives] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

[Scan Drives]

「Scan Drives」フィルタを使用すると、インベントリ対象サーバでディスク使用状況をスキャンの対象とするドライブを指定できます。

[Scan Drives] フィルタを設定するには

1 [Scan Drives] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。

4 ドライブ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上の C ドライブのディスク使用状況を Inventory Scanner でスキャンする場合は、[Scan Drives] テーブルに次の設定を指定します。

Pattern Type = System expandable expression

Platform = Windows

ドライブ = C

Inventory Scanner は、C ドライブのファイルのディスク使用状況をスキャンしてインベントリデータベースに保存します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Scan Drives] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

重要： デフォルトでは、Inventory Scanner は、インベントリ対象サーバ上のすべてのドライブのディスク使用状況をスキャンします。[Ignore Drives] フィルタを使用してディスク使用状況スキャン時にすべてのドライブを無視するように設定した一方で、特定のドライブをスキャン対象としたい場合は、[Scan Drives] フィルタを使用して特定のドライブを指定します。[Scan Drives] フィルタは、[Ignore Drives] フィルタの設定を上書きします。

[Ignore Directories]

「Ignore Directories」フィルタを使用すると、インベントリ対象サーバでディスク使用状況をスキャンの対象としないディレクトリを指定できます。

デフォルトでは、Inventory Scanner はすべてのディレクトリをスキャンします。

[Ignore Directories] フィルタを設定するには

1. [Ignore Directories] テーブルで、[Insert] をクリックして新しい行を追加します。
2. [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。
3. （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

   重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。
4. ディレクトリ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上の c:¥program files ディレクトリを Inventory Scanner によるディスク使用状況のスキャンから除外する場合は、[Ignore Directories] テーブルで次のように設定します。

Pattern Type = System expandable expression

Platform = Windows

Directory= c:¥program files

Inventory Scanner は c:¥program files のディスク使用状況をスキャンしません。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Ignore Directories] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

[Scan Directories]

「Scan Directories」フィルタを使用すると、インベントリ対象サーバでディスク使用状況をスキャンの対象とするディレクトリを指定できます。

[Scan Directories] フィルタを設定するには

1 [Scan Directories] テーブルで、[Insert] をクリックして新しい行を追加します。

2 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

3 （条件付き）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムによって、[Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。

4 ディレクトリ名を指定します。

たとえば、すべての Windows インベントリ対象サーバ上で、c:¥program files ディレクトリのディスク使用状況を Inventory Scanner でスキャンする場合は、[Scan Directories] テーブルで次のように設定します。

Pattern Type = System expandable expression

Platform = Windows

Directory= c:¥program files

Inventory Scanner は、c:¥program files のファイルのディスク使用状況のみをスキャンしてインベントリデータベース内に保管します。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Scan Directories] テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

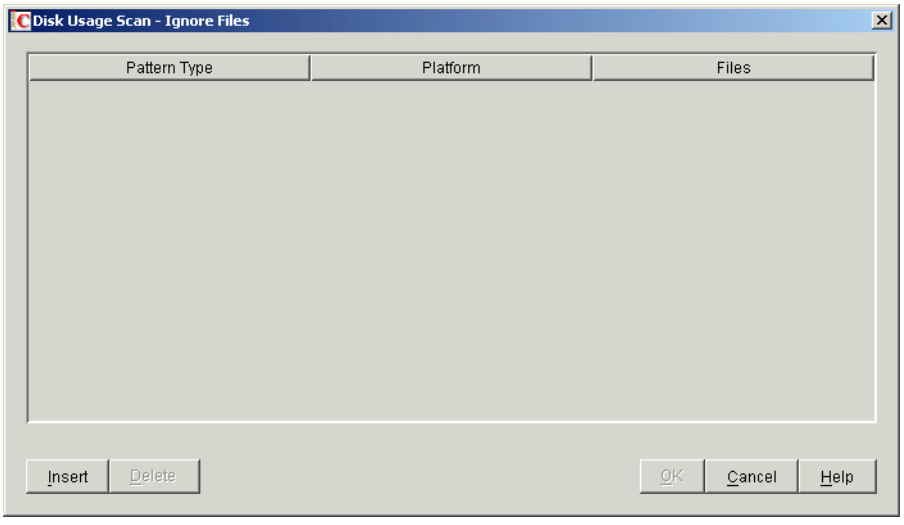
ディスク使用状況スキャンフィルタ - [Files]

[Files] フィルタを使用すると、インベントリディスク使用状況スキャン時に除外するファイルを設定できます。

このフィルタを設定するには

1 [Edit Table] をクリックします。

[Disk Usage Scan - Ignore Files] ダイアログボックスが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[System expandable expression]、[Expandable expression]、または [Regular expression] を選択します。

4 （条件）パターンタイプとして [System expandable expression] を選択した場合は、インベントリ対象サーバのオペレーティングシステムに応じて [Platform] ドロップダウンリストで [NetWare] または [Windows] を選択します。

重要： パターンタイプとして [Expandable expression] または [Regular expression] を選択すると、自動的に [Platform] 列の対応する値が [Platform] に変更されます。この値は変更できません。

5 ファイルを指定します。

6 [OK] をクリックします。

たとえば、msoffice.exe を除き、拡張子が「.exe」のすべてのファイルについてディスク使用状況をスキャンする場合は、次のようにルールを設定します。

- **ディスク使用状況スキャン - 無視するファイル：** 次の設定を指定します。

  Pattern Type = Expandable expression
  ファイル = msoffice.exe

- **[Report Disk Space used by file extensions]** 次の設定を指定します。

  Pattern Type = Expandable expression
  ファイル = exe

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

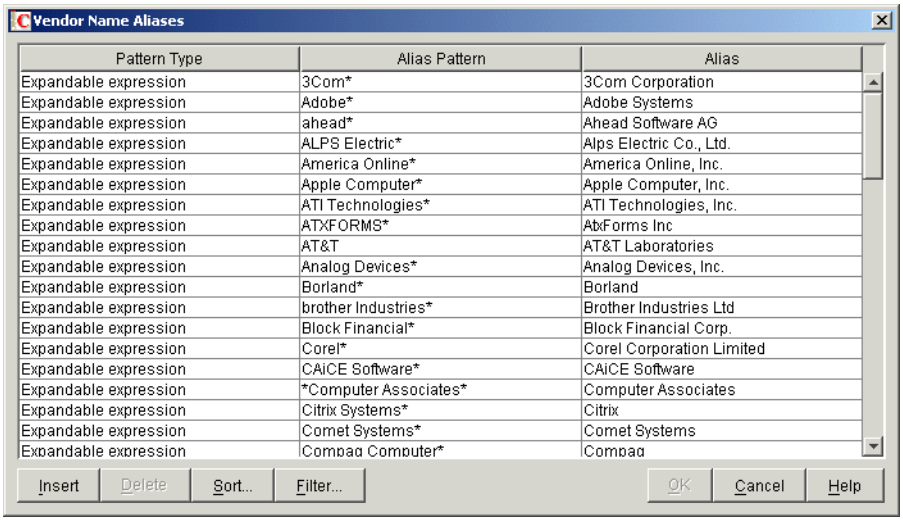
テーブルからエントリを削除するには、エントリを選択し、[Delete] をクリックします。削除できるのは、非継承エントリのみです。

[Vendor Name Aliases]

「ベンダ名の別名」ルールを使用すると、ベンダ名の別名を設定することができます。

1 [Edit Table] をクリックします。

[Vendor Name Aliases] テーブルが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

4 別名パターンを指定します。

5 別名を指定します。

6 [OK] をクリックします。

たとえば、「Microsoft」で始まるベンダ名のすべてのインスタンスを、Inventory Scanner で「Microsoft Corporation」としてインベントリデータベースにレポートする場合は、次のように設定します。

Pattern Type = Expandable expression

別名パターン = Microsoft*

Alias = Microsoft Corporation

Inventory Scanner から Microsoft、Microsoft Inc.、Microsoft Inc. Corporation がレポートされた場合、「Microsoft」で始まるベンダの名前は「Microsoft Corporation」としてインベントリデータベースに保存されます。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Vendor Name Aliases] テーブルでは、次の操作を実行することもできます。

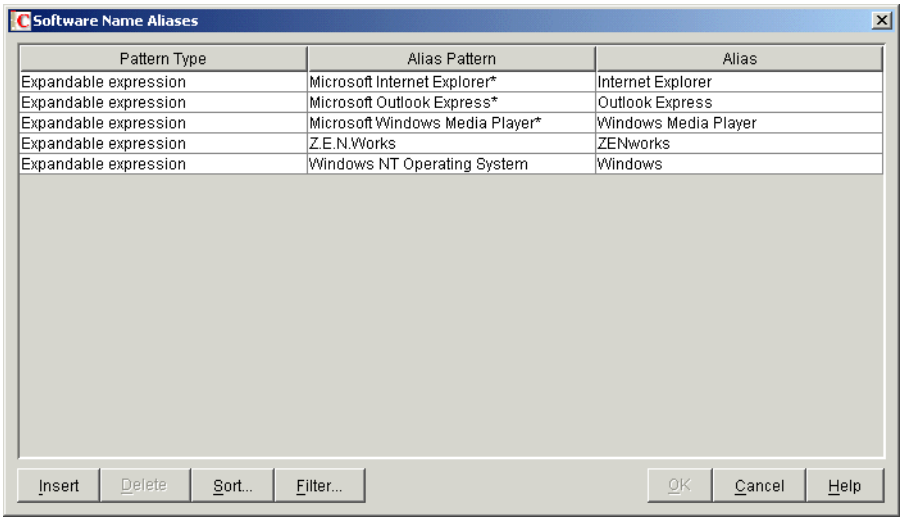
- 削除できるのは、非継承エントリのみです。
- テーブル内のエントリのソート .
- テーブル内のエントリのフィルタ処理 .
- テーブル内のエントリの更新 .

[Software Name Aliases]

[Software Name Aliases] ルールを使用すると、ソフトウェア名の別名を設定することができます。

1 [Edit Table] をクリックします。

[Software Name Aliases] テーブルが表示されます。



2 [Insert] をクリックして新しい行を追加します。

3 [Pattern Type] ドロップダウンリストで、[Expandable expression] または [Regular expression] を選択します。

4 別名パターンを指定します。

5 別名を指定します。

6 [OK] をクリックします。

たとえば、インベントリデータベース内で製品名が「WinZip」のすべてのインスタンスを、Inventory Scanner で「WinZip Application」としてインベントリデータベースにレポートする場合は、次のように設定します。

Pattern Type = Expandable expression

別名パターン = WinZip

Alias = WinZip Application

Inventory Scanner により WinZip、WinZip Executables、または WinZip Applications 製品名がスキャンされた場合、「WinZip」と完全に一致するソフトウェアの名前は「WinZip Application」としてインベントリデータベースに保存されます。残りのソフトウェアの名前は、スキャンされたとおりにレポートされます。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

[Software Name Aliases] テーブルでは、次の操作を実行することもできます。

- 削除できるのは、非継承エントリのみです。
- テーブル内のエントリのソート .
- テーブル内のエントリのフィルタ処理 .
- テーブル内のエントリの更新 .

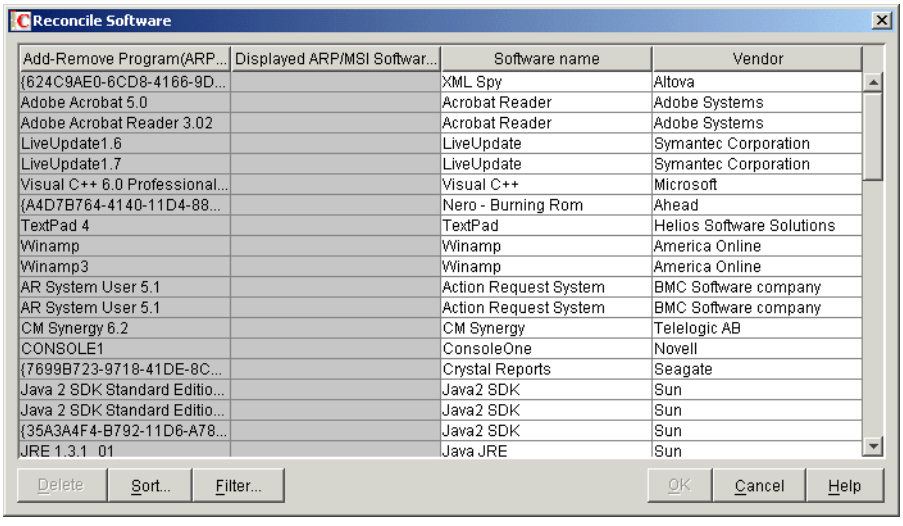
[Reconcile Software]

[Reconcile Software] ルールを使用すると、[プログラムの追加と削除] または MSI で識別されたソフトウェアを、ソフトウェアディクショナリを介して識別および設定された適切なソフトウェアおよびベンダに関連付けることができます。ZENworks ソフトウェアディクショナリに設定されているのと同じソフトウェア名およびベンダが [プログラムの追加と削除] または MSI のソフトウェアエントリに使用されているとは限らないので、関連付けは必要です。

ルールを設定するには

1 [Edit Table] をクリックします。

[Reconcile Software] テーブルが表示されます。



デフォルトでは、[Reconcile Software] テーブルには、ソフトウェアディクショナリに設定されているソフトウェアとともに、[プログラムの追加と削除] または MSI のソフトウェアの定義済みマッピングが表示されます。また、ソフトウェアとベンダ名を設定する最後のスキャン時に識別された [プログラムの追加と削除] または MSI ソフトウェアも表示されます。この表には次の列があります。

- プログラムの追加と削除 (ARP) キー。

  この属性の値は変更できません。

- [プログラムの追加と削除] または MSI に表示される ARP/MSI 名。

  [Displayed ARP/MSI Software] 名には、[プログラムの追加と削除] または MSI を介して識別され、インベントリデータベースに格納されているソフトウェアが表示されます。

この属性の値は変更できません。

- 対応する［プログラムの追加と削除］または MSI 名に関連付けられたソフトウェア名。
- 対応する［プログラムの追加と削除］または MSI 名に関連付けられたベンダ名。

重要： 継承されたルールがテーブルに含まれることがあります。これらのルールは、ディクショナリ更新ポリシーで設定されたインベントリサーバのソフトウェアディクショナリだけで編集または削除できます。ZENworks 6.5 SP1 インベントリサーバのソフトウェアディクショナリにアクセスすると、これらのルールは濃い灰色で表示されます。

2 ソフトウェアを照合するには、このテーブル内で次の操作を行います。

- ［プログラムの追加と削除］または MSI を介して識別され、まだ関連付けられていないソフトウェアのソフトウェア名およびベンダ名を指定します。
- （オプション）ソフトウェアディクショナリ内で設定されているソフトウェアのソフトウェア名およびベンダ名を変更します。

［Reconcile Software］テーブルでは、次の操作を実行することもできます。

- 削除できるのは、非継承エントリのみです。
- テーブル内のエントリのソート .
- テーブル内のエントリのフィルタ処理 .
- テーブル内のエントリの更新 .

テーブル内のエントリのソート

テーブル内のエントリを、1 つ、2 つ、または 3 つの列を使用してソートできます。

1 ［Sort］をクリックします。

［Sort］ダイアログボックスが表示されます。

2 ［Sort by］ドロップダウンリストから、エントリをソートするテーブルの列を選択します。

3 ［Ascending］または［Descending］を選択します。

4 （オプション）2 列または 3 列にソートするには、［Then by］ドロップダウンリストを設定して、［Ascending］または［Descending］を選択します。

5 ［OK］をクリックします。

テーブル内のエントリのフィルタ処理

1 ［Filter］をクリックします。

［Filter］ダイアログボックスが表示されます。

2 ［Filter］ダイアログボックスで、次の操作を行って照会を作成します。

2a 属性を選択します。

2b 演算子を選択します。表示される演算子は、手順 2a で選択した属性によって異なります。

2c 値を入力します。

2d（オプション）高度な照会を作成するには、次のいずれかの論理演算子を選択し、照会を定義します。

論理演算子	機能
AND:	新しい行を作成します。このフィルタは、AND で結合された各行の条件に一致する項目を表示します。
または	新しい行を作成します。フィルタは、OR で結合されたどちらかの行の条件に一致する項目を表示します。
[New Row]	新しい照会のために新しい行を作成します。
[Delete Row]	フィルタから行を削除します。
[End]	照会式を閉じます。他の行がその後に続く行において［End］を選択した場合、後続の行およびグループは削除されます。

3［OK］をクリックします。

フィルタを適用した後、テーブルリストには結果のエントリだけが表示されます。
フィルタをクリアするには

1［Filter］をクリックします。

［Filter］ダイアログボックスが表示されます。

2［Clear］をクリックし、［OK］をクリックします。

テーブル内のエントリの更新

ソートまたはフィルタ操作を再び適用する場合は、［Refresh］オプションを使用してください。テーブルのエントリを更新するには、［Refresh］をクリックするか、F5 を押します。

重要： ［Refresh］ボタンは、テーブルにソートまたはフィルタ操作を適用した場合にのみ表示されます。

ソフトウェアディクショナリの展開に関する基準の設定

初めてソフトウェアディクショナリを展開する際、デフォルトのディクショナリ設定が有効になり、Inventory Scanner によって次の情報が収集されます。

- 不明なソフトウェア
- 同一インベントリ対象サーバにインストールされた複数のソフトウェアインスタンス
- ソフトウェアを含まない冗長ドライブおよびディレクトリ

このスキャンによって、無関係な大量の情報がインベントリデータベースに保存されます。またこのスキャンにより、Storer やすべての Inventory ConsoleOne ユーティリティ（照会、レポート生成など）のパフォーマンスが低下します。

こうした問題を回避するため、企業内にソフトウェアディクショナリを展開する前に、それぞれの要件に合わせてソフトウェアディクショナリの微調整を行うことをお勧めします。ソフトウェアディクショナリの微調整を行うには、次の手順を実行します。

1 数台のインベントリ対象サーバで構成される、小規模な見本セットをテスト環境に展開します。

注： 一般にこの見本セットは、インベントリ情報の収集対象となる企業のすべての部門の環境を表している必要があります。

2 テストラボに展開されたスタンドアロンインベントリサーバに、これらのインベントリ対象サーバを接続します。

3 [Report Files with These File Extensions As Unidentified Software]のルールに関する表に記載されたデフォルトの条件に加えて、他のファイル拡張子をスキャンの対象に含めることにより、これらのファイルを識別されたソフトウェアとしてレポートすることができます。DLL などのアプリケーションファイルの拡張子を設定することができます。

4 スキャンのスケジュールを設定した後、インベントリデータベースにインベントリ情報が保存されるのを待ちます。

5 このデータベース内のインベントリ情報に基づいてソフトウェアディクショナリを再設定することで、問題を解決できます。

- **不明なソフトウェア：** [Report Files with These File Extensions As Unidentified Software] 設定に基づいて、不明なソフトウェアに関連するすべての情報を [Manage Unidentified Software] テーブルに表示できます。

  この結果には次のものが含まれます。

  - まだソフトウェアディクショナリによって識別されていないアプリケーション。
  - ソフトウェアディクショナリによってすでに識別されているアプリケーションファイル。
  - 必要のないアプリケーション。たとえば、オペレーティングシステムファイル、DOS ファイルなど。

  [Manage Unidentified Software] テーブルで、次の作業を実行します。

  - [Add To] ペインにある [Software Dictionary] ボタンを使用して、ソフトウェアディクショナリでまだ識別されていないアプリケーションをソフトウェアディクショナリ (Software Dictionary) に追加します。
  - [Add To] ペインにある [Ignore Files] ボタンを使用して、ソフトウェアディクショナリによってすでに識別されているアプリケーションファイルと冗長なアプリケーションファイルをソフトウェアスキャンフィルタ - [Files] テーブルに追加します。

  この操作が有効となるのは、次の前提が満たされている場合です。

  - この代表セットは、多数の不明なソフトウェアがスキャンされ、報告される点以外は、企業の部署と同じものである必要があります。
  - 企業のインベントリ対象サーバは、非標準アプリケーションをインストールおよびコピーする企業内の管理者によって、広く管理されています。

- **同じインベントリ対象サーバにおける複数のソフトウェアインスタンス** インベントリ対象サーバで、[プログラムの追加と削除] スキャンまたはMSI スキャンから 1 つのエントリがレポートされたが、ソフトウェアディクショナリの設定からも別のエントリがレポートされた場合、同一ソフトウェアが 2 度レポートされることになります。615 ページの「[Reconcile Software]」ルールには、デフォルトの設定が含まれており、こうした 2 つのエントリを統合しますが、この統合が完全には動作しない場合があります。この問題を解決するには、「Edit Add-Remove Software」ルールを手動で設定する必要があります。
- **ソフトウェアを含まない冗長ドライブおよびディレクトリ：**ソフトウェアディクショナリの [Software Scanning] ページおよび [Disk Usage Scanning] ページでルールを設定し、こうしたドライブおよびディレクトリをスキャン対象から除外します。ソフトウェアディクショナリのルールに関する詳細については、587 ページのステップ 3 を参照してください。

6 すべてのインベントリ対象サーバに対し再びスキャンを実行します。

7 インベントリ情報がインベントリデータベースに保存された後、前のスキャンでディクショナリに対してマークしたすべてのエントリがソフトウェアとしてスキャンされ、レポートされるはずです。

8 要件が満たされるまで手順 3 から 7 を繰り返し、微調整を実行します。

[Inventory Summary] でのソフトウェアインベントリ情報の表示

[Inventory Summary] にインベントリ対象サーバのソフトウェアインベントリ情報を表示するには

1 ConsoleOne で、インベントリデータベースを設定します。インベントリデータベースの設定方法の詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

2 インベントリ対象サーバを右クリックし、[Actions]、[Inventory] の順にクリックします。

3 [Summary] ダイアログボックスで、[Inventory Information] > [Hardware/Software Inventory] > [Software] > [Application Vendors] の順にクリックしてソフトウェアインベントリ情報を表示します。

アプリケーションベンダを選択する際に、ベンダの製品グループおよび製品のリストが表示されます。ソフトウェアグループには、ソフトウェアパッチ、およびグループの代表的なファイル情報が含まれることがあります。ソフトウェアには、ソフトウェアパッチ、および製品の代表的なファイル情報が含まれることがあります。

詳細については、を参照してください。626 ページの「インベントリ対象サーバのインベントリサマリの表示」

ソフトウェアインベントリレポートの生成

このリリースでは、次のソフトウェアインベントリレポートを生成できます。

- Add-Remove Programs by Machine
- Anti-Virus Signature Files by Machine
- Anti-Virus Signature Machine Count
- Disk Usage by Machine
- Exception List by Machine

- Installed NetWare Software by Machine
- Internet Explorer Installation Count
- Internet Explorer Patches by Machine
- Internet Explorer by Machine
- MSI Products by Machine
- Microsoft Office Components by Machine
- Microsoft Office Installation Count
- Microsoft Office by Machine
- Novell Client Components by Machine
- Novell Installation Count
- Novell Client by Machine
- Novell ZENworks Desktop Management Installed Agent Components by Machine
- Novell ZENworks Desktop Management Installed Server Components by Machine
- Novell ZENworks Handheld Management Installed Components by Machine
- Novell ZENworks Installed Components by Machine
- Novell ZENworks Installed Suites by Machine
- Novell ZENworks Server Management Installed Agent Components by Machine
- Novell ZENworks Server Management Installed Server Components by Machine
- Outlook Express Installation Count
- Outlook Express by Machine
- Software Dictionary Application Files by Machine
- Software Dictionary Applications by Machine
- Software Dictionary Versions Machine Count
- Software Dictionary Versions by Machine
- Software Installation Count
- Software Installations
- Software by Machine
- System Software Inventory Report
- Windows Components by Machine
- Windows Installation Count
- Windows Media Player Count
- Windows Media Player Patches by Machine
- Windows Media Player by Machine
- Windows Operating System by Machine
- Windows Security Patches by Machine

各レポートの詳細については、642 ページの「インベントリレポートの種類」を参照してください。

ZENworks for Servers 3.*X*インベントリ対象サーバのスキャン対象ソフトウェアインベントリ情報のカスタマイズ

ZENworks for Servers 3.*x*インベントリ対象サーバのソフトウェアインベントリ情報をカスタマイズする方法については、ZENworks for Servers 3.0.2 Documentation Web サイト (http://www.novell.com/documentation/zfs302/index.html) を参照してください。

インベントリデータベースからの重複するインベントリ対象サーバの削除

Inventory Removal Service は、インベントリサーバ上で実行する手動によるサービスです。Inventory Removal Service を使用すると、インベントリデータベースから、不必要なインベントリ対象サーバ、重複するインベントリ対象サーバ、または古くなったインベントリ対象サーバを削除できます。Inventory Removal Service は、serverremovallist.txt ファイルを使用して、インベントリデータベースからインベントリ対象サーバを削除します。

serverremovallist.txt ファイルには、インベントリデータベースから削除する必要があるインベントリ対象サーバのリストが含まれます。

重要： 中間サーバにインベントリ対象サーバまたはデータベースが接続されている場合のみ、中間サーバで Inventory Removal Service を実行できます。

インベントリデータベースからインベントリ対象サーバを削除するには

1 テキストエディタを使用して、次の内容のファイルを作成し、ファイル名を serverremovallist.txt と付けます。

```
;                       Enter comments, if any

DN of the inventoried server (as stored in the Inventory database) to be
removed from the Inventory database

DN of the inventoried server (as stored in the Inventory database) to be
removed from the Inventory database

...

...

DN of the inventoried server (as stored in the Inventory database) to be
removed from the Inventory database
```

削除する必要があるインベントリ対象サーバのリストを生成するには、選択された基準に基づいて照会を実行するか、インベントリ対象サーバの名前を手動で入力します。照会の詳細については、638 ページの「データベース照会によるインベントリ対象サーバのインベントリ情報の表示」を参照してください。

2 serverremovallist.txt ファイルを Netware インベントリサーバの *Inventory_server_installation_path*¥inv¥server¥wminv¥properties ディレクトリおよび Windows インベントリサーバの C:¥ ディレクトリにコピーします。

注： serverremoval.properties ファイルには、プロパティ FilePath が含まれます。これは、serverremovallist.txt ファイルのパスです。デフォルトのパスは、sys:/inv/server/wminv/properties です。serverremovallist.txt をデフォルトパス以外のパスにコピーする場合は、serverremoval.properties ファイルの FilePath の値を新しいパスに更新する必要があります。パスの区切り文字が「¥」ではなく、「/」であることを確認します。

3 サーバコンソールのプロンプトで、「**StartSer RemoveInventory**」と入力して Inventory Removal Service を起動します。

Inventory Removal Service の詳細については、次の節を参照してください。

- 622 ページの「Inventory Removal Service プロセスについて」
- 622 ページの「Inventory Removal Service を使用した同期」

Inventory Removal Service プロセスについて

Inventory Removal Service は次の処理を実行します。

1 Inventory Removal Service は、serverremovallist.txt ファイルの各行を読み込み、serverremovallist.txt ファイルに表示された各インベントリ対象サーバの delete str ファイルを作成します。

delete str ファイルは、¥scandir ディレクトリに保存されます。

2 Selector は、delete str ファイルを検証し、¥dbdir ディレクトリおよび ¥entmergedir ディレクトリにコピーします。

3 Storer は、¥dbdir ディレクトリから delete str ファイルを読み込み、接続されているインベントリデータベースからインベントリ対象サーバを削除します。

4 インベントリ展開でインベントリ情報をロールアップする場合、削除 str も次のレベルのインベントリサーバにロールアップされます。

インベントリ対象サーバは、企業レベルで展開されているすべてのインベントリサーバのインベントリデータベースから削除されます。

Inventory Removal Service を使用した同期

Inventory Removal Service は、対応するサーバオブジェクトが eDirectory から削除されると、自動的にインベントリデータベースからインベントリ対象サーバを削除します。

次の理由から、eDirectory とインベントリデータベースにあるインベントリ対象サーバが同期していないことがあります。

- Inventory Service Manager を強制終了し、eDirectory のいくつかのサーバオブジェクトを削除して、Inventory Service Manager を再起動した場合。
- eDirectoryから削除済みのサーバが含まれている以前のバージョンのインベントリデータベースを再起動した場合。

この場合、Inventory Removal Service を使用してインベントリデータベースから不要なインベントリ対象サーバを削除し、データベースを再度 eDirectory と同期させます。

インベントリ対象サーバの完全修飾 DN 名がわかっている場合は、serverremovallist.txt ファイルにこれらのサーバの DN 名を指定できます。

eDirectory から削除されたサーバオブジェクトを検索するには

1. NDSREPAIR などの eDirectory ツールを使用して、インベントリサーバに接続されているサーバオブジェクトのリストをエクスポートします。eDirectory ツールは、Cool Solutions の Web サイト（http://www.novell.com/coolsolutions/freetools.html）からダウンロードできます。
2. すべてのサーバオブジェクトを .csv ファイルにエクスポートするには、データエクスポートウィザードを使用します。

   注： すべてのインベントリ対象サーバを .csv ファイルにエクスポートしている間に、属性を選択する必要があります。

   エクスポート先の .csv ファイルには、インベントリ対象サーバの DNS 名と選択した属性が含まれます。ただし、.csv ファイルから属性値と二重引用符を削除する必要があります。
3. ファイル比較ユーティリティを使用して eDirectory のエクスポートされたファイルと .csv ファイルを比較し、.csv ファイルと一致しないインベントリ対象サーバを特定します。

   注： 正常に比較するために、eDirectory の出力ファイルと .csv ファイルは同じ形式にします。
4. 同期していないインベントリ対象サーバを特定した後、Inventory Removal Service でそのインベントリ対象サーバを選択するために、インベントリ対象サーバの DN 名を serverremovallist.txt ファイルに保存します。

17 インベントリ情報の表示

ここでは、次の内容について説明します。

- 625 ページの「ConsoleOne を使用したインベントリ情報の表示」
- 653 ページの「インベントリ情報のエクスポート」
- 660 ページの「CIM スキーマを使用しないインベントリデータベースからのインベントリ情報の取得」

ConsoleOne を使用したインベントリ情報の表示

次の節では、ConsoleOne を使用して表示できる情報の種類について説明します。

- インベントリ対象サーバで検出されたハードウェアおよびソフトウェアのコンポーネントに加え、このサーバに対して指定したカスタム情報を一覧表示することができます。

  [Inventory Summary] ウィンドウに、インベントリ対象サーバのインベントリ項目が表示されます。このウィンドウには、インベントリ対象サーバに対する最後のインベントリスキャンの情報が表示されます。詳細については、626 ページの「インベントリ対象サーバのインベントリサマリの表示」を参照してください。

- [Inventory Query] ウィンドウで指定した基準を満たすインベントリ情報を含んだインベントリ対象サーバを、インベントリデータベースから取得して一覧表示することができます。選択したデータベースサイト内のサーバについて、コンポーネントおよびその属性を指定することにより、照会を作成します。

  インベントリデータベースの照会に関する詳細については、638 ページの「データベース照会によるインベントリ対象サーバのインベントリ情報の表示」を参照してください。

- インベントリデータベースから必要なインベントリ情報を抽出して作成するレポートのリストを使用することができます。

  詳細については、641 ページの「インベントリレポートの実行」を参照してください。

インベントリデータベースの設定

データベース内に保存されたインベントリ情報を ConsoleOne から表示する場合は、データベースを設定する必要があります。設定するインベントリデータベースのインベントリ情報は、インベントリレポートの作成、インベントリ情報の参照、およびデータベースからのインベントリ情報の照会に使用されます。

インベントリデータベースを設定するには

1 ConsoleOne で、コンテナを選択します。

2 [Configure DB] を呼び出します。

- データベースオブジェクトから [DB の設定] を呼び出すには、データベースオブジェクトを右クリックして、[ZENworks Inventory] > [Configure DB] の順にクリックします。この操作により、データベースオブジェクトが設定されます。
- ConsoleOne の [Tools] メニューから [Configure DB] ダイアログボックスを呼び出すには、[Tools] > [ZENworks Inventory] > [Configure DB] の順にクリックします。

3 [Browse] をクリックして、ZENworks データベースオブジェクトを参照して選択します。

データベースオブジェクトのリストから既存の ZENworks データベースオブジェクトを選択することもできます。

このデータベースオブジェクトには、プロトコル、データベースが使用するポートなどのデータベース設定が含まれています。

4 このデータベース設定をすべてのセッションに適用するには、[Apply Configuration Across Sessions] チェックボックスを選択します。

5 [OK] をクリックします。

同じ手順を再び実行してデータベースを変更しない限り、設定したデータベースがデータの取得に使用されます。

インベントリ対象サーバのインベントリサマリの表示

[Inventory Summary] ウィンドウには、インベントリ対象サーバに対する最後のインベントリスキャンの情報が表示されます。

インベントリ対象サーバのインベントリ情報を表示するには、ConsoleOne で次の操作を実行します。

1 インベントリデータベースを設定します。

詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

2 Subscriber、Distributor、または External Subscriber オブジェクトを右クリックし、[Actions]、[Inventory] の順にクリックします。

または

[Query Results] ウィンドウで、インベントリ対象サーバをダブルクリックします。

ZENworks 6.5 Server Management は、インベントリ対象サーバから収集された次のインベントリ情報を提供します。

スキャンデータのグループ	スキャンデータの項目	説明
Inventory Information	Inventory Server	スキャンの送信先となるインベントリサーバの名前。
	Last Scan Date	指定した日時またはそれより以前にスキャンされたすべてのインベントリ対象サーバの一覧。
	Scan Mode	インベントリ対象サーバをスキャンするのに Inventory Scanner が使用するモード。

スキャンデータのグループ	スキャンデータの項目	説明
	Version	Inventory Scanner のバージョン番号。
	General Dictionary Version	一般ディクショナリのバージョン番号。
	Private Dictionary Version	プライベートディクショナリのバージョン番号。
Hardware/Software Inventory > General > System Information	Asset Tag	ROM ベースのセットアッププログラムにより作成される備品タグ番号。
	Computer Model	Compaq、Dell などのコンピュータ識別情報。
	Computer Type	IBM PC などのコンピュータの種類。
	Machine Name	インベントリ対象サーバの DNS 名。
	Management Technology	DMI、WMI など、インベントリ対象サーバで利用できるテクノロジ。
	Model Number	コンピュータのモデル番号。
	Serial Number	メーカーによってコンピュータシステムに割り当てられるシリアル番号。
	Tag	システム情報の一意の識別子。
Hardware/Software Inventory > General > System Identification	Primary Owner Name	このシステムの主なユーザまたは所有者の名前。
	Primary Owner Contact	このシステムの主なユーザの電話番号。
	Name	インベントリ対象サーバの完全修飾 DN など、eDirectory で表示されるインベントリ対象サーバの名前。
Hardware/Software Inventory > General > Login Details > eDirectory Login Details	Current login user	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーにログインしたユーザ。
	Last login user	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーに最後にログインしたユーザ。
Hardware/Software Inventory > General > Login Details > Windows Domain	Name	インベントリ対象サーバのドメイン名。
Hardware/Software Inventory > Software > Application Vendors > *Vendor_name* > *software_group_name* > *software*	Name	ベンダの商標または登録商標として示されるベンダ定義の製品名。

スキャンデータのグループ	スキャンデータの項目	説明
	Version	製品のわかりやすいバージョン。 たとえば、Windows 2000 のバージョンは 2000 です。通常、製品のバージョンはメジャー番号とマイナー番号 (Major.Minor) で構成されます。
	Category	製品が属する製品カテゴリ。 たとえば、Office は生産性ツールのカテゴリに属し、ソリティアはゲームのカテゴリに属します。
	Description	製品の説明。
	Help Link	ARP および MSI で使用可能な製品のサポート Web サイトの URL。
	Package GUID	MSI で使用可能なベンダ定義の製品 GUID。
	Product Identifier	インストールされている製品の一意な半角 16 文字の識別子。この識別子は Windows の MSI から使用できます。 書式は ABCD-1234-WXYZ-PQRS です。
	Internal Version	製品の内部バージョン。 書式は、次のいずれかです。 *major version.minor version.build.sub build number* または *major version.minor version.build*
	Language	この製品の言語を示すわかりやすい名前。
	Uninstall String	この製品をアンインストールするために呼び出すコマンド。現在、このコマンドは Windows の ARP ([プログラムの追加と削除]) および MSI で使用できます。
	Install Source	この製品をインストールするときにインストールファイルを保存したファイルシステムパスを識別します。現在、このコマンドは Windows の ARP および MSI で使用できます。
	Last Execution Time	製品が最後に実行された日付と時刻のスタンプ。
	Frequency of Usage	製品の使用回数。
	Friendly Name	ソフトウェアの表示名。
	Installation Repository	スキャンのソース ([プログラムの追加と削除]、MSI、ソフトウェアディクショナリ、または PRODUCTS.DAT)。
	Support Pack	製品のインストールされたサポートパックの番号。
	Product Edition	ベンダが定義した製品エディション。Professional など。

スキャンデータのグループ	スキャンデータの項目	説明
	Path	製品をインストールしたコンピュータシステム上のディレクトリパス。
	AntiVirus Definition Date **注：** これはアンチウィルス製品にのみ適用されます。	コンピュータにインストールされたウィルス定義ファイルの日付。一部のアンチウィルス製品は、日付とバージョンを 1 つの文字列に組み合わせています。
	AntiVirus Definition Version **注：** これはアンチウィルス製品にのみ適用されます。	コンピュータにインストールされている、ベンダが定義したバージョンのウィルス定義ファイル。
Hardware/Software Inventory > Software > Application Vendors > *Vendor_name* > *software_group_name* > *software* > Patches	Name	ベンダが定義したパッチ名。
Hardware/Software Inventory > Software > Application Vendors > *Vendor_name* > *software_group_name* > *software* > Representative File Information	File Name	ソフトウェアを示すファイル名。
	File Version	ソフトウェアを示すファイルのバージョン。
	File Size	ソフトウェアを示すファイルのサイズ。
	Last Modified	ソフトウェアを示すファイルの最終更新日。
	Internal Name	内部名。
	Product Version	このファイルが示す製品のバージョン。
	Company	ベンダ名。
	Product Name	このファイルが示す製品。
	Language	このファイルの言語を示すわかりやすい名前。
	File Path	インベントリ対象サーバ上のファイルの場所。
	Software Dictionary ID	一般ソフトウェアディクショナリで示されるファイルの ID。
Hardware/Software Inventory > Software > Disk Usage	File Extension Name	ディスク使用状況をスキャンするファイル拡張子。
	Total Disk Usage	指定された拡張子を持つすべてのファイルの総合的なディスク使用状況。

スキャンデータのグループ	スキャンデータの項目	説明
Hardware/Software Inventory > Software > Device Drivers > Pointing Device Drivers > *Pointing Device driver name*	Name	マウスドライバ名。
	Version	マウスドライバのバージョン番号。
Hardware/Software Inventory > Software > Device Drivers > Display Drivers	Install Date	ディスプレイドライバのインストール日。
	Manufacturer	ディスプレイドライバの製造元の名前。
	Is Shadowed (True または False)	True の場合、ディスプレイドライバは現在シャドウ処理されています。
	Version	ディスプレイドライバのバージョン番号。
Hardware/Software Inventory > Software > Device Drivers > Network Drivers	Description	ネットワークドライバの説明。
	Name	ネットワークドライバ名。
	Version	ネットワークドライバのバージョン番号。
Hardware/Software Inventory > Software > Operating System	Code Page	オペレーティングシステムの言語コードページ。
	OS Type	インベントリ対象サーバのオペレーティングシステム。
	Install Date	オペレーティングシステムのインストール日
	Caption	Windows 95、Windows 2000 などのオペレーティングシステム名。
	Other Description	オペレーティングシステムに関する補足説明（利用できる場合）。
	Role	サーバやワークステーションなどのオペレーティングシステムの種類。
	Total Virtual Memory Size	呼び出しプロセスの仮想アドレス領域における総バイト数。
	Total Memory Size	オペレーティングシステムの総メモリ量。
	Version	オペレーティングシステムのバージョン番号。
Hardware/Software Inventory > Hardware > Monitor	Device ID	コンピュータシステムに接続されているデスクトップモニタの一意な ID。 例： DesktopMonitor1。
	Description	モニタの説明。

スキャンデータのグループ	スキャンデータの項目	説明
	Nominal Size	モニタの対角線上の長さを示す数値（画面の片隅から反対側の隅までの距離）。 （例： 17)″ Server Inventory ポリシーを使用して HWRules の ini ファイルを設定することにより、モニタの公称サイズのスキャンをカスタマイズできます。
	Viewable Size	イメージを縁取る黒い枠を除いて、画面イメージの対角線上の長さを示す数値。 （例： 15.8)″
	Manufacturer	モニタのメーカー名。 例： DELL* Computer Corp。
	Serial Number	メーカーのモニタ識別番号。 例： 23DDC24N9067。
	Model	メーカーが付けたモニタの製品名。 例： DELL E771a。
	Manufacture Date	モニタの製造年。 （例： 2003)
	Model ID	モニタのモデルの一意な ID。メーカー ID と製品 ID の組み合わせです。 例： DELA001。
Hardware/Software Inventory > Hardware > Chassis	Asset Tag	システムシャシーの備品タグ番号。 例： S11127。
	Number of Power Cords	システムシャシーに接続されている電源コードの総数。
	Chassis Type	システムシャシーがラップトップ、デスクトップ、ノートブック、ドッキングステーションなどのいずれであるかを示します。
	Manufacturer	システムシャシー製造元の名前。 例： Compaq*。
	Serial Number	システムシャシーを識別するための製造元番号。 例： 53R661S。
	Version	システムシャシーのバージョン番号。
	Tag	特定のコンピュータに接続されているシステムシャシーの一意な ID。 例： System Enclosure 0。

スキャンデータのグループ	スキャンデータの項目	説明
Hardware/Software Inventory > Hardware > Pointing Device > *Pointing device name*	IRQ Number	このデバイスに割り当てられた割り込み。
	Name	マウスの識別情報。
	Number of Buttons	マウスのボタン数。
Hardware/Software Inventory > Hardware > Keyboard	Delay	キー入力を繰り返すまでの遅延時間。
	Description	IBM 拡張キーボード 101/102 など、キーボードに関する説明。
	Layout	キーボードのレイアウト。
	Number of Function Keys	ファンクションキーの総数。
	Subtype	キーボードの種類。
	Typematic Rate	キーの処理速度。
Hardware/Software Inventory > Hardware > Display Adapter > *Display adapter name*	Chip Set	システム機能を比較するのにコントローラが使用するチップセット。
	Current Bits/Pixel	各ピクセルに隣接するカラービット数。
	Current Horizontal Resolution	ディスプレイに表示される水平方向のピクセル数。
	Current Vertical Resolution	ディスプレイに表示される垂直方向のピクセル数。
	DAC Type	デジタルアナログコンバータの種類。
	Description	ディスプレイアダプタに関する説明。
	Maximum Memory Supported	ディスプレイアダプタが VIDEO RAM に対してサポートする最大メモリ。
	Maximum Refresh Rate	ディスプレイを再描画するためのモニタの最大リフレッシュレート（ヘルツ単位）。
	Minimum Refresh Rate	ディスプレイを再描画するためのモニタの最小リフレッシュレート（ヘルツ単位）。
	Number of Color Planes	ビデオシステムがサポートしている色平面の数。
	Provider	ベンダ名。
	Video Architecture	このシステムのビデオサブシステムのアーキテクチャ（CGA/VGA/SVGA/8514A など）。
	Video Memory Type	このアダプタ用のビデオメモリの種類（VRAM/SRAM/DRAM/EDO RAM など）。

スキャンデータのグループ	スキャンデータの項目	説明
Hardware/Software Inventory > Hardware > BIOS	BIOS Identification Bytes	BIOS でコンピュータモデルを示すバイト。
	Install Date	BIOS の製造日。
	Manufacturer	BIOS のベンダ名。
	Caption	BIOS のラベル。
	Primary BIOS	True の状態はプライマリ BIOS を示します。
	Serial Number	製造時にコンピュータに割り当てられるシリアル番号。
	Size	BIOS のサイズ。
	Version	BIOS のバージョンまたはリビジョンレベル。
Hardware/Software Inventory > Hardware > Processor	Current Clock Speed (MHz)	プロセッサの現在のクロック速度。
	Device ID	プロセッサの種類を識別する特殊な 16 進数の文字列。
	Maximum Clock Speed (MHz)	プロセッサの最大クロック速度。
	Other Family Description	MMX テクノロジを搭載した Pentium プロセッサなど、プロセッサファミリに関する詳しい説明。
	Processor Family	Pentium II、Pentium III など、プロセッサファミリの識別情報。
	Processor Stepping	マイクロプロセッサのベンダによって指定された、プロセッサのモデルを識別するための 1 バイトコード特性。
	Role	中央プロセッサ、数値演算コプロセッサなど、プロセッサの種類。
	アップグレード方法	このプロセッサのアップグレード方法 (アップグレードがサポートされている場合)。
Hardware/Software Inventory > Hardware > Modem	Description	モデムに関する詳細情報。
	Name	モデムの識別情報。
	Device ID	モデムの種類を識別する特殊な 16 進数の文字列。
	Provider	ベンダ名。
Hardware/Software Inventory > Hardware > Battery	Chemistry	リチウムイオン、ニッケル水素などバッテリの種類。
	Design Capacity	バッテリのデザイン容量 (ミリワット時間単位)。
	Design Voltage	バッテリのデザイン電圧 (ミリボルト単位)。

スキャンデータのグループ	スキャンデータの項目	説明
	Install Date	バッテリの製造日。
	Manufacturer	バッテリの製造元の名前。
	Name	Duracell* DR-36 など、このバッテリの製品名。
	Serial Number	このバッテリのシリアル番号。
	Smart Battery Version	バッテリがサポートしているスマートバッテリデータ仕様のバージョン番号。
Hardware/Software Inventory > Hardware > Power Supply	Description	この電源装置の入力電圧容量に関する詳細情報。
	Total Output Power (MilliWatts)	電源装置の総出力を表す属性値。
Hardware/Software Inventory > Hardware > Memory	Total Memory	インベントリ対象サーバの総メモリ量。
Hardware/Software Inventory > Hardware > Disk Drives > Floppy	Capacity	フロッピードライブの容量。
	Description	フロッピードライブに関する説明。
	Drive Letter	ドライブ文字名。
	Manufacturer	ベンダ名。
	Physical Cylinders	フロッピードライブのシリンダ。
	Physical Heads	フロッピードライブの読み取り / 書き込みヘッド。
	Sectors/Track	フロッピードライブの 1 トラックあたりのセクタ数。
Hardware/Software Inventory > Hardware > Disk Drives > Physical Disk > Fixed Disk	Description	説明。
	Manufacturer	ベンダ名。
	Physical Cylinders	シリンダ数。
	Physical Heads	ヘッド数。
	Sectors/Track	トラックあたりの固定ディスクドライブのセクタ数。
	Size	固定ディスクのサイズ。
Hardware/Software Inventory > Hardware > Disk Drives > Physical Disk > Removable Disk	Description	説明。
	Manufacturer	ベンダ名。

スキャンデータのグループ	スキャンデータの項目	説明
	Physical Cylinders	シリンダ数。
	Physical Heads	ヘッド数。
	Sectors/Track	トラックあたりのリムーバルディスクドライブのセクタ数。
	Size	リムーバルディスクのサイズ。
Hardware/Software Inventory > Hardware > Disk Drives > Logical Disk > *Logical disk name*	Drive Letter	ドライブ文字名。
	File System Type	FAT(File Allocation Table) など、ファイルシステムの種類。
	Free Size	ドライブの実際の容量 (MB 単位)。
	Volume Label	ハードディスクボリュームの名前。
	Size	ドライブ内の利用可能な容量 (MB 単位)。
	Volume Serial Number	ハードディスクボリュームのシリアル番号。
Hardware/Software Inventory > Hardware > Disk Drives > CDROM	Name	インベントリ対象サーバに接続されている CD ドライブの名前。
	Description	CD の説明。
	Drive Letter	CD にマップされたドライブ名。
	Manufacturer	ベンダ名。
	Caption	CD のキャプション。
Hardware/Software Inventory > Hardware > Ports > Serial Port	Address	このシリアルポートの基本入出力アドレス。
	IRQ Number	シリアルポートの IRQ 番号。
	Name	現在の運用環境で、このシリアルポート上にある I/O デバイスの論理名。
Hardware/Software Inventory > Hardware > Ports > Parallel Port	Address	このパラレルポートの基本 I/O アドレス。
	DMA Support (True または False)	True の場合、DMA がサポートされています。
	Name	現在の運用環境で、このパラレルポート上にある入出力デバイスの論理名。
	IRQ Number	パラレルポートの IRQ 番号。

スキャンデータのグループ	スキャンデータの項目	説明
Hardware/Software Inventory > Hardware > Bus	[Bus Type]	PCI、ISA などのバスの種類。
	Description	バスの説明。
	Name	バス名。
	Version	マザーボードがサポートしているバスのバージョン。
Hardware/Software Inventory > Hardware > Network Adapter	Adapter Type	FDDI、トークンリングなどのネットワークアダプタの種類。
	Auto Sense	ネットワークアダプタが、接続するネットワーク媒体の速度やその他の通信特性を自動的に判別できるかどうかを示すブール値。
	Card Manufacturer	カードの製造元の名前。
	Description	アダプタに関する説明。
	Install Date	ネットワークアダプタのインストール日。
	Maximum Speed	LAN における情報の転送速度。
	Name	ネットワークアダプタ名。
	Permanent Address	アダプタに永続的に格納されるノードアドレス。
	Provider	プロバイダ名。
Hardware/Software Inventory > Hardware > Sound Adapter	Description	サーバのマルチメディアコンポーネントの説明。
	Name	マルチメディアカードのラベル。
	Provider	プロバイダ名。
Hardware/Software Inventory > Network > DNS	DNS 名	インベントリ対象サーバの DNS 名。
Hardware/Software Inventory > Network > Network (*instance_number*) > IP	IP Address	IP インターネット上のコンピュータに割り当てられた一意のアドレス。
	Subnet Mask	インベントリ対象サーバのサブネットマスクは、IP アドレスと組み合わせられ、ネットワーク ID である IP アドレスのオクテット / ビットと、ノード ID であるオクテット / ビットを IP ルータに指定します。
Hardware/Software Inventory > Network > Network (*instance_number*) > IPX	IPX アドレス	インベントリ対象サーバの IPX™ アドレス。

スキャンデータのグループ	スキャンデータの項目	説明
Hardware/Software Inventory > Network > Network (*instance_number*) > MAC	MAC Address	一意のノードアドレスがネットワークアダプタ内に永続的に記述され、これによってネットワーク上の特定のコンピュータが識別されます。
Hardware/Software Inventory > Network > IP	IP Address	IP インターネット上のコンピュータに割り当てられた一意のアドレス。
	Subnet Mask	インベントリ対象サーバのサブネットマスクは、IP アドレスと組み合わせられ、ネットワーク ID である IP アドレスのオクテット / ビットと、ノード ID であるオクテット / ビットを IP ルータに指定します。
Hardware/Software Inventory > Network > IPX	IPX アドレス	インベントリ対象サーバの IPX アドレス。
Hardware/Software Inventory > Network > MAC	MAC Address	一意のノードアドレスがネットワークアダプタ内に永続的に記述され、これによってネットワーク上の特定のコンピュータが識別されます。
Hardware/Software Inventory > System > System IRQ	Availability	特定の IRQ チャネルの可用性。
	IRQ Number	IRQ(割り込み要求行) の数 (0 ～ 15)。
	IRQ Trigger Type	IRQ トリガの種類。
	Shareable	True の場合、デバイス間でシステム IRQ を共有できます。
Hardware/Software Inventory > System > System Cache	Associativity	システムキャッシュの連想性を定義します (ダイレクトマップ、2 ウェイ、4 ウェイ)。
	Cache Type	命令、データ、ユニファイドなど、システムのキャッシュタイプを定義します。
	Capacity	キャッシュ情報を格納しているデータストアのサイズ。
	Error Methodology	キャッシュコンポーネントがサポートしているエラー修正方式。パリティ / シングルビット ECC/ マルチビット ECC など。
	Level	マイクロプロセッサに組み込まれている内部キャッシュまたは CPU と DRAM 間にある外部キャッシュのキャッシュレベルを示します。
	Line Size	シングルキャッシュバケットまたはシングルキャッシュラインのサイズ (バイト単位)。
	Read Policy	データキャッシュが読み取り処理用であるかどうかを示します。
	Replacement Policy	再使用するキャッシュラインまたはキャッシュバケットを決定するために、キャッシュが使用するアルゴリズム。

スキャンデータのグループ	スキャンデータの項目	説明
	Speed	システムキャッシュモジュールの速度（ナノ秒単位）。
	Write Policy	キャッシュがメモリに書き込む2つの方法（ライトバックとライトスルーキャッシュ）を示します。
Hardware/Software Inventory > System > System DMA	Availability	DMA（仮想ダイレクトメモリアクセス）がサポートされているかどうかを示します。
	Description	このDMAチャネルを現在使用している論理デバイスの名前。
	DMA Burst Mode	データが通常よりも高速で送信されるデータ転送モード。
	DMA Channel Number	コンピュータとデバイスとの間で、DMAチャネルのないコンピュータよりも高速にデータを転送するためにコンピュータが使用するDMAチャネルの番号。
Hardware/Software Inventory > System > System Slot	Description	このスロットを現在使用しているカード。
	Maximum Data Width	スロットで許容されているカードの最大バス幅。
	Thermal Rating	スロットの最大熱損失量（ミリワット単位）。
Hardware/Software Inventory > System > Motherboard	Manufacturer	マザーボードの製造元の名前。
	Number of Slots	メモリの増設、グラフィック機能の追加、および特殊デバイスのサポートを実現するための、マザーボード内の拡張スロット数。
	Version	マザーボードのバージョン。
	Description	マザーボードの一般的な説明。

注： 列挙属性では、*enumerated_value [enumerated_ID]* の形式で値が表示されます。たとえば、Processor.Processor Family = Pentium (R) III [17] のように表示されます。

ステータスバーに、次の情報が表示されます。

- **ツリー名：** インベントリ対象サーバが存在するeDirectoryツリー名が表示されます。
- **[Recent Information]：** 選択したインベントリ対象サーバの最新のインベントリ情報でインベントリデータベースが更新されている場合は、[Yes] に設定されます。

データベース照会によるインベントリ対象サーバのインベントリ情報の表示

ConsoleOneを使って、インベントリデータベースに対して照会を実行し、インベントリ対象サーバのハードウェアおよびソフトウェアのコンポーネントを表示することができます。指定した基準を満たす情報が、[Inventory Query] ウィンドウに表示されます。

インベントリデータベースには、各インベントリ対象サーバに関するインベントリ情報（一般情報、ハードウェア、ソフトウェア、ネットワーク、およびシステムに関する情報）が格納されています。インベントリデータベースに対して照会を実行することにより、類似するデバイスのグループを作成し、レポートの対象を特定の種類のコンピュータに絞ることができます。たとえば、データベースに対して照会を実行して、i486D プロセッサと VGA カードを搭載したコンピュータを検索することができます。

インベントリデータベースに対して照会を実行し、インベントリ情報を取得するには

1 ConsoleOne でコンテナをクリックします。

2 [Query] を実行します。

- データベースオブジェクトからインベントリ照会を実行するには、データベースオブジェクトを右クリックし、[ZENworks Inventory] > [Inventory Query] の順にクリックします。
- ConsoleOne の [Tools] メニューからインベントリ照会を実行するには、最初にインベントリデータベースを設定し、次に [Tools]、[ZENworks Inventory]、[Inventory Query] の順にクリックします。インベントリデータベースの設定方法の詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

3 照会の基準を指定します。

[Query the Inventory database for]： デフォルトでは、[Servers] オプションが有効になります。照会式を満たすすべてのインベントリ対象サーバが検索されます。ZENworks 6.5 Server Management および Desktop Management が同じ環境にインストールされている場合は、[Workstations]、[Servers]、および [Both] の各オプションを利用できます。[Servers] を選択すると、照会式を満たすすべてのインベントリ対象サーバが検索されます。[Both] を選択すると、照会式を満たすすべてのワークステーションおよびインベントリ対象サーバが検索されます。

[Find Type]： [Quick] または [Advanced] を選択します。簡単な照会を指定する場合は [Quick] をクリックします。[Quick] 照会を選択した場合は、1 つの属性、関係演算子、および属性の値を指定します。多数の属性を指定する場合は [Advanced] を選択します。複数の照会グループを組み合わせて、グループ別に照会基準のセットを定義することができます。たとえば、[Advanced] 照会を使用して、486 プロセッサを搭載する全デバイスをデータベースから検索する照会を実行し、さらに照会コネクタを使用して別の照会を追加し、VGA カラービデオアダプタを搭載したインベントリ対象サーバを検索することができます。

[Display Machine(s) Not Satisfying the Query]： このチェックボックスを選択すると、照会を満たさないコンピュータが検索されます。

[Select Attribute]： コンポーネントまたはコンポーネント属性を選択します。インベントリ対象サーバを照会する際に指定できる属性は、[General]、[Software]、[Hardware]、[Network]、および [System] の各カテゴリに分類されます。

カスタム属性の前にはアスタリスク (*) が付けられます。

たとえば、ポインティングデバイスがインストールされていないコンピュータを検索するには、コンポーネントとして [Pointing Device] を選択します。照会で BIOS のバージョンをコンポーネントとして指定するには、コンポーネントとして [BIOS] を選択し、コンポーネント属性として [VERSION] を選択します。

[Operator] または [Relational Operator]： コンポーネントと値の間の関係を決定するために選択します。関係演算子は [Select Attribute] ウィンドウで選択した属性のデータ型に基づいて、次の表のように分類されます。

属性のデータ型	関係演算子
String	等しい (=)、等しくない (!=)、一致する ([ ])、一致しない (![ ])、および NULL かどうか (null)
Numeric	等しい (=)、等しくない (!=)、より小さい (<)、以下 (< =)、より大きい (>)、以上 (>=)、および NULL かどうか (null)
Date	後 (>)、以後 (>=)、前 (<)、以前 (< =)、および NULL かどうか (null)
Enum	等しい (=)、等しくない (!=)、および NULL かどうか (null)
Custom	String、Numeric、および Date の各データ型にグループ化されるすべての関係演算子が含まれます。

注： 属性のデータ型が Custom、関係演算子のデータ型が Numeric または Date である場合に、照会の結果が表示されないときは、Equal To (=) 演算子を使用してインベントリデータベースに保存されたカスタム属性の値を検索します。

[Select Attribute] ウィンドウでコンポーネントだけを選択した場合、[Relational Operator] はデフォルトで [NULL] に設定され、その他の関係演算子は利用できなくなります。

[Value] : 記述値は、インベントリコンポーネントが取り得る値です。たとえば、6.0 という値は DOS バージョンの属性に指定できます。記述値では大文字と小文字が区別されません。

注： 列挙属性では、*enumerated_value [enumerated_ID]* の形式で値が表示されます。たとえば、Processor.Processor Family = Pentium (R) III [17] のように表示されます。

関係演算子として Matches ([ ]) または Does Not Match (![ ]) を選択した場合は、[Value] フィールドで文字の代わりにワイルドカードを使用できます。次の表は、SQL ドキュメントに従って使用できるワイルドカードのリストを示しています。

例	レポートに含まれる項目
?	任意の 1 文字
_(アンダースコア)	任意の 1 文字
%	0 文字以上の任意の文字列
[]	指定の範囲またはセット内の任意の 1 文字
[^]	指定の範囲またはセット内にない任意の 1 文字

注： ? や [などの特殊文字を使用して照会を定義するには、[?] または [[ ] という形式で指定します。

インベントリコンポーネントについて表示される記述値リストは、コンポーネントに対応するインベントリデータベースから取得されます。

[Logical Operator] : このオプションは、[Advanced] 照会のみで使用できます。[Logical Operator] では、照会グループ間に関係演算子を使用し、前の照会グループに別の照会グループを追加できます。

[Save]：このオプションは、[Advanced] 照会のみで使用できます。照会式をファイルとして指定の場所に保存します。ただし、照会ファイルにはデフォルトの拡張子が付いていません。簡単に参照できるよう、.qry という拡張子を付けることをお勧めします。

[Load]：このオプションは、[Advanced] 照会のみで使用できます。指定した照会ファイルをロードします。拡張子付きのファイル名を入力する必要があります。

4 [Find] をクリックします。

指定した照会基準に基づいて照会が実行され、照会に一致するインベントリ対象サーバが [Query Results] ウィンドウに表示されます。

[Query Results] ウィンドウで、インベントリ対象サーバをダブルクリックするか、[File]、[Advanced Query] の順にクリックして、インベントリ対象サーバのインベントリ情報を表示します。

関係演算子の使用

- **Match:** 照会条件を満たすインベントリ対象サーバを検索する場合、Match 演算子を使用します。

  たとえば、IP アドレスが 164.99.151.% のすべてのインベントリ対象サーバを検索する場合、Match 演算子を使用します。

- **NULL:** 特定の属性はスキャンされないが、コンポーネントがスキャンされて一部の属性が取得されるインベントリ対象サーバに対して照会を実行する場合に、NULL 演算子を使用します。

  たとえば、BIOS.Manufacturer についてスキャンされないインベントリ対象サーバのリストを検索するには、BIOS.Manufacturer が NULL である照会を作成します。この照会により、BIOS のスキャンが実行されたインベントリ対象サーバが表示されます。

- **NOT SATISFYING:** 指定した照会に合致しないインベントリ対象サーバのフィルタ条件を検索する場合に NOT SATISFYING 照会（または NOT SATISFYING フィルタ条件）を使用します。

  たとえば、2 つのサーバ S1 および S2 に、シリアルポート COM1 と COM2 の両方が搭載されているとします。照会 (SerialPort='COM1') を実行すると S1 が返されますが、照会 (SerialPort!='COM1') を実行した場合も S1 が返されます。これは、S1 にシリアルポート COM2 が搭載されているためです。シリアルポート COM1 を搭載しないインベントリ対象サーバに対して照会を実行するには、<NOT SATISFYING>(SerialPort='COM1') を使用する必要があります。NOT SATISFYING オプションを使用するには、照会ウィンドウの [Display Machines Not Satisfying the Query] チェックボックスをクリックします。

インベントリレポートの実行

レポートを実行して、インベントリデータベースからインベントリ情報を収集できます。インベントリレポートは、Crystal Reports を使用するよう設計されています。

定義済みのレポートフォームセットを選択して、レポートを生成することができます。インベントリレポートは、[Crystal Viewer] ウィンドウに表示されます。

必要に応じてレポートを印刷またはエクスポートできます。必要な情報をインベントリデータベースに入力するよう ZENworks 6.5 Server Management を設定していない場合、空のレポートが生成されます。

ここでは、次のトピックについて説明します。

- 642 ページの「インベントリレポートを生成するための前提条件」
- 642 ページの「インベントリレポートの種類」
- 649 ページの「インベントリレポートの生成」
- 650 ページの「インベントリレポートの印刷」
- 651 ページの「ファイルへのインベントリレポートのエクスポート」
- 641 ページの「インベントリレポートの実行」
- 651 ページの「ユーザ定義レポートの理解」

インベントリレポートを生成するための前提条件

インベントリレポートを実行する前に、必ず、適切な ODBC クライアントがインストールされていることを確認してください。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』を参照してください。

インベントリレポートの種類

次に示すレポートを生成できます。ただし、ZENworks 6.5 Server Management の設定がすでに完了しており、必要な情報がインベントリデータベースに入力されていることが前提になります。

次の表は、オペレーティングシステムや選択基準など、Server Inventory の個別の要素に関する情報を提供する簡単なインベントリのリストです。この表では、メモリ、ハードディスク、プロセッサなどの Server Inventory の要素を各レポートに組み合わせた包括的な内容のインベントリレポートも示します。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
ハードウェアインベントリ	アセット管理レポート	[Scope]、[Machine Name]、[IP Address]、および [DNS Name] 次のオプションを選択し、レポート内で表示できます。[Memory]、[Processor]、[Display Adapter]、[Keyboard]、[Pointing Device]、[Fixed and Removable Disk]、[Floppy]、[CDROM]、[Network Adapter]、および [Monitor]	インベントリ対象サーバのメモリ、プロセッサ、ディスプレイの詳細、キーボード、ポインティングデバイス、固定ディスクおよびリムーバルディスク、フロッピードライブ、CD ドライブ、ネットワークアダプタ、およびモニタの詳細。
	BIOS Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[BIOS Install Date]、および [Manufacturer]	すべてのインベントリ対象サーバとその BIOS の製造元、BIOS リリース日、およびコンピュータの合計数のリスト。
	Battery Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Name]	指定したバッテリ名に合致するすべてのインベントリ対象サーバの一覧。
	Bus Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Bus Type]	選択したバスの種類を含むすべてのインベントリ対象サーバの一覧。
	CDROM Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Caption]、[Description]、および [Manufacturer]	指定した CD キャプション、説明、および製造元の名前に合致するすべてのインベントリ対象サーバの一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Display Adapter Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Video Architecture]、および [Description]	指定したディスプレイアダプタのビデオアーキテクチャおよび説明に合致するすべてのインベントリ対象サーバの一覧。
	Floppy Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Manufacturer]、および [Description]	指定したフロッピーの説明および製造元の名前に合致するすべてのインベントリ対象サーバの一覧。
	Hardware Summary Report	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Operating System Type]、[Operating System Version]、[Processor Family]、[Curr.Clock Speed (Lower Bound in MHz)]、[Clock Speed (Upper Bound in MHz)]、[Total Memory (Lower Bound in MB)]、[Total Memory (Upper Bound in MB)]、[Hard Disk Size (Lower Bound in GB)]、および [Hard Disk Size (Upper Bound in GB)]	各インベントリ対象サーバのオペレーティングシステム名、オペレーティングシステムのバージョン、プロセッサファミリ、プロセッサの現在のクロック速度、メモリ、およびハードディスクの容量。
	Keyboard Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Description]、および [Layout]	指定したキーボードの説明およびレイアウトに合致するすべてのインベントリ対象サーバの一覧。
	Modem Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Name]	指定したモデム名に合致するすべてのインベントリ対象サーバの一覧。
	Monitor Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Manufacturer]、[Manufacture Date]、[Nominal Size (Lower Bound in inches)]、および [Nominal Size (Upper Bound in inches)]	指定したモニタの製造元名、製造日、およびモニタの公称サイズの範囲に合致するすべてのインベントリ対象サーバの一覧。
	Network Adapter Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Name]	指定したネットワークアダプタの名前に合致するすべてのインベントリ対象サーバの一覧。
	Physical Disk Listing	[Show Chart]、[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Removable]、[Manufacturer]、[Description]、[Total Size (Lower Bound in GB)]、および[Total Size (Upper Bound in GB)]	指定した物理ディスクの製造元名、説明、合計サイズの範囲、固定ディスク、リムーバルディスクに合致するすべてのインベントリ対象サーバの一覧。 [Show Chart] ボックスを選択して、Physical Disk Listing レポートを円グラフで表示することもできます。
	Pointing Device Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Pointing Device Type]、および [Pointing Device Name]	指定したポインティングデバイスの種類および名前に合致するすべてのインベントリ対象サーバの一覧。
	Power Supply Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Description]	指定した電源の説明に合致するすべてのインベントリ対象サーバの一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Processor Listing	[Show Chart]、[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Processor Family]、[Maximum Speed (Lower Bound in MHz)]、[Maximum Speed (Upper Bound in MHz)]、[Current Speed (Lower Bound in MHz)]、および [Current Speed (Upper Bound in MHz)]	コンピュータのプロセッサファミリ (Pentium Pro など)、プロセッサの最大クロック速度、および現在のクロック速度に関するすべてのインベントリ対象サーバの一覧。 [Show Chart] ボックスを選択して、Processor Listing レポートを円グラフで表示することもできます。
	Sound Adapter Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Name]	指定したサウンドアダプタの名前に合致するすべてのインベントリ対象サーバの一覧。
	Storage Devices Inventory Report	[Scope]、[Machine Name]、[IP Address]、および [DNS Name] 次のオプションを選択し、レポート内で表示できます。[Fixed and Removable Disk]、[Logical Disk]、[Floppy]、および [CD ROM]	各インベントリ対象サーバの固定ディスク、リムーバルディスク、論理ディスク、フロッピードライブ、および CD ドライブに関する詳細。
	System Chassis Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Chassis Type]、および [Manufacturer]	指定したシステムシャシーの種類および製造元名に合致するすべてのインベントリ対象サーバの一覧。
システム設定インベントリ	Inventory Scan Listing	[Show Chart]、[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Last Scan Date (On or Before)]、[Inventory Server Name]、および [Recent Information]	最後にインベントリのスキャンを実行した日時、インベントリサーバ名、および各インベントリ対象サーバの最新情報。 [Show Chart] ボックスを選択して、System Configuration Inventory レポートを円グラフで表示することもできます。
	Memory Listing	[Show Chart]、[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Total Memory (Lower Bound in MB)]、および [Total Memory (Upper Bound in MB)]	一定の範囲のメモリ容量 (たとえば 200 ～ 400MB) を搭載したすべてのインベントリ対象サーバの一覧と、それらのサーバの合計数。 [Show Chart] ボックスを選択して、Memory Listing レポートを円グラフで表示することもできます。
	Operating System Listing	[Show Chart]、[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Operating System Type]、および [Operating System Version]	指定したオペレーティングシステムの種類およびバージョンに合致するすべてのインベントリ対象サーバの一覧。 [Show Chart] ボックスを選択して、Operating System Listing レポートを円グラフで表示することもできます。
	ネットワーク情報レポート	[Scope]、[Machine Name]、[IP Address]、および [DNS Name]	各インベントリ対象サーバのネットワークアダプタの種類、DNS、IP アドレス、MAC アドレス、IPX アドレス、および Windows ドメイン名。
	System Information Listing	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、および [Computer Manufacturer]	指定したコンピュータ製造元名に合致するすべてのインベントリ対象サーバの一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	System Internal Hardware Inventory Report	[Scope]、[Machine Name]、[IP Address]、および [DNS Name] 次のオプションを選択し、レポート内で表示できます。[System IRQ]、[System Cache]、[System DMA]、[System Slot]、および [Motherboard]	各インベントリ対象サーバの IRQ、キャッシュ、DMA、スロット、およびマザーボード。
ソフトウェアインベントリ	Add-Remove Programs by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Software Name]	各インベントリ対象サーバの [プログラムの追加と削除] リストに表示されるすべてのソフトウェアの一覧。
	Anti-Virus Signature Files by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Software Name]、[Min Virus Definition Date]、および [Max Virus Definition Date]	各インベントリ対象サーバにインストールされたアンチウィルス製品別の、すべてのアンチウィルス署名ファイルの一覧。
	Anti-Virus Signature Machine Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Software Name]、[Min Virus Definition Date]、および [Max Virus Definition Date]	任意のアンチウィルス製品がインストールされたインベントリ対象サーバの数を表す一覧。
	Disk Usage by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [File Extension]	指定したファイル拡張子に合致するすべてのインベントリ対象サーバとディスク使用状況の一覧。
	Exception List by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[File Name]、[Vendor Name]、および [Product Name]	指定したファイル名、ベンダ名、および製品名に合致するすべてのインベントリ対象サーバとファイル情報に関する一覧。
	Installed NetWare Software by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Software Name]	指定したソフトウェア名に合致するすべてのインベントリ対象 NetWare コンピュータと products.dat の詳細に関する一覧。
	Internet Explorer Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Internet Explorer Version]、および [Service Pack]	Internet Explorer がインストールされているインベントリ対象サーバの数を表す一覧。
	Internet Explorer Patches by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Internet Explorer Version]、および [Service Pack]	指定した値およびパッチ名に合致する、すべての Internet Explorer バージョンのインストール済みパッチの一覧。
	Internet Explorer by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Internet Explorer Version]、および [Service Pack]	指定したバージョンに合致するすべての Internet Explorer インストールの一覧。
	MSI Products by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Software Name]、および [Vendor Name]	各インベントリ対象サーバにインストールされ、MSI (Microsoft Installer) データベースに含まれているすべての製品の一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Microsoft Office Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Microsoft Office Version]、および [Service Pack]	指定した製品名およびベンダ名に合致し、指定したソースからインストールされたすべての製品の一覧。
	Microsoft Office Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Microsoft Office Version]、および [Service Pack]	Microsoft Office がインストールされているインベントリ対象サーバの数を表す一覧。
	Microsoft Office by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Microsoft Office Version]、および [Service Pack]	指定したバージョンに合致するすべての Microsoft Office インストールの一覧。
	Novell Client Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Novell Client Version]、および [Service Pack]	指定したバージョンに合致するすべての Novell Client コンポーネントの一覧。
	Novell Client Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Novell Client Version]、および [Service Pack]	Novell Client がインストールされているインベントリ対象サーバの数を表す一覧。
	Novell Client by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Novell Client Version]、および [Service Pack]	指定したバージョンに合致するすべての Novell Client インストールの一覧。
	Outlook Express Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および[Outlook Express Version]	Outlook Express がインストールされているインベントリ対象サーバの数を表す一覧。
	Outlook Express by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Patch Name]	指定したバージョンに合致するすべての Outlook Express インストールの一覧。
	Software Dictionary Application Files by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Vendor Name]、[Software Name]、および [Software Version]	指定したベンダ、ソフトウェア、ソフトウェアバージョンに合致する、すべてのインベントリ対象サーバとソフトウェアディクショナリアプリケーションファイルの一覧。
	Software Dictionary Applications by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Vendor Name]、[Software Name]、および [Software Category]	指定したベンダ、ソフトウェア、ソフトウェアバージョンに合致する、すべてのインベントリ対象サーバとソフトウェアディクショナリアプリケーションの一覧。
	Software Dictionary Versions Machine Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[General Dictionary Version]、および [Private Dictionary Version]	指定した一般ディクショナリおよびプライベートディクショナリのバージョンを含むすべてのインベントリ対象サーバの数を表す一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Software Dictionary Versions by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[General Dictionary Version]、および [Private Dictionary Version]	指定した一般ディクショナリおよびプライベートディクショナリのバージョンを含むすべてのインベントリ対象サーバの一覧。
	Software Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Vendor Name]、[Software Name]、および [Software Version]	指定したベンダ名、ソフトウェア、およびバージョンを含むインベントリ対象サーバの数を表す一覧。
	Software Installations	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Vendor Name]、[Software Name]、および [Software Version]	指定したベンダ名、ソフトウェア、およびバージョンを含むすべてのインベントリ対象サーバの一覧。
	Software by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Vendor Name]、[Software Name]、および [Software Version]	指定したベンダ名、ソフトウェア、およびバージョンに合致するすべてのインベントリ対象サーバとソフトウェア情報の一覧。
	System Software Inventory Report	[Scope]、[Machine Name]、[IP Address]、および [DNS Name] 次のオプションを選択し、レポート内で表示できます。[Display Driver]、[Pointing Device Driver]、[Network Adapter Driver]、および [NetWare Client]	各インベントリ対象サーバのドライバ（ポインティングデバイスドライバ、ネットワークアダプタドライバ、ディスプレイドライバなど）および Novell NetWare® Client。
	Windows Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Windows Version]、および [Service Pack]	指定したバージョンに合致するすべての Windows コンポーネントの一覧。
	Windows Installation Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Windows Version]、および [Service Pack]	Windows オペレーティングシステムがインストールされたインベントリ対象サーバの数を表す一覧。
	Windows Media Player Count	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Windows Media Player Version]	Windows Media Player がインストールされているインベントリ対象サーバの数を表す一覧。
	Windows Media Player Patches by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Windows Media Player Version]	指定したバージョンおよびパッチ名に合致する、すべての Windows Media Player 用パッチの一覧。
	Windows Media Player by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、および [Windows Media Player Version]	指定したバージョンに合致するすべての Windows Media Player インストールの一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Windows Operating System by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Windows Version]、および [Service Pack]	指定したバージョンおよびシリアル番号に合致するすべての Windows オペレーティングシステムの一覧。
	Windows Security Patches by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、[Max Last Scan Time]、[Windows Version]、および [Service Pack]	指定したバージョンおよびパッチ名に合致する、すべての Windows オペレーティングシステム用パッチの一覧。
	Novell ZENworks Desktop Management Installed Agent Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 Desktop Management のエージェントコンポーネントの一覧。
	Novell ZENworks Desktop Management Installed Server Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 Desktop Management のサーバコンポーネントの一覧。
	Novell ZENworks Handheld Management Installed Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 Handheld Management コンポーネントの一覧。
	Novell ZENworks Installed Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 コンポーネントの一覧。
	Novell ZENworks Installed Suites by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 スイートの一覧。
	Novell ZENworks Server Management Installed Agent Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および [Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされた ZENworks 6.5 Server Management のエージェントコンポーネントの一覧。

インベントリレポートグループ	レポート名	選択基準	インベントリレポートに表示される情報
	Novell ZENworks Server Management Installed Server Components by Machine	[Scope]、[Machine Name]、[IP Address]、[DNS Name]、[Min Last Scan Time]、および[Max Last Scan Time]	指定した期間内で最後に正常にスキャンされたすべてのコンピュータと、こうしたコンピュータにインストールされたZENworks 6.5 Server Management のサーバコンポーネントの一覧。
その他	User Defined Reports ユーザ定義レポートの作成方法に関する詳細については、651 ページの「ユーザ定義レポートの理解」を参照してください。	consoleone¥*consoleone_version*¥bin¥userreports.ini ファイルで指定されたオプションに基づいてレポートが生成されます。	ユーザ定義レポートを表示します。

注： [Show Chart] 選択基準を使用すると、インベントリレポートがグラフ形式で表示されます。

インベントリレポートの生成

インベントリレポートを生成するには

1 次のいずれかの方法で、インベントリレポートを生成します。

- データベースオブジェクトからインベントリレポートを生成するには、データベースオブジェクトを右クリックし、[ZENworks Reports] をクリックします。
- ConsoleOne の [Tools] メニューからインベントリレポートを実行するには、最初にインベントリデータベースを設定し、[Tools]、[ZENworks Reports] の順にクリックします。データベースの設定方法の詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

2 生成するレポートをクリックします。

画面の右側にレポートに関する説明が表示されます。

簡単なインベントリリストの一覧および包括的なインベントリレポートの一覧を示した表を参照してください。

3 選択基準を指定します。

[Scope] 選択基準は、ZENworks 6.5 Desktop Management と ZENworks 6.5 Server Management の両方が同じコンピュータにインストールされている場合に限り、使用することができます。

たとえば、Windows 2000 オペレーティングシステムを実行しているすべてのインベントリ対象サーバを表示するには、[Operating System Listing] を選択し、選択基準の [Scope] に [Both] を、[Operating System Type] に [Windows 2000] を指定します。設定されているインベントリデータベース内のすべてのサーバに関するインベントリ情報がレポートに表示されます。

作成するレポートの種類に応じて、情報にフィルタを適用できます。たとえば、Windows オペレーティングシステムを実行しているすべてのインベントリ対象サーバを表示するには、[Operating System Listing] を選択し、選択基準の [Scope] に [Both] を、[Operating System Type] に [Windows] を、[Operating System Version] に [2000] を指定します。

[Reporting] ダイアログボックスで作業する際、次のガイドラインに従います。

- ショートカットキーはサポートされていません。
- インベントリレポートでは、2 バイト文字が正しく表示されません。
- インベントリレポートの選択基準では、大文字と小文字が区別されます。

  たとえば、識別名が CN=MACHINE1.OU=ENG.O=NOVELL のコンピュータのリストを表示する場合は、選択基準として OU=ENG.O=NOVELL を指定します。識別名に OU=ENG.O=NOVELL を含むすべてのコンピュータがインベントリレポートに表示されますが、識別名に ou=eng.o=novell を含むコンピュータは表示されません。
- [レポート中] ダイアログボックスでワイルドカードの使用が許可されている場合、すべての選択基準でアスタリスク (*) または疑問符 (?) を使用することができます。ワイルドカード文字は、文字データにのみ使用できます。

  次の表に、ワイルドカードの使用例を示します。

例	レポートに含まれる項目
*	すべての項目
164.99.*	「164.99」で始まるすべての項目
164.9?.215.23	「164.9」で始まり、任意の 1 文字をはさんだ後「.215.23」で終了するすべての項目
164.96.215.23	指定した項目のみ。この例では、指定した IP アドレスのインベントリ対象サーバを表示。

4 [Run Selected Report] をクリックします。

レポート生成の進行状況を表示するステータスボックスが表示されます。このステータスボックスは、レポートの生成時にビューアに表示されます。ツールバーのボタンを使って、レポートの各ページを表示、印刷、またはエクスポートすることができます。

インベントリレポートの印刷

レポートを印刷するには

1 レポートを生成して表示します。

2 プリンタのデフォルトの設定を変更する場合は、[Printer Setup] アイコンをクリックして必要な設定を変更します。

3 プリンタのアイコンをクリックします。

ファイルへのインベントリレポートのエクスポート

ファイルにインベントリレポートをエクスポートするには

1 レポートを生成して表示します。

2 ツールバーの［Export Report］アイコン  をクリックします。

3 ［Export］ダイアログボックスで、エクスポート先の場所とファイル形式を指定します。

インベントリレポートをテキストファイルとしてエクスポートする場合には、［Export to Text］ダイアログボックスでユーザ定義オプションを選択し、値を 16 に設定します。これは、値が 16 未満の場合には、エクスポートされるデータが切り捨てられるためです。

インベントリレポートを HTML ファイルとしてエクスポートする場合は、HTML 3.2 または HTML 4.0 (DHTML) ファイル形式を選択できます。このとき、HTML 4.0 (DHTML) としてエクスポートすることをお勧めします。これは、HTML 3.2 形式でエクスポートした場合、データの書式が正しく設定されないためです。

インベントリレポートをカンマ区切り (.csv) ファイルとしてエクスポートする場合は、次の手順を実行します。

3a レポートを Microsoft* Excel にエクスポートします。

注： .csv ファイルへのエクスポートを選択しても、レポートは正しくエクスポートされません。

3b .xls ファイルを開きます。

3c ［ファイル］>［名前を付けて保存］の順にクリックします。

3d ［Save as type］フィールドで［CSV (Comma delimited) (*.csv)］を選択します。

3e ［Save］をクリックします。

4 ［OK］をクリックします。

5 エクスポートされたファイルを保存するディレクトリを参照して選択します。

6 ［OK］をクリックします。

ユーザ定義レポートの理解

Crystal Report Designer を使用して、インベントリデータベース内の情報からレポートを生成できます。

レポートを生成する前に、Crystal Report Designer 8.0/8.5 を使ってレポートファイル (.rpt) が作成されることを確認する必要があります。.rpt ファイルの作成方法の詳細については、Crystal Report のドキュメントを参照してください。

重要： ソフトウェアインベントリレポートを除き、任意のインベントリレポートをテンプレートとして使用してレポートを作成できます。

ユーザ定義インベントリレポートを生成するには

1 レポートを作成するコンピュータの ODBC DSN 名を ZenInventory に設定します。

ODBC 名を設定するには

1a ［スタート］>［設定］>［コントロールパネル］の順にクリックします。

1b ［ODBC データターゲット (32 ビット)］をダブルクリックし、［追加］をクリックします。

1c 接続先のデータベースの ODBC ドライバを選択します。

1d［終了］をクリックします。

1e データソース名に「ZenInventory」を指定し、詳細を決定します。

注： ZenInventory 以外のデータソース名を指定する場合は、ConsoleOne を通じてユーザ定義レポートを呼び出すコンピュータごとに ODBC 名を設定する必要があります。

2 レポートの作成が完了した後、レポートを ¥consoleone¥version¥reporting¥canned¥novellreporting¥zeninventory¥en ディレクトリに保存します。

3 ¥consoleone¥version¥bin ディレクトリ内の userreports.ini ファイルで値を設定します。この userreports.ini ファイルには、次の値が含まれている必要があります。

#[ReportName]〈レポートファイルの実際の名前（.rpt 拡張子は除く）〉

#DisplayName= ユーザ定義レポートの表示名

#Param1=Constant,Display name,〈組み合わせの場合には {val-1|val-2|val-3}〉

#<Param1 には .rpt ファイルに保存されるパラメータの内部名が入ります >

#<Constants には、組み合わせを選択した場合は 1、テキストフィールドの場合は 2、数値フィールドの場合は 3 が入ります >

たとえば、次のように値を設定できます。

```
[ListSystemInformation]DisplayName=System Information

Role=1,Role,{2|3|5}

IPAddress=2,IP Address

DNName=2,Distinguished Name

DNTree=2,Distinguished Tree

DNSName=2,DNS Name

[ListMemory]

DisplayName=Memory

Role=1,Role,{2|3|5}

IPAddress=2,IP Address

DNName=2,Distinguished Name

DNTree=2,Distinguished Tree

DNSName=2,DNS Name

MemoryLowerLimit=3,Memory Lower Bound
```

4 USERREPORTS.INI ファイルに値を設定した後、ユーザ定義レポートがインベントリレポートツリーに表示されます。USERREPORTS.INI ファイルで複数のレポートを指定することができます。

注： USERREPORTS.INI ファイルが空の場合は、インベントリレポートツリーにユーザ定義レポートを表示できません。

5［Run Selected Report］をクリックします。

インベントリ情報のエクスポート

ZENworks 6.5 Server Management のインベントリデータベースから CSV 形式（カンマ区切り）ファイルまたは XML ファイルにエクスポートするインベントリ情報は、カスタマイズすることができます。

オペレーティングシステム名やバージョンなど、エクスポートする必要があるインベントリコンポーネントを選択します。属性をエクスポートする元のインベントリ対象サーバを、さらに絞ることができます。たとえば、特定の速度のプロセッサが搭載されたインベントリ対象サーバだけをエクスポートできます。Data Export ツールにより、こうした照会条件を満たすすべてのインベントリ対象サーバが .csv ファイルまたは .xml ファイルにエクスポートされます。

同じデータエクスポート設定を再利用してエクスポートできるよう、データエクスポート設定を保存できます。

次に示す節では、Data Export ツールの使用方法について説明します。

- 653 ページの「インベントリ情報のエクスポート手順」
- 656 ページの「既存の環境設定ファイルのロード」
- 657 ページの「インベントリサーバからの Data Export プログラムの実行」

インベントリ情報のエクスポート手順

1 ConsoleOne で、コンテナを選択します。

2 Data Export ツールを実行します。

- データベースオブジェクトからデータエクスポートツールを実行するには、データベースオブジェクトを右クリックし、[ZENworks Inventory] > [Data Export] の順にクリックします。
- ConsoleOne の [Tools] メニューからデータエクスポートツールを実行するには、まずインベントリデータベースを設定してから、[Tools] > [ZENworks Inventory] > [Data Export] の順にクリックする必要があります。インベントリデータベースの設定方法の詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

3 [Create a New Database Query] を選択します。

このオプションにより、ハードウェア、ソフトウェア、ネットワーク、およびその他エクスポート対象になるインベントリコンポーネントを定義した新しい照会条件を追加できます。照会対象のサーバとデータベースサイトを制限する基準を指定することもできます。指定したインベントリコンポーネントと基準に従って、データベースからインベントリ情報が .csv または .xml ファイルにエクスポートされます。

注： データエクスポート用の既存の設定をロードする場合は、[Open a Saved Database Query] を選択します。このオプションを使って、データエクスポート用の設定を編集し、データを .csv または .xml ファイルにエクスポートすることができます。詳細については、656 ページの「既存の環境設定ファイルのロード」を参照してください。

4 [Next] をクリックします。

5 インベントリ対象サーバのフィルタ条件を指定します。

5a [Edit Query] をクリックします。照会の定義方法の詳細については、638 ページの「データベース照会によるインベントリ対象サーバのインベントリ情報の表示」を参照してください。

5b （オプション）サポートされているカテゴリのソフトウェアクラスおよび属性を使って照会を定義した場合に限り、[Enable Filter] オプションを選択できます。サポートされているカテゴリは次のとおりです。

カテゴリ 1:Software Group、Software Group File Information、Software Group Patch Information、Software、File Information、および Patch Information

カテゴリ 2:Exclude File Information

カテゴリ 3:Disk Usage

異なるカテゴリに属する属性が照会に含まれる場合は、[Enable Filter] オプションを選択することができません。たとえば、software.name=word、softwaregroup.name=office、および diskusage.name=exe を含む照会の場合、このオプションを利用することができません。

前の条件を満たす照会に基づいて、.csv または .xml ファイルに保存される結果のフィルタ処理を実行する場合は、[Enable Filter] チェックボックスを選択します。

5c インベントリデータベースから情報をエクスポートするためのスコープを設定します。

ConsoleOne スナップインおよびデータエクスポートツールが ZENworks 6.5 Server Management および ZENworks 6.5 Desktop Management の両方にインストールされている場合、データエクスポートツールを使って、インベントリ情報のエクスポート対象であるスコープを変更することができます。

デフォルトでは、[Servers] オプションが有効になります。照会式を満たすすべてのインベントリ対象サーバが検索されます。ZENworks 6.5 Server Management および ZENworks 6.5 Desktop Management が同じ環境にインストールされている場合は、[Workstations]、[Servers]、および [Both] の各オプションを利用できます。[Servers] を選択すると、照会式を満たすすべてのインベントリ対象サーバが検索されます。[Both] を選択すると、照会式を満たすインベントリ対象ワークステーションおよびインベントリ対象サーバがすべて検索されます。

5d 定義した照会を確認します。

5e [Next] をクリックします。

6 データベースフィールドのリストからデータベースフィールドを選択し、[Add] をクリックします。

グループコンポーネントを選択すると、グループに属するすべてのサブコンポーネントも追加されます。たとえば、Software コンポーネントグループを選択すると、Software のサブコンポーネント（ベンダ名、製品名、バージョンなど）も追加されます。

7 [Next] をクリックします。

8 データエクスポートの設定を表示します。

8a [Save Configuration] をクリックして、環境設定を .exp ファイルに保存します。.exp ファイルのファイル名を指定し、[Save] をクリックします。

環境設定ファイル (.exp) には、選択したインベントリコンポーネントなどの設定のほかに、インベントリ対象サーバのデータエクスポートにフィルタを適用するために作成した照会も含まれます。.exp ファイルを作成するのは、必要に応じて環境設定を再ロードして、.csv または .xml ファイルを生成できるようにするためです。

8b [Next] をクリックします。

9 照会を実行するコンピュータを選択します。

9a **[Perform the Query from This Computer]** : コンピュータからデータエクスポート処理を実行するには、[Perform the Query from This Computer] を選択します。このオプションは、指定したデータベースサーバのインベントリデータベースにアクセスし、.csv または .xml ファイルにデータをエクスポートします。

[Perform the Query on a Remote Server] : Server Inventory コンポーネントがインストールされているサーバから Data Export プログラムを実行するには、[Perform the Query on a Remote Server] を選択します。

10,000 以上のインベントリ対象サーバを含む大容量データベースから情報をエクスポートする場合、またはエクスポートのために 20 以上のデータベースフィールドを選択した複雑な照会を使用する場合、サーバから Data Export プログラムを実行することをお勧めします。

9b .csv または .xml ファイルにコンピュータのデフォルトのエンコードを適用する場合は、[Default Encoding] を選択します。[Default Encoding] はデフォルトで選択されています。.csv または .xml ファイルに Unicode エンコードを適用するには、[Unicode Encoding] を選択します。

注: ローカルコンピュータからデータエクスポートを実行するのに .exp ファイルを作成したが、同じ .exp を使用してリモートサーバからデータエクスポートを実行し、Unicode エンコードを使用する場合、手動で .exp ファイルを編集して、DEExportEncode の値を UNICODE に設定する必要があります。

9c [Next] をクリックします。

10 エクスポートオプションを選択します。

10a 次の中から、いずれかのオプションを選択します。

[Export to CSV] : インベントリ情報を .csv ファイルに保存します。

[Export to XML] : インベントリ情報を .xml ファイルに保存します。

10b .csv または .xml ファイルのパスとファイル名を指定します。

10c [Finish] をクリックします。

環境設定ファイルが保存されない場合、変更の保存を促すメッセージが表示されます。

これにより、指定したディレクトリ内に .csv または .xml ファイルが生成されます。

.csv ファイルにエクスポートされたデータを確認するには、Microsoft Excel やその他の CSV 対応ビューアでファイルを開きます。

.xml ファイルの場合は、XML Spy などの XML ビューアでファイルを開きます。詳細については、658 ページの「XML の概要と XML ファイルの内容」を参照してください。

既存の環境設定ファイルのロード

既存の環境設定ファイル (.exp) をロードすることができます。.exp ファイルには、選択したインベントリコンポーネントなどの設定のほかに、インベントリ対象ワークステーションのデータエクスポートにフィルタを適用するために作成した照会も含まれます。

.exp ファイルをロードした後で、データエクスポートの設定を変更し、.csv または .xml ファイルにデータをエクスポートできます。

データエクスポートのため、既存の環境設定をロードするには

1 データ環境設定ファイルが生成されていることを確認します。

653 ページの「インベントリ情報のエクスポート手順」で説明されている手順を完了します。この手順により、.csv または .xml ファイルおよびデータ環境設定ファイルが生成されます。

2 ConsoleOne でコンテナを選択し、次のいずれかの手順を実行して Data Export ツールを起動します。

- データベースオブジェクトからデータエクスポートツールを実行するには、データベースオブジェクトを右クリックし、[ZENworks Inventory] > [Data Export] の順にクリックします。
- ConsoleOne の [Tools] メニューからデータエクスポートツールを実行するには、まずインベントリデータベースを設定してから、[Tools] > [ZENworks Inventory] > [Data Export] の順にクリックする必要があります。インベントリデータベースの設定方法の詳細については、625 ページの「インベントリデータベースの設定」を参照してください。

3 [Open a Saved Database Query] を選択し、[Next] をクリックします。

.exp ファイルのデフォルトディレクトリは、consoleone¥*consoleone_version*¥reporting¥export です。[Browse] をクリックして、既存の .exp ファイルを開きます。

.exp および .cfg ファイルが無効であるか、古いバージョンである場合、データのエクスポートは実行されません。データのエクスポートにより、エクスポートの照会条件およびフィルタ条件を満たすサーバの数およびサーバが表示されます。

4 保存された照会のリストから、保存済みのデータベース照会を選択します。

4a 保存された照会のリストから、保存済みのデータベース照会を選択します。リストボックスには、consoleone¥*consoleone_version*¥reporting¥export で保存されている .exp ファイルが表示されます。

または

[Browse] をクリックして、他の場所に保存されている既存の .exp ファイルを開きます。

4b (オプション) .exp および .cfg ファイルが無効であるか、古いバージョンである場合、データのエクスポートは実行されません。データのエクスポートにより、エクスポートの照会条件およびフィルタ条件を満たすサーバの数およびサーバが表示されます。

既存の照会を編集する場合は、[Edit] をクリックして照会を編集し、新しいデータベースフィールドを選択します。照会の定義方法の詳細については、638 ページの「データベース照会によるインベントリ対象サーバのインベントリ情報の表示」を参照してください。

4c [Next] をクリックします。

5 データエクスポートの設定を表示します。

5a [Save Configuration] をクリックして、環境設定を .exp ファイルに保存します。.exp ファイルのファイル名を指定し、[Save] をクリックします。

環境設定ファイル (.exp) には、選択したインベントリコンポーネントなどの設定のほかに、インベントリ対象サーバのデータエクスポートにフィルタを適用するために作成した照会も含まれます。.exp ファイルを作成するのは、必要に応じて環境設定を再ロードして、.csv または .xml ファイルを生成できるようにするためです。

5b [Next] をクリックします。

6 照会を実行するコンピュータを選択します。

6a **[Perform the Query from This Computer]** : コンピュータからデータエクスポート処理を実行するには、[Perform the Query from This Computer] を選択します。このオプションは、指定したデータベースサーバのインベントリデータベースにアクセスし、.csv または .xml ファイルにデータをエクスポートします。

[Perform the Query on a Remote Server] : Server Inventory コンポーネントがインストールされているサーバから Data Export プログラムを実行するには、[Perform the Query on a Remote Server] を選択します。

10,000 以上のインベントリ対象サーバを含む大容量データベースから情報をエクスポートする場合、またはエクスポートのために 20 以上のデータベースフィールドを選択した複雑な照会を使用する場合、サーバから Data Export プログラムを実行することをお勧めします。

6b .csv または .xml ファイルにコンピュータのデフォルトのエンコードを適用する場合は、[Default Encoding] を選択します。[Default Encoding] はデフォルトで選択されています。.csv または .xml ファイルに Unicode エンコードを適用するには、[Unicode Encoding] を選択します。

6c [Next] をクリックします。

7 エクスポートオプションを選択します。

7a 次の中から、いずれかのオプションを選択します。

[Export to CSV] : インベントリ情報を .csv ファイルに保存します。

[Export to XML] : インベントリ情報を .xml ファイルに保存します。

7b .csv または .xml ファイルのパスとファイル名を指定します。

7c [Finish] をクリックします。

インベントリサーバからの Data Export プログラムの実行

10,000 以上のインベントリ対象サーバを含む大容量データベースから情報をエクスポートする場合、またはエクスポートのために 20 以上のデータベースフィールドを選択した複雑な照会を使用する場合、サーバから Data Export プログラムを実行することをお勧めします。

サーバから Data Export プログラムを実行するには

1 データ環境設定ファイルが生成されていることを確認します。

653 ページの「インベントリ情報のエクスポート手順」で説明した手順 1 から手順 5 を実行して、.exp ファイルに確実に設定を保存します。

.exp ファイルを保存する際、対応するデータ環境設定ファイルが .exp ファイルと同じディレクトリに同じファイル名で作成されます。拡張子は .cfg です。

2 Server Inventory コンポーネントがインストールされているサーバから Data Export プログラムを実行するには、[Perform the Query on a Remote Server] をクリックして、[Finish] をクリックします。

3 .exp ファイルおよび .cfg ファイルをサーバにコピーします。

この 2 つのファイルは、インベントリサーバの同じディレクトリに存在する必要があります。

サーバコンソールから、NetWare サーバの場合には dbexport.ncf を、Windows サーバの場合は dbexport.bat を実行します。次のように入力します。

DBEXPORT *"configuration_filename.exp" "csv_filename.csv"*

configuration_filename.exp は、データエクスポート設定を含む既存のファイルです。二重引用符内の *configuration_filename.exp* および *csv_filename.csv* にはファイル名を入力する必要があります。データベースからエクスポートされたデータは、*csv_filename.csv* に保存されます。

.exp ファイルに対応する .cfg ファイルは、.exp ファイルと同じフォルダに保存する必要があります。.cfg ファイルには、エクスポートされるデータベース属性のリストが含まれます。

.exp および .cfg ファイルが無効であるか、古いバージョンである場合、データのエクスポートは実行されません。データのエクスポートにより、エクスポートの照会条件およびフィルタ条件を満たすインベントリ対象サーバの数が表示されます。

XML の概要と XML ファイルの内容

Server Inventory により、Data Export ツールを使って、インベントリ情報をインベントリデータベースから XML(.xml) ファイルにエクスポートすることができます。

XML は、構造化されたデータを表すためのフォーマットを提供するマークアップ言語です。XML 文書はテキストベースのフォーマットです。XML のソースは、XML 要素で構成されます XML のタグは事前に定義されていないため、独自にタグを定義する必要があります。

XML に関する詳細については、W3C (World Wide Web Consortium) Activity and Information Web サイト (http://www.w3.org/XML) を参照してください。

.xml ファイルのサンプルは次のとおりです。

```
<?xml version="1.0" encoding='UTF-8'?>

<!DOCTYPE InventoryInformation [<!ELEMENT Attribute (value)>

<!ATTLIST Attribute

     name CDATA #REQUIRED

     type (custom | regular) #REQUIRED

     units CDATA #IMPLIED

>
```

```
<!ELEMENT Class (Attribute*)>
<!ATTLIST Class
     name CDATA #REQUIRED
     instance CDATA #REQUIRED
>
<!ELEMENT InventoryInformation (Machine+)>
<!ELEMENT Machine (Class+)>
<!ATTLIST Machine
     name CDATA #REQUIRED
>
<!ELEMENT value (#PCDATA)>]
>
<InventoryInformation>
  <Machine name="blr-stl-zen1.blr.novell.com">
    <Class name="Processor" instance="1">
      <Attribute name="Current Clock Speed" type="regular" units="MHz">
        <value>2800</value>
      </Attribute>
      <Attribute name="Processor Family" type="regular">
        <value>"Intel(R) Xeon(TM)"</value>
      </Attribute>
    </Class>
    <Class name="IP" instance="1">
      <Attribute name="IP Address" type="regular">
        <value>164.99.163.9</value>
      </Attribute>
      <Attribute name="Subnet Mask" type="regular">
        <value>255.255.252.0</value>
      </Attribute>
    </Class>
  </Machine>
</InventoryInformation>
```

XML は、データを説明するのに DTD(Document Type Definition) を使用します。DTD は、XML 文書内に埋め込まれます。

DTD は、文書内に含まれる要素、属性、およびエンティティを一覧表示するほか、要素と属性間の関係も定義します。

前で示したサンプル xml ファイルに埋め込まれる DTD は次のとおりです。

```
<?xml version="1.0" encoding='UTF-8'?>
<!DOCTYPE InventoryInformation [<!ELEMENT Attribute (value)>
<!ATTLIST Attribute
     name CDATA #REQUIRED
     type (custom | regular) #REQUIRED
     units CDATA #IMPLIED
>
<!ELEMENT Class (Attribute*)>
<!ATTLIST Class
     name CDATA #REQUIRED
     instance CDATA #REQUIRED
>
<!ELEMENT InventoryInformation (Machine+)>
<!ELEMENT Machine (Class+)>
<!ATTLIST Machine
     name CDATA #REQUIRED
>
<!ELEMENT value (#PCDATA)>]
>
```

次の表は、サンプル XML ファイルで使用される要素について説明しています。

サンプル XML ファイルで使用される要素	説明
[Class]	デバイス名
Type	カスタムまたは標準属性
Units	単位情報
Instance	デバイスインスタンス数

CIM スキーマを使用しないインベントリデータベースからのインベントリ情報の取得

ZENworks 6.5 Server Management SP1 には、使いやすいインベントリデータベースビューがあり、CIM スキーマを使用しなくても、インベントリデータベースからインベントリ情報を取得できます。

インベントリビューは、あらかじめ定義されたデバイス固有のビューで、ZENworks 6.5 Server Management SP1 の Server Inventory コンポーネントをインストールした後に、インベントリデータベースに自動的に作成されます。

インベントリビューの命名法は、*database_schema_name.zen_devicename* です。たとえば、mw_dba.zen_processor と指定します。

enum に関連付けられているインベントリビューは、ローカライズされたビューを持ちます。たとえば、mw_dba.zen_processor_ja は、プロセッサの日本語ビューです。

次の節では、さまざまなインベントリビューとその使用方法について説明します。

- 661 ページの「インベントリビューのリスト」
- 684 ページの「インベントリビューの使用方法」

インベントリビューのリスト

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
mw_dba.zen_asset	アセット情報を取得します。	SystemName	インベントリ対象サーバの DNS 名。	Yes
		Manufacturer	ベンダ名。	
		Model	コンピュータシステムのモデル。	
		SerialNumber	メーカーによってコンピュータシステムに割り当てられるシリアル番号。	
		Tag	システム情報の一意の識別子。	
		ManagementTechnology	DMI、WMI など、インベントリ対象サーバで利用できるテクノロジ。	
		AssetTag	ROM ベースのセットアッププログラムにより作成される備品タグ番号。	
		ModelNumber	コンピュータシステムのモデル番号。	
mw_dba.zen_battery	バッテリ情報を取得します。	Name	Duracell* DR-36 など、バッテリの製品名。	Yes
		Chemistry	リチウムイオン、ニッケル水素などバッテリの種類。	
		DesignCapacity	バッテリのデザイン容量（ミリワット時間単位）。	
		DesignVoltage	バッテリのデザイン電圧（ミリボルト単位）。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		SmartBatteryVersion	バッテリがサポートしているスマートバッテリデータ仕様のバージョン番号。	
		InstallDate	バッテリの製造日。	
		Manufacturer	バッテリの製造元の名前。	
		SerialNumber	バッテリのシリアル番号。	
mw_dba.zen_bios	BIOS 情報を取得します。	Caption	BIOS のラベル。	Yes
		InstallDate	BIOS の製造日。	
		SerialNumber	製造時にコンピュータに割り当てられるシリアル番号。	
		Version	BIOS のバージョンまたはリビジョンレベル。	
		Manufacturer	BIOS のベンダ名。	
		PrimaryBIOS	True の状態はプライマリ BIOS を示します。	
		BIOSIDBytes	BIOS でコンピュータモデルを示すバイト。	
		Size	BIOS のサイズ。	
mw_dba.zen_bus	バス情報を取得します。	BusType	PCI、ISA などのバスの種類。	Yes
		BusName	バス名。	
		BusDescription	バスの説明。	
		BusVersion	マザーボードがサポートしているバスのバージョン。	
		DeviceID	特定のバスの固有 16 進 ID。	
mw_dba.zen_cachememory	キャッシュメモリ情報を取得します。	ErrorMethodology	キャッシュコンポーネントがサポートしているエラー修正方式。パリティ / シングルビット ECC/ マルチビット ECC など。	Yes

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Level	マイクロプロセッサに組み込まれている内部キャッシュまたはCPUとDRAM間にある外部キャッシュのキャッシュレベルを示します。	
		WritePolicy	キャッシュがメモリに書き込む2つの方法（ライトバックとライトスルーキャッシュ）を示します。	
		CacheType	命令、データ、ユニファイドなど、システムのキャッシュタイプを定義します。	
		LineSize	シングルキャッシュバケットまたはシングルキャッシュラインのサイズ（バイト単位）。	
		ReplacementPolicy	再使用するキャッシュラインまたはキャッシュバケットを決定するために、キャッシュが使用するアルゴリズム。	
		ReadPolicy	データキャッシュが読み取り処理用であるかどうかを示します。	
		Associativity	システムキャッシュの連想性を定義します（ダイレクトマップ、2ウェイ、4ウェイ）。	
		Speed	システムキャッシュモジュールの速度（ナノ秒単位）。	
		Capacity	キャッシュ情報を格納しているデータストアのサイズ。	
mw_dba.zen_cdrom	CDROM情報を取得します。	DeviceID	インベントリ対象サーバ上のCDに割り当てられているドライブを表す文字。	No
		Manufacturer	CDのベンダ名。	
		Description	CDの説明。	
		Caption	CDのキャプション。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
mw_dba.zen_chassis	シャシー情報を取得します。	AssetTag	システムシャシーの備品タグ番号。例： S11127。	Yes
		NumberOfPowerCords	システムシャシーに接続されている電源コードの総数。	
		ChassisType	システムシャシーがラップトップ、デスクトップ、ノートブック、ドッキングステーションなどのいずれであるかを示します。	
		Manufacturer	システムシャシー製造元の名前。例： Compaq。	
		SerialNumber	システムシャシーを識別するための製造元番号。例： 53R661S。	
		Tag	特定のインベントリ対象サーバに接続されているシステムシャシーの一意な ID。例： System Enclosure 0。	
		Version	システムシャシーのバージョン番号。	
mw_dba.zen_computerinformation	コンピュータ情報を取得します。	ComputerName	インベントリ対象サーバの完全修飾 DN など、eDirectory で表示されるインベントリ対象サーバの名前。	No
		PrimaryOwner	このシステムの主なユーザまたは所有者の名前。	
		PrimaryOwnerContact	このシステムの主なユーザの電話番号。	
mw_dba.zen_currentlogindetails	現在のログイン情報を取得します。	CurrentUser	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーにログインしたユーザ。	No
mw_dba.zen_disk	ディスク情報を取得します。	RemovableDisk	リムーバブルディスク。	Yes
		Manufacturer	ディスクのベンダ名。	
		Description	ディスクの説明。	
		PhysicalCylinders	シリンダ数。	
		PhysicalHeads	ヘッド数。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		SectorsPerTrack	トラックあたりのリムーバルディスクドライブのセクタ数。	
		Capacity	リムーバルディスクの容量。	
mw_dba.zen_diskusage	ディスク使用状況の情報を取得します。	FileExtension	ディスク使用状況をスキャンするファイル拡張子。	No
		TotalDiskUsage	指定された拡張子を持つすべてのファイルの総合的なディスク使用状況。	
mw_dba.zen_displayadapter	ディスプレイアダプタ情報を取得します。	Description	ディスプレイアダプタに関する説明。	Yes
		VideoMemoryType	このアダプタ用のビデオメモリの種類（VRAM/SRAM/DRAM/EDO RAM など）。	
		MaxMemorySupported	ディスプレイアダプタが VIDEO RAM に対してサポートする最大メモリ。	
		CurrentBitsPerPixel	各ピクセルに隣接するカラービット数。	
		CurrentHorizontalResolution	ディスプレイに表示される水平方向のピクセル数。	
		CurrentVerticalResolution	ディスプレイに表示される垂直方向のピクセル数。	
		MaxRefreshRate	ディスプレイを再描画するためのモニタの最大リフレッシュレート（ヘルツ単位）。	
		MinRefreshRate	ディスプレイを再描画するためのモニタの最小リフレッシュレート（ヘルツ単位）。	
		VideoArchitecture	このシステムのビデオサブシステムのアーキテクチャ（CGA/VGA/SVGA/8514A など）。	
		NumberOfColorPlanes	ビデオシステムがサポートしている色平面の数。	
		ChipSet	システム機能を比較するのにコントローラが使用するチップセット。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		DACType	デジタルアナログコンバータの種類。	
		ProviderName	ベンダ名。	
mw_dba.zen_displaydriver	ディスプレイドライバ情報を取得します。	Manufacturer	ディスプレイドライバの製造元の名前。	yes
		Version	ディスプレイドライバのバージョン番号。	
		InstallDate	ディスプレイドライバのインストール日。	
		IsShadowed	True の場合、ディスプレイドライバは現在シャドウ処理されています。	
mw_dba.zen_distinguishedname	識別名を取得します。	DistinguishedName	識別名。	No
		Tree	eDirectory ツリー名	
mw_dba.zen_dma	DMA 情報を取得します。	Description	この DMA チャネルを現在使用している論理デバイスの名前。	Yes
		DMAChannel	コンピュータとデバイスとの間で、DMA チャネルのないコンピュータよりも高速にデータを転送するためにコンピュータが使用する DMA チャネルの番号。	
		Availability	DMA（仮想ダイレクトメモリアクセス）がサポートされているかどうかを示します。	
		BurstMode	データが通常よりも高速で送信されるデータ転送モード。	
mw_dba.zen_dnsname	DNS 名を取得します。	HostName	インベントリ対象サーバの DNS 名。	No
mw_dba.zen_floppy	フロッピー情報を取得します。	DeviceID	フロッピーを表すフロッピー名。	No
		Manufacturer	ベンダ名。	
		Description	フロッピードライブに関する説明。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		PhysicalCylinders	フロッピーディスクのシリンダまたはトラックの合計数。	
		PhysicalHeads	フロッピードライブの読み取り / 書き込みヘッド。	
		SectorsPerTrack	フロッピードライブの 1 トラックあたりのセクタ数。	
		Capacity	フロッピードライブの容量。	
mw_dba.zen_inventoryscanner	Inventory Scanner 情報を取得します。	LastScanDate	Scanner が最後にスキャンされた日。ミリ秒値で保存されるため、どの日付形式でも読み込みおよび表示できます。	Yes
		InventoryServer	スキャンの送信先インベントリサーバの名前。サーバ名の完全な DN ではありません。	
		Version	インベントリ対象サーバで実行している Scanner のバージョン。	
		ScanMode	WMI や DMI など、コンピュータシステムをスキャンするために Scanner で使用する管理テクノロジ。	
		RecentInformation	最新のインベントリ情報。	
		generaldictionaryversion	一般ディクショナリのバージョン。	
		privatedictionaryversion	プライベートディクショナリのバージョン。	
mw_dba.zen_ipaddress	IP アドレスを取得します。	Address	IP インターネット上のコンピュータに割り当てられた一意のアドレス。	No
		SubnetMask	インベントリ対象サーバのサブネットマスクは、IP アドレスと組み合わせられ、ネットワーク ID である IP アドレスのオクテット / ビットと、ノード ID であるオクテット / ビットを IP ルータに指定します。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
mw_dba.zen_ipxaddress	IPX アドレスを取得します。	Address	インベントリ対象サーバの IPX アドレス。	No
mw_dba.zen_irq	IRQ 情報を取得します。	IRQNumber	IRQ（割り込み要求行）の数（0 ～ 15）。	Yes
		Availability	特定の IRQ チャネルの可用性。	
		TriggerType	IRQ トリガの種類。	
		Shareable	True の場合、デバイス間でシステム IRQ を共有できます。	
mw_dba.zen_keyboard	キーボード情報を取得します。	KeyboardLayout	キーボードのレイアウト。	No
		KeyboardSubtype	キーボードの種類。	
		KeyboardDescription	IBM 拡張キーボード 101/102 など、キーボードに関する説明。	
		NumberOfFunctionKeys	ファンクションキーの総数。	
		KeyboardDelay	キー入力を繰り返すまでの遅延時間。	
		TypematicRate	キーの処理速度。	
mw_dba.zen_lastlogindetails	最新のログイン詳細を取得します。	LastUser	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーに最後にログインしたユーザ。	No
mw_dba.zen_macaddress	MAC アドレスを取得します。	MACAddress	一意のノードアドレスがネットワークアダプタ内に永続的に記述され、これによってネットワーク上の特定のコンピュータが識別されます。	No
mw_dba.zen_memory	メモリ情報を取得します。	TotalMemory	インベントリ対象サーバの総メモリ量。	No
mw_dba.zen_microsoftdomainname	Microsoft ドメイン名を取得します。	DomainName	インベントリ対象サーバのドメイン名。	No
mw_dba.zen_internalmodem	内蔵モデム情報を取得します。	Name	モデムの識別情報。	No
		Description	モデムに関する詳細情報。	
		ProviderName	ベンダ名。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		DeviceID	モデムの種類を識別する特殊な 16 進数の文字列。	
mw_dba.zen_monitor	モニタ情報を取得します。	DeviceID	インベントリ対象に接続されているデスクトップモニタの一意な ID。 例： DesktopMonitor1。	No
		ModelID	モニタのモデルの一意な ID。メーカー ID と製品 ID の組み合わせです。 例： DELA001。	
		MonitorDescription	モニタの説明。	
		NominalSize	モニタの対角線上の長さを示す数値（画面の片隅から反対側の隅までの距離）。 （例： 17)″ Server Inventory ポリシーを使用して HWRules の ini ファイルを設定することにより、モニタの公称サイズのスキャンをカスタマイズできます。	
		ViewableSize	イメージを縁取る黒い枠を除いて、画面イメージの対角線上の長さを示す数値。 （例： 15.8)″	
		ManufacturedDate	モニタの製造年。	
		MonitorSerialNumber	メーカーのモニタ識別番号。 例： 23DDC24N9067。	
		Manufacturer	モニタのメーカー名。 例： DELL* Computer Corp。	
		Model	メーカーが付けたモニタの製品名。 例： DELL E771a。	
mw_dba.zen_motherboard	マザーボード情報を取得します。	Description	マザーボードの一般的な説明。	No
		Manufacturer	マザーボードの製造元の名前。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Version	マザーボードのバージョン。	
		NumberOfSlots	メモリの増設、グラフィック機能の追加、および特殊デバイスのサポートを実現するための、マザーボード内の拡張スロット数。	
mw_dba.zen_mouse	マウス情報を取得します。	MouseType	マウスの種類。	Yes
		MouseName	マウスの識別情報。	
		NumberOfButtons	マウスのボタン数。	
		IRQNumber	このデバイスに割り当てられた割り込み。	
mw_dba.zen_mousedriver	ドライバ情報を取得します。	DriverName	マウスドライバ名。	No
		DriverVersion	マウスドライバのバージョン番号。	
mw_dba.zen_NetworkAdapter	ネットワークアダプタ情報を取得します。	Caption	ネットワークアダプタのキャプション。	Yes
		Description	ネットワークアダプタの説明。	
		InstallDate	ネットワークアダプタのインストール日。	
		Name	ネットワークアダプタ名。	
		PermanentAddress	アダプタに永続的に格納されるノードアドレス。	
		MACAddress	ネットワークアダプタに保存されている MAC アドレス。	
		MaxSpeed	LAN のデータ転送速度。	
		AdapterType	FDDI、トークンリングなどのネットワークアダプタの種類。	
		ProviderName	プロバイダ名。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
mw_dba.zen_NetworkAdapterDriver	ネットワークアダプタドライバ情報を取得します。	Description	インベントリ対象サーバにインストールされているネットワークアダプタドライバの説明。 たとえば、IBM 10/100 Ethernet アダプタ、EN-2420Px Ethernet アダプタ。	No
		Name	ネットワークアダプタドライバの名前。	
		Version	ネットワークアダプタのバージョン。	
mw_dba.zen_parallelport	パラレルポート情報を取得します。	PortName	現在の運用環境で、このパラレルポート上にある入出力デバイスの論理名。	Yes
		HasDMASupport	True の場合、DMA がサポートされています。	
		PortAddress	このパラレルポートの基本 I/O アドレス。	
		IRQNumber	パラレルポートの IRQ 番号。	
mw_dba.zen_powersupply	電源装置情報を取得します。	Description	この電源装置の入力電圧容量に関する詳細情報。	No
		TotalOutputPower	電源装置の総出力を表す属性値。	
mw_dba.zen_processor	プロセッサ情報を取得します。	DeviceID	プロセッサの種類を識別する特殊な 16 進数の文字列。	Yes
		Description	プロセッサに関する詳細情報。	
		Role	中央プロセッサ、数値演算コプロセッサなど、プロセッサの種類。	
		Family	Pentium II、Pentium III など、プロセッサファミリの識別情報。	
		OtherFamilyDescription	MMX テクノロジを搭載した Pentium プロセッサなど、プロセッサファミリに関する詳しい説明。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		UpgradeMethod	このプロセッサのアップグレード方法（アップグレードがサポートされている場合）。	
		MaxClockSpeed	プロセッサの最大クロック速度。	
		CurrentClockSpeed	プロセッサの現在のクロック速度。	
		Stepping	マイクロプロセッサのベンダによって指定された、プロセッサのモデルを識別するための 1 バイトコード特性。	
mw_dba.zen_serialport	シリアルポート情報を取得します。	PortName	現在の運用環境で、このシリアルポート上にある I/O デバイスの論理名。	No
		PortAddress	このシリアルポートの基本入出力アドレス。	
		IRQNumber	シリアルポートの IRQ 番号。	
mw_dba.zen_soundadapter	サウンドアダプタ情報を取得します。	Name	マルチメディアカードのラベル。	No
		Description	サーバのマルチメディアコンポーネントの説明。	
		ProviderName	プロバイダ名。	
mw_dba.zen_systemslot	システムスロット情報を取得します。	SlotDescription	このスロットを現在使用しているカード。	No
		MaxDataWidth	スロットで許容されているカードの最大バス幅。	
		ThermalRating	スロットの最大熱損失量（ミリワット単位）。	
mw_dba.zen_unixOS	Unix オペレーティングシステム情報を取得します。	Type	インベントリ対象サーバのオペレーティングシステム。	Yes
		Caption	オペレーティングシステム名。	
		CodePage	オペレーティングシステムの言語コードページ。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Version	オペレーティングシステムのバージョン番号。	
		InstallDate	オペレーティングシステムのインストール日	
		VirtualMemorySize	呼び出しプロセスの仮想アドレス領域における総バイト数。	
		VisibleMemorySize	オペレーティングシステムにより報告された合計メモリ。	
		ProviderName	プロバイダ名。	
		KernelVersion	オペレーティングシステムのバージョン番号。	
		SwapSpaceSize	スワップスペースの合計サイズ。	
mw_dba.zen_windowsOS	Windows オペレーティングシステム情報を取得します。	Type	インベントリ対象サーバのオペレーティングシステム。	Yes
		OtherTypeDescription	オペレーティングシステムに関する補足説明（利用できる場合）。	
		Caption	オペレーティングシステム名。	
		CodePage	オペレーティングシステムの言語コードページ。	
		Version	オペレーティングシステムのバージョン番号。	
		InstallDate	オペレーティングシステムのインストール日	
		VirtualMemorySize	呼び出しプロセスの仮想アドレス領域における総バイト数。	
		VisibleMemorySize	オペレーティングシステムにより報告された合計メモリ。	
		ProviderName	プロバイダ名。	
mw_dba.zen_NetWareOS	NetWare オペレーティングシステム情報を取得します。	Type	インベントリ対象サーバのオペレーティングシステム。	Yes

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Caption	オペレーティングシステム名。	
		CodePage	オペレーティングシステムの言語コードページ。	
		Version	オペレーティングシステムのバージョン番号。	
		InstallDate	オペレーティングシステムのインストール日	
		VirtualMemorySize	呼び出しプロセスの仮想アドレス領域における総バイト数。	
		VisibleMemorySize	オペレーティングシステムにより報告された合計メモリ。	
		SizeStoredInPagingFiles	オペレーティングシステムのページングファイルに格納できるキロバイトの合計数。	
		ProviderName	プロバイダ名。	
		AccountingVersion	NetWare サーバ固有の属性。	
		InternetBridgeSupport	NetWare サーバ固有の属性。	
		MaxNumberOfConnections	NetWare サーバ固有の属性。	
		MaxNumberOfVolumes	NetWare サーバ固有の属性。	
		PeakConnectionsUsed	NetWare サーバ固有の属性。	
		PrintServerVersion	NetWare サーバ固有の属性。	
		QueuingVersion	NetWare サーバ固有の属性。	
		RevisionLevel	NetWare サーバ固有の属性。	
		SecurityRestrictionLevel	NetWare サーバ固有の属性。	
		SFTLevel	NetWare サーバ固有の属性。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		TTSlevel	NetWare サーバ固有の属性。	
		VAPVersion	NetWare サーバ固有の属性。	
		VirtualConsoleVersion	NetWare サーバ固有の属性。	
		InternalNetworkNumber	NetWare サーバ固有の属性。	
mw_dba.zen_software	ソフトウェア情報を取得します。	Name	ベンダの商標または登録商標として示されるベンダ定義の製品名。	Yes
		Vendor	ソフトウェアのベンダ名。	
		Version	製品のわかりやすいバージョン。 たとえば、Windows 2000 のバージョンは 2000 です。通常、製品のバージョンはメジャー番号とマイナー番号 (Major.Minor) で構成されます。	
		ProductID	インストールされている製品の一意な半角 16 文字の識別子。この識別子は Windows の MSI から使用できます。 書式は ABCD-1234-WXYZ-PQRS です。	
		InternalVersion	製品の内部バージョン。 書式は、次のいずれかです。 *major version.minor version.build.sub build number* または *major version.minor version.build*	
		Language	この製品の言語を示すわかりやすい名前。	
		FriendlyName	ソフトウェアの表示名。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Uninstallstring	この製品をアンインストールするために呼び出すコマンド。現在、このコマンドは Windows の ARP（[プログラムの追加と削除]）および MSI で使用できます。	
		Supportpack	製品のインストールされたサポートパックの番号。	
		SoftwareEdition	ベンダが定義した製品エディション。Professional など。	
		LastExecutionTime	製品が最後に実行された日付と時刻のスタンプ。	
		Frequencyofusage	製品の使用回数。	
		Description	製品の説明。	
		InstallationSource	この製品をインストールするときにインストールファイルを保存したファイルシステムパスを識別します。現在、このコマンドは Windows の ARP および MSI で使用できます。	
		InformationRepository	スキャンのソース（[プログラムの追加と削除]、MSI、ソフトウェアディクショナリ、または PRODUCTS.DAT）。	
		Category	製品が属する製品カテゴリ。 たとえば、Office は生産性ツールのカテゴリに属し、ソリティアはゲームのカテゴリに属します。	
		Helplink	ARP および MSI で使用可能な製品のサポート Web サイトの URL。	
		PackageGUID	MSI で使用可能なベンダ定義の製品 GUID。	
		Path	製品をインストールしたインベントリ対象サーバ上のディレクトリパス。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
mw_dba.zen_softwaregroup	ソフトウェアグループ情報を取得します。	Name	ベンダの商標または登録商標として示されるベンダ定義のソフトウェアグループ名。	Yes
		Vendor	ソフトウェアグループのベンダ名。	
		Version	ソフトウェアグループのわかりやすいバージョン。	
		ProductID	インストールされている製品の一意な半角 16 文字の識別子。この識別子は Windows の MSI から使用できます。 書式は ABCD-1234-WXYZ-PQRS です。	
		InternalVersion	製品の内部バージョン。 書式は、次のいずれかです。 *major version.minor version.build.sub build number* または *major version.minor version.build*	
		Language	この製品の言語を示すわかりやすい名前。	
		FriendlyName	ソフトウェアの表示名。	
		Uninstallstring	この製品をアンインストールするために呼び出すコマンド。現在、このコマンドは Windows の ARP（［プログラムの追加と削除］）および MSI で使用できます。	
		Supportpack	製品のインストールされたサポートパックの番号。	
		SoftwareEdition	ベンダが定義した製品エディション。 Professional など。	
		LastExecutionTime	製品が最後に実行された日付と時刻のスタンプ。	
		Frequencyofusage	製品グループの使用回数。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Description	製品グループの説明。	
		InstallationSource	この製品をインストールするときにインストールファイルを保存したファイルシステムパスを識別します。現在、このコマンドは Windows の ARP および MSI で使用できます。	
		InformationRepository	スキャンのソース（[プログラムの追加と削除]、MSI、ソフトウェアディクショナリ、または PRODUCTS.DAT）。	
		Category	製品が属する製品カテゴリ。 たとえば、Office は生産性ツールのカテゴリに属し、ソリティアはゲームのカテゴリに属します。	
		Helplink	ARP および MSI で使用可能な製品のサポート Web サイトの URL。	
		PackageGUID	MSI で使用可能なベンダ定義の製品 GUID。	
		Path	製品をインストールしたインベントリ対象サーバ上のディレクトリパス。	
mw_dba.zen_softwarepatch	ソフトウェアパッチ情報を取得します。	productid	ソフトウェアパッチのソフトウェア ID。	No
		PatchName	ベンダが定義したパッチ名。	
mw_dba.zen_antivirus	アンチウィルス製品情報を取得します。	Name	ベンダの商標または登録商標として示されるベンダ定義のアンチウィルス製品名。	Yes
		Vendor	アンチウィルス製品のベンダ名。	
		Version	アンチウィルス製品のわかりやすいバージョン。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		ProductID	インストールされているアンチウィルス製品の一意な 16 文字の識別子。この識別子は Windows の MSI から使用できます。 書式は ABCD-1234-WXYZ-PQRS です。	
		InternalVersion	アンチウィルス製品の内部バージョン。 書式は、次のいずれかです。 *major version.minor version.build.sub build number* または *major version.minor version.build*	
		Language	このアンチウィルス製品の言語を示すわかりやすい名前。	
		FriendlyName	アンチウィルス製品の表示名。	
		Uninstallstring	この製品をアンインストールするために呼び出すコマンド。現在、このコマンドは Windows の ARP（［プログラムの追加と削除］）および MSI で使用できます。	
		Supportpack	アンチウィルス製品のインストールされたサポートパックの番号。	
		SoftwareEdition	ベンダが定義したアンチウィルス製品エディション。	
		LastExecutionTime	アンチウィルス製品が最後に実行された日付と時刻のスタンプ。	
		Frequencyofusage	アンチウィルス製品の使用回数。	
		Description	アンチウィルス製品の説明。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		InstallationSource	このアンチウィルス製品をインストールするときにインストールファイルを保存したファイルシステムパスを識別します。現在、このコマンドは Windows の ARP および MSI で使用できます。	
		InformationRepository	スキャンのソース（[プログラムの追加と削除]、MSI、ソフトウェアディクショナリ、または PRODUCTS.DAT）。	
		DefinitionDate	コンピュータにインストールされたウィルス定義ファイルの日付。一部のアンチウィルス製品は、日付とバージョンを 1 つの文字列に組み合わせています。	
		DefinitionVersion	コンピュータにインストールされている、ベンダが定義したバージョンのウィルス定義ファイル。	
		Category	アンチウィルス製品が属する製品カテゴリ。	
		Helplink	ARP および MSI で使用可能なアンチウィルス製品のサポート Web サイトの URL。	
		PackageGUID	MSI で使用可能なベンダ定義のアンチウィルス製品 GUID。	
		Path	アンチウィルス製品をインストールしたインベントリ対象サーバ上のディレクトリパス。	
mw_dba.zen_dictionaryfile	ZENworks ソフトウェアディクショナリファイル情報を取得します。	fileid	ディクショナリファイル ID。	Yes
		directoryid	ディレクトリ ID。	
		FileName	ディクショナリファイルのファイル名。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		Directory	ディクショナリファイルが保存されるディレクトリ名。	
		FileVersion	ディクショナリファイルのバージョン。	
		FileSize	ディクショナリファイルのサイズ。	
		LastModified	ディクショナリファイルが最後に変更された日付。	
		InternalName	内部名。	
		ProductVersion	このファイルが示す製品のバージョン。	
		Company	ベンダ名。	
		ProductName	このファイルが示す製品。	
		Language	このファイルの言語を示すわかりやすい名前。	
		SoftwareDictionaryID	一般ソフトウェアディクショナリで示されるファイルの ID。	
mw_dba.zen_excludedfile	除外されたファイル情報を取得します。	fileid	除外されたファイル ID。	Yes
		directoryid	ディレクトリ ID。	
		FileName	除外されたファイルのファイル名。	
		Directory	除外されたファイルが保存されるディレクトリ名。	
		FileVersion	除外されたファイルのバージョン。	
		FileSize	除外されたファイルのサイズ。	
		LastModified	除外されたファイルが最後に変更された日付。	
		InternalName	内部名。	
		ProductVersion	このファイルが示す製品のバージョン。	
		Company	ベンダ名。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		ProductName	このファイルが示す製品。	
		Language	このファイルの言語を示すわかりやすい名前。	
mw_dba.zen_locktable	ロックテーブル情報を取得します。	ComputerName	コンピュータ名。	Yes
		LastScanTime	Scanner が最後にスキャンされた日。ミリ秒値で保存されるため、どの日付形式でも読み込みおよび表示できます。	
		RecentInformation	最新情報。	
mw_dba.zen_removabledisk	リムーバブルディスク情報を取得します。	Manufacturer	リムーバブルディスクのベンダ名。	No
		Description	リムーバルディスクの説明。	
		PhysicalCylinders	ディスクのシリンダまたはトラックの合計数。	
		PhysicalHeads	ヘッド数。	
		SectorsPerTrack	1 トラックあたりのセクタ数。	
		Capacity	合計サイズ。	
mw_dba.zen_fixeddisk	固定ディスク情報を取得します。	Manufacturer	固定ディスクのベンダ名。	No
		Description	固定ディスクの説明。	
		PhysicalCylinders	ディスクのシリンダまたはトラックの合計数。	
		PhysicalHeads	ヘッド数。	
		SectorsPerTrack	1 トラックあたりのセクタ数。	
		Capacity	合計サイズ。	
mw_dba.zen_WindowsLocalFileSystem	Windows ローカルファイルシステム情報を取得します。	Name	Windows ローカルファイルシステム名。	No
		FileSystemSize	Windows ローカルファイルシステムのサイズ。	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		AvailableSpace	Windows ローカルファイルシステムの容量。	
		FileSystemType	Windows ローカルファイルシステムの種類。	
		Caption	Windows ローカルファイルシステムのキャプション。	
		DeviceID	Device ID	
		VolumeSerialNumber	Windows ローカルファイルシステムのボリューム番号。	
mw_dba.zen_NetWareLocalFileSystem	NetWare ローカルファイルシステム情報を取得します。	Name	NetWare ローカルファイルシステム名。	No
		FileSystemSize	NetWare ローカルファイルシステムのサイズ。	
		AvailableSpace	NetWare ローカルファイルシステムの空き容量。	
		FileSystemType	NetWare ローカルファイルシステムの種類。	
		Caption	NetWare ローカルファイルシステムのキャプション。	
		DeviceID	Device ID	
		VolumeSerialNumber	NetWare ローカルファイルのボリュームのシリアル番号。	
mw_dba.zen_LinuxLocalFileSystem	Linux ローカルファイルシステム情報を取得します。	Name	Linux ローカルファイルシステム名。	No
		FileSystemSize	Linux ローカルファイルシステムのサイズ。	
		AvailableSpace	Linux ローカルファイルシステムの空き容量。	
		FileSystemType	Linux ローカルファイルシステムの種類。	
		Caption	Linux ローカルファイルシステムのキャプション。	
		DeviceID	Device ID	

インベントリビュー名	機能	属性	説明	ビューはローカライズされるか？
		VolumeSerialNumber	Linux ローカルファイルシステムのボリュームのシリアル番号。	

インベントリビューの使用方法

インベントリビューを SQL 文といっしょに使用して、インベントリデータベースプロンプトまたは任意のサードパーティデータベースフロントエンドアプリケーションから SQL 文を実行できます。

重要： ZENworks 6.5 Server Management SP1 に付属のインベントリビューは編集しないでください。

例：

- プロセッサ情報を取得するには

```
select * from mw_dba.zen_processor
```

- 特定のプロセッサ情報を取得するには

```
select DeviceID, Description, Role, Family, OtherFamilyDescription,
UpgradeMethod,MaxClockSpeed, CurrentClockSpeed from mw_dba.zen_processor
```

- すべてのソフトウェア情報を取得するには

```
select * from mw_dba.zen_software
```

- ソフトウェア情報とともにスイートの詳細を取得するには

```
select soft.name, softsuite.name from mw_dba.zen_software soft,
mw_dba.zen_softwaregroup softsuite where soft.name = 'ZENworks Desktop
Management Inventory Server' and
soft.parentinstanceid=softsuite.pinstanceid;
```

- ソフトウェアパッチ情報を取得するには

```
select suite.name, patchname from mw_dba.zen_softwaregroup suite,
mw_dba.zen_softwarepatch patch where suite.pinstanceid=patch.pinstanceid
```

- ソフトウェアスイートパッチ情報を取得するには

```
select soft.name, patchname from mw_dba.zen_software soft,
mw_dba.zen_softwarepatch patch where soft.pinstanceid=patch.pinstanceid;
```

- アンチウィルスソフトウェア情報を取得するには

```
select * from mw_dba.zen_antivirus
```

18 ステータスログによる Server Inventory の監視

Novell® ZENworks® 6.5 Server Inventory では、スキャンステータス、ロールアップステータス、およびインベントリサーバステータスのログファイルを参照することにより、情報のスキャンまたはロールアップが成功したかどうかを監視できます。

インベントリ対象サーバのスキャンステータスは、ローカルログファイルを通じてレポートされます。

インベントリコンポーネントは、インベントリサーバのステータスおよびスキャン情報のロールアップのステータスを Novell eDirectory™ でレポートします。

たとえば、ステータスログを表示すると、スキャンファイルの処理が正常に完了したかどうか、またはサーバのスキャン中またはロールアップ時にエラーが発生したかどうかを確認できます。

表示されるステータス情報は次のとおりです。

- 685 ページの「インベントリ対象サーバのスキャンステータスの表示」
- 686 ページの「インベントリサーバのロールアップ履歴の表示」
- 686 ページの「インベントリサーバのインベントリコンポーネントのステータス表示」
- 687 ページの「インベントリ対象サーバでの最新スキャンステータスの表示」
- 687 ページの「インベントリサーバのロールアップログの表示」
- 688 ページの「インベントリステータスログファイルのエクスポート」
- 688 ページの「ステータスログおよびスキャンログの概要」
- 689 ページの「XML 形式でのステータスログの表示」

インベントリ対象サーバのスキャンステータスの表示

Inventory Agent は、ステータス情報とエラーを invagent.log ファイルでレポートします。このログファイルは、NetWare® サーバの場合は sys:¥etc ディレクトリに、Windows* サーバの場合は temp ディレクトリまたは windows¥temp ディレクトリに保存されます。

ネイティブ scanner は、ステータス情報とエラーを invagent.log ファイルでレポートします。このログファイルは、NetWare® サーバの場合は sys:¥etc ディレクトリに、Windows サーバの場合は temp ディレクトリまたは windows¥temp ディレクトリに保存されます。

Inventory Policy Enforcer は、ポリシーエンジンによる現在の実行のステータスを invagentpolicyenforcer.log ファイルに書き込みます。sys:¥system または %systemroot% にある invsetup.ini ファイルに、デバッグフラグを設定できます。

forceDebug=true モードでは、Inventory Agent は .str ファイル転送のステータスを invagentstrtransfer.log ファイルに書き込みます。このファイルは、NetWare サーバの場合は sys:¥system¥invscan ディレクトリに、Windows サーバの場合は *%sytem_drive%*¥invscan ディレクトリに保存されます。

インベントリサーバのロールアップ履歴の表示

ロールアップステータスは、情報のロールアップを開始したインベントリサーバからのロールアップ情報のステータスをレポートします。たとえば、インベントリセットアップが、次のレベルのルートサーバへの情報のロールアップを開始するリーフサーバで構成されている場合、ロールアップログには、そのリーフサーバのロールアップ履歴が表示されます。

インベントリサーバのインベントリコンポーネント (Sender、Receiver、および Storer) は、ロールアップ情報をロールアップステータスに書き込みます。たとえば、ロールアップログを表示して、インベントリサーバからのインベントリ情報のロールアップ中にエラーが発生したかどうかを確認できます。このログには、最上位レベルのサーバ (ルートサーバ) のデータベースに保存されたインベントリ情報の最新の保存時刻も表示されます。このログには、インベントリサーバから実行された、以前のロールアップセッション 10 件の履歴が表示されます。

次の表に、ログの詳細を示します。

ステータス情報	詳細
Roll-Up Start Time	ロールアップの日付および時刻を表示します。
Message	インベントリサーバ間でインベントリ情報を移動する際に、インベントリコンポーネントによってレポートされたメッセージを表示します。

ファイルは、.csv 形式またはタブ区切り形式のファイルとしてエクスポートできます。

[Roll-Up Status] ウィンドウを呼び出すには

1 ConsoleOne® で、ロールアップを実行する Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックし、[Properties]、[Status Report] タブ、[Roll-Up Status] の順にクリックします。

インベントリサーバのインベントリコンポーネントのステータス表示

[Server Status] ウィンドウには、選択したインベントリサーバのインベントリサーバコンポーネントのステータスがレポートされます。任意の Inventory Service オブジェクトのインベントリサーバステータスログを表示できます。たとえば、Sender がファイルを Receiver に送信したかどうか、Storer がデータベースとの接続を正常に確立できたかどうかを確認できます。[Server Status] ウィンドウには、インベントリサーバコンポーネントによって記録された最新のステータスメッセージ 10 件の詳細が表示されます。

インベントリサーバコンポーネント (Sender、Receiver、Selector、Storer、Scan Collector、Service Manager、または Roll-Up Scheduler) がインベントリサーバで実行されていない場合は、インベントリサーバのステータスに情報が表示されます。

次の表に、ログの詳細を示します。

ステータス情報	詳細
Time of Log	インベントリコンポーネントによってメッセージがレポートされた日付および時刻を表示します。
Source	ステータスメッセージのログを実行したインベントリコンポーネントを表示します。
Message Type	メッセージの重要度を表示します。
Message	インベントリコンポーネントによってレポートされたメッセージを表示します。

ログファイルは、.csv 形式またはタブ区切り形式のファイルとしてエクスポートできます。

[Server Status] ウィンドウを表示するには

1 ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を右クリックし、[Properties] をクリックします。次に、[Status Report]、[Server Status] の順にクリックします。

インベントリ対象サーバでの最新スキャンステータスの表示

NetWare サーバおよび Windows サーバでは、invagent.log ファイルおよび invnatve.log ファイルにインベントリスキャンの詳細と最新の実行ステータスが格納されます。

インベントリサーバのロールアップログの表示

ロールアップログは、コンテナに含まれる Inventory Service オブジェクトからの最新ロールアップのステータスをレポートします。たとえば、ロールアップログを表示して、Inventory Service オブジェクトのロールアップサーバからの情報の最新ロールアップが正常に完了したかどうかを確認できます。インベントリコンポーネント (Sender、Receiver、および Storer) は、ロールアップ情報をロールアップログに書き込みます。中間サーバのエラー、警告、および情報のステータスメッセージを表示するかどうかも選択できます。

次の表に、ログの詳細を示します。

ステータス情報	詳細
Roll-Up Initiated From	ロールアップを開始した中間サーバの DN を表示します。
Roll-Up Start Time	情報のロールアップを開始した日付および時刻を表示します。
Source	ステータスのログを実行するインベントリコンポーネントを表示します。
Message Type	メッセージの重要度を表示します。
Message	インベントリ対象サーバのスキャン中に、インベントリコンポーネントによってレポートされるメッセージを表示します。

ログは、.csv 形式またはタブ区切り形式のファイルとしてエクスポートできます。

[Roll-Up Log] ウィンドウを呼び出すには

1 ConsoleOne で、Inventory Service オブジェクト (Inventory Service_*server_name*) を含むコンテナをクリックし、[Tools] > [ZENworks Inventory] > [Roll-Up Log] の順にクリックします。

2 表示するメッセージの重要度タイプをクリックし、[OK] をクリックします。

インベントリステータスログファイルのエクスポート

ログファイルの詳細は、.CSV 形式またはタブ区切り形式のファイルとして保存できます。

ログをファイルとして保存するには

1 ConsoleOne で、[Status] ウィンドウを開きます。

2 [Export] をクリックします。

3 ファイルタイプを選択して、ファイル名を指定します。

4 [OK] をクリックします。

ステータスログおよびスキャンログの概要

次の表は、ステータスログおよびスキャンログの一覧です。

ステータス / スキャンログ	ステータスを記録するインベントリコンポーネント	ログの詳細	ログファイルの表示方法
インベントリ対象サーバのスキャンログ	スキャンプログラム、Policy Enforcer	フォーマットモジュール名、タイムスタンプ、ステータスコード、およびステータスメッセージ	インベントリ対象サーバでローカルに表示可能
ロールアップログ	Sender、Receiver、Storer	ロールアップ開始元、ロールアップ開始時刻、インベントリコンポーネント、メッセージタイプ、スタータスメッセージ	Inventory Service オブジェクトのコンテナをクリックし、[Tools] > [ZENworks Inventory] > [Roll-Up Log] の順にクリックします。
Invagent.log	スキャンプログラム、Inventory Agent	フォーマットモジュール名、タイムスタンプ、ステータスコード、およびステータスメッセージ	任意のテキストエディタで表示
Invnatve.log	スキャンプログラム	フォーマットモジュール名、タイムスタンプ、ステータスコード、およびステータスメッセージ	任意のテキストエディタで表示
Invagentpolicyenforcer.log	Policy Enforcer	ログの時刻、エラータイプ、説明、重要度、および状態	任意のテキストエディタで表示

ステータス / スキャンログ	ステータスを記録するインベントリコンポーネント	ログの詳細	ログファイルの表示方法
invagentstrtransfer.log（デバッグモードで作成）	Inventory Agent	ログの時刻、エラータイプ、説明、重要度、および状態	任意のテキストエディタで表示
サーバ上のインベントリコンポーネントのステータス	Sender、Receiver、Scan Collector、Selector、Storer、Service Manager、Roll-Up Scheduler	ログの時刻、ソース、メッセージタイプ、メッセージ	ConsoleOne で、Inventory Service オブジェクトを右クリックし、[Properties] > [Status Report] > [Server Status] の順にクリックします。
ロールアップステータス	Sender、Receiver、Storer	ロールアップ開始時刻、メッセージ	ConsoleOne で、Inventory Service オブジェクトを右クリックし、[Properties]、[Status Report]、[Roll-Up Status] の順にクリックします。

XML 形式でのステータスログの表示

すべてのインベントリコンポーネントは、ステータスメッセージを XML (Extensible Markup Language) 形式のログファイルに記録します。最新のステータスメッセージ 10 件の履歴しか保存しないステータスログとは異なり、XML ステータスログはすべてのステータスメッセージを保存します。

ログファイルには次の情報が含まれます。

- インベントリモジュール名
- ステータスログの日付および時刻
- メッセージの重要度
- メッセージテキストおよびステータスメッセージ番号
- DN 名（インベントリモジュールが、eDirectory 内の特定の DN オブジェクトに関連付けられている場合）
- モジュールの製品別詳細

ログファイルの形式は次のとおりです。

```
?xml version="1.0" encoding="UTF-8"?>

?xml stylesheet type="text/xsl" href="inventorylog.xsl"?

<message_log>

 <message_entry>

   <module_name>Scanner</module_name>

   <severity>Critical</severity>

   <date_time>8/3/00 12:49 PM</date_time>

    <message_tag>unable to create scan data files
    </message_tag>

    <dn_name>Inv_server</dn_name>
```

```
  </message_entry>
  </module_name>Storer</module_name>
    <severity>Critical</severity>
    <date_time>8/3/00 12:49 PM</date_time>
    <message_tag>unable to update the database</message_tag>
    <dn_name>Inv_server</dn_name>
</message_entry>
..
</message_log>
```

サンプルスタイルシートおよびDTD (Document Type Declaration) ファイルは、インベントリサーバの *inventory_installation_directory*¥inv¥server¥xmllog にあります。

inventorylog.xml ログファイルは、NetWare サーバおよびWindows インベントリサーバの *inventory_installation_directory* ¥inv¥server¥xmllog ディレクトリにあります。

ログファイルのデフォルトの最大サイズは100KB です。ログファイルの最大サイズを変更するには、inventorylog.ini ファイルを編集します。NetWare サーバおよびWindows インベントリサーバでは、このファイルは *inventory_installation_directory*¥inv¥server¥xmllog ディレクトリにあります。

inventorylog.ini の内容は次のとおりです。

```
max_file_size=100 KB
```

必要に応じてMAX_FILE_SIZE パラメータを変更します。

ファイルサイズがMAX_FILE_SIZE パラメータで指定した値を超えると、そのファイルは *filename*_old.xml という名前でアーカイブされます。最新のメッセージは新しいログファイルに記録されます。

ログデータファイルを表示するには、サードパーティのXML ブラウザを使用します。

H パフォーマンスに関するヒント

この節では、Novell® ZENworks® 6.5 Server Management の Server Inventory コンポーネントのパフォーマンスを改善するために、調整する必要があるシステムおよびデータベースパラメータについて説明します。インベントリレポート、データベースエクスポート、および照会の操作で役立つ調整のヒントを個別に紹介します。

ここで紹介する情報に加え、インターネットで公開されているベンダ提供のマニュアルや、パフォーマンスチューニングおよびデータベースチューニングの関連記事も参照することをお勧めします。

この節では、次のトピックについて説明します。

- 691 ページの「データベースパラメータの調整に関するヒント」
- 695 ページの「Inventory ConsoleOne ユーティリティのパフォーマンスに関するヒント」
- 697 ページの「参考資料」

データベースパラメータの調整に関するヒント

- 691 ページの「NetWare および Windows 環境の Sybase」
- 693 ページの「Windows 環境の Oracle」
- 695 ページの「Windows 環境の MS SQL」

NetWare および Windows 環境の Sybase

- Sybase のスタートアップで *-c* パラーメータを設定し、データベースのキャッシュサイズを次のように設定することをお勧めします。

データベース内のインベントリ対象サーバ（単位：千）	システムの合計メモリ	Sybase キャッシュメモリ
1 未満	384MB	128MB
1 - 5	512MB	128MB
5 - 10	512MB ～ 768MB	128MB ～ 256MB
10 - 25	768MB ～ 1GB	256MB ～ 400MB
25 以上	1 ～ 2GB	RAM の 30 ～ 40%

- インベントリ対象サーバが 5,000 以上ある場合は、データベースをホストするサーバに複数のプロセッサを使用し、データファイルを分散させることをお勧めします。

- インベントリ対象サーバが 10,000 以上ある場合は、データベース専用のサーバを使用することをお勧めします。
- データベースファイルが存在するドライブに、Inventory ConsoleOne ユーティリティの実行中に生成された一時ファイルを格納するための空き領域が十分にあることを確認します。
- 次のような状況で、Storer でのインベントリ情報の保存に時間がかかる場合は、Sybindex ユーティリティを実行して Storer のパフォーマンスを改善できます。
  - 多数の Inventory エージェントが同時に ZENworks 6.5 にアップグレードされた後、そのすべてのエージェントからインベントリサーバにフルスキャンが送信された場合。
  - 管理者が Inventory Service オブジェクトからフルスキャンを開始し、その結果、すべての Inventory agent がインベントリサーバにフルスキャンを送信する。
  - インベントリデータベースが再インストールまたは変更されたときに、管理者が Inventory Service オブジェクトからフルスキャンを手動で実行し、すべての Inventory エージェントからインベントリサーバにフルスキャンが送信された場合。

    Sybindex ユーティリティを実行する前に、Sybase インベントリデータベースが起動されていることを確認してから、Storer を停止してください（コンソールプロンプトで「**stopser storer**」と入力します）。

    Sybindex ユーティリティを実行するには

    NetWare サーバの場合： サーバコンソールプロンプトで、「**sybindex**」と入力します。

    Windows サーバの場合： サーバコンソールプロンプトで、*inventory_server_installation_path*¥zenworks¥inv¥server¥wminv¥bin に移動し、「**sybindex**」と入力します。

    ユーティリティの実行後に、Storer を再起動します（コンソールプロンプトで「**startser storer**」と入力します）。

NetWare データベースサーバ上でデータベースキャッシュサイズを変更するには

1. Inventory Service を停止します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。
2. インベントリデータベースへの接続をすべて切断します。
3. Sybase サーバを終了します。
4. sys:¥system ディレクトリの mgmtdbs.ncf ファイルを開きます。
5. *-c* パラメータを変更します。

   たとえば、-c 64M はキャッシュサイズを 64MB に設定します。
6. ファイルを保存します。
7. サーバコンソールでインベントリデータベースをロードします。「**MGMTDBS**」と入力します。
8. Inventory Service を起動します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

Windows データベースサーバのデータベースキャッシュサイズを変更するには

1 Inventory Service を停止します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

2 Sybase サービスを終了します。

Windows 2000/2003 の場合、コントロールパネルで［管理ツール］、［サービス］の順にダブルクリックし、［Novell Database - Sybase］を選択して［停止］をクリックします。

3 データベースサーバで、*inventory_database_installation_path*¥zenworks¥database¥dbengine ディレクトリから ntdbconfig.exe ファイルを実行します。

ntdbconfig.exe は、Windows サーバ上で Sybase を使用する ZENworks データベース用の ZENworks データベース環境設定ユーティリティです。このユーティリティを使用して、Sybase サービスを設定し直すことができます。Sybase の推奨パラメータのリストについては、491 ページの「Sybase データベース起動パラメータの理解」を参照してください。

4 *-c* パラメータを変更します。

5 ［OK］をクリックします。

6 Sybase サービスを再起動します。

Windows 2000/2003 の場合、コントロールパネルで［管理ツール］、［サービス］の順にダブルクリックし、［Novell Database - Sybase］を選択して［開始］をクリックします。

7 Inventory Service を起動します。詳細については、476 ページの「Inventory Service の開始と停止」を参照してください。

パフォーマンスに関するヒントについては、691 ページの「データベースパラメータの調整に関するヒント」を参照してください。

Windows 環境の Oracle

- 次の表は、Windows プラットフォームにおけるメモリの推奨値を示しています。

データベース内のインベントリ対象サーバ（単位：千）	システムの合計メモリ	Oracle SGA メモリ
1 未満	512MB	128MB
1 - 5	768MB	256MB
5 - 10	1 GB	400MB
10 - 100	1GB ～ 2GB	合計メモリの 40%

- サーバで実行されている不要なサービスやアプリケーションを停止し、Oracle サーバなどのバックグラウンドサービスを有効にして実行します。
- データベースファイルが存在するドライブに、Inventory ConsoleOne ユーティリティの実行中に生成された一時ファイルを格納するための空き領域が十分にあることを確認します。
- Oracle データベースは、専用サーバでホストすることをお勧めします。

- インベントリ対象サーバが 10,000 以上ある場合は、データファイルを複数の物理ディスクに分散させます。
- 仮想メモリの値を RAM の 2 ～ 4 倍に設定します。
- データベースをホストするサーバには、複数のプロセッサを使用することをお勧めします。
- Windows プラットフォームの場合は、697 ページの「参考資料」に示されている Oracle のパフォーマンス調整に関するマニュアルと、一般的な推奨事項を参照してください。
  - フォアグラウンドのアプリケーションの優先度を下げます。
  - ファイルキャッシュの値を下げ、ネットワークアプリケーションのデータを最大化します。
- 特定の組織要件に応じて init.ora ファイルを修正します。

  たとえば、260MB の Oracle SGA(db_block_size=4096) を取得する場合、init.ora ファイルを次の値に変更します。

  ```
  db_block_buffers = 50000
  shared_pool_size = 32768000
  sort_area_size = 10000000
  ```
- start.sql ファイルを起動し、行を追加します。_start.sql ファイルは、インベントリデータベースインスタンスの起動時に、mgmtdbo.ncf または mgmtdbo.bat ファイルによって起動されます。既存の _start.sql ファイルに次の行を追加します。

  ```
  connect mw_dba;alter table cim.t$product cache;
  ```
- インベントリデータベースを Oracle 9i で実行している場合は、db_block_buffers * db_block_size ではなく db_cache_size を設定します。
- フルスキャン中、Storer でのインベントリ情報の保存に時間がかかる場合は、次のスクリプトを実行して InstalledFile テーブルに追加のインデックスを作成し、保存時間を短縮します。

  ```
  create index i$installedfile$compid on mw_dba.installedfile(computerid)
  tablespace cim5 pctfree 0;
  ```
- 詳細については、Oracle の管理ガイドまたはパフォーマンスガイドを参照してください。

Oracle データベースのパフォーマンスの最適化

Oracle インベントリデータベースを使用している場合、インベントリレポートの生成時やデータベースの照会時のデータベースのパフォーマンスを向上させることができます。

データベースバッファキャッシュを使用して、最後に使用したデータブロックを保存します。データベースキャッシュは、db_block_buffers * db_block_size として指定されます。これらのパラメータは、データベースサーバの zenworks¥database¥init.ora ファイルで指定されます。

DB_BLOCK_BUFFERS はデータベースバッファ数を指定します。DB_BLOCK_SIZE は各データベースバッファのサイズをバイトで指定します。

バッファキャッシュの各バッファのサイズは、データブロックのサイズに等しくなります。

メモリが増設されている場合、init.ora ファイルで DB_BLOCK_BUFFERS パラメータの値を大きくしてデータベースキャッシュサイズを設定します。インベントリデータベースを Oracle 9i で実行している場合は、db_block_buffers * db_block_size ではなく db_cache_size を設定します。

パフォーマンスに関するヒントについては、691 ページの「データベースパラメータの調整に関するヒント」を参照してください。

Windows 環境の MS SQL

- MS SQL では専用サーバを使用することをお勧めします。
- MS SQL サーバ上で、tempdb システムデータベースが配置されているドライブに十分なディスク容量があることを確認します。
- MS SQL サーバの優先度を上げます。
- バックグラウンドサービスの最適化を有効にします。
- 次の表に示す設定を使用してください。

データベース内のインベントリ対象サーバ（単位：千）	システムの合計メモリ	MS SQL キャッシュメモリ	プロセッサ速度
10 未満	512MB	256MB	Pentium III:450MHz
10 - 20	512MB ～ 1GB	256MB ～ 384MB	Pentium 4:1.8GHz
20 - 50	1 ～ 1.5GB	512MB ～ 768MB	Pentium 4:1.8GHz

- インベントリ対象サーバが 5,000 以上ある場合は、データファイルを複数の物理ディスクに分散させます。
- データベースをホストするサーバには、複数のプロセッサを使用することをお勧めします。
- MS SQL に関するその他のヒントについては、MS SQL Server のマニュアル（http://www.ms-sql-server-performance.com）を参照してください。

Inventory ConsoleOne ユーティリティのパフォーマンスに関するヒント

この節では、Inventory ConsoleOne ユーティリティのパフォーマンスに関するヒントについて説明します。

- 696 ページの「Inventory Reports のパフォーマンスに関するヒント」
- 696 ページの「Inventory Data Export のパフォーマンスに関するヒント」
- 696 ページの「インベントリ照会のパフォーマンスに関するヒント」

注： Inventory ConsoleOne ユーティリティが大きなデータベースからデータを取得する場合、ユーティリティを実行する前に Storer サービスを停止する必要があります。これにより、ConsoleOne ユーティリティのパフォーマンスが向上します。

Inventory Reports のパフォーマンスに関するヒント

データベースに 1,000 以上のインベントリ対象サーバがある場合、すべてのサブレポートをリスト化するには時間がかかります。サブレポートのリストを指定することをお勧めします。これにより、レポートの全般的なパフォーマンスが向上します。

Inventory Data Export のパフォーマンスに関するヒント

- Inventory Data Export のパフォーマンスを最大限向上させるには、DBExport でフィルタ条件を有効にする必要があります。指定した条件に基づいて、DBExport は選択されたソフトウェアのみをエクスポートします。
- エクスポート中、使用しない属性を選択解除します。そのためには、DBExport と [Required Attributes Only] オプションを使用します。
- ソフトウェアを個別にエクスポートします。これにより、Non-Software Export 機能のパフォーマンスが大きく向上します。

インベントリ照会のパフォーマンスに関するヒント

- 複数のグループで AND 条件を使用して照会を指定するとパフォーマンスが向上します。
- いくつかの関係演算子を含む複雑な照会は、1 つの関係演算子で区切られた複数のグループに分割します。
- 複雑な照会を使用する場合は、データベースのキャッシュサイズを増やします。データベースのチューニングについては、691 ページの「データベースパラメータの調整に関するヒント」を参照してください。
- 範囲を絞った高速なクエリは、再利用できるように保存しておきます。
- 低速リンクでデータベースに接続して、Inventory Query を起動しないようにします。
- 高速リンクで複雑な照会の実行に 10 分以上要する場合、指定した条件に一致するインベントリ対象サーバはおそらくありません。次のようなメッセージが表示されます。

  照会に一致するコンピュータシステムはありません

  [Result] ウィンドウを閉じ、条件を絞ってから再度試みてください。インベントリ対象サーバが検出されるまで、条件の絞込みを繰り返します。
- 最適なパフォーマンスのために、条件では 3 つ以上の関係演算子で分割された 4 つ以上のグループを使用しないことをお勧めします。
- 正確な論理文字列がわかっている場合は、MATCHES 演算子は使用しないようにします。MATCHES 演算子は、指定したパターンに基づいて結果を検索します。これによりパフォーマンスの低下が生じます。
- インベントリデータベースに保存されていない特定のインベントリコンポーネントをチェックする場合は、正規の属性を含む照会ではなく、(ISNULL) 演算子を使用します。

参考資料

各コンポーネントのパフォーマンス調整に関するヒントについては、次のドキュメントを参照してください。

- MS SQL パフォーマンス情報 (http://www.sql-server-performance.com)
- Oracle 9i データベースおよびパフォーマンスガイドとリファレンス
- Oracle 9i データベース管理者ガイド

Inventory Scanner で収集されるハードウェア情報

ここでは、次の内容について説明します。

- 699 ページの「NetWare インベントリ対象サーバで収集されるハードウェア情報」
- 704 ページの「Windows インベントリ対象サーバで収集されるハードウェア情報」

NetWare インベントリ対象サーバで収集されるハードウェア情報

Inventory Agent は、NetWare インベントリ対象サーバに関する次のハードウェア情報を収集します。

スキャンデータ	SNMP の詳細	SMBIOS の詳細
System.Type	SNMP v2.0 RFC1213.MIB	対象外
System.MachineName	SNMP v2.0 RFC1213.MIB	対象外
System.AssetTag	対象外	SMBIOS v2.3 Type 3 構造
System.Model	対象外	SMBIOS v2.3 Type 1 構造
System.ModelNumber	対象外	SMBIOS v2.3 Type 3 構造
System.SystemIdentifier	対象外	対象外
System.ManagementTechnology	対象外	対象外
System.DNName	対象外	対象外
System.TreeName	対象外	対象外
NetworkAdpater.MACAddress	SNMP v2.0 RFC1213.MIB	対象外
IP.Address	SNMP v2.0 RFC1213.MIB	対象外
IP.Subnet（サブネットマスク）	SNMP v2.0 RFC1213.MIB	対象外
NetworkAdapter.MACAddress	対象外	対象外
IPX.Adress	SNMP v2.0 IPX.MIB	対象外
NetworkAdapter.MACAddress	SNMP v2.0 IPX.MIB	対象外
DNS.HostName	対象外	対象外
NetworkAdapter.Speed	SNMP v2.0 RFC1213.MIB	対象外
NetworkAdapter.Name	SNMP v2.0 RFC1213.MIB	対象外

スキャンデータ	SNMP の詳細	SMBIOS の詳細
NetworkAdapter.PermAddress	対象外	対象外
NetworkAdapter.AdapterType	SNMP v2.0 RFC1213.MIB	対象外
NetworkAdapter.ProviderName	SNMP v2.0 RFC1213.MIB	対象外
NetworkAdapter.DriverDescription	SNMP v2.0 RFC1514.MIB	対象外
NetworkAdapter.DriverName	SNMP v2.0 RFC1514.MIB	対象外
NetworkAdapter.DriverVersion	SNMP v2.0 RFC1514.MIB	対象外
Zenworks_ZENNetworkAdapter---offset	SNMP v2.0 RFC1514.MIB	対象外
Processor.stepping	対象外	対象外
Processor.DeviceID	対象外	SMBIOS v2.3 Type 4 構造
Processor.Family	対象外	SMBIOS v2.3 Type 4 構造
Processor.OtherFamily	対象外	SMBIOS v2.3 Type 4 構造
Processor.MaxClockSpeed	対象外	SMBIOS v2.3 Type 4 構造
Processor.CurrentClockSpeed	対象外	SMBIOS v2.3 Type 4 構造
Processor.Role	対象外	SMBIOS v2.3 Type 4 構造
Processor.UpgradeMethod	対象外	SMBIOS v2.3 Type 4 構造
Processor.Description	対象外	SMBIOS v2.3 Type 4 構造
Processor.Name	対象外	SMBIOS v2.3 Type 4 構造
BIOS.Manufacturer	対象外	SMBIOS v2.3 Type 0 構造
BIOS.BIOSDate	対象外	SMBIOS v2.3 Type 0 構造
BIOS.BIOSIDBytes	対象外	対象外
BIOS.Caption	対象外	対象外
BIOS.SerialNumber	対象外	対象外
BIOS.Version	対象外	SMBIOS v2.3 Type 0 構造
BIOS.PrimaryBIOS	対象外	対象外
BIOS.Size	対象外	対象外
Bus.Type	SNMP v2.0 RFC1514.MIB	対象外
Bus.Name	対象外	対象外
Bus.Description	SNMP v2.0 RFC1514.MIB	対象外
Bus.Version	対象外	対象外
Monitor.NumberOfColorPlanes	対象外	対象外

スキャンデータ	SNMP の詳細	SMBIOS の詳細
Monitor.HorizontalResolution	対象外	対象外
Monitor.VerticalResolution	対象外	対象外
Monitor.DisplayType	対象外	対象外
Monitor.MemoryType	対象外	対象外
Monitor.MaxMemorySupported	対象外	対象外
Monitor.Bitsperpixel	対象外	対象外
Monitor.ControllerDescription	対象外	SMBIOS v2.3 Type 10 構造
Monitor.MaxRefreshrate	対象外	対象外
Monitor.MinRefreshrate	対象外	対象外
Mointor.DACType	対象外	対象外
Monitor.ChipSet	対象外	対象外
Monitor.ProviderName	対象外	対象外
Monitor.VideoBIOSManufacturer	対象外	対象外
Monitor.VideoBIOSVersion	対象外	対象外
Monitor.VideoBIOSReleaseDate	対象外	対象外
Monitor.VideoBIOS.IsShadowed	対象外	対象外
ParallelPort.Name	対象外	SMBIOS v2.3 Type 8 構造
ParallelPort.DMASupport	対象外	対象外
ParallelPort.Address	対象外	対象外
ParallelPort.IRQ	対象外	対象外
SerialPort.Name	対象外	対象外
SerialPort.Address	対象外	SMBIOS v2.3 Type 8 構造
SerialPort.IRQ	対象外	対象外
CDROMDrive.DeviceID(*)	対象外	対象外
CDROMDrive.Manufacture	対象外	対象外
CDROMDrive.Description	SNMP v2.0 RFC1514.MIB	対象外
CDROMDrive.Caption	SNMP v2.0 RFC1514.MIB	対象外
HardDrive.Media Type	SNMP v2.0 RFC1514.MIB	対象外
HardDrive.Vendor	対象外	対象外
HardDisk.Description	SNMP v2.0 RFC1514.MIB	対象外

スキャンデータ	SNMP の詳細	SMBIOS の詳細
HardDisk.Cylinders	対象外	対象外
HardDisk.Heads	対象外	対象外
HardDisk.Sectors	対象外	対象外
HardDisk.Capacity	SNMP v2.0 RFC1514.MIB	対象外
FileSystem.Name	対象外	対象外
InventoryScanner.Version	対象外	対象外
InventoryScanner.LastScanDate	対象外	対象外
InventoryScanner.InventoryServer	対象外	対象外
InventoryScanner.ScanMode	対象外	対象外
SoundCard.Description	対象外	SMBIOS v2.3 Type 10 構造
SoundCard.Name	対象外	対象外
SoundCard.Manufacturer	対象外	対象外
Cache.Level	対象外	対象外
Cache.WritePolicy	対象外	対象外
Cache.ErrorCorrection	対象外	SMBIOS v2.3 Type 7 構造
Cache.Type	対象外	SMBIOS v2.3 Type 7 構造
Cache.LineSize	対象外	対象外
Cache.ReplacementPolicy	対象外	対象外
Cache.ReadPolicy	対象外	対象外
Cache.Associativity	対象外	SMBIOS v2.3 Type 7 構造
Cache.Speed	対象外	SMBIOS v2.3 Type 7 構造
Cache.Size	対象外	対象外
UCS.DNName	対象外	対象外
UCS.PrimaryOwnerContact	対象外	対象外
UCS.PrimaryOwnerName	対象外	対象外
Slot.Description	対象外	SMBIOS v2.3 Type 9 構造
Slot.MaxDataWidth	対象外	SMBIOS v2.3 Type 9 構造
Slot.ThermalRating	対象外	対象外
LogicalDrive.Name	対象外	対象外
LogicalDrive.DeviceID	対象外	対象外

スキャンデータ	SNMP の詳細	SMBIOS の詳細
LogicalDrive.VolumeSerialNumber	対象外	対象外
FileSystem.Name	対象外	対象外
FileSystem.Type	対象外	対象外
FileSystem.TotalSize	対象外	対象外
FileSystem.FreeSpace	対象外	対象外
FileSystem.DeviceID	対象外	対象外
Operating System.OSType	対象外	対象外
OperatingSystem.Version	対象外	対象外
OperatingSystem.Codepage	対象外	対象外
OperatingSystem.InstallDate	対象外	対象外
OperatingSystem.SizeStoredInPagingFiles	対象外	対象外
OperatingSystem.Caption	対象外	対象外
OperatingSystem.TotalVisibleMemorySize	対象外	対象外
OperatingSystem.Role	対象外	対象外
NetWareOperatingSystem.AccountingVersion	対象外	対象外
NetWareOperatingSystem.InternetBridgeSupport	対象外	対象外
NetWareOperatingSystem.MaxNumberOfConnections	対象外	対象外
NetWareOperatingSystem.PeakConnectionsUsed	対象外	対象外
NetWareOperatingSystem.PrintServerVersion	対象外	対象外
NetWareOperatingSystem.QueuingVersion	対象外	対象外
NetWareOperatingSystem.RevisionLevel	対象外	対象外
NetWareOperatingSystem.SecurityRevisionLevel	対象外	対象外
NetWareOperatingSystem.SFTLevel	対象外	対象外
NetWareOperatingSystem.TTSLevel	対象外	対象外
NetWareOperatingSystem.VAPVersion	対象外	対象外
NetWareOperatingSystem.VirtualConsoleVersion	対象外	対象外
NetWareOperatingSystem.InternalNetworkNumber	対象外	対象外

Windows インベントリ対象サーバで収集されるハードウェア情報

Inventory Agent は、Windows インベントリ対象サーバに関する次のハードウェア情報を収集します。

スキャンデータ	DMI クラスと属性	WMI クラスと属性
System.Manufacturer	DMTF|Component|1	Win32_ComputerSystemProduct.Vendor
System.MachineName	対象外	Win32_ComputerSystem.Caption
System.AssetTag	DMTF|System Enclosure|001.2	対象外
System.Model	DMTF|Component|2	Win32_ComputerSystemProduct.Name
System.ModelNumber	対象外	対象外
System.SystemIdentifier(GUID)	対象外	対象外
System.SerialNumber	DMTF|Component|3	Win32_ComputerSystemProduct.IdentifyingNumber
System.Tag	対象外	対象外
System.ManagementTechnology	対象外	対象外
eDirectory.DNName	対象外	対象外
eDirectory.TreeName	対象外	対象外
NetworkAdapter.MACAddress	対象外	Win32_NetworkAdapterConfiguration.MACAddress (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
IP.Address	対象外	Win32_NetworkAdapterConfiguration.IPAddress (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
IP.Subnet (サブネットマスク)	対象外	Win32_NetworkAdapterConfiguration.IPSubnet (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
NetworkAdapter.MACAddress	対象外	Win32_NetworkAdapterConfiguration.MACAddress (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
IPX.Address	対象外	Win32_NetworkAdapterConfiguration.IPXAddress (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
NetworkAdapter.MACAddress	対象外	Win32_NetworkAdapterConfiguration.MACAddress (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)

スキャンデータ	DMI クラスと属性	WMI クラスと属性
DNS.HostName	対象外	Win32_NetworkAdapterConfiguration.DNSHostName + DNSDomain (Win32_NetworkAdapterSetting との関連によって、Windows 2000 でのみ取得されます)
Modem.Description	対象外	Win32_POTSModem.Description
Modem.Name	対象外	Win32_POTSModem.Name
Modem.Vendor	対象外	対象外
Modem.DeviceID	対象外	Win32_POTSModem.DeviceID
NetworkAdapter.DriverVersion	DMTF|Network Adapter Driver |001.Driver Software Version	対象外
Login.CurrentLoggedinUser	対象外	対象外
Login.LastLoggedin User	対象外	対象外
Login.DomainName	対象外	Win32_ComputerSystem.Domain
NWClient.Version	対象外	対象外
Processor.stepping	対象外	CIM_Processor.Stepping
Processor.DeviceID	対象外	CIM_Processor.DeviceID
Processor.Family	DMTF|Processor|004.3	CIM_Processor.Family
Processor.OtherFamily	対象外	CIM_Processor.OtherFamilyDescription
Processor.MaxClockSpeed	DMTF|Processor|004.5	CIM_Processor.MaxClockSpeed
Processor.CurrentClockSpeed	DMTF|Processor|004.6	CIM_Processor.CurrentClockSpeed
Processor.Role	DMTF|Processor|004.2	CIM_Processor.ProcessorType
Processor.Upgrade	DMTF|Processor|004.7	CIM_Processor.UpgradeMethod
Processor.Description	DMTF|Processor|004.4	CIM_Processor.Description
Processor.Name	Enum equivalent of DMTF|Processor|004.3	CIM_Processor.Name
BIOS.Manufacturer	DMTF|SystemBIOS|001.2	Win32_BIOS.Manufacturer
BIOS.BIOSDate	対象外	Win32_BIOS.InstallDate
BIOS.BIOSIDBytes	対象外	対象外
BIOS.Copyright	対象外	Win32_BIOS.Caption
BIOS.SerialNumber	対象外	Win32_BIOS.SerialNumber
BIOS.BIOSType	DMTF|SystemBIOS|001.3	Win32_BIOS.SMBIOSBIOSVersion
BIOS.PrimaryBIOS	DMTF|SystemBIOS|001.9	Win32_BIOS.PrimaryBIOS

スキャンデータ	DMI クラスと属性	WMI クラスと属性
BIOS.Size	DMTF|SystemBIOS|001.4	対象外
Bus.Type	対象外	Win32_Bus.BusType
Bus.Name	対象外	Win32_Bus.Name
Bus.Description	対象外	Win32_Bus.Descritpion
Bus.Version	対象外	対象外
Bus.DeviceID	対象外	Win32_Bus.DeviceID
IRQ.Number	DMTF|IRQ|002.IRQNumber	CIM_IRQ.IRQNumber
IRQ.Availability	DMTF|IRQ|002.Availability	CIM_IRQ.Availability
IRQ.TriggerType	DMTF|IRQ|002.TriggerType	CIM_IRQ.TriggerType
IRQ.Shareable	DMTF|IRQ|002.Shareable	CIM_IRQ.Shareable
Keyboard.Layout	DMTF|Keyboard|003.Layout	CIM_Keyboard.Layout
Keyboard.Subtype	対象外	対象外
Keyboard.Type	DMTF|Keyboard|003.Keyboard.Type	CIM_Keyboard.Description
Keyboard.Fkeys	対象外	CIM_Keyboard.NumberOfFunctionKeys
Keyboard.Delay	対象外	対象外
Keyboard.TypematicRate	対象外	対象外
VideoAdapter.NumberOfColorPlanes (NEW)	対象外	Win32_VideoController.NumberOfColorPanes
VideoAdapter.HorizontalResolution	DMTF|Video|004.Current Horizontal Resolution	Win32_VideoController.CurrentHorizontalResolution
VideoAdapter.VerticalResolution	DMTF|Video|004.Current Vertical Resolution	Win32_VideoController.CurrentVerticalResolution
VideoAdapter.DisplayType	DMTF|Video|004.Video Type	Win32_VideoController.VideoArchitecture
VideoAdapter.MemoryType	DMTF|Video|004.Video Memory Type	Win32_VideoController.VideoMemoryType
VideoAdapter.MaxMemorySupported	DMTF|Video|004.Video RAM Memory Size	Win32_VideoController.AdapterRAM
VideoAdapter.Bitsperpixel	DMTF|Video|004.Current Number of Bits per Pixel	Win32_VideoController.CurrentBitsPerPixel

スキャンデータ	DMI クラスと属性	WMI クラスと属性
VideoAdapter.ControllerDescription	DMTF|Video|004.Video Controller Description	Win32_VideoController.Description
VideoAdapter.MaxRefreshrate	DMTF|Video|004.Maximum Refresh Rate	Win32_VideoController.MaxRefreshRate
VideoAdapter.MinRefreshrate	DMTF|Video|004.Minimum Refresh Rate	Win32_VideoController.MinRefreshRate
VideoAdapter.DACType	対象外	Win32_VideoController.AdapterDACType
VideoAdapter.ChipSet	対象外	Win32_VideoController.VideoProcessor
VideoAdapter.ProviderName	対象外	Win32_VideoController.VideoAdapterCompatibility
VideoBIOS.VideoBIOSManufacturer	DMTF|Video BIOS|001.BIOS Manufacturer	CIM_VideoBIOSElement.Manufacturer
VideoBIOS.VideoBIOSVersion	DMTF|Video BIOS|001.Video.BIOS Version	CIM_VideoBIOSElement.Version
VideoBIOS.VideoBIOSReleaseDate	DMTF|Video BIOS|001.Video.BIOS Release Date	CIM_VideoBIOSElement.InstallDate
VideoBIOS.VideoBIOS.IsShadowed	DMTF|Video BIOS|001.Video.Shadowing State	CIM_VideoBIOSElement.IsShadowed
ParallelPort.Name	DMTF|Parallel Ports|003.Parallel Port Index	CIM_ParallelController.Name
ParallelPort.DMASupport	DMTF|Parallel Ports|003.DMA Support	CIM_ParallelController.DMASupport
ParallelPort.Address	DMTF|Parallel Ports|003.Parallel Base I/O Address	対象外
ParallelPort.IRQ	DMTF|Parallel Ports|003.IRQ Used	対象外
SerialPort.Name	DMTF|Serial Ports|004.Serial Port Index	CIM_SerialController.Name
SerialPort.Address	DMTF|Serial Ports|004.Serial Base I/O Address	対象外
SerialPort.IRQ	DMTF|Serial Ports|004.IRQ Used	対象外

スキャンデータ	DMI クラスと属性	WMI クラスと属性
FloppyDrive.DeviceID	DMTF|Logical Drives|001.Logical Drive Name (DMTF|Logical Drives|001.Logical Drive Type=Floppy Drive(7) の場合)	Win32_LogicalDisk.DeviceID (Win32_LogicalDisk.DriveType = 2 (リムーバブルディスク) および Win32_LogicalDisk.MediaType = [1,10] の場合)
FloppyDrive.Manufacture	対象外	対象外
FloppyDrive.Description	Hard Code:Floppy Drive (DMTF|Disks|003.Storage Type=Floppy Disk(4) の場合)	Win32_LogicalDisk.Description (Win32_LogicalDisk.DriveType = 2 (リムーバブルディスク) および Win32_LogicalDisk.MediaType = [1,10] の場合)
FloppyDrive.MaxNumberofCylinders	対象外	対象外
FloppyDrive.NumberOfHeads	対象外	対象外
FloppyDrive.SectorsPerTrack	対象外	対象外
FloppyDrive.Size	DMTF|Logical Drives|001.Logical Drive Size (DMTF|Logical Drives|001.Logical Drive Type = Floppy Drive(7) の場合)	Win32_LogicalDisk.Size (Win32_LogicalDisk.DriveType = 2 (リムーバブルディスク) および Win32_LogicalDisk.MediaType = [1,10] の場合)
CDROMDrive.DeviceID	DMTF|Logical Drives|001.Logical Drive Name (DMTF|Logical Drives|001.Logical Drive Type = 6 の場合)	Win32_CDROMDrive.Drive
CDROMDrive.Manufacture	対象外	Win32_CDROMDrive.Manufacturer
CDROMDrive.Description	対象外	Win32_CDROMDrive.Description
CDROMDrive.Caption	ハードコード :CDROM デバイス (DMTF|Disks|001.Logical Drive Type = 6 の場合)	Win32_CDROMDrive.Caption
HardDrive.Media Type	DMTF|Disks|003.Removable Media	Win32_DiskDrive.MediaType
HardDrive.Vendor	対象外	Win32_DiskDrive.Manufacturer

スキャンデータ	DMI クラスと属性	WMI クラスと属性
HardDisk.Description	DMTF|Disks|003.Interface Description (DMTF|Disks|003.Storage Type=Hard Disk(3) の場合)	Win32_DiskDrive.Description
HardDisk.Cylinders	DMTF|Disks|003.Number of Physical Cylinders	Win32_DiskDrive.TotalCylinders
HardDisk.Heads	DMTF|Disks|003.Number of Physical Heads	Win32_DiskDrive.TotalHeads
HardDisk.Sectors	DMTF|Disks|003.Number of Physical Sectors per Track	Win32_DiskDrive.SectorsPerTrack
HardDisk.Capacity	DMTF|Disks|003.Total Physical Size	Win32_DiskDrive.Size
LogicalDrive.Name	対象外	Win32_LogicalDiskDeviceID (Win32_LogicalDisk.DriveType = 3 (ローカルディスク) の場合)
LogicalDrive.VolumeSerialNumber	対象外	Win32_LogicalDisk.VolumeSerialNumber (Win32_LogicalDisk.DriveType = 3 (ローカルディスク) の場合)
LogicalDrive.Volume (ボリュームラベル)	対象外	Win32_LogicalDisk.VolumeName (Win32_LogicalDisk.DriveType = 3 (ローカルディスク) の場合)
Operating System.OSType	対象外	Win32_OperatingSystem.OSType
OperatingSystem.Version	対象外	対象外
OperatingSystem.Codepage	対象外	Win32_OperatingSystem.CodeSet
OperatingSystem.InstallDate	対象外	Win32_OperatingSystem.InstallDate
OperatingSystem.TotalSwapSpaceSize	DMTF|System Memory Settings|001.Total Size of Paging Files	Win32_OperatingSystem.SizeStoredInPagingFiles
OperatingSystem.Description	DMTF|Operating System|001.Operating System Description	Win32_OperatingSystem.Caption
OperatingSystem.OtherTypeDescription	対象外	Win32_OperatingSystem.OtherTypeDescription
OperatingSystem.VirtualMemorySize	DMTF|System Memory Settings|001.Total Virtual Memory	Win32_OperatingSystem.TotalVirtualMemory
OperatingSystem.VisibleMemorySize	対象外	Win32_OperatingSystem.TotalVisibleMemorySize
OperatingSystem.Role	対象外	対象外

スキャンデータ	DMI クラスと属性	WMI クラスと属性
InventoryScanner.Version	対象外	対象外
InventoryScanner.LastScanDate	対象外	対象外
InventoryScanner.InventoryServer	対象外	対象外
InventoryScanner.ScanMode	対象外	対象外
InventoryScanner.GeneralDictionaryVersion	対象外	対象外
InventoryScanner.PrivateDictionaryVersion	対象外	対象外
SoundCard.Description	対象外	Win32_SoundDevice.Description
SoundCard.Name	対象外	Win32_SoundDevice.Name
SoundCard.Manufacturer	対象外	Win32_SoundDevice.Manufacturer
Cache.Level	DMTF|System Cache|003.System Cache Level	Win32_CacheMemory.Level
Cache.WritePolicy	DMTF|System Cache|003.System Cache Write Policy	Win32_CacheMemory.WritePolicy
Cache.ErrorCorrection	DMTF|System Cache|003.System Cache Error Correction	Win32_CacheMemory.ErrorCorrectType
Cache.Type	DMTF|System Cache|003.System Cache Type	Win32_CacheMemory.CacheType
Cache.LineSize	DMTF|System Cache|003.Line Size	Win32_CacheMemory.LineSize
Cache.ReplacementPolicy	DMTF|System Cache|003.Replacement Policy	Win32_CacheMemory.ReplacementPolicy
Cache.ReadPolicy	DMTF|System Cache|003.Read Policy	Win32_CacheMemory.ReadPolicy
Cache.Associativity	DMTF|System Cache|003.Associativity	Win32_CacheMemory.Associativity
Cache.Speed	DMTF|System Cache|003.System Cache Speed	Win32_CacheMemory.CacheSpeed
Cache.Size	DMTF|System Cache|003.System Cache Size	Win32_CacheMemory.MaxCacheSize
MotherBoard.Version	対象外	Win32_BaseBoard.Version

スキャンデータ	DMI クラスと属性	WMI クラスと属性
MotherBoard.Description	対象外	Win32_BaseBoard.Description
MotherBoard.Slots	DMTF|Motherboard|001.Number of Expansion slots	対象外
MotherBoard.Manufacture	対象外	Win32_BaseBoard.Manufacture
Battery.Name	DMTF|Portable Battery|002.Portable Battery Device Name	Win32_Battery.Name
Battery.Chemistry	DMTF|Portable Battery|002.Portable Battery Device Chemistry	Win32_Battery.Chemistry
Battery.Capacity	DMTF|Portable Battery|002.Portable Battery Design Capacity	Win32_Battery.DesignCapacity
Battery.Voltage	DMTF|Portable Battery|002.Portable Battery Design Voltage	Win32_Battery.DesignVoltage
Battery.Version	DMTF|Portable Battery|002.Portable Battery Smart Battery Version	Win32_Battery.SmartBatteryVersion
Battery.Manufacturer	DMTF|Portable Battery|002.Portable Battery Manufacturer	Win32_PortableBattery.Manufacturer
Battery.ManufactureDate	DMTF|Portable Battery|002.Portable Battery Manufacturer Date	Win32_Battery.InstallDate
Battery.SerialNumber	DMTF|Portable Battery|002.Portable Battery Serial Number	対象外
PowerSupply.InputVoltageDescription	DMTF|Power Supply|002.Power Supply Input Voltage Capability Description	CIM_UninterruptiblePowerSupply.Description
PowerSupply.Power	DMTF|Power Supply|002.Total Output Power	CIM_UninterruptiblePowerSupply.TotalOutputPower
DMA.Number	DMTF|DMA|001.DMA Number	CIM_DMA.DMAChannel
DMA.Description	DMTF|DMA|001.DMA Description	CIM_DMA.Description

スキャンデータ	DMI クラスと属性	WMI クラスと属性
DMA.Availability	DMTF|DMA|001.DMA Channel Availability	CIM_DMA.Availability
DMA_BurstMode	DMTF|DMA|001.DMA BurstMode	CIM_DMA.BurstMode
UCS.DNName	対象外	対象外
UCS.PrimaryOwnerContact	DMTF|General Information|001.3	CIM_UnitaryComputerSystem.PrimaryOwnerContact
UCS.PrimaryOwnerName	DMTF|General Information|001.4	CIM_UnitaryComputerSystem.PrimaryOwnerName
PointingDevice.DeviceType	DMTF|Pointing Device|Pointing Device Type(1)	CIM_PointingDevice.PointingType
PointingDevice.Type	DMTF|Pointing Device|Pointing Device Interface (2)	CIM_PointingDevice.Name
PointingDevice.NumberOfButtons	DMTF|Pointing Device|Pointing Device Buttons (4)	CIM_PointingDevice.NumberOfButtons
PointingDevice.DriverName	DMTF|Pointing Device|Pointing Device Driver Name (6)	対象外
PointingDevice.DriverVersion	DMTF|Pointing Device|Pointing Device Driver Version (7)	CIM_PointingDevice.Name
PointingDevice.IRQ	DMTF|Pointing Device|Pointing Device IRQ (3)	対象外
Slot.Description	DMTF|System Slots|003.Description	Win32_SystemSlot.SlotDesignation
Slot.MaxDataWidth	DMTF|System Slots|003.MaxDataWidth	Win32_SystemSlot.MaxDataWidth
Slot.ThermalRating	DMTF|System Slots|003.Slot Thermal Rating	Win32_SystemSlot.ThermalRating
FileSystem.Drive	対象外	Win32_LogicalDiskDeviceID (Win32_LogicalDisk.DriveType = 3（ローカルディスク）の場合)
FileSystem.FileSystemSize	対象外	Win32_LogicalDisk.Size (Win32_LogicalDisk.DriveType = 3（ローカルディスク）の場合)

スキャンデータ	DMI クラスと属性	WMI クラスと属性
FileSystem.AvailableSpace	対象外	Wind32_LogicalDisk.FreeSpace (Win32_LogicalDisk.DriveType = 3（ローカルディスク）の場合）
FileSystem.FileSystem	対象外	Win32_LogicalDisk.FileSystem (Win32_LogicalDisk.DriveType = 3（ローカルディスク）の場合）
Monitor.Device ID	対象外	対象外
Monitor.Description	対象外	対象外
Monitor.Manufacturer Date	対象外	対象外
Monitor.Model ID	対象外	対象外
Monitor.ViewableSize (inches)	対象外	対象外
Monitor.NominlaSize (inches)	対象外	対象外
Monitor.Serial Number	対象外	対象外
Monitor.Manufacturer	対象外	対象外
Monitor.Model	対象外	対象外
Chassis.Type (enum)	DMTF|Physical Container Global Table|1	Win32_SystemEnclosure.ChassisTypes
Chassis.Manufacturer	DMTF|FRU||4	Win32_SystemEnclosure.Manufacturer
Chassis.SerialNumber	DMTF|FRU||7	Win32_SystemEnclosure.SerialNumber
Chassis.AssetTag	DMTF|Physical Container Global Table|2	Win32_SystemEnclosure.SMBIOSAssetTag
Chassis.Version	対象外	Win32_SystemEnclosure.Version
Chassis.NumberOfPowerCords	対象外	Win32_SystemEnclosure.NumberOfPowerCords
Chassis.Tag	対象外	Win32_SystemEnclosure.Tag

注： PCMCIA モデムは、インベントリ対象サーバの PCMCIA スロットを介してコンピュータに接続されます。Scanner は、コンピュータ上でアクティブになっている PCMCIA モデムを検出します。コンピュータにインストールされているモデムを確認するには、Windows サーバで Windows System Device Manager を使用します。

非 PCMCIA モデムは、外部ポートを介してコンピュータに接続されます。たとえば、一部の非 PCMCIA モデムでは、シリアルポートが使用されます。Scanner は、コンピュータにインストールされている非 PCMCIA モデムを検出します。

非 PCMCIA モデムは、スキャン時にアクティブにならない場合があります。また、これらのモデムはコンピュータ上で設定されていても、接続されない場合があります。このような場合、Scanner はモデムを検出しモデムのスキャン情報をレポートします。

Inventory Scanner は 1997 年以降に製造されたモニタのインベントリ情報のみレポートします。

J ZENworks 6.5 Server Management の Inventory 属性

次の表は、ZENworks 6.5 Server Management で使用する Server Inventory 属性を示しています。

表の各行には次の項目が示されています。

- ConsoleOneのインベントリデータベースエクスポートウィザードに表示される属性名
- エクスポートされた .csv ファイルの属性名（.csv ファイルの最初の行）
- インベントリデータベースの属性名
- インベントリデータベースの属性のタイプ
- インベントリデータベースの属性の長さ
- 属性の簡単な説明

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
General-NDSName-Label	NDSName_LABEL	ManageWise.NDSName.Label	String	254	eDirectory に登録されているインベントリ対象サーバの DN 名。
SystemInfo.Description	Asset_Description	Zenworks.SystemInfo.Description	String	254	システムの備品情報の説明。
SystemInfo.Caption	Asset_Caption	Zenworks.SystemInfo.Caption	String	64	コンピュータの識別情報。
SystemInfo.Tag	Asset_Asset Tag	Zenworks.SystemInfo.Tag	String	254	ROM ベースのセットアッププログラムにより作成される備品タグ番号。これは各インベントリ対象サーバ固有の番号です。
SystemInfo.ModelNumber	Asset_Model Number	Zenworks.SystemInfo.Model	String	64	製造時に割り当てられるコンピュータのモデル番号。
SystemInfo.SerialNumber	Asset_Serial Number	Zenworks.SystemInfo.SerialNumber	String	64	製造時に割り当てられるコンピュータのモデルのシリアル番号。
SystemInfo.ManagementTechnology	Asset_Management Technology	Zenworks.SystemInfo.ManagementTechnology	整数		コンピュータシステムで利用可能な管理テクノロジ。
CurrentLoginUser.Name	Current Login User.Name	ManageWise."User".Name	String	254	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーにログインしたユーザ。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
LastLoginUser.Name	Last Login User.Name	ManageWise."User".Name	String	254	インベントリ対象サーバがスキャンされたときに、プライマリ eDirectory ツリーに最後にログインしたユーザ。
Product.Name	Applications_Name	CIM.Product.Name	String	254	ソフトウェアアプリケーション名。
Product.Vendor	Applications_Vendor	CIM.Product.Vendor	String	254	ソフトウェアアプリケーションメーカー名。
Product.Version	Applications_Version	CIM.Product.Version	String	64	ソフトウェアアプリケーションのバージョン。
Product.Location	Applications_Path	CIM.Directory.Location	String	254	製品のインストールパス。
Product.IdentifyingNumber	Applications_Identifying Number	CIM.Product.IdentifyingNumber	String	64	Microsoft 製品 ID。
WinOperatingSystem.OSType	Windows_Name	ZENworks.WINOperatingSystem.OSType	Unsigned Small Integer (enum)		オペレーティングシステム名。たとえば、Windows 2000。734 ページの「Software-Operating Systems-Windows - Name の列挙値」を参照してください。
WinOperatingSystem.Version	Windows_Version	ZENworks.WINOperatingSystem.Version	String	254	オペレーティングシステムのバージョン。
WinOperatingSystem.Caption	Windows_Caption	ZENworks.WINOperatingSystem.Caption	String	64	オペレーティングシステムの短い名前。たとえば、Windows 2000。
WinOperatingSystem.Role	Windows_Role	ZENworks.WINOperatingSystem.Role	Integer (enum)		コンピュータシステムの役割。たとえば、サーバなどです。
WinOperatingSystem.OtherTypeDescription	Windows_Other Description	ZENworks.WINOperatingSystem.Description	String	254	オペレーティングシステムの詳細。
WinOperatingSystem.InstallDate	Windows_Install Date	ZENworks.ZENOperatingSystem.InstallDate	String	25	オペレーティングシステムのインストール日。
WinOperatingSystem.CodePage	Windows_Code Page	ZENworks.WINOperatingSystem.CodePage	String	254	現在使用されている言語コードページ。
WinOperatingSystem.TotalVisibleMemorySize	Windows_Total Memory (MB)	ZENworks.WINOperatingSystem.TotalVisibleMemorySize	整数		Windows オペレーティングシステムにより報告された合計メモリ。
WinOperatingSystem.TotalVirtualMemorySize	Windows_Total Virtual Memory (MB)	ZENworks.WINOperatingSystem.TotalVirtualMemorySize			Windows オペレーティングシステムにより報告された仮想メモリの合計。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
InventoryScanner.Version	Scanner Information_Version	ZENworks.InventoryScanner.Version	String	64	インベントリ対象サーバで実行している Scanner のバージョン。
InventoryScanner.LastScanDate	Scanner Information_Last Scan Date	ZENworks.InventoryScanner.LastScanDate	Unsigned Integer		Scanner が最後にスキャンされた日。ミリ秒値で保存されるため、どの日付形式でも読み込みおよび表示できます。
InventoryScanner.Inventory Server	Scanner Information_Inventory Server	ZENworks.InventoryScanner.InventoryServer	String	254	スキャンの送信先インベントリサーバの名前。サーバ名の完全な DN ではありません。
InventoryScanner.ScanMode	Scanner Information_Scan Mode	ZENworks.InventoryScanner.ScanMode	Integer (enum)		WMI や DMI など、コンピュータシステムをスキャンするために Scanner で使用する管理テクノロジ。
NetWareClient.Version	Netware Client_Version	ZENworks.NetWareClient.Version	String	64	インベントリ対象サーバにインストールされている NetWare クライアントソフトウェアのバージョン。
NetworkAdapterDriver.Description	Network Adapter Driver_Description	ZENworks.NetworkAdapterDriver.Description	String	254	インベントリ対象サーバにインストールされているネットワークアダプタドライバの説明。たとえば、IBM 10/100 Ethernet アダプタ、EN-2420Px Ethernet アダプタ。
NetworkAdapterDriver.Name	Network Adapter Driver_Name	ZENworks.NetworkAdapterDriver.Name	String	254	インストールされているネットワークアダプタドライバソフトウェアの名前であり、アダプタに対応しています。たとえば、ne2000.sys、pppmac.vxd など。
NetworkAdapterDriver.Version	Network Adapter Driver_Version	ZENworks.NetworkAdapterDriver.Version	String	64	ネットワークアダプタドライバのバージョン。
PointingDeviceDeviceDriver.Name	Pointing Device Driver_Name	ZENworks.PointingDeviceDeviceDriver.Name	String	254	インベントリ対象サーバにインストールされているマウスドライバの名前。
PointingDeviceDeviceDriver.Version	Pointing Device Driver_Version	ZENworks.PointingDeviceDeviceDriver.Version	String	64	マウスドライバのバージョン。
PointingDevice.Name	Pointing Device_Name	CIM.PointingDevice.Name	String	254	Mouse などのポインティングデバイス名。このフィールドに保存されている文字列は、MOUSE になります。 CIM.PointingDevice.PointingType フィールドによって、ポインティングデバイスのタイプが決定します。 他のタイプのポインティングデバイスは、735 ページの「Hardware-Pointing Device-Name の列挙値」に示されています。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
PointingDevice.Numberofbuttons	Pointing Device_Number of Buttons	CIM.PointingDevice.NumberOfButtons	Unsigned Tiny Integer		ポインティングデバイスで使用されるボタンの数。
PointingDevice.IRQNumber	Pointing Device_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		Mouse ポインティングデバイスが接続されているシステム上の IRQ チャネル。この情報は、データベースの PointingDevice クラスではなく、IRQ クラスに保存されます。これらの関連付けに関する詳細については、537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。
PointingDevice.PointingType	Pointing Device_Type	CIM.PointingDevice.PointingType	Integer (enum)		ポインティングデバイスのタイプ。
ZENKeyboard.Numberoffunction keys	Keyboard_Numberof Function Keys	ZENworks.ZENKeyboard.NumberOfFunctionKeys	Unsigned Small Integer		キーボードのファンクションキーの数。
ZENKeyboard.Layout	Keyboard_Layout	ZENworks.ZENKeyboard.layout	String	254	レイアウト情報。たとえば、US English。
ZENKeyboard. SubType	Keyboard_Subtype	ZENworks.ZENKeyboard.SubType	Unsigned Integer		キーボードのサブタイプを示す数。
ZENKeyboard.Delay	Keyboard_Delay (mSecs)	ZENworks.ZENKeyboard.Delay	Unsigned Integer		キー入力を繰り返すまでの遅延時間。
ZENKeyboard.Typematicrate	Keyboard_Typematic Rate (mSecs)	ZENworks.ZENKeyboard.Typematic Rate	Unsigned Integer		キーの処理速度。
ZENKeyboard. Description	Keyboard_ Description	ZENworks. ZENKeyboard.Description	String	254	キーボードのタイプを示すキーボードの説明。 たとえば、IBM 拡張（101/102 キー）キーボード。
VideoBIOSElement. Manufacturer	Display Driver_ Manufacturer	CIM.Video BIOSElement.Manufacturer	String	254	システムにインストールされているビデオ BIOS ドライバのメーカー。
VideoBIOSElement. Version	Display Driver_Version	CIM.Video BIOSElement.Version	String	254	ビデオ BIOS ドライバのバージョン。
VideoBIOSElement. Install Date	Display Driver_Install Date	CIM.Video BIOSElement.InstallDate	String	25	ビデオ BIOS のリリース日。
VideoBIOSElement. IsShadowed	Display Driver_Is Shadowed	CIM.Video BIOSElement.ISShadowed	BIT（ブール条件に使用）		ビデオ BIOS がシャドウメモリをサポートしているかどうかを示すブール条件。0 は False、1 は True を表します。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
VideoAdapter.NumberOfcolorpanes	Display Adapter_Number of Color Planes	ZENworks.VideoAdapter.NumberOf ColorPlanes	Unsigned Integer		ビデオシステムがサポートしている色平面の数。
VideoAdapter.CurrentVerticalResolution	Display Adapter_Current Vertical Resolution	ZENworks.VideoAdapter.Current Vertical Resolution	Unsigned Integer		ディスプレイの垂直解像度。
VideoAdapter.CurrentHorizontalResolution	Display Adapter_Current Horizontal Resolution	ZENworks.VideoAdapter.Current Horizontal Resolution	Unsigned Integer		ディスプレイの水平解像度。
VideoAdapter.Description	Display Adapter_Description	ZENworks.VideoAdapter.Description	String	254	ビデオアダプタの説明。
VideoAdapter.MinRefreshRate	Display Adapter_Minimum Refresh Rate	ZENworks.VideoAdapter.MinRefresh Rate	Unsigned Integer		ディスプレイを再描画するためのモニタの最小リフレッシュレート（ヘルツ単位）。
VideoAdapter.MaxRefreshRate	Display Adapter_Maximum Refresh Rate	ZENworks.VideoAdapter.MaxRefresh Rate	Unsigned Integer		ディスプレイを再描画するためのモニタの最大リフレッシュレート（ヘルツ単位）。
VideoAdapter.VideoArchitecture	Display Adapter_Video Architecture	ZENworks.VideoAdapter.Video Architecture	Unsigned Integer (enum)		システムのビデオサブシステムのアーキテクチャ。たとえば、CGA/VGA/SVGA/8514A。734 ページの「Hardware-Display Adapter-Video Architecture の列挙値」を参照してください。
VideoAdapter.VideoMemoryType	Display Adapter_Video Memory Type	ZENworks.VideoAdapter.VideoMemoryType	Unsigned Small Integer (Enum)		アダプタのメモリのタイプ。たとえば、VRAM/SRAM/DRAM/EDO RAM。735 ページの「Hardware-Display Adapter-Video Memory Type の列挙値」を参照してください。
VideoAdapter.Maxmemorysupported	Display Adapter_Maximum Memory Supported(KB)	ZENworks.VideoAdapter.MaxMemory Supported	Unsigned Integer		ディスプレイアダプタが VIDEO RAM に対してサポートする最大メモリ。
VideoAdapter.CurrentBitsPerPixel	Display Adapter_Current Bits/Pixel	ZENworks.VideoAdapter.CurrentBits PerPixel	Unsigned Integer		各ピクセルに隣接するカラービット数。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
VideoAdapter.Chip Set	Display Adapter_ Chip Set	ZENworks. VideoAdapter.Chip Set	String	254	ビデオアダプタで使用されるチップセット。
VideoAdapter.DACType	Display Adapter_ DAC Type	ZENworks. VideoAdapter.DAC Type	String	254	ビデオアダプタで使用されるデジタルアナログコンバータのタイプ。
VideoAdapter.ProviderName	Display Adapter_ Provider	ZENworks.VideoAdapter.Provider	String	254	メーカーまたはプロバイダの名前。
ZENPOTSModem.Caption	Modem_Caption	ZENworks.ZENPOTSModem. Caption	String	64	モデムの短い名前。
ZENPOTSModem.Description	Modem_Description	ZENworks.ZENPOTSModem. Description	String	254	モデムの完全な説明。たとえば、Standard 2400bps モデム、IBM PCMCIA HPC モデム。
ZENPOTSModem.Name	Modem_Name	ZENworks.ZENPOTSModem.Name	String	254	モデムのタイプと用途を指定するモデムの名前。たとえば、Standard Windows Modem は標準 Windows アーキテクチャで使用されることを示しています。
ZENPOTSModem.ProviderName	Modem_Provider	ZENworks.ZENPOTSModem.Provider	String	254	メーカーまたはプロバイダの名前。
ZENPOTSModem.DeviceID	Modem_Device ID	ZENworks.ZENPOTSModem.DeviceID	String	64	デバイスに割り当てられた固有の ID。
BIOS.BIOSIDBytes	BIOS_BIOS Identification Bytes	ZENworks. BIOS.BIOS IDBytes	String	254	BIOS でコンピュータモデルを示すバイト。
BIOS.SerialNumber	BIOS_ Serial Number	ZENworks. BIOS.Serial Number	String	64	メーカーにより割り当てられた BIOS のシリアル番号。
BIOS.PrimaryBIOS	BIOS_Primary Bios	ZENworks. BIOS.PrimaryBIOS	BIT（ブール条件に使用）		1 は True を表し、BIOS がプライマリ BIOS であることを示します。システム内で別の BIOS チップと共に使用されます。
BIOS.InstallDate	BIOS_Install Date	ZENworks. BIOS.Install Date	String	25	メーカーによって示された BIOS のリリース日。
BIOS.Version	BIOS_Version	ZENworks. BIOS.Version	String	254	BIOS のバージョンまたはリビジョンレベル。
BIOS. Manufacturer	BIOS_ Manufacturer	ZENworks. BIOS. Manufacturer	String	254	BIOS のメーカー名。
BIOS.Caption	BIOS_Caption	ZENworks. BIOS.Caption	String	64	BIOS メーカーによって指定された BIOS の名前。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
BIOS."size"	BIOS_Size(KB)	ZENworks. BIOS.size	Unsigned Integer		BIOS のサイズ（バイト単位）。
Processor.Current ClockSpeed	Processor_Current Clock Speed(MHz)	CIM. Processor. CurrentClockSpeed	Unsigned Integer		プロセッサの現在のクロック速度（MHz 単位）。
Processor.Maxclockspeed	Processor_ Maximum Clock Speed(MHz)	CIM. Processor. MaxClock Speed	Unsigned Integer		プロセッサの最大クロック速度（MHz 単位）。
Processor.Role	Processor_Role	CIM. Processor. Role	String	254	中央プロセッサ、数値演算コプロセッサなど、プロセッサの種類。
Processor.Family	Processor_ Processor Family	CIM. Processor. Family	Unsigned Small Integer (enum)		プロセッサのファミリ。735 ページの「Hardware-Processor-Processor Family の列挙値」を参照してください。
Processor.Otherfamilydescription	Processor_Other Family Description	CIM. Processor. OtherFamily Description	String	64	ファミリを使用してプロセッサを指定できない場合のプロセッサの詳細。たとえば、MMX テクノロジ Pentium プロセッサなど。
Processor.Upgrade Method	Processor_ Upgrade Method	CIM. Processor. Upgrade Method	Unsigned Small Integer (Enum)		プロセッサのアップグレード方法（アップグレードがサポートされている場合）。 736 ページの「Hardware-Processor-Upgrade Method の列挙値」を参照してください。
Processor.Stepping	Processor_ Processor Stepping	CIM. Processor. Stepping	String	254	マイクロプロセッサのベンダによって指定された、プロセッサのステッピングモデルを識別するための 1 バイトコード特性。
Processor.Device ID	Processor_ DeviceID	CIM. Processor. DeviceID	String	64	プロセッサの種類を識別する特殊な 16 進数の文字列。
CacheMemory.Speed	Cache Memory_ Speed(nsec)	CIM.PhysicalMemory. Speed	Unsigned Integer		システムキャッシュモジュールの速度（ナノ秒単位）。これは、CIM.PhysicalMemory クラスに保存され、CIM.CacheMemory に関連付けられます。これらの関連付けの方法について詳細は、537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
CacheMemory.Capacity	Cache Memory_ Capacity(MB)	CIM.PhysicalMemory. Capacity	Unsigned Integer		システムキャッシュモジュールの容量（ナノ秒単位）。これは、CIM.PhysicalMemory クラスに保存され、CIM.CacheMemory に関連付けられます。これらの関連付けの方法について詳細は、537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。
CacheMemory.Level	Cache Memory_ Level	CIM.Cache Memory. "Level"	Unsigned Small Integer (enum)		キャッシュレベル。マイクロプロセッサに組み込まれている内部キャッシュまたは CPU と DRAM 間にある外部キャッシュのキャッシュレベルを示します。
CacheMemory.Write Policy	Cache Memory_ Write Policy	CIM.Cache Memory. WritePolicy	Unsigned Small Integer (enum)		キャッシュがメモリに書き込む 2 つの方法（ライトバックとライトスルーキャッシュ）を示します。
CacheMemory.Error methodology	Cache Memory_ Error Methodology	CIM.CacheMemory.Error Methodology	String	254	キャッシュコンポーネントがサポートしているエラー修正方式。パリティ / シングルビット ECC/ マルチビット ECC など。
CacheMemory.Cache type	Cache Memory_ Cache Type	CIM.Cache Type	Unsigned Small Integer (enum)		システムキャッシュのタイプを定義します。たとえば、Instruction、Data、Unified。
CacheMemory.LineSize	Cache Memory_ Line Size(Bytes)	CIM.Cache Memory .LineSize	Unsigned Integer		シングルキャッシュバケットまたはシングルキャッシュラインのサイズ（バイト単位）。
CacheMemory.ReplacementPolicy	Cache Memory_ Replacement Policy	CIM.Cache Memory. ReplacementPolicy	Unsigned Integer (enum)		再使用するキャッシュラインまたはキャッシュバケットを決定するために、キャッシュが使用するアルゴリズム。
CacheMemory.ReadPolicy	Cache Memory_ Read Policy	CIM.Cache Memory. ReadPolicy	Unsigned Small Integer (enum)		データキャッシュが読み取り処理用であるかどうかを示します。
CacheMemory.Associativity	Cache Memory_ Associativity	CIM.Cache Memory. Associativity	Unsigned Integer (enum)		システムキャッシュの連想性を定義します（ダイレクトマップ、2 ウェイ、4 ウェイ）。
Diskette Drive.Manufacturer	Diskette Drive_ Manufacturer	ZENworks. Physical Diskette. Manufacturer	String	254	ベンダ名。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
Diskette Drive.Description	Diskette Drive_ Description	ZENworks. Physical Diskette. Description	String	254	フロッピーディスクの説明。
Diskette Drive.PhysicalCylinders	Diskette Drive_Physical Cylinders	ZENworks. Physical Diskette. Physical Cylinders	Unsigned Integer		フロッピーディスクのシリンダまたはトラックの合計数。
Diskette Drive.PhysicalHeads	Diskette Drive_Physical Heads	ZENworks. Physical Diskette. Physical Heads	Unsigned Small Integer		ヘッド数。
Diskette Drive.Capacity	Diskette Drive_Capacity (MB)	ZENworks. Physical Diskette. Capacity	Unsigned Integer		合計サイズ。
Diskette Drive.SectorsPerTrack	Diskette Drive_Sectors/ Track	ZENworks. Physical Diskette. SectorsPer Track	Unsigned Integer		1 トラックあたりのセクタ数。
Diskette Drive.DeviceID	Diskette Drive_ DeviceID	CIM.Diskette Drive	String	64	フロッピーディスクドライブを表すドライブ名。
ZENDiskDrive.Manufacturer	Physical Disk Drive_ Manufacturer	ZENworks. PhysicalDisk.Manufacturer	String	254	ベンダ名。
ZENDiskDrive.Description	Physical Disk Drive_ Description	ZENworks. PhysicalDisk.Description	String	254	ハードディスクのベンダの説明。
ZENDiskDrive.PhysicalCylinders	Physical Disk Drive_ Physical Cylinders	ZENworks. PhysicalDisk.Physical Cylinders	Unsigned Integer		シリンダの合計数。
ZENDiskDrive.PhysicalHeads	Physical Disk Drive_Physical Heads	ZENworks. PhysicalDisk.Physical Heads	Unsigned Small Integer		ヘッド数。
ZENDiskDrive.SectorsPerTrack	Physical Disk Drive_Sectors/ Track	ZENworks. PhysicalDisk.SectorsPer Track	Unsigned Integer		1 トラックあたりのセクタ数。
ZENDiskDrive.Capacity	Physical Disk Drive_ Capacity(MB)	ZENworks. PhysicalDisk.Capacity	Unsigned Integer		ハードディスクの合計サイズ。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
ZENDiskDrive.Removable	Physical Disk Drive_ Removable	ZENworks.LogicalDiskDrive.Removable	BIT		0 は固定ディスク、1 はリムーバブルディスクを示します。
LocalFileSystem.DeviceID	Logical Disk Drive_ Device ID	ZENworks.LogicalDiskDrive.DeviceID	String	64	C: または A: などのドライブ文字。
LocalFileSystem.FileSystemSize	Logical Disk Drive_ Size(MB)	CIM.LocalFileSystem.FileSystemSize	整数		ファイルシステムまたは論理ディスクの合計サイズ。
LocalFileSystem.AvailableSpace	Logical Disk Drive_ Free Size(MB)	CIM.LocalFileSystem.AvailableSpace	整数		ファイルシステムまたは論理ディスクの使用可能なサイズ。
LocalFileSystem.VolumeSerial Number	Logical Disk Drive_ Volume Serial Number	CIM.LocalFileSystem.VolumeSerialNumber	String	254	指定されたドライブのボリュームのシリアル番号。
LocalFileSystem.Caption	Logical Disk Drive_ Caption	CIM.LocalFileSystem.Caption	String	64	指定されたドライブのボリュームラベル。
LocalFileSystem.FileSystemType	Logical Disk Drive_ File System Type	CIM.LocalFileSystem.FileSystemType	String	254	ドライブ上の FAT または NTFS などのファイルシステム。
CDROMDrive.Manufacturer	CDROM_Manufacturer	ZENworks. Physical CDROM. Manufacturer	String	254	CD-ROM ドライブのメーカー。
CDROMDrive.Caption	CDROM_Caption	ZENworks. Physical CDROM. Caption	String	64	CD-ROM ラベル。
CDROMDrive.Description	CDROM_ Description	ZENworks. Physical CDROM. Description	String	254	メーカーによる CD ドライブの説明。たとえば、ATAPI CDROM、CREATIVE CD1620E SL970520。
CDROMDrive.DeviceID	CDROM_ Device ID	ZENworks. Logical CDROM. DeviceID	String	64	インベントリ対象サーバ上の CD に割り当てられているドライブを表す文字。
SerialPort.Name	Serial Port_Name	ZENworks. SerialPort. Name	String	254	シリアルポート名。 たとえば、COM1、COM2 など。
SerialPort.Address	Serial Port_ Address	ZENworks. SerialPort. Address	Unsigned Integer		メモリにマッピングされているシリアルポートのアドレス。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
SerialPort.IRQNumber	Serial Port_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		シリアルポートが接続されているシステムの IRQ チャネル。データベースでは、この情報はシリアルポートクラスではなく IRQ クラスに保存されます。 これらの関連付けに関する詳細については、15 章 537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。
ParallelPort.Name	Parallel Port_Name	ZENworks. ParallelPort. Name	String	254	パラレルポート名。たとえば、LPT1 など。
ParallelPort.Address	Parallel Port_ Address	ZENworks. ParallelPort. Address	Unsigned Integer		パラレルポート名。たとえば、LPT1 など。
ParallelPort.DMASupport	Parallel Port_DMA Support	ZENworks. ParallelPort. DMASupport	BIT（ブール条件に使用）		True または 1 の場合、DMA は、パラレルポートに接続されているデバイスで使用するために、バルクデータ転送用に割り当てられたチャネルです。
ParallelPort.IRQNumber	Parallel Port_IRQ Number	CIM.IRQ. IRQNumber	Unsigned Integer		パラレルポートが接続されているシステムの IRQ チャネル。この情報は、データベースのパラレルポートクラスではなく IRQ クラスに保存されます。 これらの関連付けに関する詳細については、15 章 537 ページの「ZENworks 6.5 Server Management のインベントリデータベーススキーマの理解」を参照してください。
Bus.Version	Bus_Version	ZENworks. Bus.Bus Version	String	254	インベントリ対象サーバがサポートしているバスのバージョン。
Bus.Description	Bus_Description	ZENworks.Bus.Description	String	254	バスの説明。
Bus.BusType	Bus_Bus Type	ZENworks.Bus.BusType	Integer (enum)		システムのバスのタイプ。
Bus.Name	Bus_Name	ZENworks.Bus.Name	String	254	内部システムバス名。
Bus.DeviceID	Bus_Device ID	ZENworks.Bus.DeviceID	String	64	特定のバスの固有 ID。
ZENNetworkAdapter.Name	Network Adapter_ Name	CIM.ZENworks.ZENAdapter.Name	String	254	システムにインストールされているネットワークアダプタ。
ZENNetworkAdapter.MaxSpeed	Network Adapter_Max_Speed (Mbps)	CIM.ZENworks.ZENAdapter. MaxSpeed	Unsigned Integer		アダプタのデータ転送レート。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
ZENNetworkAdapter.PermanentAddress	Network Adapter_Permanent Address	CIM.ZENworks.ZENAdapter.PermanentAddress	String	64	アダプタに永続的に保存されるコンピュータアドレス（MAC アドレス）。
ZENNetworkAdapter.MACAddress	Network Adapter_Address	CIM.ZENworks.ZENAdapter.MACAddress	String	64	ネットワークアダプタに保存されている MAC アドレス。
ZENNetworkAdapter.ProviderName	Network Adapter_Provider	CIM.ZENworks.ZENAdapter.Provider	String	254	メーカーまたはプロバイダ。
ZENNetworkAdapter.AdapterType	Network Adapter_Adapter Type	CIM.ZENworks.ZENAdapter.AdapterType	String	254	アダプタのタイプ。たとえば、Ethernet や FDDI アダプタ。
SoundAdapter.Description	Multimedia Card_Description	ZENworks.SoundAdapter.Description	String	254	インベントリ対象サーバのマルチメディアコンポーネントの説明。
SoundAdapter.Name	Multimedia Card_Name	ZENworks.SoundAdapter.Name	String	254	システムにインストールされているサウンドカードの名前。
SoundAdapter.Manufacturer	Multimedia Card_Manufacturer	ZENworks.SoundAdapter.Manufacturer	String	254	ベンダ名。
SoundAdapter.ProviderName	Multimedia Card_Provider	ZENworks.SoundAdapter.Provider	String	254	マルチメディアカードのプロバイダまたはメーカー。
Battery.Name	Battery_Name	CIM.Battery.Name	String	254	システムにインストールされているバッテリの名前。
Battery.Chemistry	Battery_Chemistry	CIM.Battery.Chemistry	Unsigned Small Integer		バッテリの化学的性質を示します。たとえば、鉛、ニッケルカドミウムなど。 735 ページの「Hardware-Battery-Chemistry の列挙値」を参照してください。
Battery.DesignCapacity	Battery_Design Capacity(mWatt-hours)	CIM.Battery.Design Capacity	Unsigned Integer		バッテリのデザイン容量（ミリワット時間単位）。
Battery.DesignVoltage	Battery_Design Voltage(MilliVolts)	CIM.Battery.DesignVoltage	Unsigned Integer		バッテリのデザイン電圧（ミリボルト単位）。
Battery.SmartBatteryVersion	Battery_Smart Battery Version	CIM.Battery.SmartBatteryVersion	String	64	バッテリがサポートしているスマートバッテリデータ仕様のバージョン番号。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
Battery.Manufacturer	Battery_Manufacturer	CIM.PhysicalComponent.Manufacturer	String	254	バッテリのベンダ名。
Battery.InstallDate	Battery_Install Date	CIM.PhysicalComponent.InstallDate	String	25	バッテリの製造日。
Battery.SerialNumber	Battery_Serial Number	CIM.PhysicalComponent.SerialNumber	String	64	バッテリのシリアル番号。
PowerSupply.Description	Power Supply_Description	CIM.Power Supply.Description	String	254	システムの電源の名前と説明。
PowerSupply.TotalOutputPower	Power Supply_Total Output Power (MilliWatts)	CIM.Power Supply.Total OutputPower	Unsigned Integer		電源の合計出力。
IPProtocolEndPoint.Address	IP Address_Address	CIM.IP Protocol Endpoint.Address	String	254	インベントリ対象サーバの IP アドレス。
IPProtocolEndPoint.Subnet Mask	IP Address_Subnet Mask	CIM.IP Protocol Endpoint.SubnetMask	String	254	インベントリ対象サーバのサブネットマスク。
DNSName.LABEL	DNS_LABEL	ManageWise.DNSName.Label	String	254	インベントリ対象サーバの DNS 名。
IPXProtocolEndPoint.Address	IPX Address_Address	CIM.IPX Protocol Endpoint.Address	String	254	インベントリ対象サーバの IPX アドレス。
LANEndPoint.MACAddress	MAC Address_Address	CIM.LAN Endpoint.MACAddress	String	12	インベントリ対象サーバの MAC アドレス。
MotherBoard.Version	MotherBoard_Version	ZENworks.Motherboard.Version	String	64	マザーボードのバージョン。
MotherBoard.Description	MotherBoard_Description	ZENworks.Motherboard.Description	String	254	マザーボードの説明。
MotherBoard.Manufacturer	MotherBoard_Manufacturer	ZENworks.Motherboard.Manufacturer	String	254	マザーボードのメーカー。
MotherBoard.NumberOfSlots	MotherBoard_Number Of Slots	ZENworks.Motherboard.Numberofslots	整数		マザーボードの拡張スロット数。
IRQ.Number	IRQ_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		システムの割り込み番号。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
IRQ.Availability	IRQ_Availability	CIM.IRQ.Availability	Unsigned Small Integer (Enum)		IRQ チャネルが使用中か使用可能であるかを示します。列挙値は、次のとおりです。 1 = 「その他」 2 = 「不明」 3 = 「使用可能」 4 = 「使用中 / 使用不可」 5 = 「使用中および使用可能 / 共有可能」
IRQ.TriggerType	IRQ_IRQ Trigger Type	CIM.IRQ.TriggerType	Unsigned Small Integer		エッジ（値 =4）またはレベルトリガ（値 =3）の割り込みが発生するかどうかを示す IRQ トリガのタイプ。列挙値は、次のとおりです。 1 = 「その他」 2 = 「不明」 3 = 「レベル」 4 = 「エッジ」
IRQ.Shareable	IRQ_IRQ Shareable	CIM.IRQ.Shareable	Unsigned Small Integer		IRQ を共有できるかどうかを示すブール値。
SLOT.MaxDataWidth	Slot_Maximum Data Width	CIM.Slot.MaxData Width	Unsigned Small Integer		スロットに装着できるアダプタカードの最大バス幅（ビット単位）。値が不明の場合は、0 を入力します。値が 8、16、32、64、128 以外の場合は、1 を入力します。値はビットで示されます。
SLOT.ThermalRating	Slot_Thermal Rating (MilliWatts)	CIM.Slot.Thermal Rating	Unsigned Integer		スロットの最大熱損失量（ミリワット単位）。
SLOT.Description	Slot_Description	CIM.SlotDescription	String	254	スロットにマウントされているアダプタの説明。
DMA.DMAChannel	DMA_DMA Channel Number	CIM.DMA.DMAChannel	Unsigned Integer		DMA チャネル番号。
DMA.Description	DMA_Description	CIM.DMA.Description	String	254	DMA チャネルを使用するデバイスの名前。
DMA.Availability	DMA_Availability	CIM.DMA.Availability	Unsigned Small Integer		DMA チャネルが使用できるかどうかを示します。 列挙値は、次のとおりです。 1 = 「その他」 2 = 「不明」 3 = 「使用可能」 4 = 「使用中 / 使用不可」 5 = 「使用中および使用可能 / 共有可能」

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
DMA.BurstMode	DMA_DMA Burst Mode	CIM.DMA.BurstMode	BIT（ブール条件に使用）		DMA チャネルがバーストモードをサポートしていることを示します。
NetWareOperatingSystem.Version	NetWare.Version	ZENworks.NetWareOperating.Version	String	254	NetWare オペレーティングシステムのバージョン。
Memory.TotalMemory	Memory_TotalMemory (MB)	ZENOperatingSystem.TotalVisibleMemorySize	整数		Windows オペレーティングシステムの総メモリ量。
MSDomainName.Label	WindowsDomain_Name	ManageWise.MSDomainName	String	254	サーバに接続されている Windows ドメイン。
Monitor.DeviceID	Monitor_DeviceID	ZENworks.ZENDesktopMonitor.DeviceID	整数		コンピュータシステムに接続されているデスクトップモニタの一意な ID。
Monitor.Description	Monitor_Description	ZENworks.ZENDesktopMonitor.Description	varchar	254	モニタの説明。
Monitor.ModelID	Monitor_ModelID	ZENworks.ZENDesktopMonitor.ModelID	varchar		モニタのモデルの一意な ID。メーカー ID と製品 ID の組み合わせです。
Monitor.ManufactureDate	Monitor_ManufactureDate	ZENworks.ZENDesktopMonitor.ManufacturerDate	char	25	モニタの製造年。
Monitor.ViewableSize	Monitor_ViewableSize	ZENworks.ZENDesktopMonitor.ViewableSize	Integer		イメージを縁取る黒い枠を除いて、画面イメージの対角線上の長さを示す数値。
Monitor.NominalSize	Monitor_NominalSize	ZENworks.ZENDesktopMonitor.NominalSize	Integer		モニタの対角線上の長さを示す数値（画面の片隅から反対側の隅までの距離）。
Monitor.SerialNumber	Monitor_SerialNumber	ZENworks.ZENDesktopMonitor.SerialNumber	varchar	128	メーカーのモニタ識別番号。
Monitor.Manufacturer	Monitor_Manufacturer	ZENworks.ZENDesktopMonitor.Manufacturer	varchar	254	モニタのメーカー名。
Monitor.Model	Monitor_Model	ZENworks.ZENDesktopMonitor.Model	varchar	254	メーカーが付けたモニタの製品名。
Chassis.AssetTag	Chassis_AssetTag	ZENworks_ZENChassis	varchar	254	システムシャシーの備品タグ番号。
Chassis.ChassisType	Chassis_ChassisType	ZENworks_ZENChassis	unsigned small int		システムシャシーがラップトップ、デスクトップ、ノートブック、ドッキングステーションなどのいずれであるかを示します。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
Chassis.NumberOfPowerCords	Chassis_NumberOfPowerCords	ZENworks_ZENChassis	varchar	128	システムシャシーに接続されている電源コードの総数。
Chassis.Manufacturer	Chassis_Manufacturer	ZENworks_ZENChassis	varchar	254	システムシャシー製造元の名前。
Chassis.SerialNumber	Chassis_SerialNumber	ZENworks_ZENChassis	varchar	128	システムシャシーを識別するための製造元番号。
Chassis.Version	Chassis_Version	ZENworks_ZENChassis	varchar	64	システムシャシーのバージョン番号。
Chassis.Tag	Chassis_Tag	ZENworks_ZENChassis	varchar	64	特定のコンピュータに接続されているシステムシャシーの一意な ID。
Software.ProductIdentifier	Software_productIdentifier	MW_DBA.InstalledSoftware.productIdentifier	varchar	254	インストールされている製品の一意な半角 16 文字の識別子。この識別子は Windows の MSI から使用できます。
Software.InternalVersion	Software_InternalVersion	MW_DBA.InstalledSoftware.InternalVersion	varchar	64	製品の内部バージョン。
Software.Language	Software_Language	MW_DBA.InstalledSoftware.Language	smallint		この製品の言語を示すわかりやすい名前。
Software.UninstallString	Software_UninstallString	MW_DBA.InstalledSoftware.UninstallString	varchar	254	この製品をアンインストールするために呼び出すコマンド。現在、このコマンドは Windows の ARP（［プログラムの追加と削除］）および MSI で使用できます。
Software.InstallationSource	Software_InstallationSource	MW_DBA.InstalledSoftware.InstallationSource	varchar	254	この製品をインストールするときにインストールファイルを保存したファイルシステムパスを識別します。現在、このコマンドは Windows の ARP および MSI で使用できます。
Software.FriendlyName	Software_FriendlyName	MW_DBA.InstalledSoftware.FriendlyName	varchar	254	ソフトウェアの表示名。
Software.LastExecutionTime	Software_LastExecutionTime	MW_DBA.InstalledSoftware.LastExecutionTime	bigint		製品が最後に実行された日付と時刻のスタンプ。
Software.FrequencyOfUsage	Software_FrequencyOfUsage	MW_DBA.InstalledSoftware.FrequencyOfUsage	smallint		製品の使用回数。
Software.Description	Software_Description	MW_DBA.InstalledSoftware.Description	varchar	254	製品の説明。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
Software.DefinitionDate	Software_DefinitionDate	MW_DBA.InstalledVirusScanner.DefinitionDate	bigint		コンピュータにインストールされたウィルス定義ファイルの日付。一部のアンチウィルス製品は、日付とバージョンを 1 つの文字列に組み合わせています。
Software.DefinitionVersion	Software_DefinitionVersion	MW_DBA.InstalledVirusScanner.DefinitionVersion	varchar	64	コンピュータにインストールされている、ベンダが定義したバージョンのウィルス定義ファイル。
Software.Edition	Software_Edition	MW_DBA.ProductEdition.Name	varchar	128	ベンダが定義した製品エディション。Professional など。
Software.SupportPack	Software_Supportpack	MW_DBA.SupportPack.Name	varchar	128	サポートパック名。
Software.Path	Software_Path	MW_DBA.Directory.Path	varchar	254	製品をインストールしたコンピュータシステム上のディレクトリパス。
Software.Name	Software_Name	MW_DBA.Software.Name	varchar	254	ベンダの商標または登録商標として示されるベンダ定義の製品名。
Software.Vendor	Software_Vendor	MW_DBA.Software.Vendor	varchar	254	ソフトウェアベンダ名
Software.Version	Software_Version	MW_DBA.Software.Version	varchar	64	製品のわかりやすいバージョン。
Software.Category	Software_Category	MW_DBA.Software.Category	varchar	64	製品が属する製品カテゴリ。
Software.HelpLink	Software_HelpLink	MW_DBA.Software.HelpLink	varchar	254	ARP および MSI で使用可能な製品のサポート Web サイトの URL。
Software.PackageGUID	Software_PackageGUID	MW_DBA.Software.PackageGUID	varchar	64	MSI で使用可能なベンダ定義の製品 GUID。
Software.PatchName	Software_PatchName	MW_DBA.Patch.Name	varchar	254	ベンダが定義したパッチ名。
File.Name	File_Name	MW_DBA.File.Name	varchar	254	ソフトウェアを示すファイル名。
File.FileVersion	File_FileVersion	MW_DBA.File.FileVersion	varchar	64	ソフトウェアを示すファイルのバージョン。
File.InternalName	File_InternalName	MW_DBA.File.InternalName	varchar	254	内部名。
File.ProductVersion	File_ProductVersion	MW_DBA.File.ProductVersion	varchar	64	このファイルが示す製品のバージョン。
File.Size	File_size	MW_DBA.File.size	bigint		ソフトウェアを示すファイルのサイズ。
File.LastModified	File_LastModified	MW_DBA.File.LastModified	bigint		ソフトウェアを示すファイルの最終更新日。

エクスポートウィザードの属性名	エクスポート属性名（.csv ファイルの列見出し）	データベーススキーマの属性名	データ型	長さ	属性の説明
File.Company	File_Company	MW_DBA.File.Company	varchar	254	ベンダ名。
File.ProductName	File_ProductName	MW_DBA.File.ProductName	varchar	254	このファイルが示す製品。
File.Language	File_Language	MW_DBA.File.Language	smallint		このファイルの言語を示すわかりやすい名前。
File.SoftwareDictionaryID	File_SoftwareDictionaryID	MW_DBA.File.SoftwareDictionaryID	varchar	64	一般ソフトウェアディクショナリで示されているファイルの ID。
DiskUsage.TotalDiskUsage	DiskUsage.TotalDiskUsage	MW_DBA.DiskUsage.TotalDiskUsage	bigint		指定された拡張子を持つすべてのファイルの総合的なディスク使用状況。
DiskUsage.Name	DiskUsage.Name	MW_DBA.DiskUsage.Name	varchar	32	ディスク使用状況をスキャンするファイル拡張子。

K 列挙値

ここでは、次の内容について説明します。

- 733 ページの「General-System Information-Management Technology の列挙値」
- 734 ページの「General-Inventory Information-Scan Mode の列挙値」
- 734 ページの「Software-Operating Systems-Windows - Name の列挙値」
- 734 ページの「Installation Repository の列挙値」
- 734 ページの「Hardware-Display Adapter-Video Architecture の列挙値」
- 735 ページの「Hardware-Display Adapter-Video Memory Type の列挙値」
- 735 ページの「Hardware-Pointing Device-Name の列挙値」
- 735 ページの「Hardware-Battery-Chemistry の列挙値」
- 735 ページの「Hardware-Processor-Processor Family の列挙値」
- 736 ページの「Hardware-Processor-Upgrade Method の列挙値」
- 736 ページの「Hardware-Chassis-Chassis Type の列挙値」
- 736 ページの「Hardware-Bus-Protocol Supported の列挙値」
- 736 ページの「Hardware-Processor-Role の列挙値」
- 737 ページの「System-System Cache-Level の列挙値」
- 737 ページの「System-System Cache-Cache Type の列挙値」
- 737 ページの「System-System Cache-Replacement Policy の列挙値」
- 737 ページの「System-System Cache-Read Policy の列挙値」
- 737 ページの「System-System Cache-Write Policy の列挙値」
- 737 ページの「System-System Cache-Associativity の列挙値」
- 738 ページの「System-System IRQ-Availability の列挙値」
- 738 ページの「System-System IRQ-IRQ Trigger Type の列挙値」
- 738 ページの「System-System DMA-Availability の列挙値」
- 738 ページの「Language の列挙値」

General-System Information-Management Technology の列挙値

1 = 不明
2 = その他
3 = DMI 対応
4 = WMI 対応
5 = SNMP 対応
6 = DMI および WMI 対応

General-Inventory Information-Scan Mode の列挙値

1 = 不明
2 = その他
3 = DMI
4 = WMI
5 = SNMP
6 = DMI および WMI

Software-Operating Systems-Windows - Name の列挙値

0 = 不明
1 = その他
16 = WIN95
17 = WIN98
18 = WINNT
21 = NetWare
36 = Linux
58 = Windows
59 = 専用
63 = Windows (R) Me
67 = Windows XP

Installation Repository の列挙値

Installation Repository の次の列挙値は、[Software] > [Software Group Components] > [Software Group and Software] > [Software Components] > [Software] クラスに表示されます。

0 = その他
1 = MSI
2 = プログラムの追加と削除
3 = MSI、プログラムの追加と削除
4 = ソフトウェアディクショナリ
5 = MSI、ソフトウェアディクショナリ
6 = プログラムの追加と削除、ソフトウェアディクショナリ
7 = MSI、プログラムの追加と削除、ソフトウェアディクショナリ
8 = NetWare Products.dat
12 = ソフトウェアディクショナリ、NetWare Products.dat
16 = プローブ
17 = MSI、プローブ
18 = プログラムの追加と削除、プローブ
19 = MSI、プログラムの追加と削除、プローブ
20 = ソフトウェアディクショナリ、プローブ
21= MSI、ソフトウェアディクショナリ、プローブ
22 = プログラムの追加と削除、ソフトウェアディクショナリ、プローブ
23 = MSI、プログラムの追加と削除、ソフトウェアディクショナリ、プローブ
24 = NetWare Products.dat、プローブ
28 = ソフトウェアディクショナリ、NetWare Products.dat、プローブ

Hardware-Display Adapter-Video Architecture の列挙値

1 = その他
2 = 不明
3 = CGA
4 = EGA
5 = VGA
6 = SVGA
7 = MDA
8 = HGC
9 = MCGA
10 = 8514A
11 = XGA
12 = リニアフレームバッファ
160 = PC-98

Hardware-Display Adapter-Video Memory Type の列挙値

1 = その他
2 = 不明
3 = VRAM
4 = DRAM
5 = SRAM
6 = WRAM
7 = EDO RAM
8 = 同期バースト DRAM
9 = パイプラインバースト SRAM
10 = CDRAM
11 = 3DRAM
12 = SDRAM
13 = SGRAM

Hardware-Pointing Device-Name の列挙値

1 = その他
2 = 不明
3 = マウス
4 = トラックボール
5 = トラックポイント
6 = グライドポイント
7 = タッチパッド
8 = タッチスクリーン
9 = 光センサーマウス

Hardware-Battery-Chemistry の列挙値

1 = その他
2 = 不明
3 = 鉛酸
4 = ニッケルカドミウム
5 = ニッケルメタル水素
6 = リチウムイオン
7 = 亜鉛空気
8 = リチウムポリマー

Hardware-Processor-Processor Family の列挙値

1 = その他
2 = 不明
11 = Pentium(R) ブランド
12 = Pentium(R) Pro
13 = Pentium(R) II
14 = MMX(TM) テクノロジ搭載の Pentium(R) プロセッサ
15 = Celeron(TM)
16 = Pentium(R) II Xeon(TM)
17 = Pentium(R) II
24 = AMD Duron(TM) プロセッサファミリ
25 = K5 ファミリ
26 = K6 ファミリ
27 = K6 -2
28 = K6 -3
29 = AMD Athlon (TM) プロセッサファミリ
30 = AMD29000 ファミリ
31 = K6-2+
130 = Itanium(TM) プロセッサ
176 = Pentium(R) III Xeon(TM)
177= Intel(R) SpeedStep(TM) テクノロジ搭載の Pentium(R) III プロセッサ
178 = Pentium(R) 4 プロセッサ
181 = Inter(R) Xeon (TM) プロセッサ MP
182 = AMD Athlon XP(TM) プロセッサファミリ
183 = AMD Athlon MP(TM) プロセッサファミリ
300 = 6 x 86

Hardware-Processor-Upgrade Method の列挙値

1 = その他
2 = 不明
3 = ドータボード
4 = ZIF ソケット
5 = 交換 / ピギーバック
6 = なし
7 = LIF ソケット
8 = スロット 1
9 = スロット 2
10 = 370 ピンソケット
11 = スロット A
12 = スロット M

Hardware-Chassis-Chassis Type の列挙値

1 = その他
2 = 不明
3 = デスクトップ
4 = ロープロファイルデスクトップ
5 = ピザボックス
6 = ミニタワー
7 = タワー
8 = ポータブル
9 = ラップトップ
10 = ノートブック
11 = ハンドヘルド
12 = ドッキングステーション
13 = オールインワン
14 = サブノートブック
15 = 省スペース
16 = ランチボックス
17 = メインシステムシャシー
18 = 拡張シャシー
19 = サブシャシー
20 = バス拡張シャシー
21 = 周辺機器シャシー
22 = 記憶装置シャシー
23 = ラックマウント方式シャシー
24 = 密閉ケース PC
25 = マルチシステムシャシー

Hardware-Bus-Protocol Supported の列挙値

0 = 内部
1 = ISA
2 = EISA
3 = MicroChannel
4 = TurboChannel
5 = PCI バス
6 = VME バス
7 = NuBus
8 = PCMCIA バス
9 = C バス
10 = MPI バス
11 = MPSA バス
12 = 内部プロセッサ
13 = 内部パワーバス
14 = PNP ISA バス
15 = PNP バス
16 = 最大インタフェースタイプ

Hardware-Processor-Role の列挙値

1 = その他
2 = 不明
3 = 中央プロセッサ
4 = 数値演算プロセッサ
5 = DSP プロセッサ
6 = ビデオプロセッサ

System-System Cache-Level の列挙値

1 = その他	3 = ライトバック	5 = アドレスによって異なる
2 = 不明	4 = ライトスルー	6 = I/O ごとに決定

System-System Cache-Cache Type の列挙値

1 = その他	3 = インストラクション	5 = ユニファイド
2 = 不明	4 = データ	

System-System Cache-Replacement Policy の列挙値

1 = その他	4 = FIFO (First In First Out)	7 = MFU (Most Frequently Used)
2 = 不明	5 = LIFO (Last In First Out)	8 = データ依存の複数のアルゴリズム
3 = LRU (Least Recently Used)	6 = LFU (Least Frequently Used)	

System-System Cache-Read Policy の列挙値

1 = その他	3 = Read	5 = Read および Read-Ahead
2 = 不明	4 = Read-Ahead	6 = I/O ごとに決定

System-System Cache-Write Policy の列挙値

1 = その他	3 = ライトバック	5 = アドレスによって異なる
2 = 不明	4 = ライトスルー	6 = I/O ごとに決定

System-System Cache-Associativity の列挙値

1 = その他	4 = 2 ウェイセットアソシエイティブ	7 = 8 ウェイセットアソシエイティブ
2 = 不明	5 = 4 ウェイセットアソシエイティブ	8 = 16 ウェイセットアソシエイティブ
3 = ダイレクトマップ	6 = フルアソシエイティブ	

System-System IRQ-Availability の列挙値

1 = その他	3 = 使用可能	5 = 使用中および使用可能 / 共有可能
2 = 不明	4 = 使用中 / 使用不可	

System-System IRQ-IRQ Trigger Type の列挙値

1 = その他	3 = レベル
2 = 不明	4 = エッジ

System-System DMA-Availability の列挙値

1 = その他	3 = 使用可能	5 = 使用中および使用可能 / 共有可能
2 = 不明	4 = 使用中 / 使用不可	

Language の列挙値

次の Language 列挙値は、[Software Group]、[Software Group File Information]、[Software]、[File Information]、[Exclude Information] クラスに表示されます。

0 = ニュートラル	97 = サポートなし	1095 = Windows XP: グジャラート語。これは Unicode のみです。
1 = アラビア語	101 = ディベヒ語	1037 = ヘブライ語
2 = ブルガリア語	127 = インバリアントロケール	1081 = Windows 2000/XP: ヒンディー語。これは Unicode のみです。
3 = カタロニア語	1024 = プロセスまたはユーザのデフォルト言語	1038 = ハンガリー語
4 = 中国語	2048 = システムのデフォルト言語	1039 = アイスランド語
5 = チェコ語	1078 = アフリカーンス語	1057 = インドネシア語
6 = デンマーク語	1052 = アルバニア語	1040 = イタリア語 (標準)
7 = ドイツ語	1025 = アラビア語 (サウジアラビア)	2064 = イタリア語 (スイス)
8 = ギリシャ語	2049 = アラビア語 (イラク)	1041 = 日本語
9 = 英語	3073 = アラビア語 (エジプト)	1099 = Windows XP: カナラ語。これは Unicode のみです。
10 = スペイン語	4097 = アラビア語 (リビア)	1111 = Windows 2000/XP: コンカニ語。これは Unicode のみです。

11 = フィンランド語

12 = フランス語

13 = ヘブライ語

14 = ハンガリー語。

15 = アイスランド語

16 = イタリア語

17 = 日本語

18 = 韓国語

19 = オランダ語

20 = ノルウェー語

21 = ポーランド語

22 = ポルトガル語

24 = ルーマニア語

25 = ロシア語

26 = クロアチア語

27 = スロバキア語

28 = アルバニア語

29 = スェーデン語

30 = タイ語

31 = トルコ語

32 = ウルドゥー語

33 = インドネシア語

34 = ウクライナ語

35 = ベラルーシ語

36 = スロベニア語

5121 = アラビア語（アルジェリア）

6145 = アラビア語（モロッコ）

7169 = アラビア語（チュニジア）

8193 = アラビア語（オマーン）

9217 = アラビア語（イエメン）

10241 = アラビア語（シリア）

11265 = アラビア語（ヨルダン）

12289 = アラビア語（レバノン）

13313 = アラビア語（クウェート）

14337 = アラビア語(U.A.E.)

15361 = アラビア語（バーレーン）

16385 = アラビア語（カタール）

1067 = Windows 2000/XP: アルメニア語。これは Unicode のみです。

1068 = アゼルバイジャン語（ラテン）

2092 = アゼルバイジャン語（キリル）

1069 = バスク語

1059 = ベラルーシ語

1026 = ブルガリア語

1109 = ビルマ語

1027 = カタロニア語

1028 = 中国語（台湾）

2052 = 中国語（中国）

3076 = 中国語（香港特別行政区）

4100 = 中国語（シンガポール）

5124 = Windows 98/Me、Windows 2000/XP: 中国語（マカオ特別行政区）

1042 = 韓国語

2066 = Windows 95

1088 = Windows XP: キルギス語。

1062 = ラトビア語

1063 = リトアニア語

2087 = Windows 98 のみ：リトアニア語（古典）

1071 = FYRO マケドニア語

1086 = マレー語（マレーシア）

2110 = マレー語（ブルネイ・ダルサラーム）

1102 = Windows 2000/XP: マラーティ語。これは Unicode のみです。

1104 = Windows XP: モンゴル語

1044 = ノルウェー語（ブークモール）

2068 = ノルウェー語（ニーノシク）

1045 = ポーランド語

1046 = ポルトガル語（ブラジル）

2070 = ポルトガル語（ポルトガル）

1094 = Windows XP: パンジャブ語。これは Unicode のみです。

1048 = ルーマニア語

1049 = ロシア語

1103 = Windows 2000/XP: サンスクリット語。これは Unicode のみです。

3098 = セルビア語（キリル）

2074 = セルビア語（ラテン）

1051 = スロバキア語

1060 = スロベニア語

1034 = スペイン語（スペイン、トラディショナルソート）

37 = エストニア語
38 = ラトビア語
39 = リトアニア語
41 = ペルシア語
42 = ベトナム語
43 = アルメニア語
44 = アゼルバイジャン語
45 = バスク語
47 = FYRO マケドニア語
54 = アフリカーンス語
55 = グルジア語
56 = フェロー語
57 = ヒンディー語
62 = マレー語
63 = カザフ語
64 = キルギス語
65 = スワヒリ語
67 = ウズベク語
68 = タタール語
69 = サポートなし
70 = パンジャブ語
71 = グジャラート語
72 = サポートなし
73 = タミール語
74 = テルグ語

1050 = クロアチア語
1029 = チェコ語
1030 = デンマーク語
1125 = Windows XP: ディベヒ語。これは Unicode のみです。
1043 = オランダ語（オランダ）
2067 = オランダ語（ベルギー）
1033 = 英語 (U.S.)
2057 = 英語 (U.K.)
3081 = 英語（オーストラリア）
4105 = 英語（カナダ）
5129 = 英語（ニュージーランド）
6153 = 英語（アイルランド）
7177 = 英語（南アフリカ）
8201 = 英語（ジャマイカ）
9225 = 英語（カリブ地域）
10249 = 英語（ベリーズ）
11273 = 英語（トリニダード）
12297 = Windows 98/Me、Windows 2000/XP: 英語（ジンバブエ）
13321 = Windows 98/Me、Windows 2000/XP: 英語（フィリピン）
1061 = エストニア語
1080 = フェロー語
1065 = ペルシア語
1035 = フィンランド語
1036 = フランス語（標準）
2060 = フランス語（ベルギー）

2058 = スペイン語（メキシコ）
3082 = スペイン語（スペイン、モダンソート）
4106 = スペイン語（グアテマラ）
5130 = スペイン語（コスタリカ）
6154 = スペイン語（パナマ）
7178 = スペイン語（ドミニカ共和国）
8202 = スペイン語（ベネズエラ）
9226 = スペイン語（コロンビア）
10250 = スペイン語（ペルー）
11274 = スペイン語（アルゼンチン）
12298 = スペイン語（エクアドル）
13322 = スペイン語（チリ）
14346 = スペイン語（ウルグアイ）
15370 = スペイン語（パラグアイ）
16394 = スペイン語（ボリビア）
17418 = スペイン語（エルサルバドル）
18442 = スペイン語（ホンジュラス）
19466 = スペイン語（ニカラグア）
20490 = スペイン語（プエルトリコ）
1072 = スツ語
1089 = スワヒリ語（ケニア）
1053 = スェーデン語
2077 = スェーデン語（フィンランド）
1114 = Windows XP: シリア語。これは Unicode のみです。
1097 = Windows 2000/XP: タミール語。これは Unicode のみです。

75 = カナラ語

76 = サポートなし

77 = サポートなし

78 = マラーティ語

79 = サンスクリット語

80 = モンゴル語

86 = ガリシア語

87 = コンカニ語

88 = サポートなし

89 = サポートなし

90 = シリア語

96 = サポートなし

3084 = フランス語（カナダ）

4108 = フランス語（スイス）

5132 = フランス語（ルクセンブルグ）

6156 = Windows 98/Me、Windows 2000/XP: フランス語（モナコ）

1110 = Windows XP: ガリシア語

1079 = Windows 2000/XP: グルジア語。これは Unicode のみです。

1031 = ドイツ語（標準）

2055 = ドイツ語（スイス）

3079 = ドイツ語（オーストリア）

4103 = ドイツ語（ルクセンブルグ）

5127 = ドイツ語（リヒテンシュタイン）

1032 = ギリシャ語

1092 = タタール語（タタルスタン）

1098 = Windows XP: テルグ語。これは Unicode のみです。

1054 = タイ語

1055 = トルコ語

1058 = ウクライナ語

1056 = Windows 98/Me、Windows 2000/XP: ウルドゥー語（パキスタン）

2080 = ウルドゥー語（インド）

1091 = ウズベク語（ラテン）

2115 = ウズベク語（キリル）

1066 = Windows 98/Me、Windows NT 4.0 以降：ベトナム語

L ドキュメントの更新

この章では、Novell® ZENworks® 6.5 Server Management の初回リリース後に、Server Inventory の『*管理*』ガイドに加えられたマニュアル内容の変更に関する情報を提供します。お使いのドキュメントを最新の状態に更新するために、この情報を役立ててください。

この節で列挙する変更はすべてドキュメントにも反映されているものです。マニュアルは、Web 上で HTML と PDF の 2 つの形式で提供されています。HTML および PDF ドキュメントは、ここに示すドキュメントの変更に基づいて最新の状態になっています。

ドキュメントの変更が発行された日付ごとに、更新情報をグループ化しています。同じ日付のセクション内では、変更は Server Inventory の主な目次の節の名前に基づいて、アルファベット順に表示されています。

使用している PDF ドキュメントのコピーが最新の内容であるかどうかを確認するには、PDF ドキュメントのタイトルページ、またはタイトルページのすぐ後ろの法的通知の欄で、発行された日付を参照してください。

ドキュメントは次に示す日付で更新されました。

- 743 ページの「2005 年 2 月 11 日」
- 744 ページの「2004 年 11 月 10 日」
- 745 ページの「2004 年 9 月 2 日」
- 745 ページの「2004 年 7 月 28 日」

2005 年 2 月 11 日

次の節が更新されました。

場所	変更
576 ページの「ZENworks 6.5 インベントリ対象サーバでスキャンするソフトウェアインベントリ情報のカスタマイズ」	この節は、ZENworks 6.5 Server Management Support Pack 1 に関して多くの箇所が変更されました。
660 ページの「CIM スキーマを使用しないインベントリデータベースからのインベントリ情報の取得」	新しい節です。

2004 年 11 月 10 日

次の節が更新されました。

場所	変更
443 ページの「インベントリサーバの役割の理解」	次の節に、特定のインベントリサーバ役割を選択する条件を追加しました。 • 443 ページの「ルートサーバ」 • 444 ページの「Root Server with Inventoried Servers（インベントリ対象サーバが接続されているルートサーバ）」 • 445 ページの「中間サーバ」 • 446 ページの「データベースが接続されている中間サーバ」 • 447 ページの「Intermediate Server with Inventoried Servers（インベントリ対象サーバが接続されている中間サーバ）」 • 448 ページの「Intermediate Server with Database and Inventoried Servers（データベースとインベントリ対象サーバが接続されている中間サーバ）」 • 449 ページの「リーフサーバ」 • 450 ページの「データベースが接続されているリーフサーバ」 • 451 ページの「スタンドアロンサーバ」
453 ページの「単純な展開」	1. 節の見出し「標準展開 - 単一のサイトにおけるインベントリの展開」を「単純な展開」に変更しました。 2. この節では、単純な展開シナリオで Server Inventory を展開するための情報が更新されました。
457 ページの「高度な展開」	1. 節の見出し「カスタム展開 - 複数または企業サイトにおけるインベントリの展開」を「高度な展開」に変更しました。 2. この節では、高度な展開シナリオで Server Inventory を展開するための情報が更新されました。
474 ページの「Server Inventory のインストールの効果の理解」	scandir ディレクトリおよび dictdir ディレクトリに許可される権限について説明を追加しました。

2004 年 9 月 2 日

ガイド全体を通して、グラフィックのフォントを変更し、新しいアイコンを使用しました。グラフィックの内容には、目立った変更はありません。

次の節が更新されました。

場所	変更
505 ページの「MS SQL 2000 を実行するインベントリデータベースへのインベントリサーバと ConsoleOne の接続」	Microsoft SQL Server の Web サイトの URL が、Windows 英語版の Microsoft JDBC ドライバのダウンロード先を表すように修正されました。

2004 年 7 月 28 日

次の節が更新されました。

場所	変更
517 ページの「Inventory Service Manager の理解」> 517 ページの「サービスのリスト」	この節に次の情報が追加されました。 Inventory Service Manager は、*inventory_server_installation_directory_or_volume*¥zenworks¥inv¥server¥wminv¥properties ディレクトリでサーバプロパティファイル (config.properties) および役割ベースプロパティファイルを読み取り、必要なサービスとサーバコンポーネントをロードします。 **重要：** 更新でサービスや Service Manager のロードに失敗する場合があるため、プロパティファイルは変更しないでください。
571 ページの「インベントリ用に配備されたインベントリサーバの表示」	次の注が追加されました。 **注：** ショートカットキーを使ってインベントリツリーを折りたたむことはできません。
649 ページの「インベントリレポートの生成」	[Reporting] ダイアログボックスを使用するときに従う必要がある、次のガイドラインが追加されました。 インベントリレポートでは、2 バイト文字が正しく表示されません。

III Remote Management（リモート管理）

Novell® ZENworks® 6.5 Server Management の Remote Management コンポーネントは、管理コンソールからリモートサーバを管理するための機能を提供します。ZENworks 6.5 Server Management を使用して、Novell NetWare® 5.1/6/6.5 または Windows* 2000/2003 サーバをリモート管理できます。

Remote Management を使用すると、管理者と組織の時間と費用を節約できます。たとえば、管理者または組織のヘルプデスクは、ユーザのサーバまで実際に出向かなくてもサーバの問題を分析してリモートで解決できます。このため、問題解決に要する時間が短縮され、生産性が向上します。

このドキュメントは次の章で構成されています。

- 19 章 749 ページの「NetWare サーバのリモート管理」
- 20 章 759 ページの「Windows サーバのリモート管理」
- 783 ページの付録 M、「ドキュメントの更新」

19 NetWare サーバのリモート管理

Novell® ZENWorks® 6.5 Server Management 用の Java* ベースのリモートコンソールユーティリティ（RConsoleJ）を使用して、Novell NetWare® サーバを制御し、次のタスクを実行できます。

- サーバコンソールと同様にコンソールコマンドを使用する
- サーバコンソールと同様に NLM™ プログラムを使用する（ファイルを編集する edit.nlm など）
- Buffer Input を使用して RConsoleJ Client からサーバのネイティブ言語でコンソールコマンドを送信する
- RConsoleJ を使用して別のサーバからサーバを制御する
- NetWare サーバをアップグレードする（テキストベースの UI のみ）
- Secure Socket Layer（SSL）ベースの安全なセッション

この節では、次のトピックについて説明します。

- 749 ページの「RConsoleJ コンポーネントの概要」
- 750 ページの「RConsoleJ の設定」
- 752 ページの「RConsoleJ」
- 755 ページの「起動時のエージェントのロード」
- 756 ページの「RConsoleJ のセキュリティの設定」
- 756 ページの「リモート NetWare サーバの管理」

RConsoleJ コンポーネントの概要

RConsoleJ には次のコンポーネントがあります。これらのコンポーネントは、NetWare サーバのリモートコントロールセッションで相互に通信します。

- 749 ページの「RConsoleJ クライアント」
- 750 ページの「RConsoleJ Agent」
- 750 ページの「RConsoleJ Proxy Agent」

RConsoleJ クライアント

RConsoleJ Client は、ワークステーションで実行される Java ベースのユーティリティです。RConsoleJ Client から、NetWare コンソールのすべての操作をリモートで制御および監視できます。

RConsoleJ Agent

RConsoleJ Agent（rconag6.nlm）は、ターゲット NetWare サーバ上で実行されるユーティリティです。ターゲット NetWare サーバには、RConsoleJ Agent 上で実行される IP、IPX™、または IP/IPX を介して接続できます。RConsoleJ Agent は、RConsoleJ Client のすべての要求を処理します。

RConsoleJ Agent は、NetWare 5.*x* 以降が実行されるコンピュータで Service Location Protocol（SLP）を使用してサービスをアドバタイズします。

RConsoleJ Proxy Agent

RConsoleJ Proxy Agent（rconprxy.nlm）は NetWare サーバ上で実行されるユーティリティです。Netware 5.*x* 以降でのみサポートされています。このユーティリティは、すべての IP パケットの IPX へのルーティングとその逆のルーティングを行います。

RConsoleJ Proxy Agent は、Service Location Protocol（SLP）を使用してそのサービスをアドバタイズします。

重要： ターゲット NetWare サーバが IPX だけを使用している場合、RConsoleJ Proxy Agent がロードされるその NetWare サーバには、IP および IPX の両方のスタックがインストールされている必要があります。

RConsoleJ の設定

RConsoleJ を設定するには、次の節の説明に従ってください。

- 750 ページの「RConsoleJ Agent のロード」
- 751 ページの「RConsoleJ Client の実行」
- 751 ページの「プロキシサーバへの RConsoleJ Proxy Agent のロード」

RConsoleJ Agent のロード

1 サーバコンソールプロンプトで、次のように入力します。

rconag6

2 RConsoleJ を使用してターゲット NetWare サーバにアクセスするときにネットワーク管理者が使用するパスワードを入力します。

3 TCP ポート番号を入力します。

デフォルト値は 2034 です。

サーバが IPX のみを使用して通信する場合は、「**-1**」を入力して TCP リスニングを無効にします。

動的に割り当てられるポートでのリスニングを有効にするには、「**0**」を入力します。

4 RCONAG6 がプロキシサーバをリスニングする SPX™ ポート番号を入力します。

デフォルトでは、[16800] が選択されています。

サーバが IP のみを使用して通信する場合は、「**-1**」を入力して SPX リスニングを無効にします。

動的に割り当てられるポートでのリスニングを有効にするには、「**0**」を入力します。

注： 純粋な IPX サーバを使用している場合、/DEV/TCP および /DEV/TCPSSL は失敗します。

ファイアウォールを介して RConsoleJ を有効にするには、ポート 2034、2035、および 2036 を開いておく必要があります。

RConsoleJ Client の実行

ワークステーションまたは NetWare サーバから RConsoleJ クライアントを実行できます。

- 751 ページの「ワークステーションからの RConsoleJ Client の実行」
- 751 ページの「NetWare サーバ上での RConsoleJ Client の実行」

ワークステーションからの RConsoleJ Client の実行

次のいずれかの方法を使用して、ワークステーション上で RConsoleJ Client を実行できます。

- Windows* 2000/XP ワークステーションから、*ConsoleOne_installation_directory*¥1.2 を参照し、rconj.exe を実行します。
- Novell ConsoleOne™ で、リモートコントロールする NetWare サーバオブジェクトを右クリックし、[Remote Management] をクリックします。
- ConsoleOne で、NetWare サーバオブジェクトを選択した後、[Tools] メニューから [ZENworks Remote Management] > [Remote Console] > [NetWare] の順にクリックします。
- ConsoleOne で、Subscriber または Distributor オブジェクトを右クリックし、[Remote Management] をクリックします。
- ZENworks 6.5 Management and Monitoring Services をインストールしている場合は、[Atlas Namespace] で NetWare サーバを選択し、[Remote Management] をクリックします。

NetWare サーバ上での RConsoleJ Client の実行

次のいずれかの方法を使用して、NetWare サーバ上で RConsoleJ Client を実行できます。

- ConsoleOne で、リモートコントロールする NetWare サーバオブジェクトを右クリックして [Remote Management] をクリックするか、NetWare サーバオブジェクトをクリックして [Tools] オプションから [ZENworks Remote Management] > [Remote Console] > [NetWare] の順にクリックします。
- サーバコンソールプロンプトから、「**rconj.ncf**」と入力します。
- サーバの GUI から、[Novell] > [Programs] > [RConsoleJ] の順にクリックします。

プロキシサーバへの RConsoleJ Proxy Agent のロード

RConsoleJ Proxy Agent をロードする NetWare サーバには、IP/IPX スタックがロードされている必要があります。

1 サーバコンソールプロンプトで次のコマンドを入力します。

```
rconprxy
```

2 RCONPRXY が RConsoleJ をリスニングする TCP ポート番号を入力します。

デフォルトでは、[2035] が選択されています。

動的に割り当てられるポートでのリスニングを有効にするには、「**0**」を入力します。

NetWare サーバが RConsoleJ Proxy Agent を実行している場合、RConsoleJ Client は RConsoleJ Proxy Agent を介して、通信に IPX だけを使用しているターゲット NetWare サーバと通信することができます。

RConsoleJ

ここでは、次のような構成で RConsoleJ を開始する方法について説明します。

- 752 ページの「シナリオ 1:IP NetWare サーバを制御する IP クライアント」
- 754 ページの「シナリオ 2:IPX NetWare サーバを制御する IP クライアント」

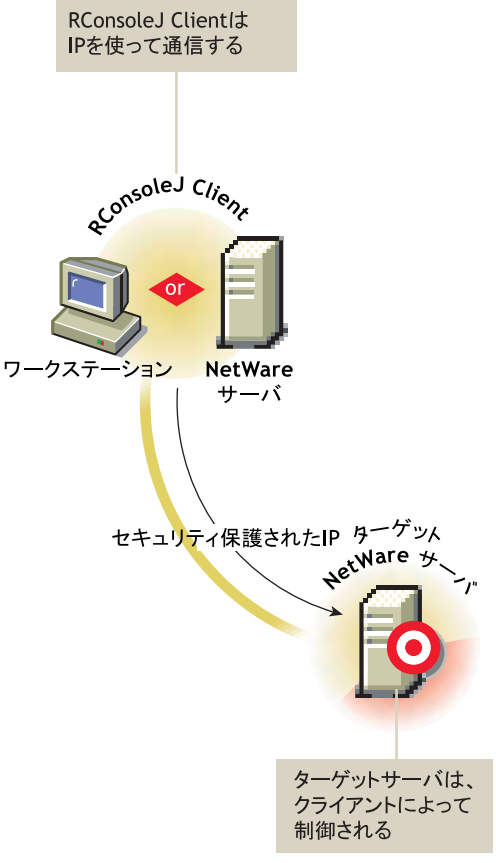
シナリオ 1:IP NetWare サーバを制御する IP クライアント

前提条件

- 750 ページの「RConsoleJ Agent のロード」
- 751 ページの「RConsoleJ Client の実行」

セキュリティ保護された IP 接続の設定

RConsoleJ Client は、TCP/IP を使用して RConsoleJ Agent と直接通信します。



セキュリティ保護された IP 接続を設定するには、次の手順に従います。

1 [RConsoleJ Connection] ダイアログボックスで、[Secure IP] を選択します。

2 ターゲット NetWare サーバの IP アドレスを入力するか、[Remote Servers] アイコンをクリックしてリストからターゲット NetWare サーバを選択します。

3 RConsoleJ Agent をターゲットサーバにロードするときに指定したパスワードを入力します。

4 ポート番号を入力します。

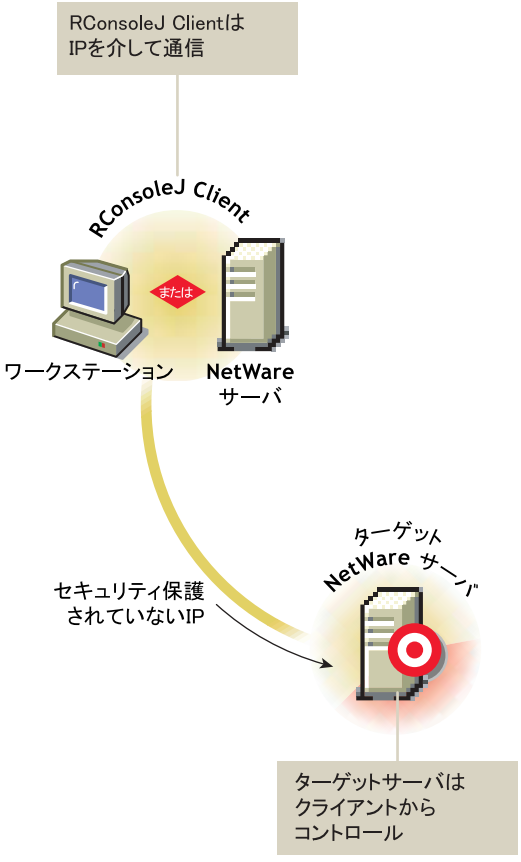
デフォルトでは、[2036] が選択されています。

5 [Connect] をクリックします。

6 サーバ認証を行うには、ターゲットサーバが発行する Untrusted Certificate Verification サーバ証明書に目を通し、[OK] をクリックして承諾します。

セキュリティ保護されていない IP 接続の設定

RConsoleJ Client は、TCP/IP を使用して RConsoleJ Agent と直接通信します。



ConsoleOne から RConsoleJ Client を実行する場合、[Novell RConsoleJ] ダイアログボックスに NetWare サーバの IP アドレスが表示されます。RConsoleJ Client を実行する方法については、751 ページの「RConsoleJ Client の実行」を参照してください。

IP 接続を開始するには

1 RConsoleJ Agent のロード時に指定したパスワードを入力します。

2 ポート番号を入力します。

デフォルトでは、[2034] が選択されています。

3 [Connect] をクリックします。

シナリオ 2:IPX NetWare サーバを制御する IP クライアント

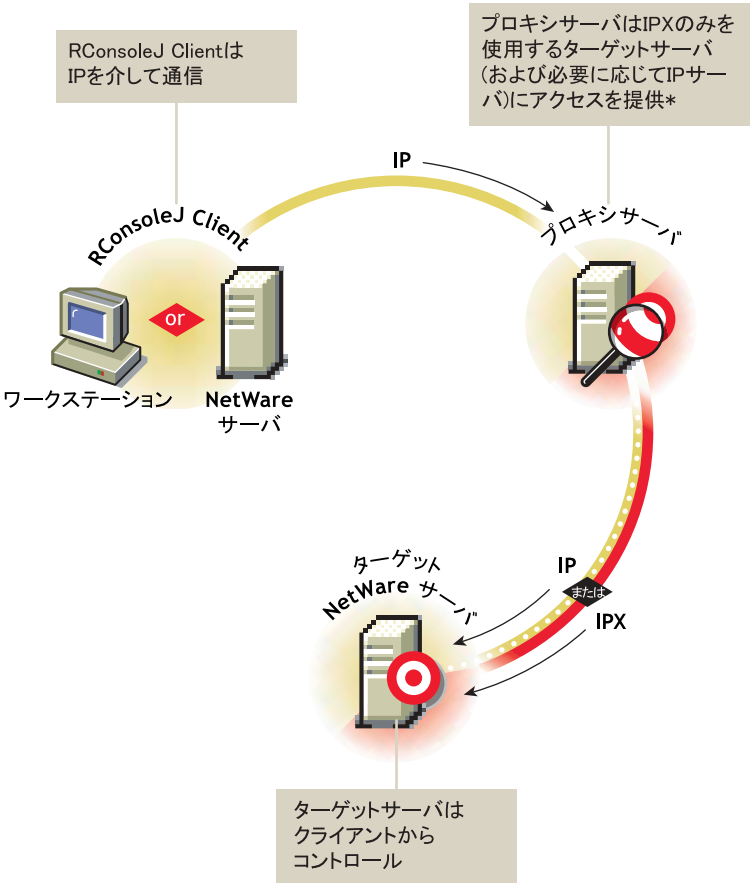
前提条件

- 750 ページの「RConsoleJ Agent のロード」
- 751 ページの「RConsoleJ Client の実行」
- 751 ページの「プロキシサーバへの RConsoleJ Proxy Agent のロード」

IPX 接続の開始

RConsoleJ Client は RConsoleJ Proxy Agent を介して RConsoleJ Agent と通信します。これは、ターゲット NetWare サーバが IPX だけを使用しているからです。

RConsoleJ Proxy Agent は、IP と IPX の両方のスタックがロードされている NetWare サーバ (プロキシサーバ) にロードされます。RConsoleJ Proxy Agent は、RConsoleJ Client からすべての IP 要求を受信し、それを IPX 要求に変換して、RConsoleJ Agent に送信します。逆の場合も同様です。



*ターゲットサーバがIPXを使用する場合、プロキシサーバにはIPとIPXの両方のスタックがロードされている必要があります。

ConsoleOne から RConsoleJ Client を実行する場合、[Novell RConsoleJ] ダイアログボックスに NetWare サーバの IP アドレスが表示されます。RConsoleJ Client を実行する方法については、751 ページの「RConsoleJ Client の実行」を参照してください。

IPX 接続を開始するには

1 [Connect Type] ドロップダウンリストから、[Connect through Proxy] を選択します。IPX アドレスを取得するには [SPX] を、IP アドレスを取得するには [TCP] を選択します。

2 前の手順で変更を行うと、デフォルトのポートが選択されます。

デフォルトは、IPX アドレスの場合は 16800、IP アドレスの場合は 2034 です。

3 プロキシサーバの IP アドレスを入力するか、[Remote Servers] アイコンをクリックし、リストからプロキシサーバを選択します。

4 RConsoleJ Proxy Agent のロード時に指定したポート番号を入力します。

RConsoleJ Client はこのポート上で RConsoleJ Proxy Agent と通信します。

デフォルトでは、[2035] が選択されています。

5 [Connect] をクリックします。

起動時のエージェントのロード

起動時に、RConsoleJ Agent および RConsoleJ Proxy Agent をロードできます。

- 755 ページの「起動時の RConsoleJ Agent のロード」
- 756 ページの「起動時の RConsoleJ Proxy Agent のロード」

起動時の RConsoleJ Agent のロード

次のいずれかの方法を使用して、RConsoleJ Agent (rconag6.nlm) をロードできます。

- 755 ページの「暗号化されたパスワードの使用（推奨）」
- 756 ページの「プレーンテキストパスワードの使用」

暗号化されたパスワードの使用（推奨）

1 ldrconag.ncf スクリプトファイルを準備します。

1a コンソールプロンプトで、「**rconag6 encrypt**」と入力します。

1b RConsoleJ Agent サーバの画面で、パスワードとポート番号を入力します。

1c「**Y**」と入力します。

2 起動時に ldrconag.ncf スクリプトファイルを実行するように、autoexec.ncf ファイルを準備します。

2a 次の行をコメントにします。

```
load rconag6 user_defined_password_here 2034 16800 2036
```

2b 次の行を入力します。

```
ldrconag
```

注： インストールウィザードで管理対象サーバのパスワードを指定した場合、ZENworks 6.5 Server Management Remote Management Agent のインストールではこれらの手順が自動的に実行されます。

プレーンテキストパスワードの使用

次の行を autoexec.ncf に入力します。

```
load rconag6 your_password 2034 16800 2036
```

起動時の RConsoleJ Proxy Agent のロード

起動時に RConsoleJ Proxy Agent (rconprxy.nlm) をロードするには、次の行を autoexec.ncf に入力します。

```
load rconprxy 2035
```

RConsoleJ のセキュリティの設定

エージェントのパスワードを変更して、RConsoleJ セッションのセキュリティを保護することができます。

リモート管理する NetWare サーバのエージェントのパスワードを変更するには

1. NetWare Console のプロンプトで、「**unload rconag6**」と入力して rconag6.nlm をアンロードします。
2. 「**rconag6 encrypt**」と入力します。
3. 新しいパスワードを入力します。
4. TCP ポート番号を入力します。デフォルトは 2034 です。
5. SPX ポート番号を入力します。デフォルトは 16800 です。
6. 次のコマンドラインを ldrconag.ncf ファイルに保存するには、「**y**」と入力します。

   「**n**」を入力すると、ldrconag.ncf ファイルは更新されません。新しいパスワードは現在のセッションでのみ有効になります。後で、RCONAG6 を ldrconag.ncf ファイルからロードした場合、以前に保存したパスワードが使用されます。

   新しいパスワードは、サーバを再起動した後、エージェントが LDRCONAG スクリプトファイルからロードされたときに有効になります。

この代わりに、次のコマンドを使用してパスワードを変更することもできます。

- Netware 4.*x* および 5.*x* の場合：

  ```
  LOAD RCONAG6 - E encrypted_password TCP_port_number SPX_port_number
  ```

- Netware 6.*x* の場合：

  ```
  LOAD RCONAG6 - E encrypted_password TCP_port_number SPX_port_number
  Secure_port_number
  ```

リモート NetWare サーバの管理

RConsoleJ で NetWare サーバとの接続を確立すると、デスクトップからターゲット NetWare サーバを表示および管理できます。

次の節では、リモート NetWare サーバを効果的に管理するために実行できるタスクを説明します。

- 757 ページの「サーバのネイティブ言語でのコンソールコマンドの送信」
- 757 ページの「RConsoleJ Client とターゲット NetWare 画面との同期」

サーバのネイティブ言語でのコンソールコマンドの送信

次の図に示されているように、[Buffer Input] を使用して、RConsoleJ Client からサーバのネイティブ言語でコンソールコマンドを送信できます。このバッファには、10 個の履歴コマンドのリストが格納されます。



コンソールコマンドを送信するには、次の操作を行います。

1 [Novell RConsoleJ Client] ウィンドウから、ターゲットサーバで実行するコマンドを [Buffer Input] フィールドに入力します。

2 [Send] をクリックします。

RConsoleJ Client とターゲット NetWare 画面との同期

ターゲット NetWare サーバに表示される画面と、RConsoleJ Client に表示される画面とを、互いに同期することができます。RConsoleJ Client で画面を切り替えると、ターゲットサーバのコンソールでも画面が切り替わります。逆の場合も同じです。

画面を同期するには、[Novell RConsoleJ] ウィンドウで [Sync] をクリックします。

サーバコンソールの画面を、RConsoleJ Client で現在アクティブ化されている画面に切り替えるには、[Activate] をクリックします。

20 Windows サーバのリモート管理

Novell® ZENworks® 6.5 Server Management の Remote Management コンポーネントによって、使用しているコンピュータで Windows* 2000/2003 サーバをリモート管理できます。

この章では、次のトピックについて説明します。

- 759 ページの「Remote Management の用語」
- 760 ページの「Windows サーバのリモート管理の理解」
- 761 ページの「Remote Management のセキュリティの設定」
- 765 ページの「リモート Windows サーバの管理」

Remote Management の用語

次の簡単な用語集は、Remote Management で使用される用語の基本的な定義を記載したものです。

管理対象サーバ： リモート管理する Windows サーバ。このサーバには ZENworks 6.5 Remote Management Agent をインストールする必要があります。サーバリモート管理ポリシーを適用してこのサーバを管理する場合は、ZENworks 6.5 Subscriber コンポーネントもインストールする必要があります。

管理コンソール： Novell ConsoleOne® を実行し、ZENworks 6.5 Remote Management ConsoleOne スナップインがインストールされている Windows 2000/XP ワークステーションまたは Windows 2000/2003 サーバ。管理コンソールは、ネットワークを管理するためのインタフェースになります。

管理サーバ： Novell eDirectory™ および ZENworks 6.5 Distributor コンポーネントがインストールされたサーバ。サーバリモート管理ポリシーを適用してサーバを管理する場合は、eDirectory および Distributor コンポーネントをインストールする必要があります。管理サーバを管理対象サーバに設定することができます。

リモートオペレータ： サーバをリモート管理できるユーザ。

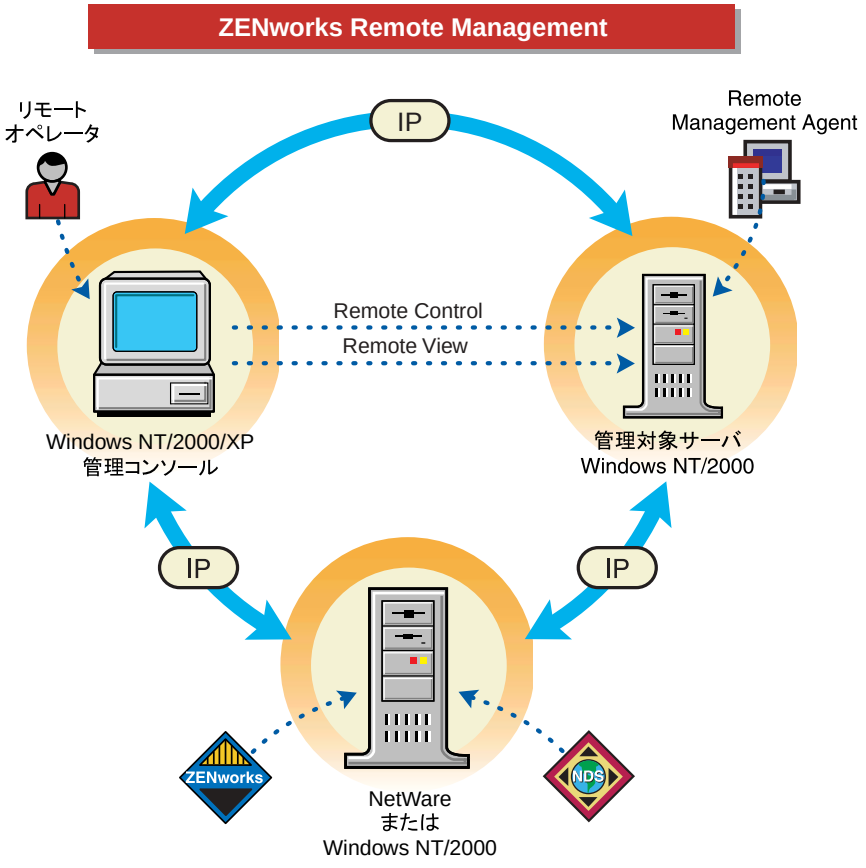
管理者： Remote Management コンポーネントをインストールする権利のある人。管理者もリモートオペレータですが、すべてのリモートオペレータが管理者というわけではありません。

Remote Management Agent: リモートオペレータがリモートからサーバを管理できるようにするために管理対象サーバにインストールする Server Management コンポーネント。Remote Management Agent は、管理対象サーバの起動時に自動的に起動し、リモートセッションの開始時にリモートオペレータを認証します。

[Viewing] ウィンドウ： 管理対象サーバのデスクトップの内容。これは、リモートオペレータが Remote Management セッションを開始すると、管理コンソールに表示されます。

Windows サーバのリモート管理の理解

次の図は、後で説明する ZENworks 6.5 Remote Management の機能を示しています。



サーバをリモート管理するには、サーバに ZENworks 6.5 Remote Management Agent コンポーネントがインストールされている必要があります。詳細については、『Novell ZENworks 6.5 Server Management インストールガイド』の「Policy-Enabled Server Management のインストール」を参照してください。

Remote Management Agent は、管理対象サーバの起動時に自動的に起動されます。エージェントのパスワードは、Remote Management のインストール時に管理者が設定している場合と、インストール後に管理対象サーバでユーザが設定している場合があります。リモートオペレータは、管理対象サーバで Remote Management セッションを開始するときにパスワードを入力する必要があります。検証されると、Remote Management セッションが続行され、管理コンソールに [Viewing] ウィンドウが表示されます。

管理対象サーバを使用しているユーザは、エージェントのパスワードを変更できます。パスワードを変更する場合は、新しいパスワードがリモートオペレータに通知される必要があります。セキュリティの危険を避けるために、パスワードは頻繁に変更することをお勧めします。新しいエージェントのパスワードを設定したり、既存のエージェントのパスワードを変更する方法の詳細については、764 ページの「管理対象サーバでのエージェントのパスワードの設定」を参照してください。

Remote Management のセキュリティの設定

次の節では、Remote Management セッションのセキュリティの設定に役立つ情報を示します。

- 761 ページの「Remote Management ポリシーの設定」
- 764 ページの「管理対象サーバでのエージェントのパスワードの設定」

Remote Management ポリシーの設定

Remote Management ポリシーを設定するには、次の作業を行う必要があります。

- 761 ページの「ポリシーパッケージの作成」
- 762 ページの「TED オブジェクトの作成と設定」
- 762 ページの「サーバリモート管理ポリシーの設定」
- 764 ページの「Remote Management 用の Distribution オブジェクトの設定」
- 764 ページの「Distributor オブジェクトと Subscriber オブジェクトの設定」

管理対象サーバのセキュリティ設定は、*ZENworks_agent_directory*¥rmagent¥zfsrcpol.ini ファイルの［Remote Management Policy］セクションを編集することによって変更することもできます。

ポリシーパッケージの作成

ZENworks 6.5 は、eDirectory ツリー内に、サーバポリシーを保持できるポリシーパッケージを必要とします。後でサーバポリシーを設定して有効にすることができます。

ポリシーパッケージは、オブジェクトタイプ別にグループ化されたポリシーのコレクションが含まれている eDirectory オブジェクトです。ポリシーパッケージを保持する部門（OU）を作成する必要があります。この OU を配置する場所を決定するときは、次の点に考慮してください。

- ツリー内にパーティションがあるかどうか
- eDirectory 内の完全識別名の 256 文字までの制限
- ポリシーパッケージを見つけるための検索ポリシーの使用方法

ツリーに ZENworks 6.5 Desktop Management をインストールする場合は、ZENworks Server Management のポリシーと Desktop Management のポリシーを Server_Policies と Desktop_Policies などの独立したコンテナに保存できます。

Remote Management の場合は、2 つのコンテナを作成します。1 つは Tiered Electronic Distribution（TED）オブジェクト用で、もう 1 つは Remote Management ポリシーパッケージ用です。

コンテナを作成するには

1. ConsoleOne で、ポリシーパッケージ用のコンテナを配置するコンテナを右クリックします。
2. ［New］>［Object］>［Organizational Unit］>［OK］の順にクリックします。
3. コンテナに Server_Policies などの名前を付けて、［OK］をクリックします。

重要： WAN を介してアクセスされるパーティションがある場合は、Policy/Package Agents がロードされるように、ポリシーパッケージオブジェクトをサーバオブジェクトと同じパーティションに配置してください。また、検索ポリシーで、サーバオブジェクトが存在するパーティション以外のパーティションを検索する必要がないようにしてください。

Remote Management では、Distributed Server Package を作成する必要があります。Distributed Server Package は、Remote Management ポリシーを管理対象サーバに配布して適用するために必要です。

Distributed Server Package を作成するには

1 ConsoleOne で、ポリシーパッケージのコンテナを右クリックし、[New] > [Policy Package] の順にクリックします。

Policy Package ウィザードが表示されます。

2 [Policy Packages] リストで、[Distributed Server Package] を選択し、[Next] をクリックします。

3 Distributed Server Package の名前を入力し、[Next] > [Finish] の順にクリックします。

TED オブジェクトの作成と設定

Remote Management では、次の TED オブジェクトを作成して設定する必要があります。

- TED Distribution
- TED Channel

TED オブジェクトの作成と設定については、3 章 87 ページの「Tiered Electronic Distribution」を参照してください。

サーバリモート管理ポリシーの設定

サーバリモート管理ポリシーによって、Remote Management Agent の動作を定義します。このポリシーは、指定した Windows 管理対象サーバに、TED を使用して配布されます。これによって、リモートオペレータは、管理コンソールから、Remote Management ポリシーを Windows 管理対象サーバのグループに関連付けることができます。

サーバリモート管理ポリシーを設定するには

1 ConsoleOne で、[Distribute Server Package] オブジェクトを右クリックし、[Properties] をクリックします。

2 [Policies] タブをクリックし、[Windows] サブオプションを選択します。

3 [Enabled] 列の下にある [Server Remote Management Policy] のチェックボックスを選択します。

4 [Properties] ボタンをクリックし、[Remote Management] タブをクリックします。

5 [General] タブをクリックし、次のいずれかのオプションを選択します。

- **[Enable Session Encryption]:** Remote Control セッションおよび Remote View セッションを暗号化します。リモートオペレータは、暗号化有効の状態を非暗号化モードへ変更できません。このチェックボックスを選択しない場合、デフォルトではリモートセッションは暗号化されません。この場合、リモートオペレータには、コンソールから暗号化モードに切り替えるオプションがあります。暗号化セッションは、高速接続に対するリモートセッションの性能に若干影響します。

重要： このオプションは、ZENworks for Servers 3.*x* および以前のバージョンの Remote Management Agent では機能しません。

- **[Allow User to Request Remote Session]：** 管理対象サーバのユーザが、管理コンソールのリモートオペレータに対してリモートセッションの実行を要求できるようにします。

  重要： このオプションは、ZENworks for Servers 3.*x* および以前のバージョンの Remote Management Agent では機能しません。

- **[Display Remote Management Agent Icon To Users]：** Remote Management Agent を実行している Windows 2000 または Windows 2003 管理対象サーバのシステムトレイに［Remote Management Agent］アイコンを表示します。

6 ［Remote Control］タブをクリックし、次のいずれかのオプションを選択します。

- **[Prompt User for Permission to Remote Control]：** リモートオペレータが開始した Remote Control セッションを受け入れるか拒否するかを管理対象サーバのユーザが選択できるようにします。
- **[Give User Audible Signal when Remote Controlled]：** リモートオペレータが管理対象サーバをリモート制御するたびに、管理対象サーバに通知音を発生させます。通知音を発生させる時間間隔を変更することができます。
- **[Give User Visible Signal when Remote Controlled]：** リモートオペレータが管理対象サーバをリモート制御するたびに、リモートオペレータとコンソールコンピュータの名前を示すビジュアル信号を管理対象サーバに表示します。名前を表示する時間間隔を変更することができます。
- **[Allow Blanking User's Screen]：** リモートコントロールセッションの際に、リモートオペレータが管理対象サーバの画面を消去したり、マウス操作やキーボード操作をロックしたりできるようにします。
- **[Allow Locking User's Keyboard and Mouse]：** リモートコントロールセッションの際に、リモートオペレータが管理対象サーバのキーボード操作やマウス操作をロックできるようにします。

7 ［Remote View］タブをクリックし、次のいずれかのオプションを選択します。

- **[Prompt User for Permission to Remote View]：** リモートオペレータが開始した Remote View セッションを受け入れるか拒否するかを管理対象サーバのユーザが選択できるようにします。
- **[Give User Audible Signal when Remote Viewed]：** リモートオペレータが管理対象サーバをリモート表示するたびに、管理対象サーバに通知音を発生させます。通知音を発生させる時間間隔を変更することができます。
- **[Give User Visible Signal when Remote Viewed]：** リモートオペレータが管理対象サーバをリモート表示するたびに、リモートオペレータとコンソールコンピュータの名前を示すビジュアル信号を管理対象サーバに表示します。名前を表示する時間間隔を変更することができます。

8 ［Apply］>［Close］の順にクリックします。

9 サーバリモート管理ポリシーを右クリックし、［Edit Schedule］を選択します。

10 スケジュールを変更します。

11 ［Apply］>［Close］の順にクリックします。

12 サーバリモート管理ポリシーを管理対象サーバに関連付けるには、［Distribution］タブをクリックします。

13 [Add] をクリックします。

14 Distribution オブジェクトを参照して選択し、[OK] をクリックします。

15 [Apply] > [Close] の順にクリックします。

Remote Management 用の Distribution オブジェクトの設定

Remote Management ポリシーを配布するための Distribution オブジェクトを設定する必要があります。

Distribution オブジェクトを設定するには

1 ConsoleOne で、Distribution オブジェクトを右クリックし、[Properties] をクリックします。

2 [Type] タブをクリックします。

3 [Select Type] ドロップダウンリストから [Policy Package] を選択します。

4 [Add] をクリックし、サーバリモート管理ポリシーが含まれている Distributed Server Package を選択します。

5 [Schedule] タブをクリックします。

6 スケジュールを変更します。

7 [Apply] > [Close] の順にクリックします。

Distributor オブジェクトと Subscriber オブジェクトの設定

Distributor オブジェクトと Subscriber オブジェクトを設定する方法については、3 章 87 ページの「Tiered Electronic Distribution」を参照してください。

管理対象サーバが別の eDirectory ツリーにある場合や、Windows 2000/2003 サーバに eDirectory がインストールされていない場合、他のツリー内の管理対象サーバに存在する Subscriber に Distribution を送信するには、External Subscriber オブジェクトを作成して設定する必要があります。External Subscriber の詳細については、160 ページの「External Subscriber」を参照してください。

管理対象サーバでのエージェントのパスワードの設定

管理対象サーバのユーザは、Remote Management セッションをセキュリティで保護するために、Remote Management Agent のパスワードを変更できます。

エージェントのパスワードを変更するには

1 Windows 2000/2003 管理対象サーバのシステムトレイにある [Remote Management Agent] アイコンを右クリックします。

2 [Security] > [Set Password] の順にクリックします。

10 文字以内の ASCII（非拡張）文字を使用してパスワードを作成します。パスワードでは、大文字と小文字が区別されます。また、空欄にすることはできません。

パスワードを変更するたびに、新しいパスワードをリモートオペレータに通知する必要があります。

リモート Windows サーバの管理

次の節では、Windows 2000/2003 サーバ上で Remote Management セッションを効果的に管理するために役立つ情報を提供します。

- 765 ページの「Remote Management セッションの開始」
- 767 ページの「Windows XP SP2 での動作」
- 767 ページの「Remote Management ポートの設定」
- 768 ページの「Remote View セッションの管理」
- 771 ページの「Remote Control セッションの管理」
- 779 ページの「リモートオペレータ識別情報の表示」
- 779 ページの「Remote Management セッションの監査ログの表示」
- 779 ページの「Remote Management のパフォーマンスの向上」
- 780 ページの「Remote Management Agent のシャットダウンと再起動」

Remote Management セッションの開始

ConsoleOne から Remote Management セッションを開始するには、いくつかの方法があります。たとえば、次のような方法です。

- 765 ページの「ConsoleOne の[Tools]メニューからの Remote Management セッションの開始」
- 765 ページの「eDirectory/NDS ネームスペースからの Remote Management セッションの開始」
- 766 ページの「Atlas ネームスペースからの Remote Management セッションの開始」
- 766 ページの「Remote Management Agent からの Remote Management セッションの開始」

ConsoleOne の［Tools］メニューからの Remote Management セッションの開始

1. ConsoleOne で、［Tools］>［ZENworks Remote Management］>［Remote Console］>［Windows］の順にクリックします。
2. ［Remote Management］ダイアログボックスで、管理対象サーバの IP アドレスまたは DNS 名を入力します。
3. エージェントのパスワードを入力します。
4. 管理対象サーバで開始する Remote Management の操作を選択します。
5. ［OK］をクリックします。

eDirectory/NDS ネームスペースからの Remote Management セッションの開始

次のいずれかの方法で、ConsoleOne の eDirectory（NDS）ネームスペースから Remote Management セッションを開始できます。

1. ConsoleOne で、管理対象サーバを選択します。
2. ［Tools］>［ZENworks Remote Management］>［Remote Console］>［Windows］の順にクリックします。

3 [Remote Management] ダイアログボックスで、[Agent] ドロップダウンリストから管理対象サーバの IP アドレスを選択します。

選択した管理対象サーバの IP アドレスは、自動的に [Agent] ドロップダウンリストに追加されます。

4 エージェントのパスワードを入力します。

5 管理対象サーバで開始する Remote Management の操作を選択します。

6 [OK] をクリックします。

次の手順を使用することもできます。

1 ConsoleOne で、管理対象サーバを右クリックします。

2 [Remote Management] をクリックします。

3 [Remote Management] ダイアログボックスで、[Agent] ドロップダウンリストから管理対象サーバの IP アドレスを選択します。

選択した管理対象サーバの IP アドレスは、自動的に [Agent] ドロップダウンリストに追加されます。

4 エージェントのパスワードを入力します。

5 管理対象サーバで開始する Remote Management の操作を選択します。

6 [OK] をクリックします。

Atlas ネームスペースからの Remote Management セッションの開始

ConsoleOne で Atlas ネームスペースから Remote Management セッションを開始する前に、NetWare® Management Agent™ (NMA) がインストールされ、Discovery によってネットワークトポロジが検出されていることを確認します。

Remote Management セッションを開始するには

1 ConsoleOne で、管理対象サーバを右クリックします。

2 [Actions] > [Remote Control] または [Remote View] の順にクリックします。

3 IP アドレスおよびエージェントのパスワードを選択します。

選択した管理対象サーバの IP アドレスは、自動的に [Agent] ドロップダウンリストに追加されます。

4 [OK] をクリックします。

Remote Management Agent からの Remote Management セッションの開始

管理対象サーバが動的 NAT の内側に設定されている場合、管理コンソールから管理対象サーバにアクセスすることはできませんが、管理対象サーバから管理コンソールにアクセスすることはできます。この問題を解決するには、次の操作を行います。

1 管理対象サーバのユーザが、[Request Session] オプションを使用して、リモートオペレータに Remote Management セッションの要求を開始する必要があります。

重要： Remote Management Agent から Remote Management セッションを開始する前に、リモートオペレータは管理コンソールで ConsoleOne が実行されていることを確認する必要があります。

注： Remote Management Agent からターミナルサーバ上で実行されている管理コンソールへのセッション要求が開始されたときに、ConsoleOne の最初のインスタンスが要求を受信します。ConsoleOne が最初に起動されたセッションの ConsoleOne インスタンスがすべて終了するまで、ConsoleOne インスタンスではセッションの要求が受信されません。セッションの要求を受信するには、任意のターミナルセッションで ConsoleOne を再び起動する必要があります。

セッションを要求するには、管理対象サーバのユーザが次の操作を行う必要があります。

1a [Remote Management Agent] アイコンを右クリックします。

1b [Request Session] を選択します。

1c 管理コンソールの IP アドレスまたは DNS 名を入力します。

1d ドロップダウンリストから、[Remote Control] または [Remote View] 操作を選択します。

1e [OK] をクリックします。

2 Remote Management Listener が要求をリスニングし、リモートオペレータに要求を通知します。リモートオペレータは要求を受け付けて、[Select Authentication Mode] ダイアログボックスで次のアカウント情報を指定する必要があります。

2a 認証用のパスワードを入力します。

2b [OK] をクリックします。

Windows XP SP2 での動作

Windows XP SP2 には、デフォルトで有効になっているファイアウォールが付属しています。その結果、Windows XP SP2 で実行されている Remote Control Listener は、Remote Management Agent によって開始された接続を受信できません。

Remote Control Listener が接続を受信できるように、ファイアウォール設定を指定する必要があります。

Remote Control Listener は、デフォルトで TCP ポート 1762 にバインドされています。ポートを変更するには、768 ページの「Remote Control Listener ポートの設定」を参照してください。

Remote Management ポートの設定

ここでは、次の内容について説明します。

- 767 ページの「Remote Management Agent ポートの設定」
- 768 ページの「Remote Control Listener ポートの設定」

Remote Management Agent ポートの設定

Remote Management Agent ポートは、デフォルトでは TCP ポート 1761 にバインドします。次の手順に従うと、別の TCP ポート上で実行するように設定できます。

1 *ZENworks_agent_directory¥rmagent¥rmcfg.ini* ファイルを開きます。

2 ファイルの Remote Management Agent Port セクションで、DefaultCommPort を目的のポート番号に設定します。

3 Novell ZfS Remote Management Agent サービスを再起動します。

1761 以外のポート上で Remote Management Agent を実行している管理対象サーバに対するリモートセッションを開始するには、管理コンソールで次の変更を行う必要があります。

1 *ConsoleOne_directory*¥1.2¥bin¥rmports.ini ファイルを開きます。

2 ファイルの Remote Management Agent Ports セクションで、ポート番号を追加します。

注： 複数の Remote Management Agent を別々の管理対象サーバの別々のポート上で実行している場合は、Remote Management Agent Ports セクションで、他のポート番号の下に 1 ずつポート番号を指定します。

Remote Control Listener ポートの設定

Remote Control Listener ポートは、デフォルトでは ConsoleOne の起動時に TCP ポート 1762 にバインドします。次の手順に従うと、別の TCP ポート上で実行するように設定できます。

1 *ConsoleOne_directory*¥1.2¥bin¥rmports.ini ファイルを開きます。

2 ファイルの Remote Control Listener Port セクションで、DefaultCommPort を目的のポート番号に設定します。

3 ConsoleOne を再起動します。

1762 以外のポート上で Remote Control Listener を実行している管理コンソールに対するリモートセッションを開始するには、管理対象サーバで次の変更を行う必要があります。

1 *ZENworks_agent_directory*¥rmagent¥rmcfg.ini ファイルを開きます。

2 ファイルの Remote Control Listener Ports セクションで、ポート番号を追加します。

注： 複数の Remote Control Listener を別々の管理コンソールの別々のポート上で実行している場合は、Remote Control Listener Ports セクションで、他のポート番号の下に 1 ずつポート番号を指定します。

Remote View セッションの管理

Remote Management セッションを開始し、操作として［Remote View］を選択すると、管理対象サーバを表示するためのいくつかのオプションを選択できます。

- 768 ページの「［Viewing］ウィンドウの表示の制御」
- 770 ページの「［Viewing］ウィンドウのアクセラレータキーの使用」
- 771 ページの「アクセラレータキーのカスタムシーケンスの定義」

［Viewing］ウィンドウの表示の制御

コントロールオプションを使用することによって、［Viewing］ウィンドウの表示を制御できます。

コントロールオプションを有効にするには

1 ［Viewing］ウィンドウの左上隅にある［Remote Management Agent］アイコンをクリックします。

2 [Configure] をクリックします。

オプション	説明
高品質スケーリングを有効にする	[Scale To Fit] モードのイメージの品質を向上させます。
アクセラレータキーの有効化	管理コンソールのアクセラレータキーを有効にして、リモートセッション中にデフォルトのアクセラレータキーシーケンスを変更できるようにします。
暗号化を有効にする	暗号化はオプションの機能で、セッションごとに有効になります。保存されている設定で暗号化が有効の場合、セッションはセッション開始時から暗号化されます。 セッション全体を暗号化すると、ネットワーク経由で転送されるデータが暗号化されて、そのデータがネットワーク上でキャプチャされた場合でも重要な内容を解読することは難しいため、セキュリティが向上します。ただし、パフォーマンスには多少の影響があります。暗号化は、セキュリティがどうしても必要な場合にのみ使用することをお勧めします。
壁紙を非表示にする	管理対象サーバで表示されている壁紙を非表示にします。デフォルトではこのオプションが有効にされています。Remote View セッション中に管理対象サーバの壁紙を表示する場合は、このオプションを無効にします。
Color Quality	デフォルトの場合、高速リンクでは色の品質は [Normal] に設定され、低速リンクでは色の品質は [256 Colors] に設定されます。低速リンクまたは高速リンクの色の品質を、次のいずれかに変更できます。 ◆ 16 Colors:Remote Management セッション中に、管理対象サーバで 16 色のカラーパレットを使用するように強制します。これによって、特に低速リンクでの Remote Management のパフォーマンスが向上します。 ◆ 256 Colors:Remote Management セッション中に、管理対象サーバで 256 色のカラーパレットを使用するように強制します。これによって、低速リンクでの Remote Management のパフォーマンスが向上します。 ◆ Normal: 色の品質は変更されず、設定は Remote Management セッション中の管理対象サーバと同じです。
ネットワークタイプ	管理対象サーバが LAN で接続されている場合は、[Fast Links] オプションを選択すると、Remote Management のパフォーマンスが向上します。 管理対象サーバがダイヤルアップリンクまたは WAN で接続されている場合は、[Slow Links] オプションを選択すると、Remote Management のパフォーマンスが向上します。

3 [Control Parameter] の設定を保存するには、[Save on Exit] チェックボックスを選択します。

保存された設定は次の Remote View セッションで適用されます。

4 [OK] をクリックします。

[Viewing] ウィンドウのアクセラレータキーの使用

アクセラレータキーを使用して、コントロールオプションにショートカットキーを割り当てたり、[Viewing] ウィンドウの表示を制御したりできます。各アクセラレータキーオプションには、デフォルトのアクセラレータキー操作が割り当てられています。[Accelerator Keys] ダイアログボックスの各アクセラレータキーオプションの [Edit] フィールドにデフォルトのキー操作が表示されます。カスタムのアクセラレータキー操作を定義して、デフォルト操作を変更できます。詳細については、771 ページの「アクセラレータキーのカスタムシーケンスの定義」を参照してください。

アクセラレータキーオプションを有効にするには

1. [Viewing] ウィンドウの左上隅にある [Remote Management Agent] アイコンをクリックします。
2. [Configure] をクリックします。
3. [Enable Accelerator Keys] を選択します。
4. [OK] をクリックします。

[Accelerator Keys] ダイアログボックスを開くには

1. [Viewing] ウィンドウの左上隅にある [Remote Management Agent] アイコンをクリックします。
2. [Accelerator Keys] をクリックします。

次の表は、Remote View セッション中に使用できるアクセラレータキーのオプションについての説明です。

オプション	デフォルトのキー操作	説明
フルスクリーン切り替え	(Ctrl)+(Alt)+(M)	管理コンソールと管理対象サーバの解像度の設定が同じである場合にのみ適用できます。 [Viewing] ウィンドウのサイズを、ウィンドウの境界線を表示せずに画面のサイズに変更します。
リフレッシュスクリーン	(Ctrl)+(Alt)+(R)	[Viewing] ウィンドウをリフレッシュします。
セッションの再起動	(Ctrl)+(Alt)+(T)	管理対象サーバへの接続を再度確立します。
アクセラレータキーの有効化	(Ctrl)+(Alt)+(A)	デフォルトのアクセラレータキーシーケンスの有効または無効の切り替えを可能にします。
ビュー停止	左 (Shift)+(Esc)	[Viewing] ウィンドウを閉じます。
ダイアログの設定	(Alt)+(M)	[Control Parameters] ダイアログボックスを開きます。
アクセラレータキーダイアログ	(Alt)+(A)	[Accelerator Keys] ダイアログボックスを開きます。
フルスクリーンのポーリング	(Alt)+(L)	管理対象サーバの画面全体の情報をスキャンしてレンダリングします。
サイズの調整	(Ctrl)+(Alt)+(G)	スクロールバーを非表示にして、[Remote Management] ウィンドウのサイズを画面に合うように調整します。

アクセラレータキーのカスタムシーケンスの定義

アクセラレータキーオプションにデフォルトで割り当てられているキー操作は、[Accelerator Keys] ダイアログボックスの各アクセラレータキーオプションの右側の編集フィールドに表示されています。デフォルトのキー操作を使用しない場合は、アクセラレータキーのシーケンスを変更し、カスタムシーケンスを定義することができます。

アクセラレータキーのカスタムシーケンスを定義するには

1 [Viewing] ウィンドウの左上隅にある [Remote Management Agent] アイコンをクリックします。

2 [Accelerator Keys] をクリックします。

3 アクセラレータキーのカスタムシーケンスを定義するアクセラレータキーオプションの編集フィールドをクリックします。

4 新しいキーシーケンスを押します。

5 [OK] をクリックします。

重要： (Shift) キーについては左右どちらのキーを使用したかが区別され、[Control Options] ダイアログボックスに「LShift」または「RShift」のように表示されます。(Ctrl)+(C)、(Ctrl)+(V)、(Shift)+(Del) などの標準のキーシーケンスは使用しないでください。

Remote Control セッションの管理

Remote Management セッションを開始し、操作として [Remote Control] を選択すると、管理コンソールから管理対象サーバを制御して、ユーザサポートを提供したり、サーバの問題解決を支援したりできます。リモートコントロール接続を確立することで、リモートオペレータは管理対象サーバを参照するだけでなく制御することもできるようになります。

[Viewing] ウィンドウのコントロールオプション、[Viewing] ウィンドウのツールバーのボタン、および [Remote Management Agent] アイコンのオプションで次の作業を行うことによって、Remote Control セッションを効果的に管理できます。

- 772 ページの「[Viewing] ウィンドウの表示の制御」
- 773 ページの「[Viewing] ウィンドウのアクセラレータキーの使用」
- 775 ページの「[Viewing] ウィンドウのツールバーボタンの使用」
- 776 ページの「管理対象サーバ上の壁紙の有効化」
- 777 ページの「[Remote Management Agent] アイコンの使用」
- 777 ページの「管理対象サーバのパスワードの設定」
- 778 ページの「Remote Management セッションについての情報の取得」
- 778 ページの「一般情報の取得」
- 778 ページの「セキュリティ情報の取得」

[Viewing] ウィンドウの表示の制御

管理対象サーバの表示は、[Viewing] ウィンドウのコントロールオプションを使用して制御します。

コントロールオプションを有効にするには

1 [Viewing] ウィンドウの左上隅にある [Remote Management Agent] アイコンをクリックします。

2 [Configure] をクリックします。

3 リモートセッションのために有効にするコントロールオプションを選択します。

次の表は、[Viewing] ウィンドウの表示の制御に使用できるオプションについての説明です。

オプション	説明
Block Mouse Movements to Agent	ネットワーク帯域幅の消費を少なくするには、Agent に対するすべてのマウス操作をブロックします。
高品質スケーリングを有効にする	[Scale To Fit] モードでイメージの品質が向上します。
アクセラレータキーの有効化	管理コンソールのアクセラレータキーを有効にして、リモートセッション中にデフォルトのアクセラレータキーシーケンスを変更できるようにします。
暗号化を有効にする	暗号化はオプションの機能で、セッションごとに有効になります。保存されている設定で暗号化が有効の場合、セッションはセッション開始時から暗号化されます。 セッション全体を暗号化すると、ネットワーク経由で転送されるデータが暗号化されて、そのデータがネットワーク上でキャプチャされた場合でも重要な内容を解読することは難しいため、セキュリティが向上します。ただし、パフォーマンスには多少の影響があります。暗号化は、セキュリティがどうしても必要な場合にのみ使用することをお勧めします。
システムキーパス	管理コンソール上での (Alt) キーシーケンスを管理対象サーバに渡します。 **注：** Remote View セッション中は、[System Key pass-Through] オプションが有効になっていません。
壁紙を非表示にする	管理対象サーバで表示されている壁紙を非表示にします。デフォルトではこのオプションが有効にされています。Remote Control セッションまたは Remote View セッション中に管理対象サーバの壁紙を表示する場合は、このオプションを無効にします。
暗号化を有効にする	暗号化はオプションの機能で、セッションごとに有効になります。保存されている設定で暗号化が有効の場合、セッションはセッション開始時から暗号化されます。 セッション全体を暗号化すると、ネットワーク経由で転送されるデータが暗号化されて、そのデータがネットワーク上でキャプチャされた場合でも重要な内容を解読することは難しいため、セキュリティが向上します。ただし、パフォーマンスには多少の影響があります。暗号化は、セキュリティがどうしても必要な場合にのみ使用することをお勧めします。

オプション	説明
Color Quality	デフォルトの場合、高速リンクでは色の品質は［Normal］に設定され、低速リンクでは色の品質は［256 Colors］に設定されます。低速リンクまたは高速リンクの色の品質を、次のいずれかに変更できます。 • **16 Colors:** Remote Management セッション中に、管理対象サーバで 16 色のカラーパレットを使用するように強制します。これによって、特に低速リンクでの Remote Management のパフォーマンスが向上します。 • **256 Colors:** Remote Management セッション中に、管理対象サーバで 256 色のカラーパレットを使用するように強制します。これによって、低速リンクでの Remote Management のパフォーマンスが向上します。 • **Normal:** 色の品質は変更されず、設定は Remote Management セッション中の管理対象サーバと同じです。
ネットワークタイプ	管理対象サーバが LAN で接続されている場合は、［Fast Links］オプションを選択すると、Remote Management のパフォーマンスが向上します。 管理対象サーバがダイヤルアップリンクまたは WAN で接続されている場合は、［Slow Links］オプションを選択すると、Remote Management のパフォーマンスが向上します。

4 ［Control Parameter］の設定を保存するには、［Save on Exit］チェックボックスを選択します。

保存された設定は次のリモートコントロールセッションで適用されます。

［Viewing］ウィンドウのアクセラレータキーの使用

アクセラレータキーを使用して、コントロールオプションにショートカットキーを割り当てたり、［Viewing］ウィンドウの表示を制御したりできます。各アクセラレータキーオプションには、デフォルトのアクセラレータキー操作が割り当てられています。［Accelerator Keys］ダイアログボックスの各アクセラレータキーオプションの［Edit］フィールドにデフォルトのキー操作が表示されます。カスタムのアクセラレータキー操作を定義して、デフォルト操作を変更できます。詳細については、771 ページの「アクセラレータキーのカスタムシーケンスの定義」を参照してください。

アクセラレータキーオプションを有効にするには

1 ［Viewing］ウィンドウの左上隅にある［Remote Management Agent］アイコンをクリックします。

2 ［Configure］をクリックします。

3 ［Enable Accelerator Keys］を選択します。

［Accelerator Keys］ダイアログボックスを開くには

1 ［Viewing］ウィンドウの左上隅にある［Remote Management Agent］アイコンをクリックします。

2 ［Accelerator Keys］をクリックします。

次の表は、［Viewing］ウィンドウの表示の制御に使用できるアクセラレータキーのオプションについての説明です。

オプション	デフォルトのキー操作	説明
フルスクリーン切り替え	(Ctrl)+(Alt)+(M)	管理コンソールと管理対象サーバの解像度の設定が同じである場合にのみ適用できます。 [Viewing] ウィンドウのサイズを、ウィンドウの境界線を表示せずに画面のサイズに変更します。
リフレッシュスクリーン	(Ctrl)+(Alt)+(R)	[Viewing] ウィンドウをリフレッシュします。
セッションの再起動	(Ctrl)+(Alt)+(T)	管理対象サーバへの接続を再度確立します。
アクセラレータキーの有効化	(Ctrl)+(Alt)+(A)	デフォルトのアクセラレータキー操作を変更できるようにします。
ビュー停止	左 (Shift)+(Esc)	[Viewing] ウィンドウを閉じます。
ダイアログの設定	(Alt)+(M)	[Control Parameters] ダイアログボックスを開きます。
アクセラレータキーダイアログ	(Alt)+(A)	[Accelerator Keys] ダイアログボックスを開きます。
フルスクリーンのポーリング	(Alt)+(L)	画面全体の情報をスキャンしてレンダリングします。
サイズの調整	(Ctrl)+(Alt)+(G)	スクロールバーを非表示にして、[Remote Management] ウィンドウのサイズを画面に合うように調整します。
システムキーパス	(Ctrl)+(Alt)+(S)	管理コンソール上での (Alt) キーシーケンスを管理対象サーバに渡します。
Mouse/Keyboard Lock	(Ctrl)+(L)	管理対象サーバでのキーボードおよびマウスのコントロールをロックします。 このオプションは、サーバリモート管理ポリシーで、[Allow Locking User's Keyboard and Mouse] オプションが有効になっている場合にのみ使用できます。
Blank Screen	(Ctrl)+(Alt)+(B)	管理対象サーバの画面を消去するオプションです。 このオプションは、サーバリモート管理ポリシーで、[Allow Blanking User's Screen] オプションが有効になっている場合にのみ使用できます。
Reboot	(Ctrl)+(Alt)+(D)	管理対象サーバに (Ctrl)+(Alt)+(Del) キー操作を送信します。 管理対象サーバ上の [Security] ウィンドウを表示します。
開始	(Alt)+(R)	Windows サーバ上の [Start] メニューを呼び出します。
Switch Applications	(Ctrl)+(T)	管理対象サーバ上のアプリケーションを切り替えます。

[Viewing] ウィンドウのツールバーボタンの使用

次の表は、[Viewing] ウィンドウのツールバーオプションについての説明です。

ボタン	デフォルトのキー操作	主要な機能
Screen Blanking 	(Ctrl)+(L)	管理対象サーバの有効なリモートコントロールポリシーで [Allow Blanking User's Screen] オプションが有効になっている場合のみ使用できます。 管理対象サーバの画面を消去するオプションです。リモートオペレータがこのオプションを選択すると、管理対象サーバの画面が黒くなり、管理対象サーバ上でリモートオペレータが実行する操作が、管理対象サーバのユーザ側からは見えなくなります。 一部のディスプレイアダプタでは、この機能を使用することができません。この機能をサポートしていないディスプレイアダプタのリストについては、ZENworks 6.5 Server Management Readme を参照してください。
Mouse and Keyboard Lock 	(Ctrl)+(Alt)+(B)	管理対象サーバでのキーボードおよびマウスのコントロールをロックします。リモートオペレータがこのオプションを選択すると、管理対象サーバのユーザは、管理対象サーバのキーボードとマウスを使えなくなります。
System Start 	(Alt)+(R)	管理対象サーバ上の [Start] メニューを呼び出します。
Application Switcher 	(Ctrl)+(T)	管理対象サーバに (Alt)+(Tab) キーシーケンスを送信します。 管理対象サーバ上のアプリケーションを切り替えます。 アプリケーションを切り替えるには 1. [Viewing] ウィンドウで [Application Switcher] アイコンをクリックするか、Application Switcher のショートカットキーを押します。 2. 必要なアプリケーションを選択するには、[Application Switcher] アイコンを使用します。 3. アプリケーションを表示するには、(Tab) キーを押します。
System Key Pass Through 	(Ctrl)+(Alt)+(S)	システムキーの送信を [On] または [Off] に設定します。 (Alt) キーシーケンスを管理コンソールから管理対象サーバに渡します。 (Ctrl)+(Esc)、(Alt)+(Tab)、(Ctrl)+(Alt)+(Del)、および (Alt)+(PrintScreen) といった特定のキー操作は、[System Key Pass-Through] が [On] に設定されている場合でも使用できません。ただし、[Viewing] ウィンドウのツールバーボタンを使って、(Ctrl)+(Esc)、(Alt)+(Tab)、および (Ctrl)+(Alt)+(Del) などのキー操作を実行できます。

ボタン	デフォルトのキー操作	主要な機能
Reboot 	(Ctrl)+(Alt)+(D)	管理対象サーバに (Ctrl)+(Alt)+(Del) キー操作を送信します。 管理対象サーバ上の [Security] ウィンドウを表示します。
リフレッシュスクリーン 	(Ctrl)+(Alt)+(R)	[Viewing] ウィンドウを更新します。
Full Screen Polling 	(Alt)+(L)	管理対象サーバの画面全体の情報を継続的にスキャンしてレンダリングします。
サイズの調整 	(Ctrl)+(Alt)+(G)	スクロールバーを非表示にして、[Remote Management] ウィンドウのサイズを画面に合わせます。
セッションの暗号化 		暗号化はオプションの機能で、セッションごとに有効になります。保存済みの設定で暗号化のオプションが有効になっている場合、セッションは開始の時点から暗号化されます。 セッション全体を暗号化すると、ネットワーク経由で転送されるデータが暗号化されて、そのデータがネットワーク上でキャプチャされた場合でも重要な内容を解読することは難しいため、セキュリティが向上します。ただし、パフォーマンスには多少の影響があります。暗号化は、セキュリティがどうしても必要な場合にのみ使用することをお勧めします。

デフォルトのキーシーケンスを使用しない場合は、キーのカスタムシーケンスを定義できます。詳細については、771 ページの「アクセラレータキーのカスタムシーケンスの定義」を参照してください。

管理対象サーバ上の壁紙の有効化

リモートオペレータが Remote Control セッションを開始したときは、管理対象サーバのデスクトップに表示されていた壁紙が非表示になります。この機能は、管理コンソールからの要求に対する管理対象サーバからの応答時間を短縮するためのもので、壁紙を非表示にすることにより、ネットワーク上に生じるトラフィックが軽減されます。

このオプションのコントロールパラメータは、デフォルトの設定を変更して、管理対象サーバ上の壁紙を表示できるように設定することもできます。Remote Control セッションを終了すると、非表示にされていた壁紙が復元されます。

管理対象サーバの非表示にされている壁紙を有効にするには

1 左上隅にある [Remote Management Agent] アイコンをクリックし、[Configure] をクリックします。

2 [Hide Wallpaper] オプションの選択を解除します。

[Remote Management Agent] アイコンの使用

デフォルトでは、[Remote Management Agent] アイコンは、Windows サーバのシステムトレイに表示されます。このアイコンは、Remote Management Agent が管理対象サーバにロードされていることを示します。

管理対象サーバのユーザは [Remote Management Agent] アイコンを右クリックして、次のオプションを選択できます。

オプション	説明
RC/RV セッションを終了する	管理対象サーバ上のリモートセッションを切断、終了し、管理コンソールにリモートセッションが閉じられたことを示すメッセージを表示します。
セキュリティ	管理対象サーバのユーザがサーバのパスワードを設定またはクリアできるようにします。
情報	リモートセッションのために管理対象サーバにアクセスしているユーザ、セキュリティ設定、およびリモートセッションに使用されているプロトコルなどに関する情報を表示します。 詳細については 778 ページの「Remote Management セッションについての情報の取得」を参照してください。 [Remote Management Agent] アイコンを右クリックまたはダブルクリックすると、[Information] ウィンドウを表示することができます。
Shutdown Agent	このオプションは、管理対象サーバでは常にグレー表示されています。管理対象サーバで Remote Management Agent をシャットダウンするには、[Service Control Panel] に移動して「Novell ZFS Remote Management Agent」サービスを停止します。
セッションを要求する	管理対象サーバのユーザがリモートオペレータに対してリモートセッションの実行を要求できるようにします。
ヘルプ	Remote Management Agent のヘルプを表示します。

管理対象サーバのパスワードの設定

管理対象サーバのユーザがエージェントのパスワードを設定できます。このパスワードによって、ZENworks 6.5 Remote Management のインストール時に管理者が設定したパスワードは上書きされます。

エージェントのパスワードを設定するには

1 管理対象サーバから、[Remote Management Agent] アイコンを右クリックします。

2 [Security] > [Set Password] の順にクリックします。

10 文字以内の半角英数文字を使用してパスワードを作成します。パスワードでは、大文字と小文字が区別されます。また、空欄にすることはできません。

Remote Management セッションが終了した後、エージェントのパスワードをクリアできます。エージェントのパスワードをクリアすると、リモートオペレータは Remote Management の操作を実行できません。

エージェントのパスワードをクリアするには

1 管理対象サーバで、[Remote Management Agent] アイコンを右クリックします。

2 [Security] > [Clear Password] の順にクリックします。

Remote Management セッションについての情報の取得

[Information] ウィンドウを使用すると、管理対象サーバを使用しているユーザが、リモートオペレータの名前、サーバをリモート管理する方法、セキュリティ設定、およびリモートセッションに使用されているプロトコルなど、セッションについての詳細情報を表示することができます。

リモートセッションについての情報を表示するには

1 管理対象サーバで、[Remote Management Agent] アイコンを右クリックします。

2 [Information] をクリックします。

3 [General] タブをクリックすると一般情報を、[Security] タブをクリックするとセキュリティ情報を表示できます。

詳細については、次の節を参照してください。

- 778 ページの「一般情報の取得」
- 778 ページの「セキュリティ情報の取得」

一般情報の取得

次の表は、[Information] ウィンドウから Remote Management セッションについて取得できる一般情報についての説明です。

パラメータ	説明
[RM Operation]	実行中のリモート管理セッションを一覧表示します。
RM Information > Initiator	リモートオペレータの名前を表示します。
RM Information > Protocol	リモートセッション中に Remote Management Agent が管理コンソールと通信するために使用するプロトコルを表示します。
Optimization Status > RC/RV Optimization	Remote Management セッションの最適化ドライバが有効か無効かを表示します。最適化ドライバが有効になっている場合、リモートセッションのパフォーマンスが向上します。

セキュリティ情報の取得

[Security Information] ダイアログボックスには、Remote Control セッションと Remote View セッションに基づく情報が表示されます。

オプション	説明
Permission Required	リモートオペレータが、管理対象サーバでリモート管理セッションを実行しようとするたびに、管理対象サーバのユーザから許可を取得する必要があるかどうかを指定します。
Audible Signal Required	リモートオペレータが管理対象サーバにアクセスするたびに、管理対象サーバに通知音を送信するかどうかを指定します。
Beep Every	管理対象サーバに通知音を定期的に送信する時間間隔を指定します。
Visual Signal Required	リモートオペレータが管理対象サーバにアクセスするたびに、管理対象サーバにビジュアル信号を送信するかどうかを指定します。

オプション	説明
Session Encryption Enabled	リモートセッションが暗号化されるかどうかを指定します。[Session Encryption Enabled] は、Remote Control セッションおよ Remote View セッションに適用できます。
Display Name Every	管理対象サーバにビジュアル信号を定期的に送信する時間間隔を指定します。
Screen Blanking Allowed	リモートオペレータが管理対象サーバの画面を消去できるかどうかを指定します。[Screen Blanking Allowed] は Remote Control にのみ適用されます。
Locking Control Allowed	リモートオペレータが管理対象サーバのキーボードとマウスのコントロールをロックできるかどうかを指定します。[Locking Control Allowed] は Remote Control にのみ適用されます。

リモートオペレータ識別情報の表示

Remote Management Agent は、管理対象サーバ上の次のダイアログボックスに、リモートオペレータの識別情報を表示します。

- [Permission] ダイアログボックス
- [Visible signal] ダイアログボックス

表示される情報は、*console_machine_name¥console_windows_username* です。

Remote Management セッションの監査ログの表示

ZENworks Server Management では、Windows 管理対象サーバ上のログ情報を記録します。

Remote Management セッションの監査ログを表示するには

1 [Start] > [Programs] > [Administrative Tools] > [Event Viewer] の順にクリックします。

2 [Log] > [Application] の順にクリックします。

3 ソース Remote Management Agent に関連付けられているイベントをダブルクリックします。

Remote Management Agent に関係するイベントのみを表示する場合は、[Filter] ダイアログボックスの [Source] ドロップダウンリストから [Remote Management Agent] を選択します。

Remote Management のパフォーマンスの向上

強化された圧縮機能を使用することにより、特に低速リンクでの Remote Management のパフォーマンスが向上しています。

低速リンクまたは高速リンクにおける Remote Management セッション中のパフォーマンスはネットワークトラフィックの影響を受けます。応答時間を短縮するために、次の手順を 1 つまたは複数実行してみてください。

管理コンソールでの手順

- [Control Parameters] ダイアログボックスで管理対象サーバの [Hide Wallpaper] オプションを選択します。
- 管理コンソールのカラー設定を管理対象サーバよりも高いものにするか、管理コンソールと管理対象サーバのカラー設定を同じにします。
- [Control Parameters] ダイアログボックスで [16 Colors] または [256 Colors] モードを選択して Remote Management のパフォーマンスを向上させます。
- 管理コンソールの速度は、クライアントコンピュータの処理速度により決まります。Pentium* III、500MHz（以降）のシングルプロセッサクライアントを使用することをお勧めします。

管理対象サーバでの手順

- [ポインタの影を有効にする] オプションの選択を解除してから、Remote Control セッションまたは Remote View セッションを開始します。

  [ポインタの影を有効にする] の選択を解除するには

  1. Windows のデスクトップから、[スタート] > [設定] > [コントロールパネル] の順にクリックし、[マウス] をダブルクリックします。
  2. [ポインタ] をクリックします。
  3. [ポインタの影を有効にする] の選択を解除します。
  4. [適用] > [OK] の順にクリックします。
- 管理対象サーバの背景を無地にします。壁紙パターンは設定しません。
- ターゲットコンピュータでタスクマネージャが開いている場合は、閉じるか最小化することをお勧めします。
- 管理対象サーバで、スクロールテキスト（デバッグウィンドウなど）とアニメーションがアクティブになっていないことを確認します。
- 使用していないダイアログボックスが最小化されているか、閉じられていることを確認します。
- 管理対象サーバでの操作の実行には、可能であれば、メニューのオプションではなくツールバーのオプションを使用します。
- WAN での Remote Management のパフォーマンスを最大化するには、管理対象サーバで [Control Parameters] ダイアログボックスの次の設定を行います。
  - 管理対象サーバのカラーモードを 16 色に設定します。
  - [Slow Link] オプションを選択します。

Remote Management Agent のシャットダウンと再起動

次の節では、リモートセッション中の Remote Management Agent の使い方を説明します。

- 781 ページの「Remote Management Agent のシャットダウン」
- 781 ページの「Remote Management Agent の再起動」

Remote Management Agent のシャットダウン

Remote Management Agent はリモートセッション中にシャットダウンできます。Remote Management Agent をシャットダウンすると、リモートセッションが中止されます。別のリモートセッションを開始する場合は、Remote Management Agent を再起動する必要があります。詳細については、781 ページの「Remote Management Agent の再起動」を参照してください。

Windows 2000/2003 管理対象サーバ上で Remote Management Agent をシャットダウンするには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell ZFS Remote Management Agent］>［停止］の順にクリックします。

重要： Windows 2000/2003 サーバ上で Remote Management Agent を停止できるのは、この Windows サービスを停止する権利がある場合のみです。

Remote Management Agent の再起動

Remote Management Agent は、ZENworks Server Management のインストール中に、管理対象サーバにインストールされ、管理対象サーバの起動時に自動的に起動されます。リモートセッション中に Remote Management Agent をシャットダウンすると、リモートセッションが停止します。別のリモートセッションを開始する場合は、管理対象サーバ上で Remote Management Agent を再起動する必要があります。

Windows 2000/2003 管理対象サーバ上で Remote Management Agent を再起動するには

1 コントロールパネルで［管理ツール］をダブルクリックします。

2 ［サービス］をダブルクリックします。

3 ［Novell ZFS Remote Management Agent］>［Start］の順にクリックします。

重要： Windows 2000/2003 サーバ上で Remote Management Agent を起動できるのは、この Windows サービスを起動する権利がある場合のみです。

M ドキュメントの更新

この節では、Novell® ZENworks® 6.5 Server Management の初回リリース後に、『*管理ガイド*』の Policy and Distribution Services に関する項で変更された内容について説明します。お使いのドキュメントを最新の状態に更新するために、この情報を役立ててください。

この節で列挙する変更はすべてドキュメントにも反映されているものです。マニュアルは、Web 上で HTML と PDF の 2 つの形式で提供されています。HTML および PDF ドキュメントは、ここに示すドキュメントの変更に基づいて最新の状態になっています。

ドキュメントの更新が発行された日付ごとに、更新情報をグループ化しています。日付の付いた節の中では、Policy and Distribution Services の目次に記載されている節名に基づいて、アルファベット順に変更を示しています。

使用している PDF ドキュメントのコピーが最新の内容であるかどうかを確認するには、PDF ドキュメントのタイトルページ、またはタイトルページのすぐ後ろの法的通知の欄で、発行された日付を参照してください。

ドキュメントは次に示す日付で更新されました。

- 783 ページの「2005 年 2 月 11 日」
- 784 ページの「2004 年 9 月 2 日」

2005 年 2 月 11 日

次の節が更新されました。変更内容は次のとおりです。

- 435 ページの「Desktop Application Distribution」

Windows サーバのリモート管理

各節に次の変更が加えられました。

場所	変更
767 ページの「Windows XP SP2 での動作」	この新しい節が追加されました。
766 ページの「Remote Management Agent からの Remote Management セッションの開始」	手順 1 に次の注意を追加しました。 **注：** Remote Management Agent からターミナルサーバ上で実行されている管理コンソールへのセッション要求が開始されたときに、ConsoleOne の最初のインスタンスが要求を受信します。ConsoleOne が最初に起動されたセッションの ConsoleOne インスタンスがすべて終了するまで、ConsoleOne インスタンスではセッションの要求が受信されません。セッションの要求を受信するには、任意のターミナルセッションで ConsoleOne を再び起動する必要があります。

2004 年 9 月 2 日

ガイド全体を通して、グラフィックのフォントを変更し、新しいアイコンを使用しました。グラフィックの内容には、目立った変更はありません。

IV [Management and Monitoring Services]

Novell® ZENworks® 6.5 Server Management には、マルチプロトコル LAN/WAN ネットワークとサーバのサポートなど、異種ネットワーク環境で使用可能な業界標準ベースのモニタリングサービス、管理サービス、およびレポート作成サービスが用意されています。

Management and Monitoring Services コンポーネントを使用すると、ネットワークの問題にすばやく対応し、システム全体の可用性を強化できるため、Novell NetWare®、Windows*、および Linux サーバを積極的に管理できます。

Management and Monitoring Services は次のコンポーネントで構成されています。

- **Novell ConsoleOne®** ネットワークを管理するためのインタフェースを提供します。
- **Management Site Services** 次の機能を使用できます。
  - アラーム管理
  - データベース管理
  - MIB ツール管理
  - Monitoring Services
  - ネットワーク検出
  - レポート機能
  - Role-Based Services
  - トポロジマッピング
- **Server Management** ネットワーク上のすべてのサーバを監視します。
- **Traffic Analysis** イーサネット、トークンリング、または FDDI (Fiber Distributed Data Interface) のネットワークセグメント上のすべてのトラフィックを監視します。
- **Advanced Trending Agent** 監視に使用されます。

Management and Monitoring Services のガイドは、次の章で構成されています。

- 21 章 787 ページの「Management and Monitoring Services の設定」
- 22 章 817 ページの「Novell ConsoleOne での Management and Monitoring Services の使用」
- 23 章 829 ページの「ネットワーク検出とアトラス管理の理解」
- 24 章 883 ページの「アラーム管理の理解」
- 25 章 907 ページの「サーバ管理の理解」
- 26 章 951 ページの「MIB ツールの使用」

- 27 章 975 ページの「Monitoring Services」
- 28 章 981 ページの「トラフィック分析の理解」
- 29 章 1073 ページの「エージェントの環境設定のカスタマイズ」
- 30 章 1091 ページの「Novell ZENworks Server Management でサポートされるプロトコルデコードスイート」
- 31 章 1101 ページの「Novell ZENworks Management and Monitoring Services データベース」
- 32 章 1105 ページの「Management and Monitoring Services でのレポートの使用」
- 33 章 1119 ページの「SNMP コミュニティ文字列の使用」
- 34 章 1125 ページの「View Builder の理解」
- 1135 ページの付録 N、「ドキュメントの更新」

21 Management and Monitoring Services の設定

Management and Monitoring Services を効果的に使用するには、ネットワークにコンポーネントを正しくインストールして設定する必要があります。最初に、Novell® ZENworks® 6.5 Server Management の基本インストールを実行してください（『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」を参照してください）。

次の節では、Management and Monitoring Services を設定し、その機能を使用してネットワークを管理するのに役立つ概念と手順について説明します。

- 787 ページの「Management and Monitoring Services の理解」
- 792 ページの「設定の計画」
- 795 ページの「役割ベース管理」
- 811 ページの「Management and Monitoring Services の設定」

Management and Monitoring Services の理解

この節では、次の Management and Monitoring Services コンポーネントについて説明します。

- 787 ページの「Management Site Services」
- 791 ページの「Server Management」
- 791 ページの「Traffic Analysis」
- 792 ページの「Novell ConsoleOne」

Management Site Services

Management Site Services では、次の機能を使用できます。

- 788 ページの「ネットワーク検出」
- 788 ページの「データベース管理」
- 788 ページの「アラーム管理」
- 789 ページの「Role-Based Services」
- 789 ページの「レポート機能」
- 790 ページの「トポロジマッピング」
- 790 ページの「MIB (Management Information Base) ツール管理」
- 791 ページの「Monitoring Services」

ネットワーク検出

ネットワーク自動検出が開始されると、SNMP (Simple Network Management Protocol) 対応のサーバ、ルータ、スイッチと、これらのデバイスおよびワークステーションでホストされるサービスが自動的に検出されます。検出されたデータは .dat ファイルに保存され、Novell ConsoleOne® のアトラスマップに表示されます。

マップには、管理サーバで設定された検出スコープが反映されます。デフォルトでは、管理サーバが通信を確立できるすべてのデバイスが検出され、これらのデバイスは管理サーバに保存されます。NetExplorer™ のスコープを定義すると、検出されるオブジェクトの数を制限できます。

ネットワーク検出の詳細については、23 章 829 ページの「ネットワーク検出とアトラス管理の理解」を参照してください。

データベース管理

Novell ZENworks Server Management では、管理サーバ上で CIM (Common Information Model) 準拠の Sybase* データベースを一元管理できます。このデータベースは、サーバやネットワークのデータのリポジトリとして機能します。このデータをさまざまな方法で表示または整理して、ネットワーク管理に必要な情報を得ることができます。Server Management データは、次の 3 つの論理データベースで構成されるトポロジデータベースに保存されます。

- トポロジ
- アラーム
- マップ情報

多くのデータベース機能は自動的に実行されるため、管理する必要はほとんどありません。Server Management データベースの詳細については、31 章 1101 ページの「Novell ZENworks Management and Monitoring Services データベース」を参照してください。

アラーム管理

Server Management によって認識されるアラームには、SNMP トラップ、接続テスト、およびしきい値のプロファイリングがあります。アラーム管理では、トラップと独自のアラームが処理され、そのアラームに割り当てられている Novell ConsoleOne にアラームが転送されます。

アラーム処理でアクションを指定することにより、アラームの発生時に特定のアクションを実行できます。プログラムの実行、電子メールによる通知メッセージの送信、およびアーカイブ、コンソールのビープ音、チッカーテープメッセージの作成など、いくつかのアクションは自動的に実行されます。アクションは、処理された特定のアラームを他の Server Management サーバに転送するように設定できるほか、未処理の SNMP トラップをサードパーティによる管理アプリケーションのターゲットアドレスに直接転送するようにも設定できます。

Role-Based Services

Management and Monitoring Services では、Novell eDirectory™ による役割ベース管理とタスク管理がサポートされています。Novell ZENworks Server Management は、Role-based Services を使用して、Management and Monitoring Services タスクを役割別に分類し、役割にスコープ情報を割り当てます。

Role-based Services の役割は、ユーザが実行できるタスクを指定します。Role-based Services の役割を定義するには、Role-based Services の役割オブジェクトを作成し、その役割が実行できるタスクを指定します。

Role-based Services の役割オブジェクトの作成と、Role-based Services の役割が実行可能なタスクの指定に関する一般情報については、809 ページの「役割ベース管理の設定」を参照してください。

Novell ZENworks Server Management に役割ベースサービスを実装する方法については、795 ページの「役割ベース管理」を参照してください。

レポート機能

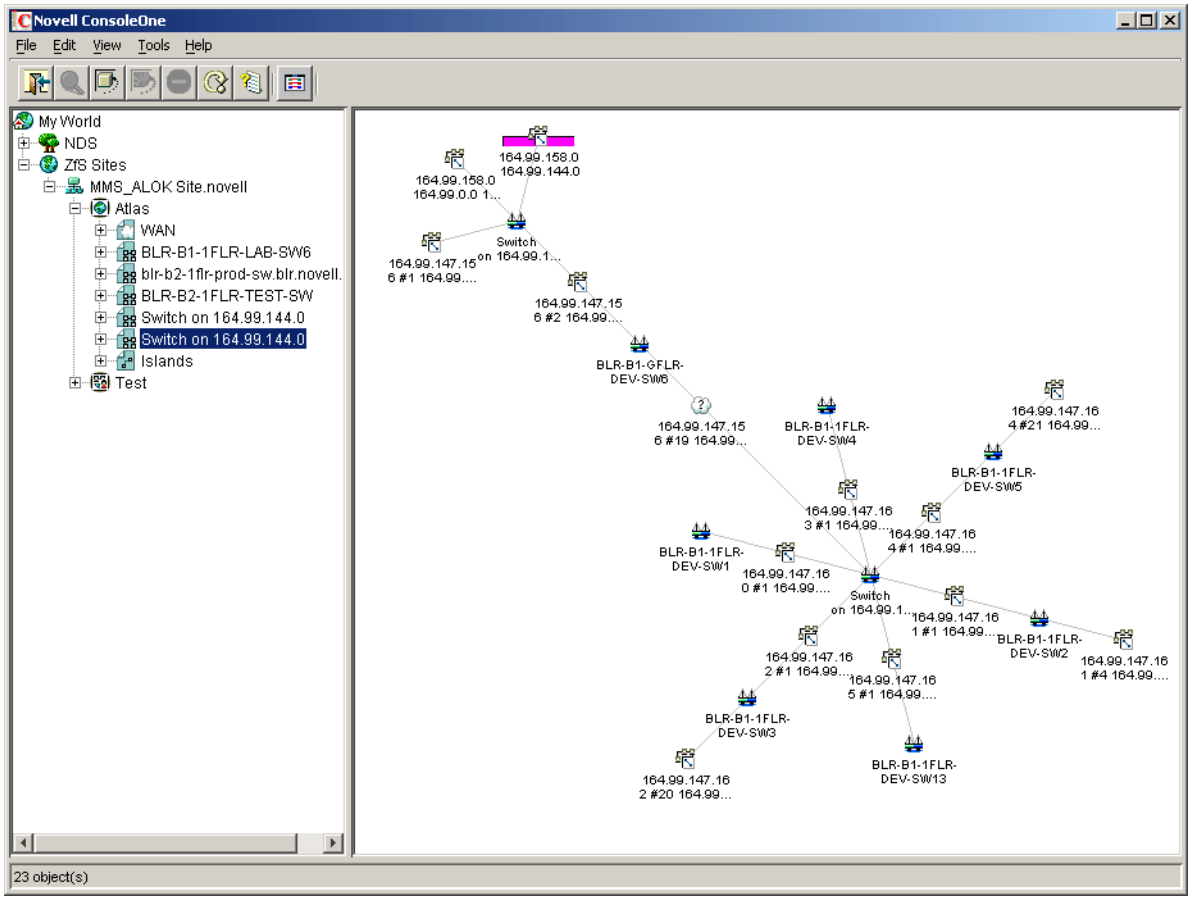
Novell ZENworks Server Management では、統計情報を生成するレポート作成サービスを使用できます。これらのレポートは、Novell ConsoleOne に表示したり、データベースおよび Web 形式にエクスポートしたりすることができます。Server Management では、次の種類のレポートを作成できます。

- ヘルスレポート
- トポロジレポート
- アラームレポート

Management and Monitoring Services のレポートの詳細については、1105 ページの「Management and Monitoring Services でのレポートの使用」を参照してください。

トポロジマッピング

トポロジマッピングによって、次の図に示すように、Novell ZENworks Server Management の階層アトラスにマップを表示できます。マップには、管理サーバで設定された検出スコープが反映されます。



トポロジマッピングの詳細については、874 ページの「アトラスの管理」を参照してください。

MIB (Management Information Base) ツール管理

Novell ZENworks Server Management の MIB Compiler と MIB Browser を使用して、SNMP デバイスを管理できます。

MIB ツールには次の機能が用意されています。

- SNMP トラップ受信用アラームテンプレートの設定
- SNMP デバイスでの値の表示と設定
- アラームテンプレートデータベースでのトラップ定義の更新
- サードパーティの MIB の注釈付け

MIB ツールの詳細については、26 章 951 ページの「MIB ツールの使用」を参照してください。

Monitoring Services

Monitoring Services（SNMP サービス）を使用すると、ネットワークデバイスでサービスの接続性と可用性をテストできます。サービスのステータスが変更されると、Novell ConsoleOne に通知されます。監視できるサービスは、DHCP、DNS、エコー、FTP、HTTP、HTTPS、IP、IPX™、NFS、NNTP、SMTP、SNMP、タイムサービス、TFTP、および WUser です。

Monitoring Services の詳細については、27 章 975 ページの「Monitoring Services」を参照してください。

Server Management

Server Management コンポーネントを使用すると、ネットワーク上のすべてのサーバを監視できます。このコンポーネントは、Novell ConsoleOne を使用して監視するサーバごとにインストールする必要があります。Novell ZENworks Server Management のインストール時に、Server Management コンポーネントをインストールするサーバを選択できます。

管理ニーズに合わせて、サーバ監視ソフトウェアコンポーネントの一部、またはすべてを配備できます。Server Management の詳細については、907 ページの「サーバ管理の理解」を参照してください。

Traffic Analysis

トラフィック管理のコンポーネントでは、NetWare® または Windows* サーバ版の Traffic Analysis サービスを使用して、イーサネット、FDDI（Fiber Distributed Data Interface）、またはトークンリングのネットワークセグメント上のすべてのトラフィックを監視できます。

次の Traffic Analysis サービスを利用できます。

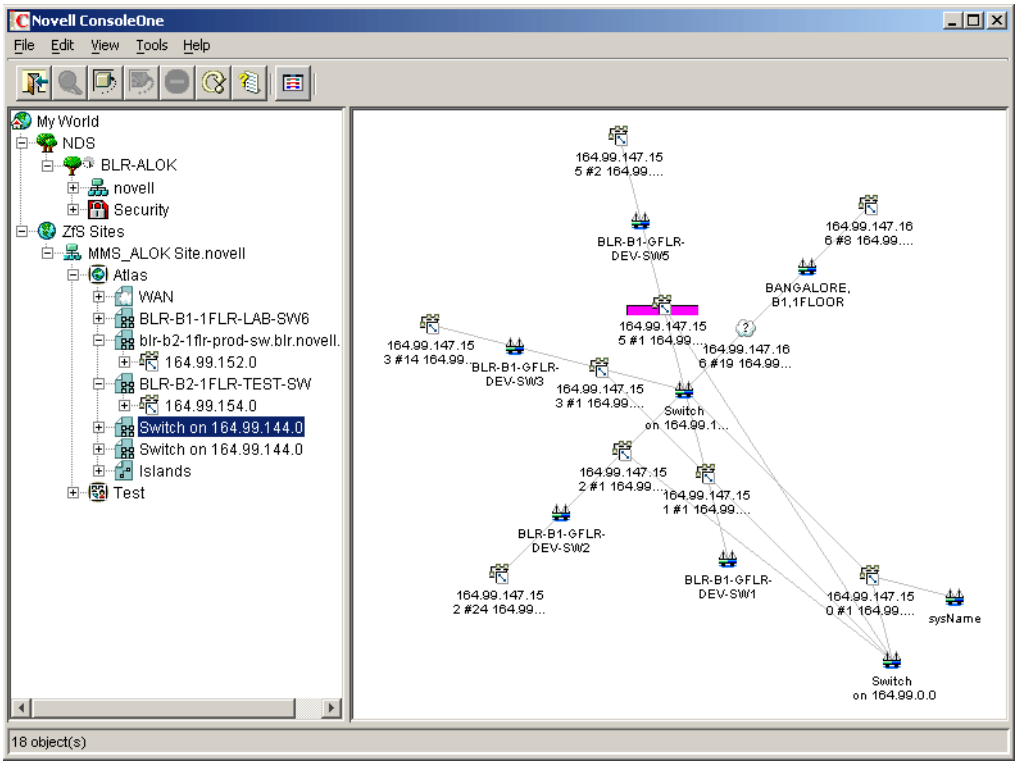
- 標準および企業向けのリモートネットワーク監視用 RFC 1757 MIB 定義
- RMON（Remote Monitor）エージェント設定など、Novell eDirectory に追加された拡張機能
- ネットワークトラフィックのトレンドおよび分析ツール
- ネットワークヘルスレポートテンプレート
- トポロジマップとの統合
- パフォーマンスしきい値の設定とプロファイリング
- ネットワークセグメント上の通信と使用率の表示
- パケットキャプチャツールと表示

管理ニーズに合わせて、トラフィック分析ソフトウェアコンポーネントの一部またはすべてを展開できます。ネットワークトラフィックの分析の詳細については、28 章 981 ページの「トラフィック分析の理解」を参照してください。

Novell ConsoleOne

Novell ConsoleOne には、ネットワークを管理するためのインタフェースが用意されています。Novell ConsoleOne は、ネットワーク管理スナップインを統合するプログラム（スナップイン）をホストしているため、単一のインタフェースを使用してネットワークを管理できます。

ZENworks 6.5 Server Management は、次の図に示すように、Novell ZENworks Server Management ネームスペースの下に、Novell ConsoleOne への GUI（グラフィカルユーザインタフェース）スナップインを提供します。これにより、Novell ZENworks Server Management に固有の機能にアクセスできます。



Novell ConsoleOne の詳細については、Novell ConsoleOne Web サイト（http://www.novell.com/products/netconsole/consoleone）を参照してください。

設定の計画

この節では、ネットワーク上の Management Site Services、および Novell ZENworks Server Management エージェントの一部（アラーム、サーバ、およびトラフィック）を設定する一般的な計画オプションについて説明します。役割ベース管理の計画と実装方法についても説明します。

Management and Monitoring Services ソフトウェアをインストールする前に、ネットワークを有効に管理するために必要な情報を決定する必要があります。この節では、ネットワーク管理に必要な情報の種類を決定するのに役立つ次のトピックについて説明します。

この節では、Management and Monitoring Services の設定方法についても説明します。

- 793 ページの「必要な管理情報の定義」
- 793 ページの「ネットワーク管理戦略の計画」
- 794 ページの「ネットワークの設定」

このガイドの次の節では、Server Management とセグメント監視の計画についても説明します。

- 910 ページの「サーバ管理の計画」
- 995 ページの「セグメント監視の計画」

必要な管理情報の定義

Novell ZENworks Server Management は、さまざまなネットワーク設定が必要なビジネスに対応できる柔軟性を備えています。組織内のグループで必要になる情報を理解し、そのニーズに合わせてソフトウェアを適切に配備する必要があります。

一般に、社内のグループは、最前線のヘルプデスク担当者、後方の情報システム管理者、および管理レベルの調整者で構成され、グループごとに計画、予算管理、トラブルシューティング、またはその他の問題に関する特定の情報が必要になります。

たとえば、あるグループが重要なサーバセットを 24 時間監視する必要があるとします。この場合は、サーバをリアルタイムで監視し、サーバに重大なエラーが発生した際に通知が送信されるようにします。定義したサーバのグループについて、サーバトレンドのレポートを毎週生成することが必要な場合もあります。

ネットワーク管理戦略の計画

Novell ZENworks Server Management でネットワーク上のデバイスを監視および管理するには、ネットワーク上のネットワークセグメントとデバイスを頻繁にポーリングする必要があります。Novell ZENworks Server Management では、ネットワークオブジェクトのポーリングが標準プロトコル (SNMP、TCP/IP、および IPX) によって実行されます。

Novell ZENworks Server Management コンポーネントは、SNMP エージェントおよび RMON (Remote Monitor) エージェントをホストするサーバ上にトレンド分析情報を保存することで、ネットワーク性能に与える影響を最小限に抑えられるよう設計されています。ポーリングは、接続された Novell ConsoleOne からの要求に基づき、管理サーバによって直接実行されます。

Novell ZENworks Server Management のシステム管理者は、ポーリング頻度を設定して、ネットワーク環境に適切な監視レベルを提供する必要があります。最適な監視レベルを設定するには、まず、重要な操作を担当するシステムを特定します。次に、システムとセグメントを 3 つの基本管理カテゴリに分類します。

- **非常に重要：**頻繁に監視する必要のあるセグメントとデバイス。ポーリング頻度を高く設定して監視する必要があります。
- **重要：** 頻繁な監視を必要としないセグメントとデバイス。ポーリングのオーバーヘッドとパフォーマンスの間で均衡を保つ必要のあるサービスをシステムがホストする場合は、このカテゴリに分類されます。ポーリング頻度は、数分ごと、数時間ごと、または数日ごとに設定する必要があります。

- **重要でない：** 監視をほとんど必要としないセグメントとデバイス。要求に応じてポーリングを実行し、セグメントとデバイスを監視するか、またはポーリング頻度を低く設定します。

デバイスをポーリングしない場合、またはポーリング頻度が低い場合は、管理サーバにアラーム（トラップ）を送信するようにデバイスを設定して、システムで発生したエラーが通知されるようにできます。

ネットワークの設定

Management and Monitoring Services コンポーネントでは、ネットワーク上のデバイスとの通信に、標準ネットワークプロトコルが使用されます。ネットワークとそのデバイスを検出し、正確に監視するには、通信チャネルに矛盾がなく、適切に設定されていることを確認する必要があります。

次の節では、ネットワーク設定の重要な一面について説明します。

- 794 ページの「IP アドレス戦略」
- 794 ページの「IPX 転送ソフトウェア」
- 794 ページの「Novell eDirectory と DNS ネームレゾリューション」
- 795 ページの「SNMP 設定」

IP アドレス戦略

IP で通信するデバイスを検出する場合は、デバイスを管理できるように、有効な IP アドレスが設定されていることを確認してください。TCP/IP は指定の Novell ConsoleOne ワークステーションにバインドし、IP は管理サーバにバインドする必要があります。Novell ConsoleOne ワークステーションでは DHCP (Dynamic Host Configuration Protocol) アドレス指定を使用できますが、スタティックアドレスは管理サーバに割り当てる必要があります。

IPX 転送ソフトウェア

IPX で通信するすべてのデバイスを検出し管理するには、IPX/SPX 準拠の転送ネットワークソフトウェアスタックでデバイスを設定する必要があります。NetWare ドライバと Windows ドライバは、オペレーティングシステムのインストールソフトウェアに含まれています。ZENworks Server Management は、Novell IP 互換モードドライバと互換性があります。

Novell eDirectory と DNS ネームレゾリューション

ネットワークの検出を開始する前に、NetWare および Windows サーバと、ネットワークデバイス名が適切であることを確認してください。ネームレゾリューションは、ローカルホストファイル、Novell eDirectory 名、またはバインダリテーブルの形式をとります。IP または IPX アドレスの代わりに、サーバ名またはホスト名がマップと設定ビューに表示されます。

SNMP 設定

NetWare および Windows サーバとその他の SNMP 対応ネットワークデバイスの SNMP エージェントと RMON エージェントには、デバイス上で識別されるコミュニティ文字列が必要です。SNMP 対応デバイスごとに、コミュニティ文字列とトラップターゲットを設定する必要があります (Novell ZENworks Server Management サーバを含む)。

コミュニティ文字列は、マネージャとエージェント間の安全な通信を確立するために使用されます。Novell ZENworks Server Management システムがエージェントと通信するためには、マネージャとエージェントのコミュニティ文字列が等しく、同じポートを使用している必要があります。情報があらゆるユーザからアクセスされることを防ぐには、コミュニティ文字列を変更する必要があります。

コミュニティ文字列 GET および SET を PUBLIC から変更した場合は、ネットワーク上の名前と一致するように、Novell ConsoleOne と管理サーバの設定を変更する必要があります ([load NXPCON] > [SNMP] > [Add/Edit Community Name] の順にクリックします)。Management Services のインストール後にコミュニティ文字列を変更する方法の詳細については、867 ページの「SNMP コミュニティ文字列の変更」を参照してください。

NetWare および Windows サーバのエージェントの設定については、28 章 981 ページの「トラフィック分析の理解」を参照してください。

役割ベース管理

Novell ConsoleOne では、Novell ネットワーク管理ユーティリティを実行する、ディレクトリ対応のフレームワークを使用できます。Novell ConsoleOne への Novell ZENworks Server Management スナップインでは、Novell eDirectory を十分に活用して、役割ベース管理と高水準のセキュリティを実現できます。Novell eDirectory により、ユーザは一度ログインすると、特定スコープ内で役割によって指定された管理コンポーネントにアクセスできます。

Novell ConsoleOne への Server Management スナップインを使用すると、管理者間でネットワーク管理タスクを分割できます。Novell ConsoleOne では、Server Management の機能とタスクが、組織の各管理者の役割に基づいてカスタマイズされたさまざまなビューにまとめられます。

次の節では、役割ベース管理について説明します。

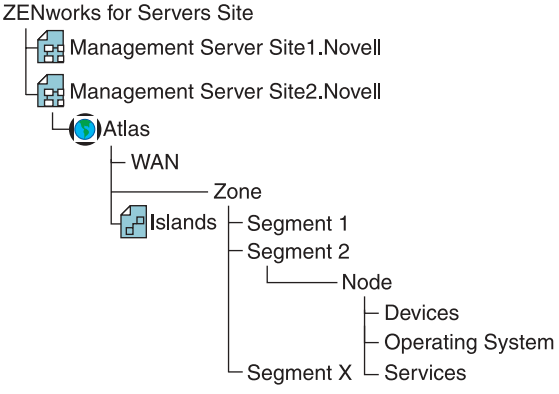
- 796 ページの「Novell ZENworks の管理サイト」
- 797 ページの「Novell ZENworks Server Management の一般的な役割」
- 798 ページの「Novell ZENworks Server Management の役割ベースモジュールと役割」
- 809 ページの「役割ベース管理の設定」

Novell ZENworks の管理サイト

Novell ZENworks の管理サイトは、役割ベースサービスによって管理サーバ上のオブジェクトデータにアクセスする際の境界を設定します。役割とタスクを作成し、ネットワークのコンテナスペースからネットワークオブジェクトと情報にアクセスする際のレベルを定義できます。

Management and Monitoring Services をインストールすると、管理サイト、システム管理者の役割 (Role-based Services Admin)、およびすべてのサイトオブジェクトが Novell eDirectory に作成されます。管理サイトは、ネットワークで検出されるオブジェクト (ネットワーク、セグメント、ルータ、ブリッジ、スイッチ、サーバ、ワークステーションなど) のスコープを定義します。ネットワークのサイズ、またはネットワーク管理要件に応じて、1 つまたは複数のサイトを作成できます。管理サイトには、単一のローカルネットワークが含まれる場合や、ネットワーク全体が含まれる場合があります。サイトの境界は、ネットワーク検出のスコープによって定義されます。ネットワーク検出は、デフォルトでは、接続されたネットワークとネットワークノードをすべて検出するように設定されています。サイトオブジェクトは、サーバオブジェクトと同じコンテキストに作成されます。

インストール時に作成されるデフォルトの管理サイトを次に示します。1 つの管理役割には、管理システムのすべての設定タスクと管理タスクに対する権限と許可が付与されています。



ネットワークトラフィックを監視し、アラームを処理し、サーバシステムを管理する役割がデフォルトで用意されており、これらの役割にユーザを追加できます。役割を新規作成する場合のサンプルとして、これらの役割を使用することもできます。

Server Management の役割ベースサービス (Role-based Services) では、ネットワークオブジェクト、設定、および情報へのアクセスに必要な許可が役割に関連付けられます。Novell eDirectory ユーザオブジェクトは、適切な役割に割り当てられることができます。役割の抽象レベルを次に示します。

- 役割 - 組織内でさまざまなネットワーク管理機能を実行するために作成します。適切な役割を作成することで、許可の付与を簡素化し、管理ツールとデータへのアクセス権を制限できます。
- タスク - 特定の責任に基づいて管理システムのコンポーネントを利用するために実行されるアクションです。
- コンポーネント / モジュール - ネットワーク管理機能を提供するソフトウェアツールです。Server Management のコンポーネントを使用すると、サーバを管理し、セグメントトラフィックを監視し、共通サービス (データベース管理、アラーム処理、およびレポート生成) を提供することができます。

役割に追加されたユーザは、Novell eDirectory ユーザアカウントによって付与されたアクセス権、許可、およびポリシーを保持しています。たとえば、ユーザが Novell eDirectory によってサーバにアクセスし、設定することは許可されていても、Server Management の Role-based Services によってサーバを管理することは許可されていない場合があります。つまり、このユーザが割り当てられている管理役割では、Novell ZENworks Server Management システムの管理サービスまたはコンポーネント / モジュールへのアクセスが制限されています。

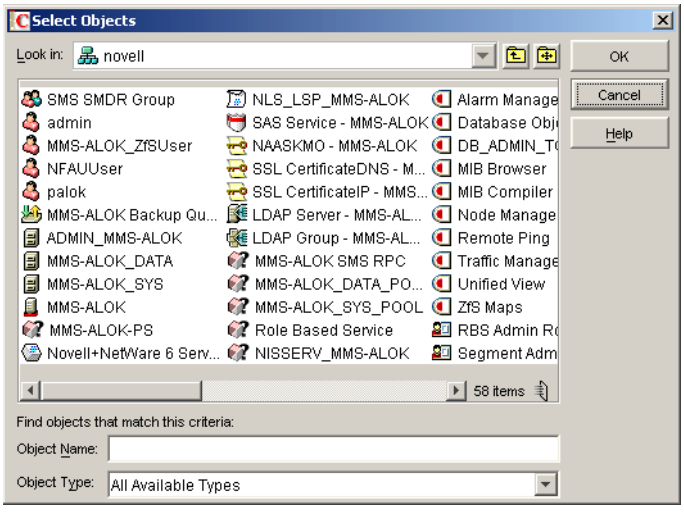
Novell ZENworks Server Management の一般的な役割

Novell ZENworks Server Management のコンポーネントは、Novell eDirectory による役割ベースサービス (Role-based Services) とタスク管理をサポートしています。Server Management は、Role-based Services を使用して、Novell ZENworks Server Management タスクを役割別に分類し、役割、ユーザ、またはグループにスコープ情報を割り当てます。

Role-based Services の役割は、ユーザが実行できるタスクを指定します。Role-based Services の役割を定義するには、Role-based Services の役割オブジェクトを作成し、その役割が実行できるタスクを指定します。

Role-based Services の役割が実行可能なタスクは、Role-based Services のタスクオブジェクトとして Novell eDirectory ツリーに表示されます。これらのオブジェクトは 1 つまたは複数の Role-based Services モジュールにまとめられます。モジュールは、各 Server Management コンポーネントに相当するコンテナです。Novell ZENworks Server Management には、次の図に示すように、定義済みのモジュールと Role-based Services 役割オブジェクトが用意されています。

重要： 新しいモジュールやタスクの作成はできません。用意されている定義済みのモジュールとタスクから選択する必要があります。



モジュールとタスクを使用してあらゆる役割を作成できます。各モジュールには 1 つまたは複数のタスクを指定できます。たとえば、Role-based Services は、Monitoring Services のタスクを［Enable Remote Ping］として定義しています。このタスクを役割に割り当てると、その役割のユーザは Monitoring Services 機能を使用できます。Novell ZEworks Server Management の定義済みのモジュールと役割、および関連付けられたタスクのリストについては、798 ページの「Novell ZENworks Server Management の役割ベースモジュールと役割」を参照してください。

タスクとモジュールを使用した役割オブジェクトの作成に関する詳細については、809 ページの「役割ベース管理の設定」を参照してください。

Novell ZENworks Server Management の役割ベースモジュールと役割

この節では、次の表が示されます。

- Novell ZENworks Server Management の役割ベースモジュールと関連付けられたタスク
- Novell ZENworks Server Management の Role-based Services の定義済み役割と関連付けられたタスク

  次の表は、Novell ZENworks Server Management の Role-based Services の各モジュールと、そのモジュールで実行可能なタスクを示しています。

Novell ZENworks Server Management の Role-based Services のモジュール	関連付けられたタスク
Alarm Manager	◆ Add Alarm Note ◆ Assign Alarm ◆ Define Alarm Disposition ◆ Delete Alarm ◆ View Active Alarms ◆ View Active Alarm History ◆ View Alarm Summary
Database Object Editor	Database Object Editor
DB_Admin_Tool	◆ DB_BACKUP ◆ Database Password Change
MIB Browser	Enable MIB Browser
MIB Compiler	Enable MIB Compiler

Novell ZENworks Server Management の Role-based Services のモジュール	関連付けられたタスク
Node Management	◆ Clearing a Connection ◆ Create Health Profiles ◆ Create Health Reports ◆ Delete Health Profiles ◆ Delete Health Reports ◆ Downing a Server ◆ Loading an NLM ◆ Mounting and Dismounting a Volume ◆ Read Only All ◆ Read Only All Tabular View ◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Only Homepage ◆ Read Only HostFileSystemView ◆ Read Only InstalledSoftwareView ◆ Read Only Novell NetWareLoadableModuleView ◆ Read Only Novell NetWareUserView ◆ Read Only NetworkPerformanceView ◆ Read Only NTDiskListview ◆ Read Only NTMemoryUsageView ◆ Read Only NTNetworkView ◆ Read Only NTPartitionView ◆ Read Only NTApadpterView ◆ Read Only NTConnectionListView ◆ Read Only NWDiskListView ◆ Read Only NWMemoryUsageView ◆ Read Only NWNetworkMediaView ◆ Read Only NWProtocolView ◆ Read Only NWFileListView

Novell ZENworks Server Management の Role-based Services のモジュール	関連付けられたタスク
	◆ Read Only NWPartitionView ◆ Read Only NWQueueJobsListView ◆ Read Only NWQueueListView ◆ Read Only NWVolumeListView ◆ Read Only NWVolumeSegmentView ◆ Read Only NWVolumeUsageView ◆ Read Only NWRunningSoftwareView ◆ Read Only Set Parameter ◆ Read Only Trend ◆ Read Write All ◆ Read Write All TabularView ◆ Read Write Health Profiles ◆ Read Write Health Reports ◆ Read Write Set Parameter ◆ Read Write Trend ◆ Remote Controlling ◆ Restarting a Server ◆ Unloading an NLM
Remote Ping（リモート Ping）	Enable Remote Ping
Traffic Management	◆ Adding_Nodes_For_InactivityMonitoring ◆ Adding_Protocols_For_ProtocalDirectory ◆ Capture_Packets ◆ Deleting_Nodes_For_Inactivity ◆ Deleting_Protocols_For_ProtocolDirectory ◆ Freeing Agent Resources ◆ Setting_Segment_Alarms ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary

Novell ZENworks Server Management の Role-based Services のモジュール	関連付けられたタスク
	◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
Unified View（統合ビュー）	◆ Unified View for Devices ◆ Unified View for Segments
Novell ZENworks Server Management Maps	◆ Import ◆ Layout ◆ Print ◆ Rebuild ◆ Rename ◆ Save

次の表は、Novell ZENworks Server Management の定義済みの Role-based Services と、各役割で実行可能な特定のタスクを示しています。

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Role-based Services_Administrator	すべてのモジュール	すべてのタスク

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Segment_ Administrator	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Assign Alarms ◆ Add Alarm Note
	DM_Admin_Tool	なし
	MIB Browser	なし
	MIB Compiler	Enable MIB Compiler
	Node Management	◆ Read Only Health Profiles ◆ Read Only Health Reports
	Remote Ping（リモート Ping）	Enable Remote Ping
	Traffic Management	◆ Adding_Nodes_For_InactivityMonitoring ◆ Adding_Protocols_For_ProtocolDirectory ◆ Capture_Packets ◆ Setting_Segment_Alarms ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary ◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
	Novell ZENworks Server Management Maps	◆ Layout ◆ Print
	Unified Views	Unified Views for Segments

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Segment Manager	Alarm Manager	◆ Assign Alarms ◆ Define Alarms Disposition ◆ Delete Alarms ◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Add Alarm Note
	DM_Admin_Tool	なし
	Database Object Editor	Database Object Editor
	MIB Browser	Enable MIB Browser
	MIB Compiler	Enable MIB Compiler
	Node Management	◆ Create Health Profiles ◆ Create Health Reports ◆ Delete Health Profiles ◆ Delete Health Reports ◆ Read Write Health Profiles ◆ Read Only Health Profiles ◆ Read Write Health Reports ◆ Read Only Health Reports
	Remote Ping (リモート Ping)	Enable Remote Ping

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Segment Manager *（続き）*	Traffic Management	◆ Adding_Nodes_For_InactivityMonitoring ◆ Adding_Protocols_For_ProtocalDirectory ◆ Capture_Packets ◆ Deleting_Nodes_For_InactivityMonitoring ◆ Deleting_Protocols_For_ProtocolDirectory ◆ Freeing Agent Resources ◆ Setting_Segment_Alarms ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary ◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
	Novell ZENworks Server Management Maps	◆ Import ◆ Layout ◆ Print ◆ Rebuild ◆ Rename ◆ Save

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Segment Monitor	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History
	DM_Admin_Tool	なし
	MIB Compiler	なし
	MIB Browser	なし
	Node Management	◆ Read Only Health Profiles ◆ Read Only Health Reports
	Remote Ping（リモート Ping）	Enable Remote Ping
	Traffic Management	◆ Capture_Packets ◆ View_Conversations ◆ View_LANZ_Agents ◆ View_Protocol_Directory ◆ View_RMON_Summary ◆ View_Segment_Alarms ◆ View_Segment_Dashboard ◆ View_Segment_Monitor_Nodes_For_Inactivity ◆ View_Segment_Protocal_Distribution ◆ View_Segment_Stations ◆ View_Segment_Summary ◆ View_Segment_Trends ◆ View_Switch_Port_Traffic ◆ View_Switch_Summary
	Novell ZENworks Server Management Maps	◆ Layout ◆ Print
	Unified Views	Unified View for Segments

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Server Administrator	Alarm Manager	◆ Assign Alarm ◆ Define Alarm Disposition ◆ Delete Alarm ◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Add Alarm Note
	DM_Admin_Tool	なし
	MIB Browser	Enable MIB Browser
	MIB Compiler	なし
	Node Management	◆ Clearing a Connection ◆ Loading an NLM ◆ Mounting and Dismounting a Server Volume ◆ Downing a Server ◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Write All ◆ Restarting a Server ◆ Unloading an NLM
	Remote Ping（リモート Ping）	Enable Remote Ping
	Traffic Management	なし
	Novell ZENworks Server Management Maps	◆ Layout ◆ Print
	Unified Views	Unified Views for Devices

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Server Manager	Alarm Manager	◆ Assign Alarm ◆ Define Alarm Disposition ◆ Delete Alarm ◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History ◆ Add Alarm Note
	DM_Admin_Tool	なし
	MIB Browser	なし
	MIB Compiler	なし
	Node Management	◆ Clearing a Connection ◆ Create Health Profiles ◆ Create Health Reports ◆ Delete Health Profiles ◆ Delete Health Reports ◆ Downing a Server ◆ Loading an NLM ◆ Mounting and Dismounting a Server Volume ◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Write All ◆ Read Write Health Profiles ◆ Read Write Health Reports ◆ Restarting a Server ◆ Unloading an NLM
	Remote Ping（リモート Ping)	なし
	Traffic Management	なし
	Novell ZENworks Server Management Maps	◆ Import ◆ Layout ◆ Print ◆ Rebuild ◆ Rename ◆ Save

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Server Manager *（続き）*	Database Object Editor	Database Object Editor
	Unified Views	Unified View for Devices
Server Monitor	Alarm Manager	◆ View Alarm Summary ◆ View Active Alarms ◆ View Alarm History
	DM_Admin_Tool	なし
	MIB Browser	なし
	MIB Compiler	なし
	Node Management	◆ Read Only Health Profiles ◆ Read Only Health Reports ◆ Read Only Homepage ◆ Read Only HostFileSystemView ◆ Read Only InstalledSoftwareView ◆ Read Only Novell NetWareLoadableModulesView ◆ Read Only Novell NetWareUserView ◆ Read Only NetworkPerformanceView ◆ Read Only NTDiskListview ◆ Read Only NTMemoryUsageView ◆ Read Only NTNetworkView ◆ Read Only NWConnectionListView ◆ Read Only NWOpenListView ◆ Read Only NWDiskListView ◆ Read Only NWMemoryUsageView ◆ Read Only NWNetworkMediaView ◆ Read Only NWFileListView ◆ Read Only NWVolumeListView ◆ Read Only NWVolumeUsageView ◆ Read Only RunningSoftwareView ◆ Read Only Trend
	Remote Ping（リモート Ping）	Enable Remote Ping
	Traffic Management	なし
	Novell ZENworks Server Management Maps	◆ Layout ◆ Print

Management and Monitoring Services の Role-based Services の定義済み役割	Management and Monitoring Services の Role-based Services のモジュール	割り当てられたデフォルトタスク
Site Database Administrator	Alarm Manager	なし
	DM_Admin_Tool	◆ DB_BACKUP ◆ Database Password Change
	MIB Browser	なし
	MIB Compiler	なし
	Node Management	なし
	Remote Ping（リモート Ping）	なし
	Traffic Management	なし
	Novell ZENworks Server Management Maps	なし

役割ベース管理の設定

Role-based Services の役割を定義するには、Role-based Services の役割オブジェクトを作成し、その役割が実行できるタスクを指定します。

次の節では、役割ベース管理の設定方法について説明します。

- 809 ページの「Role-based Services の役割の定義」
- 810 ページの「外部スコープの作成」
- 811 ページの「Role-based Services の役割のメンバーシップとスコープの割り当て」

Role-based Services の役割の定義

Role-based Services の役割は、ユーザが特定の管理アプリケーションで実行できるタスクを指定します。次の節では、Role-based Services の役割の定義方法について説明します。

- 809 ページの「Role-based Services の役割オブジェクトの作成」
- 810 ページの「Role-based Services の役割が実行可能なタスクの指定」

Role-based Services の役割オブジェクトの作成

Role-based Services の役割オブジェクトを作成するには

1. Novell ConsoleOne で、Role-based Services の役割オブジェクトを作成するコンテナを右クリックし、[New] > [Object] の順にクリックします。
2. [Class] の下で [Role-based Services:Role] を選択し、[OK] をクリックします。
3. Role-based Services の新しい役割オブジェクトの名前を入力します。

   Novell eDirectory の命名規則に必ず従うようにしてください。Novell eDirectory の命名規則については、『Novell eDirectory 管理ガイド (http://novell.com/documentation/japanese/)』を参照してください。

   例 Password Administrator Role
4. [OK] をクリックします。

Role-based Services の役割が実行可能なタスクの指定

タスクを指定するには

1 Novell ConsoleOne で、Role-based Services の役割を右クリックし、[Properties] をクリックします。

Role-based Services のタスクオブジェクトは、Role-based Services のモジュールコンテナにのみ配置されます。

2 [Role Based Services] タブで、必要に応じて関連付けます。

3 [Role Content] ページを選択します。役割が実行できるタスクのリストを追加します。

4 [OK] をクリックします。

外部スコープの作成

外部スコープを作成するには

1 Novell ConsoleOne で、スコープオブジェクトを作成するコンテナを右クリックし、[New] > [Object] の順にクリックします。

2 [Class] の下で [MW:Scope] を選択し、[OK] をクリックします。

3 [MW:Scope] の新規オブジェクトの名前を入力します。

Novell eDirectory の命名規則に必ず従うようにしてください。Novell eDirectory の命名規則については、『Novell eDirectory 管理ガイド (http://novell.com/documentation/japanese/)』を参照してください。

例 Password Administrator Role

4 [OK] をクリックします。

スコープオブジェクトの設定

スコープオブジェクトを設定するには

1 Novell ConsoleOne で、スコープオブジェクトを右クリックし、[Properties] をクリックします。

2 スコープを関連付けるサイトオブジェクトを参照します。

3 [Site] スコープで、サイトスコープに対するコンピュータを参照して選択します。

4 SQL スクリプトで、ドロップダウンリストからオブジェクトと演算子を選択して、スコープを指定します。

5 [OK] をクリックします。

重要： デフォルトでは、スコープオブジェクトはすべてのサイトにアクセスできます。

SQL スクリプトで指定したオブジェクトとサイトスコープを組み合わせると、効果的なスコープになります。

Role-based Services の役割のメンバーシップとスコープの割り当て

Role-based Services の役割とスコープをユーザに割り当てるには

1. Novell ConsoleOne で、役割とスコープを割り当てるユーザオブジェクトを右クリックし、[Properties] をクリックします。
2. [Role Based Services] タブをクリックし、[Assigned Roles] をクリックします。
3. [Add] をクリックして、必要な役割をユーザに追加します。
4. [Scope] をクリックして、スコープをユーザに追加します。
5. [OK] をクリックします。

重要： スコープが異なる 2 つの役割がユーザに割り当てられた場合、各スコープに関係なく、ユーザは、役割 1 と役割 2 のタスクを合わせたすべてのタスクに対する権限を所有します。

ユーザグループおよび組織単位に役割とスコープを割り当てることはできません。

Management and Monitoring Services の設定

Novell ZENworks Server Management は複数のコンポーネントで構成されています。コンポーネントには、使用前のセットアップ作業が必要なものと必要でないものがあります。

次のコンポーネントでは、セットアップ作業は必要ありません。

- Novell ZENworks Server Management データベース
- 役割ベースサービス (Role-based Services)
- MIB (Management Information Base) ツール
- Novell ConsoleOne
- レポート機能
- SNMP サービス

次の節では、次のコンポーネントを準備して実行するのに必要なセットアップ作業について説明します。

- 812 ページの「Management and Monitoring Services の停止と起動」
- 812 ページの「検出プロセスのセットアップとバックエンドプロセスの起動」
- 813 ページの「アラーム管理システムのセットアップ」
- 814 ページの「監視のセットアップ」
- 814 ページの「Traffic Analysis Agent のセットアップ」

Management and Monitoring Services の停止と起動

サーバ上で他のソフトウェアのインストールや他のメンテナンス機能の実行が必要になった場合は、Management and Monitoring Services を停止して、サーバを停止します。メンテナンスの実行後は、Management and Monitoring Services を再開するために、サーバを再起動してからサービスをもう一度起動します。

Management and Monitoring Services を停止および起動するには、管理サーバのコンソールプロンプトで次の操作を行います。

1. Management and Monitoring Services を停止してアンロードするには、「**stopmms**」と入力します。
2. すべての JAVA プロセスを停止するには、「**java -kill**」と入力します。
3. JAVA を終了するには、「**java -exit**」と入力します。
4. サーバを再起動するには、「**restart server**」と入力します。

   サーバを停止するには、「**down server** と入力します。サーバを再起動する必要があります。
5. すべての Management and Monitoring Services を停止してアンロードするには、「**stopmms -n**」と入力します。

Management and Monitoring Services のインストール時に、バックエンドプロセスと検出プロセスを起動する適切なコマンド (SLOADER と NETEXPLOR) が autoexec.ncf ファイル挿入されているため、サーバを再起動するとこれらのプロセスが起動します。autoexec.ncf ファイルを変更して、これらのプロセスを手動で起動する必要がある場合は、813 ページの「検出プロセスとバックエンドプロセスの手動による起動」を参照してください。

検出プロセスのセットアップとバックエンドプロセスの起動

管理サーバの検出ソフトウェアは、ネットワーク上のノードを自動的に検出します。ネットワークノードとは、サーバ、デスクトップ、ルータ、スイッチ、およびその他のネットワークデバイスです。検出は、Novell ZENworks Server Management ソフトウェアが管理サーバにロードされると自動的に開始され、毎日 24 時間継続されます。データベースの構築にかかる時間は、ネットワークのサイズによって異なります。小規模ネットワークでは 1 ～ 2 時間、大規模ネットワーク（数千ノード）では数日かかる場合があります。

システムを使用する場合は、検出プロセスにかかる時間が長くなるため、ネットワーク検出をスタンドアロンで実行することをお勧めします。

インストール後のサーバは、次のいずれかの状態になっています。

- 検出サービスとバックエンドサービスが実行中です。

  インストール時に［Yes］を選択して、自動検出プロセスとバックエンドサービスを起動した場合は、Novell ZENworks Server Management サーバでネットワークの検出が開始され、そのまま継続されます。検出の設定については他に何もする必要はありません。ただし、最初の検出結果を確認して検出パラメータを変更する場合を除きます。検出結果の確認と検出パラメータの変更については、23 章 829 ページの「ネットワーク検出とアトラス管理の理解」を参照してください。

  重要： 検出パラメータの変更後に、812 ページの「Management and Monitoring Services の停止と起動」の説明に従ってサーバを再起動する必要があります。

- 検出サービスとバックエンドサービスが実行されていません。

  インストール時に［No］を選択して、自動検出プロセスとバックエンドサービスを起動しなかった場合は、デフォルト検出パラメータの変更後に検出を開始する必要があります。検出パラメータの変更の詳細については、23 章 829 ページの「ネットワーク検出とアトラス管理の理解」を参照してください。

  ネットワークを検出する前に、次の検出パラメータを変更できます。

  - SNMP コミュニティ文字列。使用するデバイスのコミュニティ文字列が検出時に設定されていることを確認してください。
  - 検出スコープ。デフォルトでは、正しいコミュニティ文字列が提供されている場合にネットワーク全体が検出されます。何らかの理由で検出スコープを制限する必要がある場合は、検出スコープを変更できます。
  - IPX 検出。IPX 検出は、Novell ZENworks Server Management サーバで有効な IPX アドレスがバインドされている場合にのみ発生します。Server Management サーバに IPX アドレスがバインドされておらず、IPX ネットワークを検出する必要がある場合は、CMD モードで NetWare サーバをインストールします（SCMD をロードします）。

  重要： 検出パラメータの変更後に、812 ページの「Management and Monitoring Services の停止と起動」の説明に従ってサービスを再起動する必要があります。検出サービスとバックエンドサービスが実行されていない場合は、813 ページの「検出プロセスとバックエンドプロセスの手動による起動」の説明に従って手動でサービスを起動できます。

検出プロセスとバックエンドプロセスの手動による起動

自動検出サービスを起動し、バックエンドサービスをロードするコマンドは、インストールプログラムによって autoexec.ncf ファイルに挿入されます。サーバを再起動すると、これらのプロセスが自動的に起動します。ただし、これらのコマンドを削除した場合は、手動で自動検出を起動し、バックエンドサービス（Management Site Services）をロードする必要があります。

インストール時に、管理サーバプログラムのファイルパス（Novell ZENworks¥mms¥mwserver¥bin）の autoexec.ncf ファイルに検索パスが追加されます。

検出プロセスとバックエンドプロセスを起動するには、サーバで **startmms.ncf** を入力します。

サーバは、バックエンドプロセスが完全にロードされた後にのみ、Novell ConsoleOne からの要求を受け付けます。

アラーム管理システムのセットアップ

Novell ZENworks Server Management のアラーム管理システムでは、SNMP 対応デバイス、またはプロキシ SNMP エージェントをホストするコンピュータからの SNMP トラップを受信できます。NetWare 版 Management Agent、Windows 版 Management Agent、NetWare 版 Traffic Analysis Agent、または Windows 版 Traffic Analysis Agent ソフトウェアをネットワークデバイスで使用している場合は、そのデバイスが自動的に検出されます。ソフトウェアのインストール後にセットアップする必要はありません。

サードパーティの SNMP エージェントは、トラップを受信するためのセットアップが必要です。サードパーティの SNMP エージェントのセットアップについては、795 ページの「SNMP 設定」を参照してください。

監視のセットアップ

NetWare 版 Management Agent と Windows 版 ManageWise® Agent は、SNMP に基づいているため、ネットワーク管理コンソールからサーバに指示されるすべてのアクションには、マネージャからエージェントへの SNMP SET 要求および GET 要求が含まれます。Novell ConsoleOne が管理サーバからのデータを要求する場合は、SNMP GET 要求を発行します。SNMP SET コマンドは、サーバのアラームしきい値や設定パラメータを設定するために必要です。Novell ConsoleOne からこのような管理操作を実行する場合は、セキュリティが確保されているかどうかが問題になります。特に、許可されていないユーザがサーバで設定パラメータを設定すると、パフォーマンスのエラーが発生したり、ネットワーク操作ができなくなったりします。

このため、管理システムと SNMP エージェント間で安全な通信を確立する必要があります。SNMP セキュリティの詳細については、795 ページの「SNMP 設定」を参照してください。

Traffic Analysis Agent のセットアップ

NetWare 版 Traffic Analysis Agent は、Novell ZENworks Server Management を補強する分散型ネットワークアナライザです。Novell ZENworks Server Management の他のエージェントは、特定のネットワークノード（サーバなど）に関するデータを収集しますが、NetWare 版 Traffic Analysis Agent は、特定の LAN セグメントでこれらのノード間の通信を監視します。このエージェントは NetWare サーバにインストールされます。NetWare 版 Traffic Analysis Agent をセットアップするには、815 ページの「NetWare 版 Traffic Analysis Agent の起動」を参照してください。

Windows 版 Traffic Analysis Agent は、管理サーバとの通信に SNMP を使用します。Windows 版 Traffic Analysis Agent をインストール後に操作するには、SNMP サービスを起動する必要があります。SNMP サービスを起動するには、815 ページの「Windows 版 Traffic Analysis Agent SNMP サービスの起動」の手順に従ってください。

エージェントのセットアップ後に、エージェントが属する Windows サーバを再起動する必要があります。

NetWare 版 Traffic Analysis Agent の起動

NetWare 版 Traffic Analysis Agent のインストールプログラムは、エージェントが自動的に起動するように、autoexec.ncf ファイルを変更します。そのため、他に何も設定する必要はありません。ただし、Traffic Analysis Agent の旧バージョン (Traffic Analysis エージェント) からアップグレードした際に、旧バージョンをアンインストールしなかった場合は、エージェントをアップグレードした各サーバで新しい Traffic Analysis Agent が実行されることを確認する必要があります。

アップグレードした NetWare サーバで新しい Traffic Analysis Agent が実行されることを確認するには

1 Novell ZENworks Server Management の Traffic Analysis Agent をアップグレードした各 NetWare サーバで、sys:¥system の autoexec.ncf ファイルを開きます。

2 次の行の先頭に # を挿入して、各行をコメントアウトします。

```
#Search add lanzdir

#LANZ.NCF
```

最初のステートメントは、旧エージェントがインストールされた *lanzdir* ディレクトリを含む検索パスを定義します。次のステートメントは旧エージェントをロードします。

3 ファイルを保存して、サーバを再起動します。

新しいエージェントが自動的にロードされて、実行されます。*agentinstallfolder*¥lanz の lanz.ncf ファイルが Traffic Analysis Agent を起動します。同じフォルダの ulanz.ncf ファイルは Traffic Analysis Agent を停止します。

Windows 版 Traffic Analysis Agent SNMP サービスの起動

SNMP サービスが自動的に起動されるように Windows を設定した場合、Windows にインストールされたエージェントは、Windows の起動時に SNMP サービスを起動します。

SNMP サービスが自動的に起動されるように Windows を設定しなかった場合は、次のいずれかの操作を行います。

- コマンドプロンプトで、「**net start snmp**」と入力します。
- Windows 2000/2003 の場合 :Windows のコントロールパネルで [管理ツール] > [サービス] の順にダブルクリックし、サービスの一覧で [SNMP] を選択して [開始] をクリックします。

  SNMP サービスが起動されると、Windows 版 Traffic Analysis Agent も起動します。

22 Novell ConsoleOneでのManagement and Monitoring Services の使用

Novell® ZENworks® Server Management コンソールは、Novell ConsoleOne® 管理ツールへのスナップインです。Novell ZENworks Server Management は、メニューオプション、既存の Novell eDirectory™ オブジェクトのプロパティページ、およびネットワークリソースの参照方法と構成方法を追加して、Novell ConsoleOne 管理機能を拡張します。この章の次の節では、Server Management に固有の Novell ConsoleOne 機能について説明します。

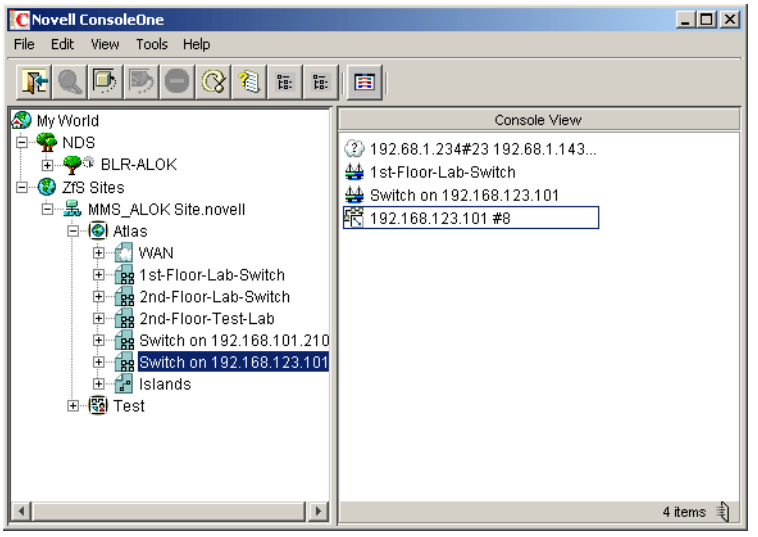
- 817 ページの「Novell ZENworks Server Management のネームスペースについて」
- 819 ページの「Novell ZENworks Server Management のオプションの選択」
- 821 ページの「ビューの使用」

Novell ConsoleOne の基本機能の詳細については、『Novell ConsoleOne 管理ガイド (http://novell.com/documentation)』を参照してください。

Novell ZENworks Server Management のネームスペースについて

Novell ConsoleOne では、ネットワークとそのリソースがオブジェクトのセットと見なされ、さまざまなコンテナに配置されます。最上部の各オブジェクトは、ネームスペースと呼ばれます。Novell ConsoleOne でネットワークとそのリソースを表示するには、Management Site Server オブジェクトを含む Novell eDirectory ツリーにログインする必要があります。

Novell ZENworks Server Management Novell ConsoleOne は、次の図に示すように、Novell ConsoleOne の Novell ZENworks Server Management サイトネームスペースの下にスナップインされます。

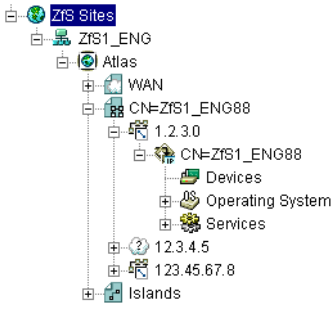


通常は、左側のフレームでオブジェクトを参照し、オブジェクトを右クリックして、オプションをクリックすると、管理タスクを実行できます。Novell ZENworks Server Management ネームスペース内のオブジェクトは、次の階層に分類されています。

1. **Novell ZENworks Server Management サイトオブジェクト：** Novell ZENworks Server Management のネームスペースのコンテナです。Novell ZENworks Server Management のネームスペース階層の最上部に位置します。このオブジェクトを展開すると、Server Management の管理サイトが一覧表示されます。
2. **管理サイト：** このオブジェクトは、Novell ZENworks の管理サーバを表します。サービスグループを構成する検出オブジェクトの集まりを定義する Novell eDirectory オブジェクトを表します。このオブジェクトを展開すると、サイトのアトラスが表示されます。
3. **[Atlas]：** 検出されたすべてのトポロジオブジェクトのためのコンテナオブジェクトです。アトラスには次のページが含まれます。
   - **[WAN] ページ：** ネットワーク全体の概要を表示します。
   - **領域ページ：** ネットワーク上のセグメントを表示します。ネットワークの構成方法によって、複数の領域ページが存在する場合があります。
   - **[Islands] ページ：** 接続が未確定のセグメントを表示します。
4. **セグメント：** 各アトラスページ内で、そのアトラスセクションに含まれるセグメントオブジェクトの一覧です。
5. **ノード：** 各セグメントオブジェクト内で、そのセグメントに属するサーバオブジェクトとノードオブジェクトの一覧です。表示されるアイコンはノードタイプによって異なります。
6. ノードの詳細：ノードオブジェクトを展開すると、システムの内部コンポーネントの一覧が表示されます。サーバデータは次の 3 つのカテゴリに分類されます。
   - Devices
   - オペレーティングシステム
   - サービス

[Devices]、[Operating System]、[Services] の各オブジェクトの隣に表示されるプラス記号をクリックして、サーバ設定をさらにドリルダウンし、サーバの内部コンポーネントに関する詳細を表示することができます。内部コンポーネントには、プロセッサ、インストールされたソフトウェア、ボリューム、カーネル、およびサーバに接続されるアダプタが含まれます。ノードオブジェクトの詳細については、929 ページの「オブジェクトの階層構造」を参照してください。

次の図は、Novell ZENworks Server Management のネームスペース階層を示しています。



Novell ZENworks Server Management のオプションの選択

Novell ZENworks Server Management のオプションを表示するには、監視または管理するオブジェクトを左側のフレームで右クリックします。使用できるオプションが表示されます。Novell ZENworks Server Management には、3 つの主要なオプションが用意されています。

- 819 ページの「ビュー」
- 820 ページの「プロパティ」
- 820 ページの「アクション」

ビュー

ビューは、さまざまな方法で情報を表示します。Novell ZENworks Server Management の多数のビューを使用すると、さまざまな方法でネットワークの情報を表示できます。次のビューを使用できます。

- **[Atlas]**：検出されたネットワークトポロジ、ノードの物理的な場所、ノード設定、およびアラーム情報をグラフ形式で表示します。
- **[Console]**：選択されたコンテナオブジェクトに属するオブジェクトを表示します。このビューは、Novell ZENworks Server Management サイトを移動する場合に便利です。
- **[Trend]**：現在または過去のトレンドデータを時間、日、週、月、または年単位でグラフで表示します。監視したトレンドデータは、使用中のサーバとその使用者の割り出し、問題のトラブルシューティング、複数のサーバ間での負荷分散、およびリソースの計画などの作業に役立ちます。
- **[Active Alarm]**：管理サイトごとに、セグメントまたはデバイスから受信した現在のアラームすべてに関するアラーム統計を表形式で表示します。このビューは、ネットワークに新しいアラームが発生するたびにリフレッシュされます。

- [Alarm History]：各アラームの処理ステータスなど、アーカイブされたすべてのアラームを表形式で表示します。このビューは、ネットワークに新しいアラームが発生するたびにリフレッシュされます。
- [Alarm Summary]：受信したアラームの概要をグラフ形式で表示します。このビューは、円グラフパネル、棒グラフパネル、トレンドパネルの 3 つの表示パネルに分割されます。各アラームの処理ステータスなど、アーカイブされたすべてのアラームを表形式で表示します。
- [Summary]：選択したオブジェクトの設定情報を表形式で表示します。たとえば、サーバオブジェクトの［Summary］ビューには、NetWare Loadable Module™ ファイル、メモリ使用量、アダプタ、ネットワークインタフェース、ディスクとディスクコントローラ、ボリューム、キュー、ユーザ、接続、開いているファイル、アラーム、およびインストールされたソフトウェアについての情報が表示されます。

これらの主要なビューのほかにも、Novell ZENworks Server Management には、階層内の多くのオブジェクトに適したビューが用意されています。たとえば、メモリオブジェクトを選択すると、ディスクキャッシュメモリの使用率を表示するディスクキャッシュビューを選択できます。利用可能なビューと、オブジェクトビューに表示される情報の詳細については、930 ページの「オブジェクトビューの詳細」を参照してください。

プロパティ

Novell ZENworks Server Management Novell ConsoleOne には、Novell ZENworks Server Management 固有の設定を制御できる複数のプロパティページが用意されています。Novell ZENworks Server Management のプロパティページにアクセスするには、オブジェクトを右クリックして、［Properties］をクリックします。

- サイトレベルでは、アラーム処理、Novell ZENworks Server Management データベース設定、SNMP（Simple Network Management Protocol）設定、MIB（Management Information Base）プールエントリ、およびヘルスレポートプロファイルなどのグローバルプロパティを編集できるプロパティページが用意されています。
- サーバレベルでは、SNMP 設定を変更できるプロパティページが用意されています。

Novell ConsoleOne プロパティページの使用に関する一般情報については、『Novell ConsoleOne 管理ガイド（http://novell.com/documentation）』を参照してください。

アクション

複数のオブジェクトで、1 つまたは複数のアクションを実行できます。たとえば、サーバオブジェクトを右クリックして表示されるアクションメニューには、サーバを再起動またはシャットダウンするオプションが表示されます。ボリュームオブジェクトを右クリックして表示されるアクションメニューには、ボリュームのマウントやマウント解除のためのオプションが表示されます。管理オブジェクトでのアクションの実行に関する詳細については、927 ページの「サーバコマンドの実行」を参照してください。

ビューの使用

Novell ZENworks Server Management Novell ConsoleOne には、表形式（リスト）ビューとグラフィックビューの 2 種類があります。[Console] ビュー、[Active Alarm] ビュー、および [Alarm History] ビューは、すべて表形式ビューです。[Atlas] ビューと [Trend] ビューは、両方ともグラフィックビューです。[Summary] ビューには、表形式要素とグラフィック要素が表示されます。

すべてのビューに共通する多くの特徴があります。この節では、Server Management のビューで実行できる共通のタスクについて説明します。

- 821 ページの「ビューの外観の変更」
- 822 ページの「列の変更」
- 823 ページの「ビューのフィルタ処理」
- 824 ページの「ビューのソート」
- 825 ページの「ビューの印刷」
- 825 ページの「ビューのエクスポート」
- 825 ページの「ビューの保存」
- 826 ページの「カスタムビューの削除と名前の変更」
- 826 ページの「Novell ConsoleOne のビューへの複数ビューの表示」

ビューの外観の変更

ビューでは、次の要素を変更できます。

- 821 ページの「表示フォントの変更」
- 822 ページの「グリッドのカスタマイズ」
- 822 ページの「ビュータイトルの表示」

表示フォントの変更

表形式ビューの見出しまたは行でテキストのフォントを変更するには

1. [View] > [Settings] > [Appearance] の順にクリックします。

   [Appearance] ダイアログボックスが表示されます。
2. 見出しまたは行のフォントを変更するには、次のボタンをクリックします。
   - 見出しのフォントを変更するには、[Header Font] ボタンをクリックします。
   - 行のフォントを変更するには、[Row Font] ボタンをクリックします。

   [Fonts] ダイアログボックスが表示されます。
3. フォントオプションを選択し、[OK] をクリックして、[Fonts] ダイアログボックスを閉じます。
4. ビューの変更を保存するには、[View] > [Saving] > [Save] の順にクリックします。

グリッドのカスタマイズ

デフォルトでは、Novell ZENworks Server Management のビューにはグリッドが表示されません。水平グリッドまたは垂直グリッドを表示し、グリッドの色を選択するには

1 [View] > [Settings] > [Appearance] の順にクリックします。

[Appearance] ダイアログボックスが表示されます。

2 [Style] ドロップダウンリストで、使用するグリッドスタイルを選択します。次のスタイルを選択できます。

- グリッドなし（デフォルト）
- 水平グリッドのみ
- 垂直グリッドのみ
- 垂直グリッドと水平グリッド

3 グリッドの色を選択する場合は、[Color] ボタンをクリックします。

[Color Chooser] ダイアログボックスが表示されます。このダイアログボックスの [Color Swatches]、[HSB]、または [RGB] タブページにより、3 つの方法で色を選択できます。

4 3 つのタブページのいずれかを使用してグリッドの色を選択し、[OK] をクリックして、[Color Chooser] ダイアログボックスを閉じます。

5 [OK] をクリックして [Appearance] ダイアログボックスを閉じます。

6 ビューの変更を保存するには、[View] > [Saving] > [Save] の順にクリックします。

ビュータイトルの表示

右側のフレームの上部にビューの名前を表示すると、Novell ZENworks Server Management Novell ConsoleOne 内の現在の場所をすぐに知ることができるため便利です。

ビューのタイトルを表示するには

1 [View] > [Show View Title] の順にクリックします。

列の変更

表形式ビューでは、次の方法で列を変更できます。

- 822 ページの「列のサイズ調整」
- 823 ページの「列の追加と削除」
- 823 ページの「列の表示順の変更」

列のサイズ調整

列のサイズを調整するには

1 調整する列の間で、列の端にマウスポインタを移動します。

2 ポインタがサイズ変更矢印に変わったら、列をドラッグして幅を調整します。

3 ビューの変更を保存するには、[View] > [Saving] > [Save] の順にクリックします。

列の追加と削除

ビューに列を追加または削除するには

1 [View] > [Settings] > [Column Selector] の順にクリックします。

2 列を追加するには、[Available Fields] リストで列の名前を選択し、[Add] をクリックします。

3 列を削除するには、[Show These Fields in This Order] リストで列の名前を選択し、[Remove] をクリックします。

4 [OK] をクリックします。

5 ビューの変更を保存するには、[View] > [Saving] > [Save] の順にクリックします。

列の表示順の変更

列の表示順を変更するには

1 [View] > [Settings] > [Column Selector] の順にクリックします。

2 [Show These Fields in This Order] リストで移動する列を選択し、[Move Up] ボタンまたは [Move Down] ボタンをクリックして列の場所を変更します。

3 [OK] をクリックします。

4 ビューの変更を保存するには、[View] > [Saving] > [Save] の順にクリックします。

ビューのフィルタ処理

表形式ビューでは、フィルタ条件に基づいてアラームを表示できます。フィルタは現在の管理セッションにのみ適用され、Novell ConsoleOne の終了後に解除されます。

4 つのドロップダウンリストから条件を選択するか、条件を入力して、フィルタをセットアップします。1 行だけのシンプルなフィルタを使用することも、複数行または行グループで構成される複雑なフィルタを使用することもできます。複数行を使用してフィルタをセットアップする場合は、行または行グループ間の論理的関係を指定することも必要です。

フィルタをセットアップするには

1 必要なビューに移動します。

2 [View] > [Settings] > [Filter] の順にクリックします。

3 最初のドロップダウンリストで、アラームにフィルタを適用する列を選択します。

4 2 つ目のドロップダウンリストから演算子を選択します。

演算子は、列に設定される制限値を定義します。アラーム表示が、3 つ目のドロップダウンリストで選択する値と等しい、等しくない、より大きい、より小さい、より大か等しい、より小か等しい、含む、またはその値で始まるという条件を指定できます。使用できる演算子のリストは、選択した列によって異なります。

5 3 つ目のドロップダウンリストから値を選択します。

6 4 つ目のドロップダウンリストから値を選択して、このフィルタステートメントと、このほかに定義するステートメントとの関係を指定します。

- フィルタステートメントが 1 つだけの場合、またはグループの最後のステートメントの場合は、[End] を選択します。
- 現在のフィルタステートメントの下に 1 行追加する場合は、[New Row] を選択します。新しい行が追加されます。前の行と新しい行との論理的関係を定義する必要があります。アラームは、指定した論理的条件に基づいて表示されます。両方のフィルタ条件を満たすには、[And] を選択します。表示されるアラームにいずれかのフィルタ条件を適用するには、[Or] を選択します。
- 前の行と関係のない行を 1 つまたは複数追加する場合は、[New Group] を選択します。新しい行が追加されます。ドロップダウンリストが追加され、新しい行が前の行から分離されます。このドロップダウンリストから値を選択して、フィルタステートメント間の関係を指定します。両方のフィルタステートメントが満たされるようにするには、[And] を選択します。いずれかのグループのフィルタステートメントが 1 つだけ満たされるようにするには、[Or] を選択します。新しいグループを追加した場合は、4 つ目のドロップダウンリストで [End] を選択します。

7 フィルタの定義が終了したら、[OK] をクリックします。

ビューが更新され、定義したフィルタ条件に一致するエントリのみが表示されます。

ビューのソート

ソート機能を使用して、表形式ビューのエントリの順序を変更できます。エントリは、次の 2 つの方法でソートできます。

- 824 ページの「ビューの 1 列だけのソート」
- 824 ページの「ビューの複数列のソート」

アラームのソートについては、891 ページの「アラームのソート」を参照してください。

ビューの 1 列だけのソート

ビューに表示されるエントリを 1 列だけソートするには

1 エントリをソートする列の列見出しをダブルクリックします。

列見出しをダブルクリックすると、ビューのエントリがその列によって降順でソートされます（最新のエントリが先頭）。エントリを昇順（最古のエントリが先頭）でソートするには、列見出しをもう一度ダブルクリックします。

ビューの複数列のソート

ビューの複数列をソートするには

1 [View] > [Settings] > [Sort] の順にクリックします。

2 [Sort Items By] フィールドで、エントリをソートする列のうち最初の列を選択します。

3 適切なラジオボタンを選択して、エントリのソート方法を昇順または降順に指定します。

4 [Then By] フィールドで、エントリをソートする列のうち 2 つ目の列を選択し、[Ascending] または [Descending] ラジオボタンをクリックしてソート順を指定します。

5 エントリをソートする残りの各列について、ステップ 4 を繰り返します。

6 [OK] をクリックします。

指定した基準に従ってエントリがソートされます。

ビューの印刷

ビューを印刷するには

1 印刷するビューを表示します。

2 [File] > [Print] の順にクリックします。

3 [Print] ダイアログボックスで印刷オプションを選択し、[OK] をクリックします。

4 次の [Print] ダイアログボックスで [OK] をクリックします。

ビューのエクスポート

表形式ビューまたはグラフィックビューは、次のいずれかのファイル形式にエクスポートできます。

- HTML
- カンマ区切りテキストファイル (.CSV)
- タブ区切りテキストファイル (.TXT)
- 空白区切りテキストファイル (.TXT)

ビューをエクスポートするには

1 エクスポートするビューを表示します。

2 [File] > [Export] の順にクリックします。

3 [Export File Type] ドロップダウンリストで、ビューをエクスポートする形式を選択します。

4 保存するファイルのパスと名前を [Filename] フィールドに入力するか、または [Browse] をクリックしてファイルをエクスポートする場所を探します。

5 [OK] をクリックします。

ビューの保存

デフォルトでは、ビューの外観、内容、ソート、またはフィルタに関する変更はすべて、Novell ConsoleOne の終了時に破棄されます。変更を保存する場合は、ビューを直接保存する必要があります。

この節では、次のトピックについて説明します。

- 826 ページの「既存ビューの保存」
- 826 ページの「新しいビューの作成」
- 826 ページの「カスタムビューの削除と名前の変更」

既存ビューの保存

既存のビューを永続的に変更し、その変更を反映するには、次の手順でビューを簡単に保存できます。

1 ビューを変更します。

2 [View] > [Saving] > [Save] の順にクリックします。

次にビューを表示するときは、変更が保存されています。

新しいビューの作成

場合によっては、変更を含む新しいビューを作成すると便利です。既存のビューは変更されず、別の名前で新しいビューを保存できます。

新しい名前でビューを保存するには

1 ビューを変更します。

2 [View] > [Saving] > [Save As] の順にクリックします。

3 [Enter New View Name] フィールドにビューの名前を入力し、[OK] をクリックします。

カスタムビューの削除と名前の変更

保存したカスタムビューの名前を変更または削除するには

1 [View] > [Saving] の順にクリックします。

2 カスタムビューの名前を変更するには、[Saved Views] リストからビューを選択し、[Rename] をクリックします。

または

カスタムビューを削除するには、[Saved Views] リストからビューを選択し、[Delete] をクリックします。

3 保存済みのビューの変更が終了したら、[Close] をクリックします。

Novell ConsoleOne のビューへの複数ビューの表示

[View in a New Window] オプションにより、複数の表形式ビュー、トレンドビュー、および混合ビューを、Novell ConsoleOne のビューウィンドウに表示できます。

[View In New Window] アイコン  は、Novell ConsoleOne のビューに表示できるビューを示します。

Novell ConsoleOne のビューに複数のビューがある場合は、リフレッシュに時間がかかります。

重要： Novell ConsoleOne のビューにすべてのビューを表示することはできません。

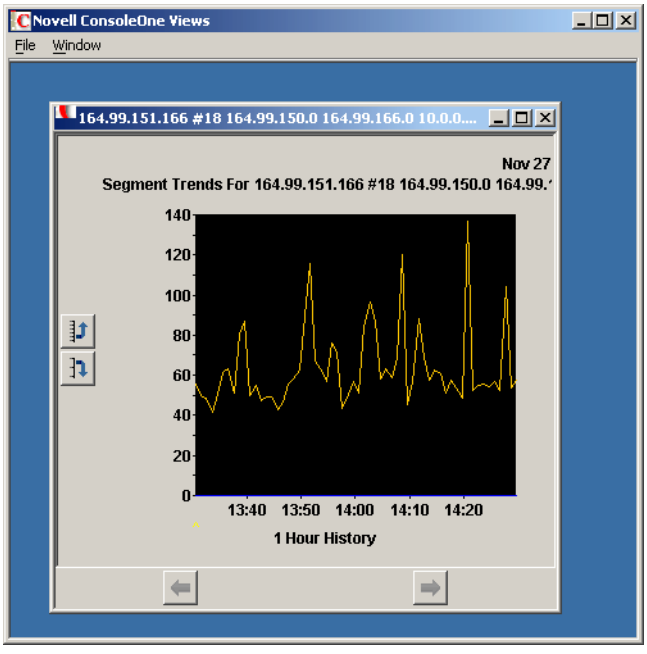
Novell ConsoleOne のビューウィンドウにビューを表示するには

1 Novell ConsoleOne でビューを選択します。

2 [File] を選択し、[View in New Window] を選択します。

または

をクリックします。



ビュー名を変更したり、ビューを並べて表示または重ねて表示したりすることもできます。

ビューの名前を変更するには

1 Novell ConsoleOne のビューで、[File] > [Rename] の順にクリックします。

2 新しい名前を指定して、[OK] をクリックします。

ビューを並べて表示または重ねて表示するには

1 Novell ConsoleOne のビューで、[Window] をクリックし、[Tile] をクリックします。

または

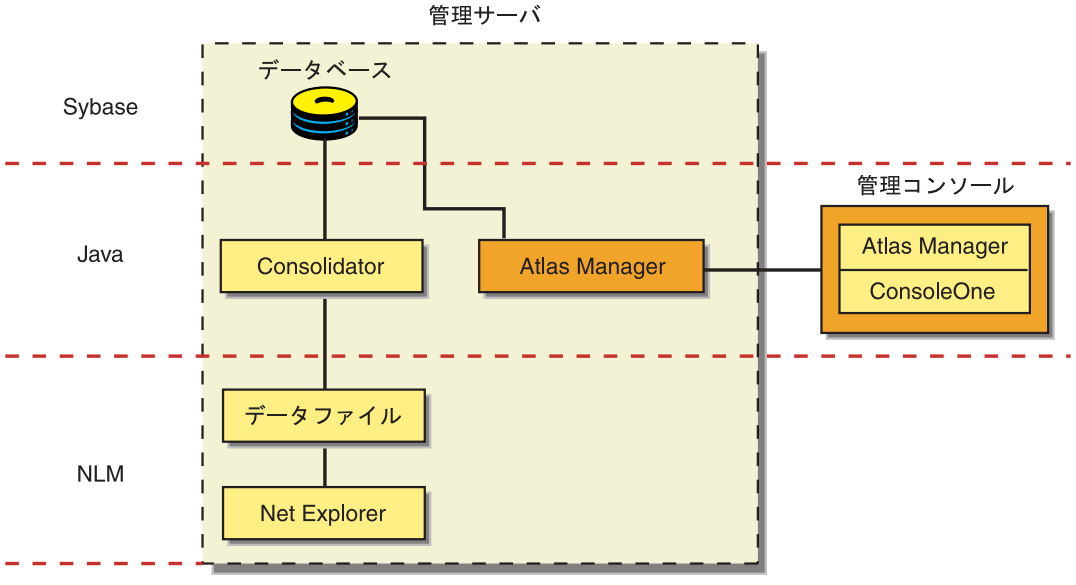
[Window] をクリックし、[Cascade] をクリックします。

23 ネットワーク検出とアトラス管理の理解

検出は、ネットワークのトポロジを決定するプロセスです。ネットワークコンポーネントは、Novell® ConsoleOne® から管理、監視、および表示できます。検出プロセスには、Novell ZENworks® Server Management ソフトウェアの次の 3 つの主要コンポーネントが含まれます。

- **検出ソフトウェア：**管理サーバで実行され、ネットワークトポロジを検出する、Novell NLM™ (NetWare Loadable Module™) ファイルです。
- **Consolidator ソフトウェア：**管理サーバで実行され、検出ソフトウェアが検出したデータを読み取ってトポロジデータベースに格納します。
- **Atlas Manager ソフトウェア：**トポロジデータベースを読み取ってアトラスデータベースを作成し、Novell ConsoleOne のアトラスにネットワークトポロジを表示します。

次の図は、Discovery コンポーネントの概念図です。



この章では、次のトピックについて説明します。

- 830 ページの「ネットワーク検出の理解」
- 862 ページの「検出のセットアップ」
- 874 ページの「アトラスの管理」

ネットワーク検出の理解

NetExplorer™ ソフトウェアは、管理サーバ上で検出プロセスを実行します。検出された情報は、トポロジデータベースに格納されます。Atlas Manager は、トポロジ情報を含む関連アトラスデータベースを作成し、マップの表示方法に関する情報を追加します。

次の節では、ネットワーク検出プロセスについて説明します。

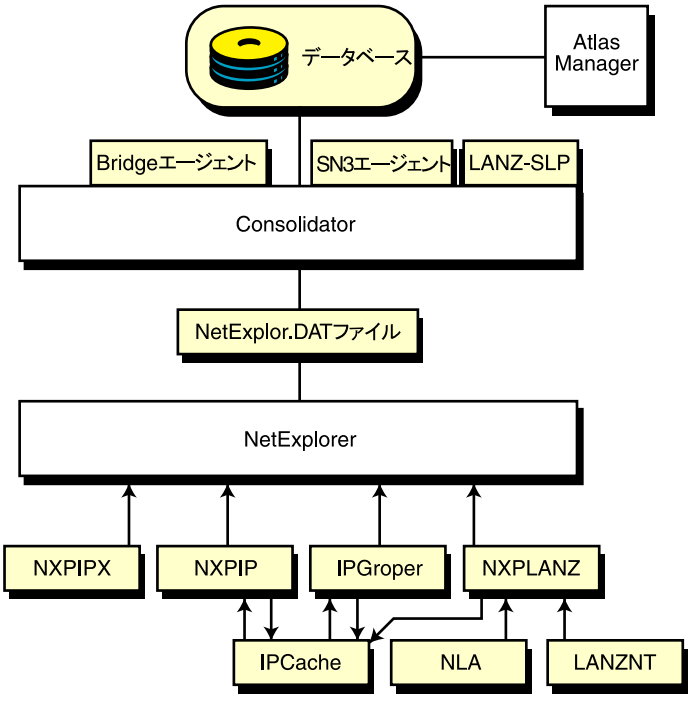
- 830 ページの「Discovery コンポーネント」
- 840 ページの「検出プロセス」
- 847 ページの「検出されるネットワークオブジェクト」
- 855 ページの「ファイルベースの検出」

Discovery コンポーネント

NetExplorer ソフトウェアと Consolidator ソフトウェアは管理サーバで実行され、ネットワークの検出とデータベースの更新に役立ちます。

NetExplorer を最初に起動すると、ネットワークは NetExplorer によって自動的に検出されます。

次の図は、サーバ上の Discovery コンポーネントを示しています。



NetExplorer システムは、次の相互依存コンポーネントで構成されます。

- 831 ページの「Discovery」
- 833 ページの「Consolidator」
- 834 ページの「Atlas Manager」
- 835 ページの「Database Object Editor」
- 839 ページの「管理コンソールソフトウェア」
- 839 ページの「Novell ZENworks Server Management の追加コンポーネント」

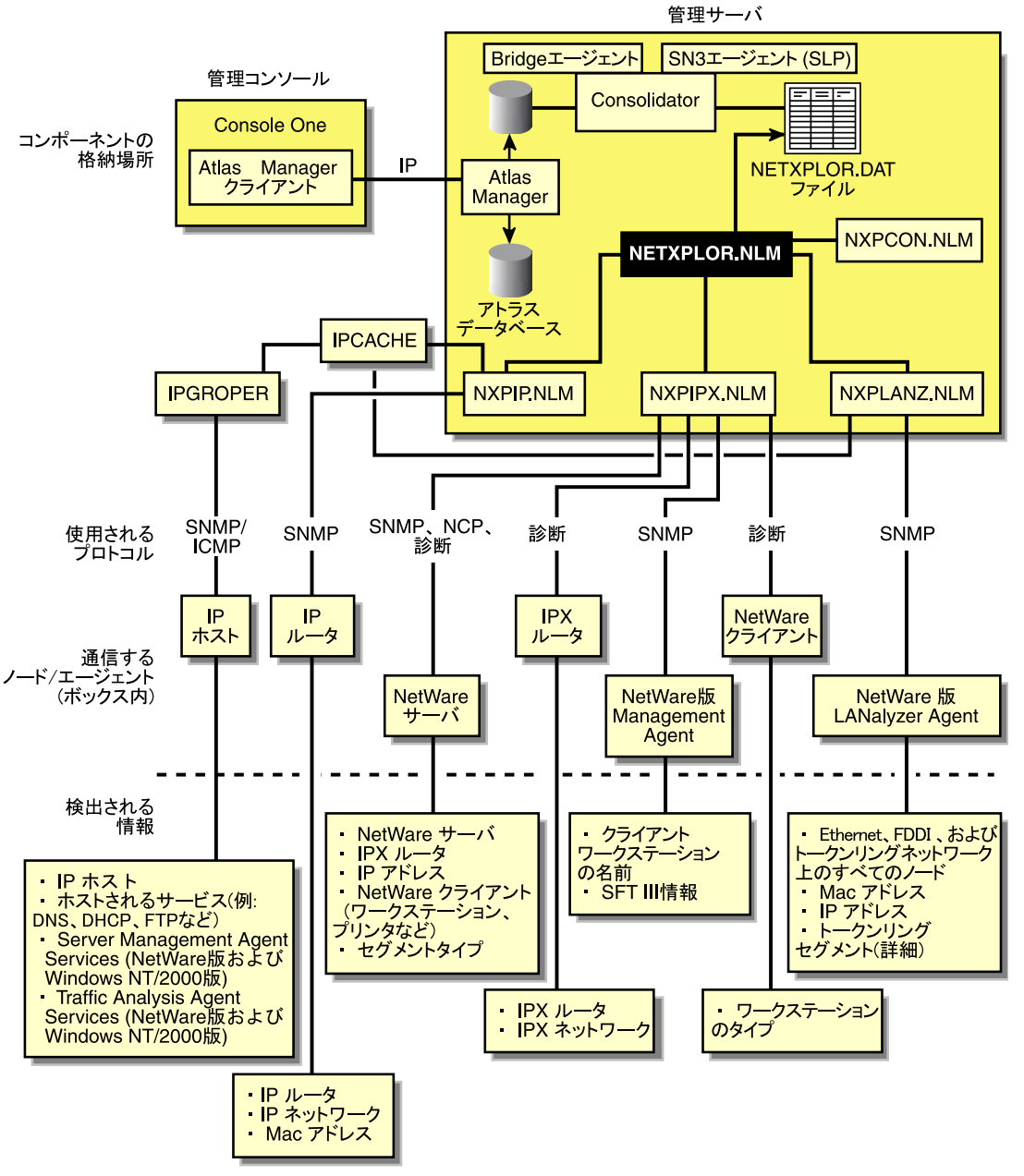
Discovery

検出ソフトウェアは管理サーバで実行され、検出 NLM™ ソフトウェアを使用してさまざまなネットワークデバイスを検出します。

- nxpip.nlm は、IP ネットワーク上の IP ルータを検出し、IP ルータ情報を NetExplorer に送信します。IPCACHE モジュールと通信して、この情報を IPGROPER と共有します。
- IPGROPER は、IP ホストアドレスに加えて、DNS (Domain Name System) 名、DHCP (Dynamic Host Configuration Protocol) サービス、Telnet、HTTP (Hypertext Transfer Protocol)、SMTP (Simple Mail Transfer Protocol)、および FTP (File Transfer Protocol) を検出します。
- nxpipx.nlm は、IPX™ ネットワーク上のさまざまな NetWare® システムを検出し、システム情報を NetExplorer に送信します。
- nxplanz.nlm は、NetWare 版および Windows* 版 Traffic Analysis Agent と通信し、監視セグメントで通信するすべてのシステムについての情報を収集して、この情報を NetExplorer に送信します。

次の図は、検出システムのアーキテクチャと、さまざまなコンポーネント、ネットワークシステム、およびエージェントソフトウェアの役割を示しています。

重要： Discovery コンポーネントでは、サーバとトラフィックの管理エージェントを使用して、特定の検出情報が収集されます。これらのエージェントの使用は必須ではありませんが、ネットワークで使用すると、Novell ConsoleOne の論理マップを正確および詳細に表示できます。



サポートされるプロトコル

Novell ZENworks Server Management ソフトウェアは、検出速度を速めるために、NetWare ネットワーク上で SLP (Service Location Protocol) をサポートしています。

NetWare 版の Server Management と Traffic Analysis Agent は、他のコンポーネントとの識別に、SAP (Service Advertising Protocol) を使用しています。SAP フィルタリングは、ルータによる SAP パケットの配送を停止します。管理サーバと Novell ConsoleOne が SAP パケットを受信し、管理可能なサーバ、HMI (Hub Management Interface) ハブ、またはその他のサーバを識別できるようにするには、SAP パケットをフィルタ処理するルータを設定して、配送する必要のある特定の SAP 番号を指定します。NetWare システムと ZENworks Server Management コンポーネントは、次の表に示す SAP 番号を使用しています。

コンポーネント	SAP 番号 (10 進)	SAP 番号 (16 進)
NetExplorer NLM	567	237
Novell Server Management Agent	635	27B
Windows サーバ版 ManageWise Agent	651	28B
NetWare 版 Traffic Analysis Agent	570	23A
プリントサーバ	7	7
Novell NetWare ファイルサーバ	4	4

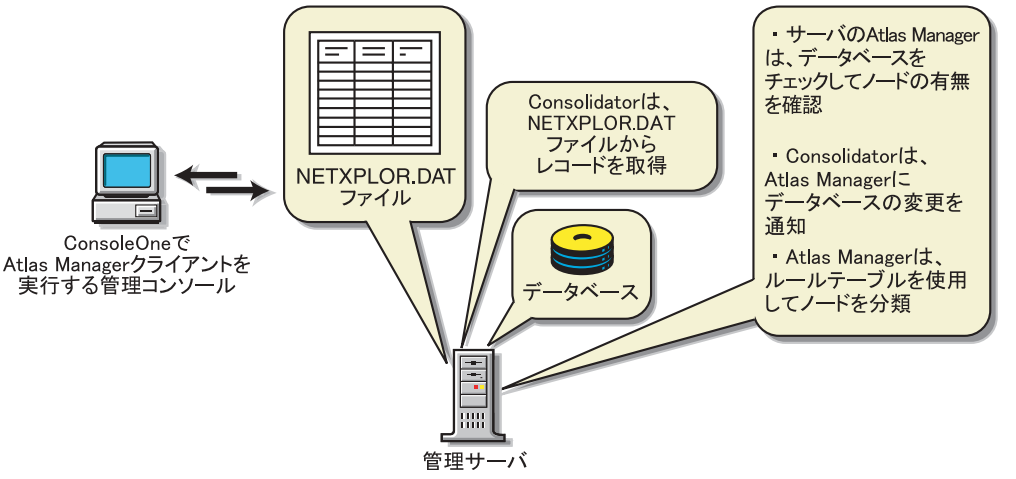
Consolidator

Consolidator ソフトウェアは管理サーバで実行され、次のタスクを実行します。

- 検出されたすべての情報を含む NetExplorer データファイルを読み取ります。
- netxplor.dat ファイルのレコードを解釈します。
- そのシステムがトポロジデータベースにすでに作成されているかどうかを確認します。トポロジデータベースにシステムが存在しない場合、Consolidator はそのシステムを作成します。
- Bridge エージェントを使用して IP ネットワークの Bridge Management Information Base を照会し、ブリッジのポートに接続されるシステムを検出します。
- SN3 エージェントを使用して NetWare サーバの Novell eDirectory 名を取得します。SN3 エージェントは、SLP を使用することで検出機能を強化し、NetWare サーバを検出します。
- 検出されたすべてのデバイスで mibcompiler.rule ファイルを実行し、ルールファイルに記載された MIB をこれらのデバイスで検証して、データベースを更新します。MIBCompiler.rule に対して MIB を追加または削除することもできます。
- Novell ZENworks Server Management データベースに検出情報を書き込みます。

次の図は、Consolidator のタスクを示しています。netxplor.nlm は netxplor.dat ファイルを作成し、Consolidator はそのファイルからのレコードの読み取りを開始します。NetExplorer プロセスが再起動されると、netxplor.dat ファイルが再作成され、Consolidator は新しいファイルの最初のレコードを要求します。

Consolidator は、netexplor.dat ファイルからレコードを取得する際に、データベースのレコードを検索します。システムがデータベースに存在しない場合、Consolidator はそのシステムを挿入し、Atlas Manager に更新を通知します。



コマンドラインオプション

Consolidator を手動で操作する場合は、次の表のコマンドラインオプションを使用してください。

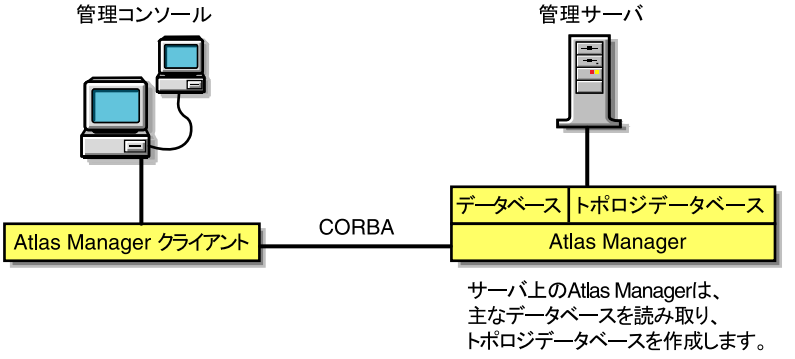
オプション	Consolidator の機能
-notify	データベースの更新を Atlas Manager に通知します。
-database *data_path*	操作を実行するデータベースファイルの位置を指定します。

Atlas Manager

Atlas Manager ソフトウェアは、サーバコンポーネントとクライアントコンポーネントで構成されています。サーバコンポーネントは、管理サーバ上で Novell ZENworks Server Management トポロジデータベースとともに使用されます。Atlas Manager サーバコンポーネントは、トポロジデータベースから検出データを取得し、独自のアトラスデータベースを作成します。

Atlas Manager のクライアントコンポーネントは Novell ConsoleOne で使用されます。サーバコンポーネントは、複数のコンソールコンポーネントといつでも通信できます。コンソールのマップに対する変更（名前の変更、インポート、レイアウトなど）は、Atlas Manager サーバコンポーネントに通知され、アトラスデータベースが更新されます。

次の図は、Atlas Manager のサーバとクライアントのソフトウェアを示しています。



Atlas Manager は、システムの分類に役立つルールテーブルのルールを検索します。このルールは、マップにシステムを表示するためのアイコンを Atlas Manager が決定する際に役立ちます。レコード内のシステムがルールのいずれかに一致すると、Atlas Manager はそのルールに従ってデータベースを更新します。

Database Object Editor

Database Object Editor は、検出システムの機能を強化します。自動検出では、ネットワーク上のデバイスが検出されない場合や、ネットワーク上のデバイスに関する間違った情報が表示される場合があります。Database Object Editor を使用すると、不足しているエンティティをデータベースに追加したり、間違ったエンティティ情報を編集したりできます。

Database Object Editor クライアントは、ConsoleOne スナップインを使用してユーザインタフェースを表示します。Database Object Editor を使用すると、セグメントまたはノードに関する操作を実行できます。

Database Object Editor サーバは、Consolidator と通信してノードオブジェクトやセグメントオブジェクトに関する情報を処理し、この情報を含むトポロジデータベースを作成します。

Database Object Editor を使用すると、セグメントやノードを追加または削除したり、セグメント情報やノード情報を変更したりできます。

セグメントまたはノードを追加するには

1 ConsoleOne で［Atlas］を選択し、［Tools］>［Database Object Editor］>［New］の順にクリックします。

2 セグメントまたはノードの詳細情報を入力します。

3 ［OK］をクリックします。

セグメント情報またはノード情報を編集するには

1 ConsoleOne で、編集するセグメントまたはノードを選択します。

2 ［Tools］>［Database Object Editor］>［Edit］の順にクリックします。

必要な情報を変更します。

3 ［OK］をクリックします。

セグメントまたはノードを削除するには

1 ConsoleOne で、削除するセグメントまたはノードを選択します。

2 ［Tools］>［Database Object Editor］>［Delete］の順にクリックします。

MIB のリストをノードに追加またはノードから削除するには

1 ConsoleOne で、MIB を追加または削除するノードを選択します。

2 ［Tools］>［Database Object Editor］>［Edit］の順にクリックします。

3 左側のペインで［Implemented MIBs］を選択し、MIB を追加または削除します。

サービスのリストをノードに追加またはノードから削除するには

1 ConsoleOne で、サービスを追加または削除するノードを選択します。

2 ［Tools］>［Database Object Editor］>［Edit］の順にクリックします。

3 左側のペインで［Services］を選択し、サービスを追加または削除します。

注： LANalyzer サービスは RMON サービスがないと機能しません。したがって、LANalyzer サービスをノードにインストールすると、RMON サービスも自動的にインストールされます。[Database Object Editor] の [Service] ペインには、LANalyzer サービスのみが表示されます。

ノードのインタフェースを追加、削除、または変更するには

1 ConsoleOne で、インタフェースを追加 / 削除 / 変更する対象のノードを選択します。

2 [Tools] > [Database Object Editor] > [Edit] の順にクリックします。

3 左側のペインで [Interface Summary] を選択し、インタフェースを追加 / 削除 / 変更します。

ノードのオペレーティングシステムを変更するには

1 ConsoleOne で、オペレーティングシステムを変更する対象のノードを選択します。

2 [Tools] > [Database Object Editor] > [Edit] の順にクリックします。

3 [Operating System] フィールドで、オペレーティングシステムのタイプを変更します。

スイッチポートをエンドノード接続に追加、エンドノード接続から削除、または変更するには

1 ConsoleOne で、接続を追加 / 削除 / 変更する必要があるスイッチを選択します。

2 [Tools] > [Database Object Editor] > [Edit] の順にクリックします。

3 左側のペインで [Switch Summary] を選択し、ノード接続に対してスイッチポートを追加 / 削除 / 変更します。

アンナンバードリンクの使用

アンナンバードリンクは、WAN リンクの両端のインタフェースに IP アドレスをバインドしない、ルータ間のポイントツーポイントリンクです。

ルータ検出モジュール (NXPIP) は、次の方法でルータ間のアンナンバード WAN リンクを検出します。

- **アンナンバードリンクの自動検出**： この方法では、各ルータのルータテーブルが使用されます。2 つのルータ間のアンナンバードリンクは、互いにポイントするルータを関連付けることで認識されます。
- **アンナンバードリンクの手動設定**： 自動検出でリンクが検出されなかったり、間違ったリンクが検出されたりした場合に、この検出方法を使用します。nxpip.ini ファイルは、アンナンバードインタフェースを持つ 2 つのルータ間のリンクを指定する場合や、自動検出がリンクを作成しないようにする場合に使用します。設定の詳細については、*installation_directory*¥novell zenworks¥mms¥mwserver¥nmdisk ディレクトリの nxp.ini ファイルを参照してください。

検出されたアンナンバードリンクのインタフェースタイプが、PPP、ATM、フレームリレー、および X.25 以外の場合、そのアンナンバードリンクは、不明なインタフェースタイプとして作成されます。

アンナンバードリンクの検出を有効にするには、netxplor.ncf ファイルを次のように変更します。

1 *installation_directory*¥novell zenworks¥mms¥mwserver¥nmdisk ディレクトリの netexplor.ncf ファイルを開きます。

2 Load NXPIP 行を探します。この行が見つからない場合は、NXPCON を使用して NXPIP モジュールを有効にします。この行が netexplor.ncf ファイルに追加されます。

3 次のオプションを追加します。**/autould/iniuld**. 行は次のようになります。
Load NXPIP /autould/iniuld

注： ルータのナンバード IP アドレスの 1 つを追加ルータのリストに追加してください。ルータの追加方法の詳細については、871 ページの「シードルータと追加 IP ルータの指定」を参照してください。

NetExplorer を再起動すると、アンナンバードリンクが検出され、Atlas ネームスペースに表示されます。

Atlas ネームスペースへのアンナンバードリンクの表示

ルータのアンナンバードリンクを表示するには

1 ルータのプロパティページに移動します。

2 [Computer Attributes] タブを選択します。

3 [IP Address] フィールドに、「Unnumbered IP Address (*n*)」という文字列が表示されます。n はルータのアンナンバードインタフェースの数です。

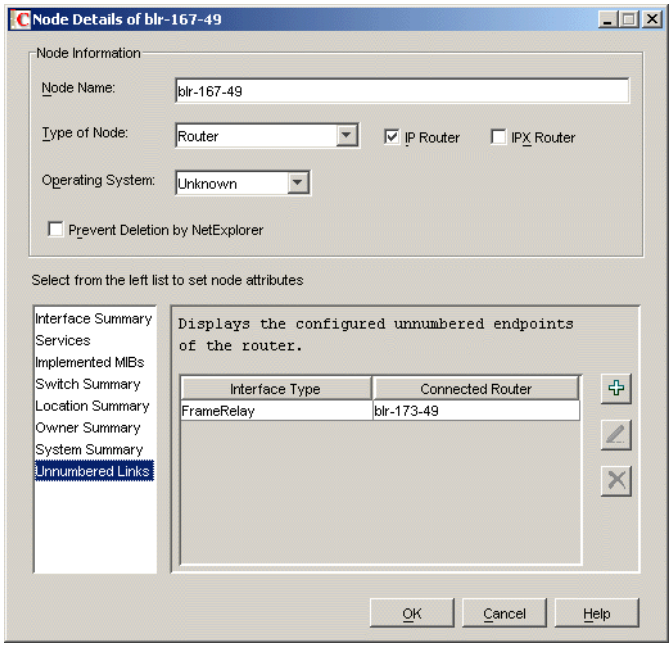
セグメントのアンナンバードリンクを表示するには

1 セグメントのプロパティページに移動します。

2 [Segment Attributes] タブを選択します。

[IP Address] フィールドに「Unnumbered Network」という文字列が使用され、アンナンバードリンクのネットワーク番号が表示されます。

Database Object Editor の [Unnumbered Links] タブを使用して、ルータのアンナンバードリンクを追加、変更、または削除できます。アンナンバードリンクには、インタフェースタイプと、接続されたルータが含まれます。作成および設定したすべてのアンナンバードリンクが一覧表示されます。



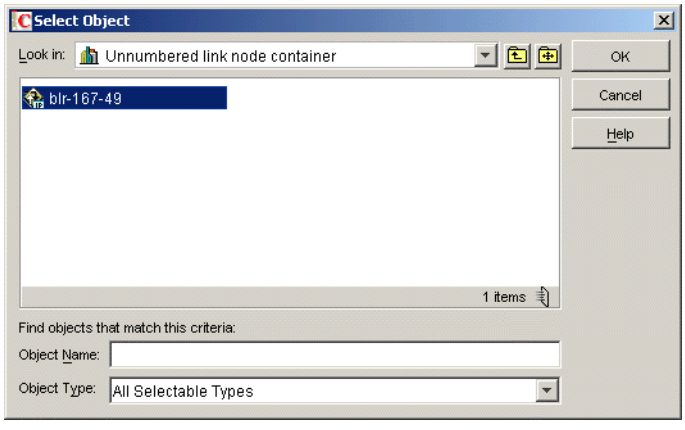
アンナンバードリンクの追加

1 [Unnumbered Links] タブで [Add] をクリックします。



2 [Interface Type] ドロップダウンリストから、ルータのインタフェースタイプを選択します。

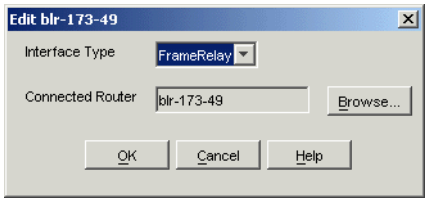
3 [Browse] をクリックして、接続するルータを選択します。



4 [OK] をクリックします。

アンナンバードリンクの編集

1 [Unnumbered Links] タブで、編集するアンナンバードリンクをリストから選択し、[Edit] をクリックします。



2 [Interface Type] ドロップダウンリストで、ルータのインタフェースタイプを変更します。

3 [Browse] をクリックして、接続するルータを選択します。

4 [OK] をクリックします。

アンナンバードリンクの削除

1 [Unnumbered Links] タブで、削除するアンナンバードリンクをリストから選択します。

2 [Delete] をクリックします。

接続されたノードを削除すると、対応するアンナンバードリンクも削除されます。このアンナンバードリンクに関連する、データベース内のすべての情報が更新されます。

管理コンソールソフトウェア

管理コンソールソフトウェアは、Novell ConsoleOne へのスナップインです。管理サイトが Novell ConsoleOne に作成されます。各サイトには、検出情報の完全性を維持するアトラスが作成されます。

Novell ZENworks Server Management の追加コンポーネント

nxpip.nlm、nxpipx.nlm、および nxplanz.nlm ソフトウェアは、次のコンポーネントと組み合わせて実行されます。

- 839 ページの「NetWare サーバ版 Traffic Analysis Agent」
- 839 ページの「NetWare サーバ版 Server Management Agent」
- 839 ページの「Novell NetWare サービスのバインダリ」

NetWare サーバ版 Traffic Analysis Agent

NetWare 版 Traffic Analysis Agent は、イーサネット、FDDI (Fiber Distributed Data Interface)、またはトークンリングのセグメントのトラフィック分析を提供する NLM ファイルセットです。Traffic Analysis Agent は、システムが使用するプロトコルに関係なく、監視するセグメント上のシステムをすべて検出します。各セグメントにエージェントを配置すると、複数のセグメントを監視できます。

管理サーバ上の nxplanz.nlm ソフトウェアは、SNMP を使用して、セグメント上の各システムの情報を、Traffic Analysis Agent を実行するサーバに照会します。

重要： Traffic Analysis Agent がソースルートされた各トークンリングセグメントを必ず監視するようにすると、検出プロセスを効率的に実行できます。

NetWare サーバ版 Server Management Agent

IPX サーバとワークステーションを検出する場合、管理対象サーバは、Server Management Agent がインストールされた NetWare サーバになります。Server Management Agent は、サーバにログインされたワークステーションのユーザ名とアドレスに関する nxpipx.nlm からの SNMP 照会に応答します。nxpipx.nlm は、Server Management Agent から SFT III™ サーバ情報を取得します。有効な結果を得るには、ネットワーク上のすべての NetWare サーバに Management Agent をインストールする必要があります。

Novell NetWare サービスのバインダリ

nxpipx.nlm は、すべての NetWare サーバにバインダリ情報を照会します。すべての NetWare サーバでは、セキュリティ設定がデフォルト値に設定されている場合、検出プロセスによってバインダリが確認されます。

NetWare サーバに接続されているワークステーションのログイン名が NetExplorer NLM ソフトウェアによって検出されるには、Server Management Agent がサーバにインストールされている必要があります。

検出プロセス

NetExplorer は、ネットワーク検出の実行を継続します。次の節では、検出プロセスについて説明します。

- 840 ページの「検出サイクル」
- 844 ページの「継続される検出」

検出サイクル

初期検出の開始後は、基準データが作成されるまで実行を継続する必要があります。検出は、小規模ネットワークでは 1 ～ 2 時間、大規模ネットワーク（数千ノード）では 1 ～ 2 日かかる場合があります。

検索プロセスはサイクル単位で発生します。1 サイクルは、検出モジュールがすべてのノードを一度に認識するプロセスです。特定のアドレスだけが検出されるようにサーバを設定すると、サイクル時間を短縮できます。詳細については、868 ページの「検出スコープの変更」を参照してください。

初期サイクルは、デバイスが検出されなくなるまで継続されます。初期サイクルで収集された情報は、デバイスを分類したり、各デバイスの正しいセグメントを特定したりするには不十分な場合があります。検出サイクルを継続して実行すると、新しい情報や変更された情報が追加されます。検出サイクルが進行するにつれて、情報の精度が高まります。

各検出プロセスは、異なるシステム検出方法を使用して、ネットワークに照会します。各検出サイクルでは、次に示す順序で、4 つの異なる検出モジュールが実行されます。

1. **IP ネットワークだけの IP ルータ検出**

   このプロセスは、NXPIP モジュールによって実行され、ローカルルータから開始します。NXPIP は、ローカルルータのルーティングテーブル情報を使用して、ネットワーク上の他のルータを検出します。次に、検出したルータのルーティングテーブル情報を使用して、ネットワークの検出を続けます。このプロセスは、検出されたルータごとに繰り返されます。

   NXPIP モジュールは、ルータアドレス情報と、IP バインドネットワークデバイスの情報を IPCACHE モジュールに保存します。

   nxpip.nlm は、管理サーバにインストールされます。IP ルータの検出には SNMP が使用されます。この NLM を使用するには、少なくとも 1 つのネットワークインタフェースボードにバインドされた TCP/IP が管理サーバで実行されている必要があります。nxpip.nlm は、システムテーブル、ルーティングテーブル、インタフェーステーブル、インタフェースのデータリンクタイプとフレームタイプ、セグメントのデータリンクタイプなどの MIB-II 情報を使用します。複数のベンダ向けにさまざまなバージョンの MIB-II 実装が存在するため、受信する情報は異なる場合があります。

   重要： 制御レベルを追加して、特定の IP アドレスがルータへの SNMP 照会を実行するようにした場合は、Novell ZENworks Server Management サーバに指定した IP アドレスが、ネットワークのすべてのルータに照会できることを確認してください。照会できない場合は、完全な検出結果が得られず、アトラスの［Islands］ページには不十分なネットワーク情報が表示されます。

2. **ワークステーションとサーバの IP 検出**

   このプロセスは、IPGROPER モジュールによって実行され、NXPIP が入力として IPCACHE に書き込んだルータ情報とネットワーク情報を受け取ります。NXPLANZ モジュールによって実行される RMON ベースの検出では、検出されたネットワークと IP ホストの情報が IPCACHE に書き込まれます。この情報も、IPGROPER モジュールへの入力として処理されます。

   このプロセスは、NXPIP によって検出された各ルータに、ARP テーブルを照会し、ネットワーク上のアクティブな各 IP ホストを特定します。IPGROPER は、どのルータの ARP テーブルにも見つからない IP アドレスについて、ping を実行し、その IP アドレスによるホストがアクティブかどうかを特定しようとします。

   IPGROPER は、ホストされるサービス (HTTP、DHCP、Telnet、SMTP、および DNS) に関する情報を、アクティブと特定した各 IP ホストに照会します。このホストに Server Management ソフトウェアと Traffic Analysis Agent がインストールされ、実行されているかについても検証します。

   同時に、IPGROPER モジュールは、管理サーバの sys:¥ect¥resolv.cfg ファイルで指定されている DNS サーバに、これらすべての IP ホストの DNS 名を照会します。

   重要： サーバとセグメントを管理可能にするには、そのサーバまたはセグメント上の IP ホストで実行されている Server Management Agent と Traffic Analysis Agent を検出することが重要です。

3. **NetWare/IP ネットワークを含む、すべてのネットワーク上での IPX 検出**

   このプロセスは、NXPIPX モジュールによって管理サーバから開始され、IPX アドレス、各アダプタの LAN タイプ、およびその他の既知のデバイスとサービスに関する SAP 情報を検出します。NXPIPX は、この情報の収集後に、バインダリに一覧表示されている各デバイスからの同種類の情報を要求します。このプロセスは、NXPIPX が新しいデバイスを検出するたびに繰り返されます。

   nxpipx.nlm は、NetWare、SNMP、および IPX プロトコル (IPX 診断など) を使用して、NetWare サーバ、IPX ルータ、および IPX ワークステーションを検出します。

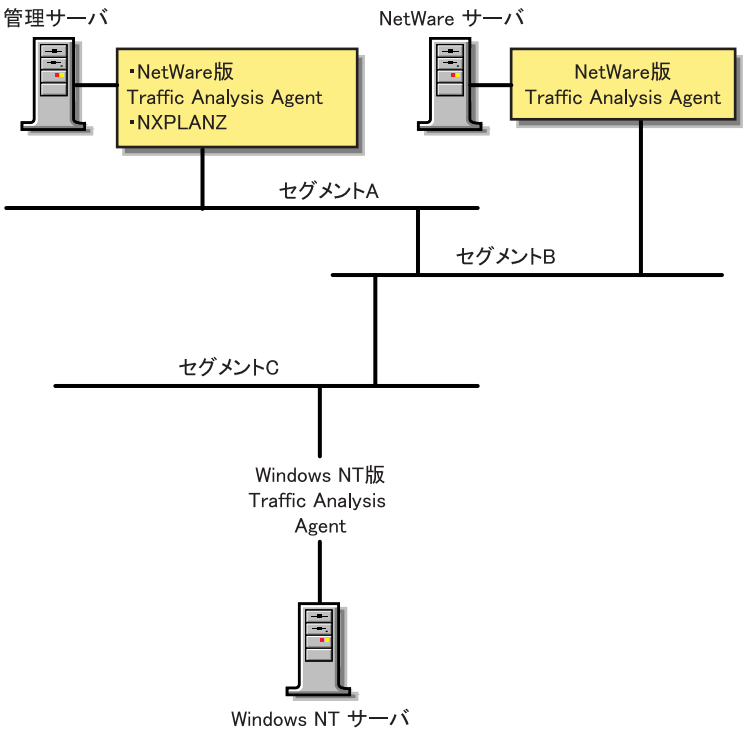
   重要： nxpipx.nlm がロードされると、デフォルトでは、*installation_volume*¥*install_dir*¥Novell ZENworks¥mms¥mwserver¥nmdisk サブディレクトリの下に NXPWORK という作業ディレクトリが作成されます。インストール時に、NXPWORK サブディレクトリに別のパスを指定することもできます。NXPIPX は、すべての一時ファイルをこのディレクトリに保存します。このディレクトリ内でファイルを読み取り、変更、または削除すると、検出プロセスが機能しなくなる場合があります。

4. **RMON ベースの IP ホスト検出**

   このプロセスは、NXPLANZ モジュールによって実行され、NetWare 版および Windows 版 Traffic Analysis Agent を含む、すべてのリモートエージェントを特定します。セグメント上の Traffic Analysis Agent は、そのセグメント上で転送されるパケット内のデータにバインドされた IP アドレスと MAC アドレスに基づいて、デバイスを検出します。管理サーバの NXPLANZ モジュールは、SNMP を使用して Traffic Analysis Agent と通信し、データを取得します。

   NXPLANZ モジュールは、ネットワーク上の Traffic Analysis Agent と、これらの Traffic Analysis Agent に監視されるセグメントの IP ホストに関する情報を NetExplorer に報告します。Traffic Analysis Agent によって監視されるネットワークと、監視されるネットワーク上の IP ホストに関する情報は、IPCACHE にも書き込まれるため、IPGROPER モジュールによる検出サービスの効率が向上します。

   次の図は、セグメント B とセグメント C 上の Traffic Analysis Agent ソフトウェアに個別に照会する NXPLANZ を示しています。



検出の効率を高めるには、検出する各ネットワークセグメントに Traffic Analysis Agent をインストールして実行するようにしてください。SLP がネットワーク上で無効になっているか、またはルータに SAP パケットのフィルタが適用されていると、NXPLANZ はネットワークの Traffic Analysis Agent をすべて検出できない場合があります。

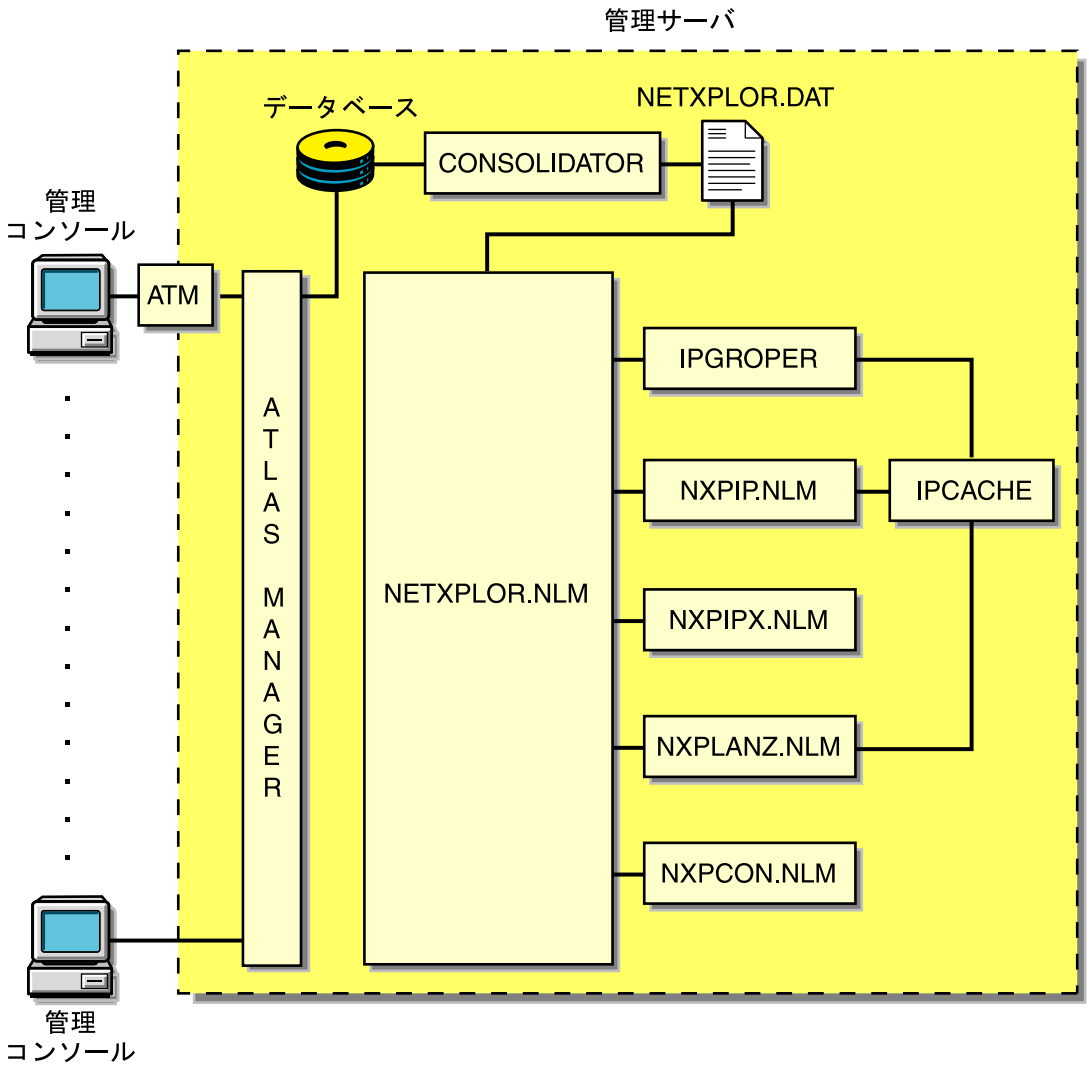
ネットワークのすべての Traffic Analysis Agent が NZPLANZ モジュールまたは NXPLANZ モジュールによって照会されるようにするには、NXPCON を使用してこれらの Traffic Analysis Agent を明示的に指定します。

初期検出サイクルでは、これらのモジュールが順次実行されます。そのため、Traffic Analysis Agent ソフトウェアに関する情報は最後に検出されます。

その後の検出サイクルでは、4 つのモジュールが同時に実行されます。これらのモジュールは検出プロセスを継続しますが、新しいデータまたは変更されたデータのみを netxplor.nlm に送信します。この追加データにより、セグメントの統合、適切なセグメントへのデバイスの配置、および新しいデバイスの検出を行うことができます。

異なる検出 NLM ファイルをサイクルごとに連続して実行することで、最終的にデバイスを特定し、NetExplorer が統合するのに十分なデータを提供する重要情報が得られる場合があります。

NLM プロセスによって検出されたデータは、Atlas Manager によって Novell ConsoleOne と通信されます。次の図は、検出 NLM プロセス、NetExplorer、および Novell ConsoleOne の関係を示しています。これらの各部分を組み合わせて操作し、ネットワークの内容とトポロジを検出する方法の詳細については、840 ページの「検出プロセス」を参照してください。



次の表は、各検出モジュールについてのデフォルトのシードとスコープ、およびユーザ定義可能な変更を示しています。

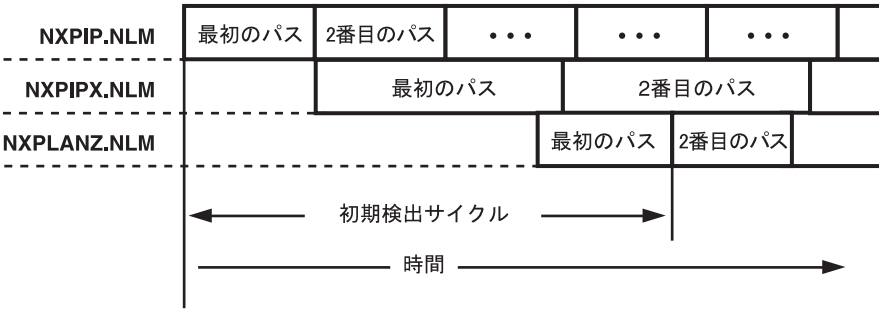
検出モジュール	デフォルトシード情報	デフォルトスコープ	ユーザ定義可能な変更
NXPIP	管理サーバのルーティングテーブルを調べます。 IPCACHE モジュールにルータアドレスを保存します。	コミュニティ文字列が一致する場合はすべてのネットワーク。	NXPCON で IP スコープ情報を指定してスコープを制限します。 SNMP コミュニティ文字列の public が使用されていない場合、NXPCON でルータの SNMP コミュニティ文字列のリストを作成します。
IPCACHE	NetExplorer のサポートモジュールです。NXPIP、IPGROPER、および NXPLANZ で使用される、デバイスとネットワークの一時情報を含みます。		

検出モジュール	デフォルトシード情報	デフォルトスコープ	ユーザ定義可能な変更
IPGROPER	1. IPCACHE 内の各ルータアドレスに ARP テーブルを照会して、ネットワークデバイスを特定します。 2. ネットワークデバイスがホストするサービス (FTP、HTTP、Telnet、SMTP、DNS、および DHCP) と DNS 名を、各ネットワークデバイスに照会します。 3. Server Management と Traffic Analysis Agent を実行するホストを検出します。	NXPIP によってすでに検出されたルータに接続されているすべての IP ネットワーク。	• 自動検出の有効化または無効化 • ファイルベースの検出の有効化または無効化
NXPIPX	管理サーバの設定を調べます。	すべての IPX インターネットワーク。	NXPCON で IPX スコープ情報を指定してスコープを制限します。
NXPLANZ	NXPCON に一覧表示される Traffic Analysis Agent ソフトウェアを実行中のサーバのリストを調べます。	Traffic Analysis Agent ソフトウェアのすべてのセグメント。	NXPCON で Windows 版 Traffic Analysis Agent の名前と IP アドレスを指定します。SLP が無効になっているか、または SAP にフィルタが適用されている場合は、NXPCON で NetWare 版 Traffic Analysis Agent の名前とアドレスを指定します。

継続される検出

NetExplorer は、NETXPLOR.NLM が開始および制御するプロセスによって、NetExplorer が所属するインターネットワークを検出します。最初に、各検出 NLM はそれぞれを NETXPLOR.NLM に対して特定し、次に NETXPLOR.NLM は初期検出サイクルを開始します。このサイクルは、NXPIP 検出、NXPIPX 検出、NXPLANZ 検出の順で開始されます。IPGROPER の検出サイクルは netxplor.nlm では制御されません。起動後は、実行が継続されます。NetExplorer によって収集された情報は、管理サーバの netexplor.dat ファイルに格納されます。

次の図は、各検出プロセスと時間の関係を示しています。NXPIP の最初のパスが終了した後に、NXPIPX が開始され、NXPIP がもう一度開始されます。NXPIPX の最初のパスが終了した後に、NXPLANZ が開始され、NXPIPX の 2 回目のパスが開始されます。他に指定しない限り、この 3 つの検出プロセスは継続して実行され、ネットワークに対する変更を検出します。ネットワークへの変更は、netexplor.dat ファイル内のレコードとして保存されます。3 つの検出プロセスすべてが 1 つのパスを終了すると、初期検出サイクルが完了します。



次の節では、各シーケンスの詳細について説明します。

- 845 ページの「NXPIP」
- 845 ページの「NXPIPX」
- 845 ページの「NXPLANZ」
- 846 ページの「NETXPLOR」
- 846 ページの「SNMP コミュニティ文字列の検出」

NXPIP

NetExplorer 検出サイクルの最初のシーケンスでは、IP ルータが検出されます。NXPIP は、TCP/IP 設定情報を使用してローカルルータを探します。次に、ネットワーク上の他のルータ ID をそのルータに照会します。NXPIP は、SNMP を使用してルータ上の MIB に照会し、IP アドレス、インタフェースタイプ、および MAC アドレスを収集します。

デフォルトでは、NXPIP はすべての IP ネットワークの検出を試みます。NXPCON でスコープ情報を指定すると、IP 検出スコープを制限できます。

NXPIPX

NXPIPX は、SNMP、RIP、IPX、および SPX™ 診断などの一連の技術を使用して、接続されている IPX または NetWare/IP インターネットワークを検出します。NXPIP の最初のパスが完了したら、NXPIPX は管理サーバで検出を開始します。NXPIPX は所属するサーバを調べて、他のサーバの名前を検出します。次に、これらの各サーバに照会してその他のサーバを検出し、サーバが発見されなくなるまでこのプロセスを繰り返します。

NXPIPX は各 NetWare サーバの接続テーブルを読み取り、NetWare クライアントがそのサーバにログインしているかどうかを判断します。IPX 診断パケットを各クライアントに送信して、追加情報を収集します。接続テーブルに表示されないクライアントは、最近ログインされておらず、診断機能が無効になっているため、このようなクライアントは NXPIPX によって検出されません。そのため、NetWare クライアントの IPX 診断を有効にしておくことが重要です。

NXPIPX は、ネットワークの IPX ルータも検出します。サードパーティの IPX ルータは、ルートされたセグメントに NetWare サーバがある場合にのみ検出されます。ルートされたセグメントに NetWare サーバがない場合は、NXPIPX はインタフェース情報を検出しません。

デフォルトでは、NXPIPX はすべての IPX インターネットワークの検出を試みます。NXPCON を使用して IPX ネットワーク番号のリストを指定すると、検出スコープを制限できます。NXPIPX で他の IPX ノードを検出するには、IPX 番号のいずれかが管理サーバに必ずバインドされるようにしてください。

NXPLANZ

NetWare 版 Traffic Analysis Agent は、所属するネットワークセグメントの各パケットを監視します。ローカルメモリ上のセグメントで通信するすべてのシステムの物理 (MAC) アドレスと IP アドレスのリストを作成します。NXPIPX の最初のパスが完了したら、NXPLANZ は SNMP を使用して、Traffic Analysis Agent がインストールされたすべてのサーバに照会し、ネットワークで通信するワークステーションのリストを読み取ります。NXPLANZ は、サーバで実行中のエージェントのリストを NXPIPX から取得します。

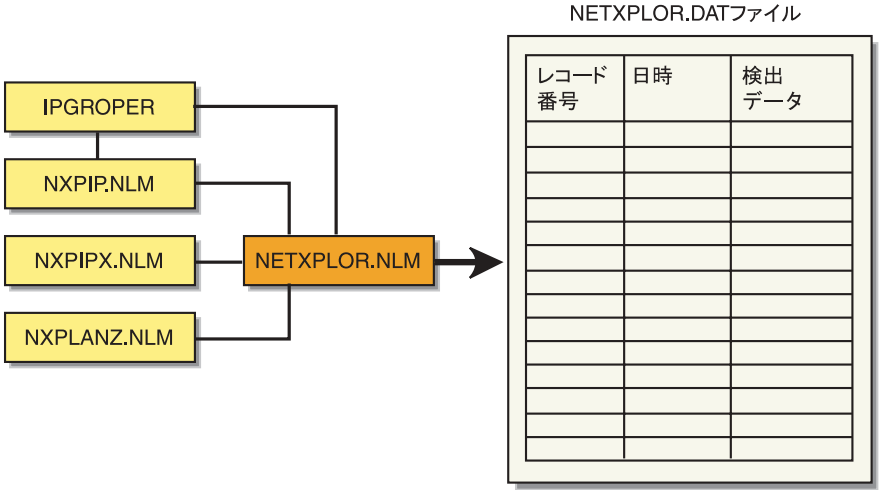
IPGROPER

NXPIP によって IPCACHE に書き込まれたルータとネットワークセグメントの情報と、NXPLANZ によって IPCACHE に書き込まれたネットワークセグメント情報およびホストが、IPGROPER モジュールへの入力を形成します。IPGROPER は、各ネットワークセグメントについて、そのネットワーク上のすべてのホスト、ホストの DNS 名、ホストされるサービス、Server Management Agent、および Traffic Analysis Agent の検出を試みます。

NETXPLOR

検出プロセスは、ネットワーク上のシステム情報を収集して、関連データのパケットを netexplor.nlm に転送します。netexplor.nlm は、次の図に示すように、これらのパケットにレコード番号とタイムスタンプを追加して netexplor.dat ファイルに格納します。

注： 検出プロセスは、netexplor.nlm がロードされるたびに netexplor.dat ファイルを再作成します。そのため、前回の NetExplorer NLM プロセスの実行によって管理サーバに保存された検出データは、netexplor.nlm が再起動された場合は保持されません。



SNMP コミュニティ文字列の検出

NetExplorer が SNMP によってシステムにアクセスしようとするたびに、管理サーバでは NXPCON ユーティリティを使用して設定したコミュニティ文字列が使用されます。新しいシステムを発見すると、NetExplorer は設定した各コミュニティ文字列を試します。特定の IP アドレスまたは IPX アドレスのコミュニティ文字列が見つかると、NetExplorer は後続のサイクルで他の設定名をもう一度試すことのないように、この名前をファイルに記録します。

NXPCON を使用して、これらのコミュニティ文字列を表示できます。コミュニティ文字列は、指定された順序で使用されます。そのため、最もよく使用されるコミュニティ文字列は、リストの先頭に設定する必要があります。

重要： 無効な SNMP コミュニティ文字列を使用して SNMP 照会を実行すると、ターゲットシステムからの応答がないまま要求時間が終了します。

検出されるネットワークオブジェクト

NXPIP、NXPIPX、および NXPLANZ は、さまざまな技術を使用して次のカテゴリのネットワークオブジェクトを検出し、アトラスに表示します。

- 847 ページの「システム」
- 853 ページの「ネットワークセグメント」

通常は、ネットワークマップにシステムを正確に配置するには、NXPIP と NXPIPX によって収集される情報だけで十分です。NXPIP と NXPIPX がシステムを検出しなかった場合は、NXPLANZ が Traffic Analysis Agent によって収集される MAC アドレスを取得して、新しいシステムがデータベースに追加されます。これにより、Traffic Analysis Agent によって監視されるセグメント上のすべてのシステムが検出されます。

システム

次の表に、検出されるシステムのさまざまな種類を示します。

システム	コメント
Novell Server Management Agent	サービスタイプが 10 進で 563(Novell Server Management Agent 1.5 または 1.6) または 635(Novell Server Management Agent 2.6)、または MIB が実装された Novell Server Management Agent。
Windows 版 Management Agent	MIB が実装された Management Agent。
NetWare 版 Traffic Analysis Agent	サービスタイプ 570 (10 進) または MIB が実装された Traffic Analysis。
Windows 版 Traffic Analysis Agent	MIB が実装された Traffic Analysis。
Novell NetWare ファイルサーバ	サービスタイプ 4 (ファイルサーバ)。NXPIPX はすべての NetWare サーバを検出します。
Novell NetWare Print Server™	サービスタイプ 71 または 7 (10 進)。
IPX ルータ	IPX ネットワークに接続されている 1 つ以上のアダプタを持つシステム。
IP ルータ	MIB-II で IP ルータとして設定されたシステム (IP 転送可能)。
Novell NetWare クライアントワークステーション	IPX ワークステーションとして IPX 診断要求に応答するシステム (Novell NetWare Shell をロード)。
SFT III IO エンジン	IPX 検出モジュールによって検出され、診断情報に応答します。
SFT III MS エンジン	IPX 検出モジュールによって検出されます。
ネットワークプリンタ	プリンタがよく知られているサービスタイプを生成する場合に検出されます。
Novell NetWare Connect™	サービスタイプ 590 (10 進)。
Novell NetWare 通信サーバ	Novell NetWare for SAA*Service Manager 製品によって使用され、サービスタイプは 304 (10 進) です。
Management Server	検出 NLM ファイルを実行し、サービスタイプは 567 (10 進) です。
その他のシステム	Traffic Analysis Agent が監視している LAN セグメントに接続されたシステムはすべて検出されます。

検出されるサービスは、Telnet、HTTP、DNS、SMTP、DHCP、ルータ、Novell eDirectory、SFTIII、および SNMP です。

次の節では、検出されるさまざまなシステムの詳細について説明します。

- 848 ページの「Novell NetWare クライアントワークステーション」
- 849 ページの「IP ルータ」
- 849 ページの「Novell NetWare SFT III」
- 850 ページの「IPX Diagnostic Responder を装備していないシステム」
- 851 ページの「MAC アドレスを重複使用しているルータ」
- 851 ページの「サードパーティのルータ」
- 852 ページの「WAN ポートを使用する Novell NetWare MultiProtocol Router」
- 852 ページの「IPX ネットワーク」
- 852 ページの「IP ネットワーク」
- 852 ページの「オンデマンドリンク」
- 852 ページの「WAN ポートを使用するサードパーティのルータ」
- 852 ページの「Novell NetWare Connect サーバ」
- 853 ページの「仮想スイッチ」

Novell NetWare クライアントワークステーション

NXPIPX は、検出された NetWare サーバに接続されているすべての Novell NetWare クライアントソフトウェアを検出します。電源が切られているクライアントや、サーバに接続されていないクライアントは検出されません。このため、NetExplorer プロセスを夜間や週末に実行すると、正確なマップが作成されない場合があります。NetWare クライアントでは、IPX 診断を有効にしておく必要があります。

NetWare クライアントでバインダリログインを実行できるように構成する場合は、次の点を考慮してください。

サーバ	バインダリログイン時の検出
Server Management Agent がインストールされた Novell NetWare	ワークステーションは検出される。Novell NetWare 4.*x* および Novell NetWare 5.*x* の転送として IPX でログインした場合のみ名前が検出される。
Novell NetWare	ワークステーションは検出される。名前は検出されない。

クライアントを設定してディレクトリログインを実行できるようにすると、NetExplorer は Novell eDirectory ツリーに「ログインしている」システムだけを検出し、Novell eDirectory ツリーに単に「接続された」システムは検出しません。NXPIPX は、SNMP コミュニティ文字列を使用して Management Agent と通信し、すべての NetWare サーバにユーザ名を照会します。

NetExplorer による NetWare クライアントの検出後に、NXPIPX は IPX 診断プロトコルを使用してクライアントに照会し、検出を確認して詳細情報を収集します。IPX 診断が無効になっている場合は、NXPIPX はそのシステムを報告しません。これはプリンタにも適用されます。

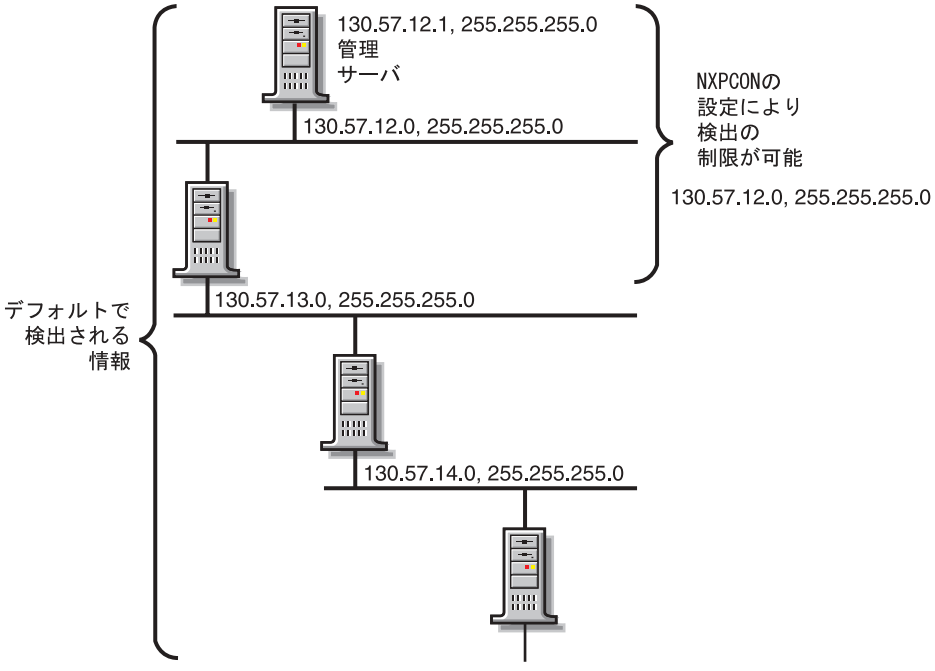
IP ルータ

NXPIP は、ルータで使用される SNMP コミュニティ文字列を使用して、ネットワーク上のすべての IP ルータを照会します。NXPCON を使用して、ルータで使用されるコミュニティ文字列のリストを入力する必要があります。

SNMP MIB Browser などの SNMP 設定ツールを使用すると、ルータの MIB 内の情報を設定できます。ルータの SNMP MIB でシステム名などのルータ情報を設定した場合、検出プロセスはその情報をデータベースに記録して、IP ルータが意味のある名前で表示されるようにします。

デフォルトでは、IP 検出はすべてのネットワークを検出します。NXPCON の [Discovery Scope] で [IP Discovery Scope] オプションを使用してネットワーク番号を指定すると、検出を制限できます。重複 IP ルータがある場合は、NXPCON の [IP Discovery] で [IP Routers] オプションを使用して、重複 IP ルータアドレスを指定します。指定しない場合、NXPIP はこのルータを検出しません。次の図に示すように、管理サーバ IP アドレスが 130.57.12.0 の場合、IP 検出 NLM は 10.57.85.0 ネットワーク全体とそのサブネットを検出します。

次の図は、Novell ZENworks での IP ルータ検出のしくみを示しています。

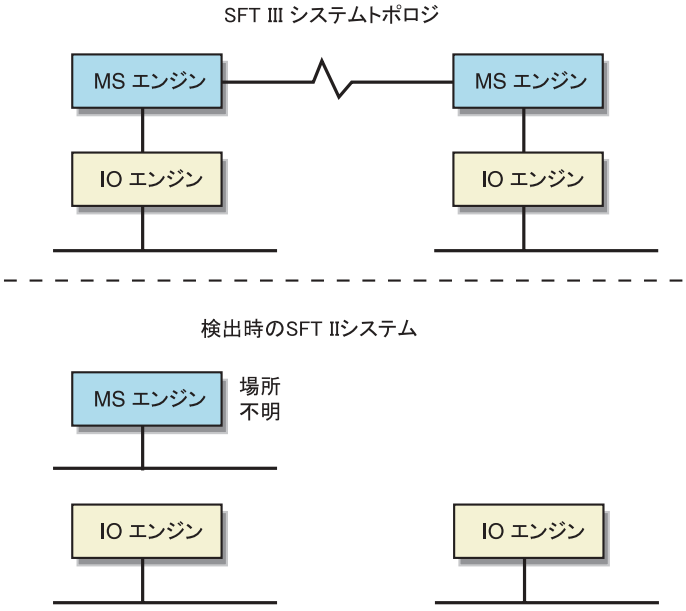


Novell NetWare SFT III

NetWare SFT III™ サーバは、通常は 2 つのコンピュータシステムで構成され、各システムには入出力エンジン (IO エンジン) とミラーサーバエンジン (MS エンジン) が含まれます。そのため、物理的には 2 つの IO エンジンと 2 つの MS エンジンが存在し、論理的には 2 つの IO エンジンと 1 つの MS エンジンが存在しています。

Novell Server Management Agent が SFT III サーバにロードされている場合は、MS エンジンと 2 つの IO エンジンが名前を含めて正確に検出され、アトラス内の正しいセグメントに配置されます。ただし、MS エンジンは [Islands] ページに配置されます。これは、2 つの MS エンジンがネットワーク上の 1 つの論理サーバに関連付けられており、MS エンジンのどちらのコピーがその時点でプライマリになっているかによって、MS エンジンの場所が変わる場合があるからです。

次の図は、NetWare SFT III サーバの検出を示しています。



MS エンジンに Server Management Agent がロードされていない場合は、検出時にプライマリである MS エンジンと IO エンジンだけが検出されます。プライマリ IO エンジンは、領域ページで「Noname」と 表示されます。セグメントマップで IO エンジンの名前を変更するには、アイコンを右クリックし、[Rename] をクリックします。

IPX Diagnostic Responder を装備していないシステム

NXPIPX は次のシステムを検出しますが、これらのシステムはアトラスに必ずしも正確に配置されるわけではありません。

- NetWare for UNIX* サーバ
- ポータブル NetWare
- アクセスサーバ
- モデムサーバ
- プリントサーバ

これらのシステムは IPX 診断に応答しないため、NXPIPX からの照会に応答できません。このため、マップにこれらのシステムを配置するのに必要な LAN 情報は利用できない場合があります。この場合、NetExplorer はこれらのシステムをアトラスの [Islands] ページに配置します。多くの場合、これらのシステムが属する各セグメントの Traffic Analysis Agent によって、NetExplorer は不足情報を取得し、システムをマップに正しく配置します。

システムが IP を実行している場合は検出され、マップに正確に配置されます。

MAC アドレスを重複使用しているルータ

NetExplorer では、ルータで使用されるアダプタ認識方法が原因で、いくつかのルータの検出が困難になることもあります。場合によっては、同じ MAC アドレスがルータの複数のネットワークインタフェースで使用されることもあります。この場合、NetExplorer は、複数のセグメントに 1 つのアダプタが接続されていると判断します。他に指定しない限り、NetExplorer は複数のアダプタを 1 つのアダプタとして解釈します。

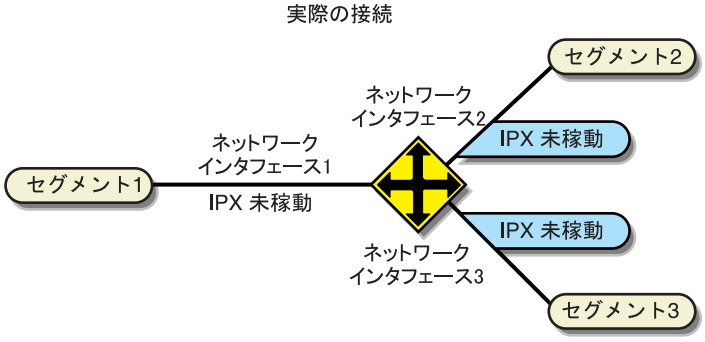
これらのアダプタに接続されている複数のセグメントは、1 つのセグメントと見なされ、NetExplorer はこれらのセグメントを統合します。

サードパーティのルータ

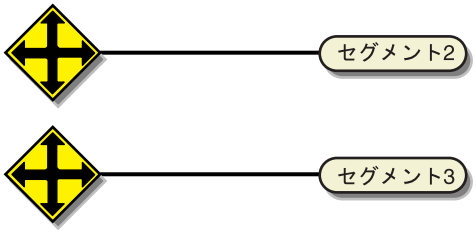
NXPIP は、IP バインドインタフェースのみを検出します。ルータで IP が実行されていない場合、NetExplorer は IPX バインドインタフェースを検出し、結果は次のようになります。

- ルータのインタフェースごとに別々のアイコンが表示されます。
- 検出されたインタフェースはアトラスの同じルータに配置されません。そのため、インターネットワークマップの相互接続は正確でなく、ルータは異なる複数のルータとして表示され、各ルータには実際のルータからの 1 つのネットワークインタフェースが含まれます。

次の図のルータでは、ネットワークインタフェース 2 と 3 では IPX が実行され、ネットワークインタフェース 1 では IPX が実行されていません。NetExplorer は、このルータを 2 つの個別のシステムとしてインターネットワークマップに配置します。図のように、セグメント 1 への接続は表示されず、セグメント 2 と 3 への接続は 2 つの個別のシステムに接続されるものとして表示されます。



ZENworks for Serversインターネットワークマップでの接続



WAN ポートを使用する Novell NetWare MultiProtocol Router

Novell NetWare MPR™ (MultiProtocol Router) 3.0 は、現在、Novell NetWare 5.*x* にバンドルされています。

IPX ネットワーク

Novell NetWare MPR 3.0 は、WAN リンクの正しいセグメントタイプを報告します。NetExplorer は、このセグメントタイプを検出し、適切なアイコンで表示します。

Novell NetWare MPR 3.0 システム間の IPXWAN リンクには、システムに関連付けられた IPX ネットワークがありません。NetExplorer はこのようなリンクを検出すると、#UNNUM -*n* という形式の WAN セグメント名を作成します。*n* は、セグメント名を一意にするために割り当てられた整数です。フレームリレーや X.25 などのマルチアクセスネットワークの場合、ネットワークの各接続には、セグメント名に他の #UNNUM -*n* が追加されます。

IP ネットワーク

Novell NetWare MPR 3.0 では、ナンバードおよびアンナンバードの両方の IP リンクを設定できます。NetExplorer は、ナンバードリンクを正確に検出します。アンナンバード IP リンクは検出されないため、[Islands] ページに表示されます。

サードパーティのルータで IP が実行され、管理サーバで NXPIP が実行される場合、NetExplorer は IP バインドインタフェースのみを検出します。ルータはアトラスに正しく表示されます。サードパーティのルータでは IP が実行されず、管理サーバでは NXPIP が実行される場合、NetExplorer は IPX バインドインタフェースを検出します。ただし、これらの IPX バインドインタフェースはアトラスの同じルータアイコンに配置されません。

オンデマンドリンク

オンデマンドリンクは、2 つのルータ間の WAN 接続であり、ユーザデータだけ (ルーティングトラフィックなし) がリンクを介して交換されます。このリンクは、データを送信するときにだけ確立されます。

NetExplorer は、十分なスタティックルーティング情報が設定されていて、管理サーバがオンデマンドリンクの接続先にアクセスできる場合に、オンデマンド IP リンクと IPX リンクを正確に検出します。

ただし、リンクがオンデマンドのアンナンバード IP リンクの場合、このリンクのリモートエンドのトポロジ全体は検出されません。NXPCON ユーティリティで、[IP Discovery] > [Additional IP Routers] の順にクリックすると、不足しているルータの追加 IP ルータアドレスを設定できます。

WAN ポートを使用するサードパーティのルータ

NetExplorer は、サードパーティのルータが MIB-II SNMP をサポートしている場合は、このルータを検出します。サードパーティのルータの中には、IP ネットワーク番号または IPX ネットワーク番号のない WAN リンクが使用されるものもあります。この場合、この WAN リンクは検出されません。

Novell NetWare Connect サーバ

NetExplorer は Novell NetWare Connect サーバを検出します。ただし、ネットワークに複数の Novell NetWare Connect® サーバがある場合、NetExplorer はこれらのサーバを統合し、1 つのサーバとして表示します。

仮想スイッチ

仮想スイッチは、アトラスマップではスイッチまたはブリッジに使われるものと同じアイコンで表示されます。仮想スイッチの表示名は、常に、「switch on *IP address of network*」として表示されます。仮想スイッチは、検出情報が不完全な場合に意味のあるネットワークトポロジを表示するために、アトラスマップで主に使用されます。アドレスが不明なため、仮想スイッチの MAC アドレスは、接続タイプに基づいてイーサネットポート、トークンリングポート、または FDDI ポートとして指定されます。

仮想スイッチは、次の条件の下でアトラスマップに表示されます。

- 2 つ以上の異なる物理メディアがスイッチによって接続され、そのスイッチがまだ検出されていないとき。仮想スイッチは、実際のスイッチが検出されるとすぐに削除されます。
- 2 つ以上の異なる物理メディアがスイッチによって接続され、そのスイッチが public 以外の SNMP コミュニティ文字列で設定され、そのスイッチの SNMP コミュニティ文字列が検出の起動前に NXPCON によって提供されなかったとき。
- 2 つ以上の異なる物理メディアが、管理不可能なスイッチまたはハブによって接続されたとき。

ネットワークセグメント

NetExplorer は次のネットワークセグメントを検出します。

- 853 ページの「LAN および WAN のセグメントタイプ」
- 854 ページの「ソースルートブリッジトークンリング」

NetExplorer は次のものを完全には検出できません。

- 855 ページの「トランスペアレントブリッジ」
- 855 ページの「設定の変更」

LAN および WAN のセグメントタイプ

NetExplorer は、次の表に示す LAN および WAN のセグメントタイプを検出します。

CIM データベースの既知のセグメント	CIM データベースの未知のセグメント
ATM	LAN:ARCnet
LAN:FDDI	LAN:LocalTalk*
LAN: イーサネット	SMDS
LAN: トークンリング	WAN:ISDN
WAN:X.25	WAN:SDLC
WAN:PPP	WAN: シリアル
WAN:Frame_Relay	WAN:T1
	WAN:T3

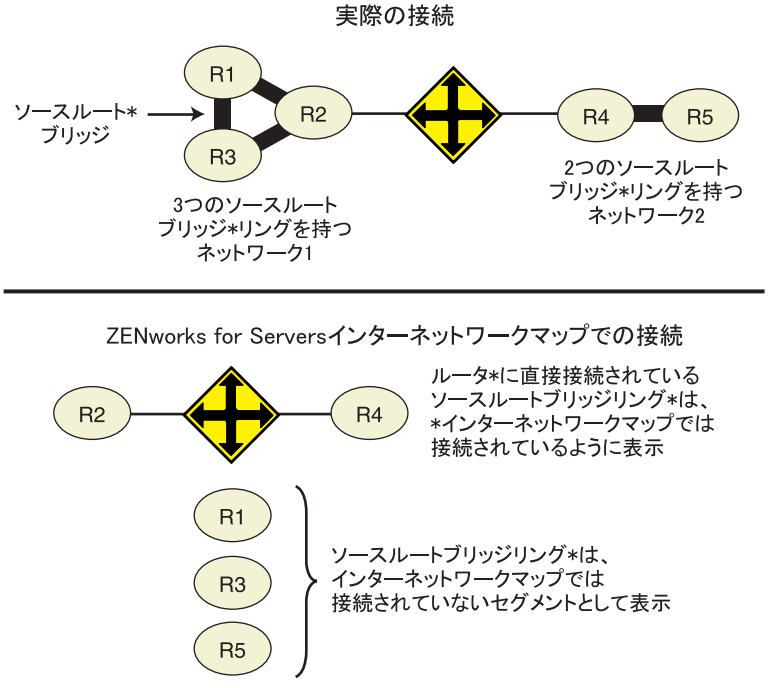
これらの値は、セグメントに接続されたシステムが MIB-II RFC 1573 からのインタフェースタイプで応答する場合に、正確に検出されます。

ソースルートブリッジトークンリング

Atlas Manager は、NetWare 版 Traffic Analysis Agent が各リングにインストールされているかどうかによって、異なる方法でソースルートブリッジトークンリングを表示します。

- NetWare 版 Traffic Analysis Agent がネットワークの各ソースルートブリッジトークンリングにインストールされていない場合、NetExplorer はこのネットワークを検出しますが、同じ IPX ネットワーク番号または IP サブネットを共有するソースルートブリッジトークンリングはすべて 1 つのセグメントに統合されます。たとえば次の図では、リング R1、R2、および R3 は 1 つのセグメントとしてインターネットワークマップに表示され、リング R4 と R5 は個別のセグメントとして表示されます。
- NetWare 版 Traffic Analysis Agent が各ソースルートブリッジトークンリングにインストールされている場合、NetWare 版の各 Traffic Analysis Agent は所属するリング（セグメント）とそのリング上のすべてのシステムを検出します。Atlas Manager は、このリングを未接続のセグメントとしてインターネットワークマップに表示します。
- NetWare 版 Traffic Analysis Agent がルータに接続されたソースルートブリッジトークンリングにインストールされている場合は、正しい接続がアトラスの［WAN］ページに表示されます。ただし、2 つのネットワークにそれぞれ複数のリングが存在し、各ネットワークの 1 つのリングだけがルータに接続されている場合、［WAN］ページには、ルータに直接接続されているリングのみについて正しい接続が表示されます。各ネットワークのその他のソースルートブリッジトークンリングは、未接続セグメントとして［WAN］ページに表示されます。

  2 つ目の例を次の図に示します。



どの場合でも、ブリッジ情報は検出されません。その結果、ソースルートブリッジの各インタフェースは、ネットワーク上の個別のシステムとして検出されます。ソースルートブリッジの各インタフェースのアトラスには、1 つのアイコンが表示されます。

NetWare 版 Traffic Analysis Agent が IPX ソースルートブリッジネットワークの各リング上の 1 つのサーバにインストールされている場合、[WAN] ページに表示されるセグメント名は、IPX ネットワーク番号と、リングに対するそのサーバのインタフェースの MAC アドレスで構成されます。NetWare 版 Traffic Analysis Agent が複数のインタフェースを監視している場合、リングに表示されるアドレスは、そのリングを監視しているインタフェースの MAC アドレスです。

トランスペアレントブリッジ

トランスペアレントブリッジは完全には検出されません。同じネットワーク番号のトランスペアレントブリッジセグメントのグループは、マップでは 1 つのセグメントに統合されます。

設定の変更

インタフェースの追加、再設定、削除など、ネットワークトポロジのほとんどの変更は検出され、アトラスに反映されます。ただし、ネットワークからシステムを削除する場合は、そのネットワークの別の場所にシステムを移動しない限り、そのシステムは検出されません。

ファイルベースの検出

IPGroper.NLM の拡張機能により、DiscNodes.txt ファイルを使用して IP アドレスと、検出されるノードセットのマスクを指定できます。ノード情報は SNMP によって取得されます。

IPGroper NLM は、DiscNodes.txt ファイルからの入力を受け付けることができるように、特定のオプションを指定してロードする必要があります。これらのオプションを指定しないと、NLM は検出時にファイルからの入力を受け付けることができません。検出を開始する前に、DiscNodes.txt ファイルを zfs-install-dir/mwserver/nmdisk ディレクトリに保存しておく必要があります。初期検出の実行後に、検出されるノードを追加する場合は、新しいノードエントリを含む DiscNodes.txt ファイルを新規作成し、同じディレクトリに保存する必要があります。これらのノードは、次の検出サイクルで照会されます。

DiscNodes.txt 入力ファイルの個々の IP アドレスの形式を次に示します。

- 個々の IP アドレスの指定形式

  IPAddress <, SubnetMask>

- 正規表現を使用したアドレス指定

  IPAddress <, SubnetMask>

  IPAddress -> AddressPattern

  AddressPattern に使用できる文字は、数字 0-9、ピリオド (.)、疑問符 (?) (1 文字を表す)、アスタリスク (*) (複数文字を表す) が最大 3 つまで。

- ワイルドカード文字は、サブネットマスクでは使用できません。

164.99.149.*	164.99.149.1 から 164.99.149.254 までのすべてのアドレス
164.99.14?.*	164.99.140.1 から 164.99.149.254 までのすべてのアドレス
164.99.149.?	164.99.149.1 から 164.99.149.9 までのすべてのアドレス

注： 164.99.149.0 はこの範囲には含まれません。? がオクテット内の唯一の文字の場合は 0 を表しません。

164.99.149.1?0 - 164.99.149.100 から 164.99.149.190 までのすべてのアドレスです。ここでは、? は 0 からの数を表します。

- テキストファイルでは、# で始まる行がすべてコメント行として処理されます。

ファイルベースの検出は、次の 2 つの場合に使用できます。

- 856 ページの「ファイルに指定されたノードの検出」
- 856 ページの「他の検出モジュールによるノードの検出」
- 856 ページの「他の検出モジュールによるノードの検出」

ファイルに指定されたノードの検出

デフォルトでは、Novell ZENworks Server Management をインストールすると、NXPCON ユーティリティにはすべての検出モジュールがロードされ、ファイルベースの検出が有効になります。

入力ファイルに指定されたノードだけを検出するには

1. NXPCON で、[Configuration Options] > [Discovery Modules] の順にクリックします。
2. [Individual Discovery Modules] を選択して、(Enter) キーを押します。
3. モジュールをアンロードするために [No] を選択し、(Enter) キーを押します。
4. (Esc) キーを押して、[Discovery Modules] ダイアログボックスを終了します。
5. [Yes] をクリックして、変更を保存します。
6. [Configuration Options] > [IP Discovery] の順にクリックします。
7. [IP Host Discovery] を選択し、(Enter) キーを押します。
8. [Enable IP Host Discovery] を選択し、(Enter) キーを押します。
9. [No] を選択して、IP ワークステーションの自動検出を無効にします。
10. [Enable File-Based Discovery] オプションが [Yes] に設定されていることを確認します。
11. (Esc) キーを押して、[IP Host Discovery] ダイアログボックスを終了します。
12. 管理サーバのプロンプトで「**unxp**」と入力し、NetExplorer をアンロードします。
13. 「**netxplor**」と入力し、NetExplorer モジュールを再ロードします。

他の検出モジュールによるノードの検出

デフォルトでは、Novell ZENworks Server Management をインストールすると、すべての検出モジュールが起動され、ファイルベースの検出が有効になります。起動するモジュールを個別に選択したり、設定を変更したりするには、次の手順に従ってください。

入力ファイルに指定されたノードだけを検出するには

1. NXPCON で、[Configuration Options] > [Discovery Modules] の順にクリックします。
2. [Individual Discovery Modules] を選択して、(Enter) キーを押します。

3 各モジュールについて、ロードする場合は［Yes］、アンロードする場合は［No］を選択し、(Enter) キーを押します。

4 (Esc) キーを押して、［Discovery Modules］ダイアログボックスを終了します。

5 ［Yes］をクリックして、変更を保存します。

6 ［Configuration Options］>［IP Discovery］の順にクリックします。

7 ［IP Host Discovery］を選択し、(Enter) キーを押します。

8 ［Enable IP Host Discovery］を選択し、(Enter) キーを押します。

9 ［No］を選択して、IP ワークステーションの自動検出を無効にします。

10 ［Enable File-Based Discovery］オプションが［Yes］に設定されていることを確認します。

11 (Esc) キーを押して、［IP Host Discovery］ダイアログボックスを終了します。

12 管理サーバのプロンプトで「**unxp**」と入力し、NetExplorer をアンロードします。

13「**netxplor**」と入力し、NetExplorer モジュールを再ロードします。

IPGROPER のコマンドラインオプション

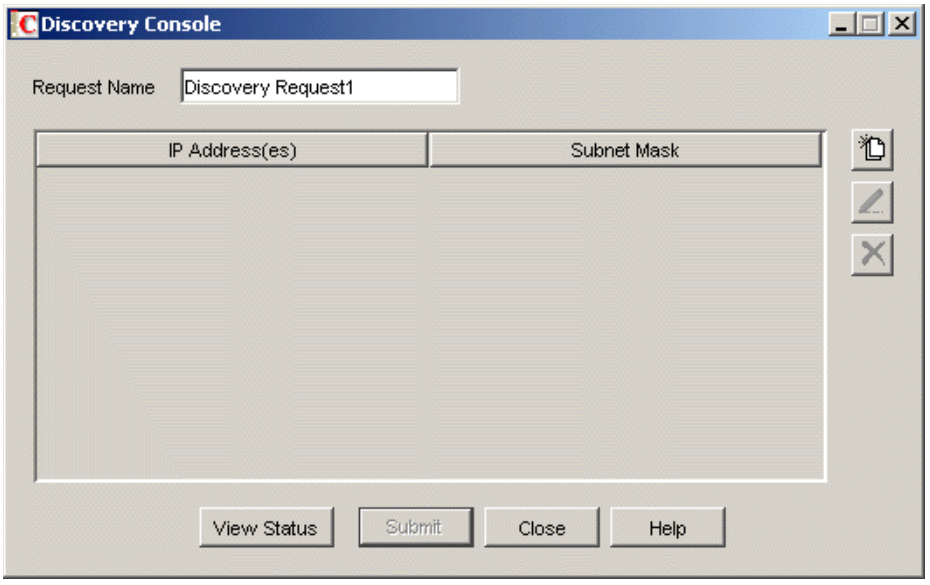
IPGROPER.NLM には、DISCNODES.TXT ファイルに指定したノードを検出する 3 つのコマンドラインがあります。

コマンドライン	説明
/Fonly	discnodes.txt ファイルに指定されたノードだけを検出します。 このオプションは、［Enable IP Host Discovery］オプションに［No］を設定し、［Enable File-Based Discovery］オプションに［Yes］を設定したときに使用できます。
/Falso	discnodes.txt ファイルに指定されたノードに加えて、IPGROPER はその他のノードも検出します。 このオプションは、［Enable IP Host Discovery］オプションと［Enable File-Based Discovery］オプションの両方に［Yes］を設定したときに使用できます。
/Flog	ノードの検出時に発生したすべてのエラーとイベントについてログを記録します。エラーとイベントは、<zfsinstall>¥mwserver¥nmdisk¥discnodesbak¥discnodeslog.log ファイルに記録されます。このコマンドラインオプションは、netxplor.ncf ファイルに手動で入力する必要があります。 **重要：** /fonly または /flog を指定したときだけ、discnodeslog.log ファイルが作成されます。

Discovery Console

Discovery Console では、Novell ConsoleOne を使用して IP アドレスのセットを検出する要求を送信できます。ホストアドレスのリスト、サブネット上のすべてのホスト、アドレス範囲、または正規表現形式のアドレスを検出できます。Discovery Console では、送信済みの要求のステータスを確認したり、要求を削除したりできます。

重要： Discovery Console を使用するには、IPGROPER が実行されていることを確認してください。



検出要求を作成して送信するには

1 Novell ConsoleOne で、[Tools] > [Discovery Console] の順にクリックします。

[Discovery Console] ダイアログボックスが表示され、[Request Name] にデフォルト名が表示されます。

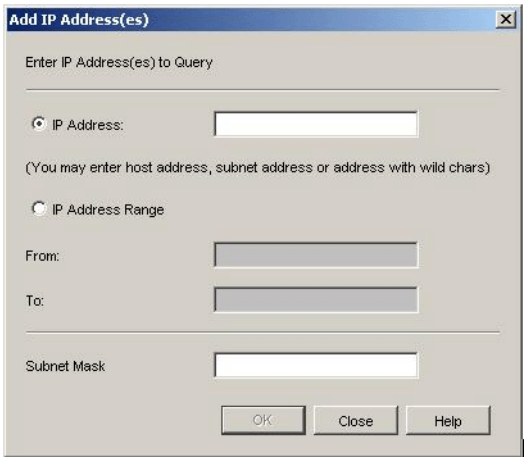
2 デフォルトの要求名を変更する場合は、別の要求名を入力します。

次の操作を実行できます。

- 858 ページの「IP アドレスの追加」
- 859 ページの「IP アドレスの編集」
- 859 ページの「IP アドレスの削除」
- 859 ページの「要求ステータスの確認」

IP アドレスの追加

1 [Discovery Console] ダイアログボックスで、  をクリックします。



2 次の情報を入力します。

- [IP Address]：ホストアドレスまたはサブネットアドレス。IP アドレスの指定には、ワイルドカード文字を使用できます。サブネットアドレスの場合は、正確なサブネットマスクを指定してください。
- [IP Address Range]：照会する IP アドレス範囲。たとえば、160.100.144.1 から 160.100.144.254 まで。
- [Subnet Mask]：指定したアドレスの正確なサブネットマスク。

3 [OK] をクリックします。

4 [Discovery Console] ダイアログボックスで、[Submit] をクリックします。

IP アドレスの編集

1 [Discovery Console] ダイアログボックスで、編集する IP アドレスを選択し、  をクリックします。

2 必要な情報を変更します。

3 [OK] をクリックします。

4 [Discovery Console] ダイアログボックスで [Submit] をクリックし、要求を送信します。

IP アドレスの削除

要求を追加していない場合は、IP アドレスを削除できます。

1 [Discovery Console] ダイアログボックスで、削除する IP アドレスを選択し、  をクリックします。

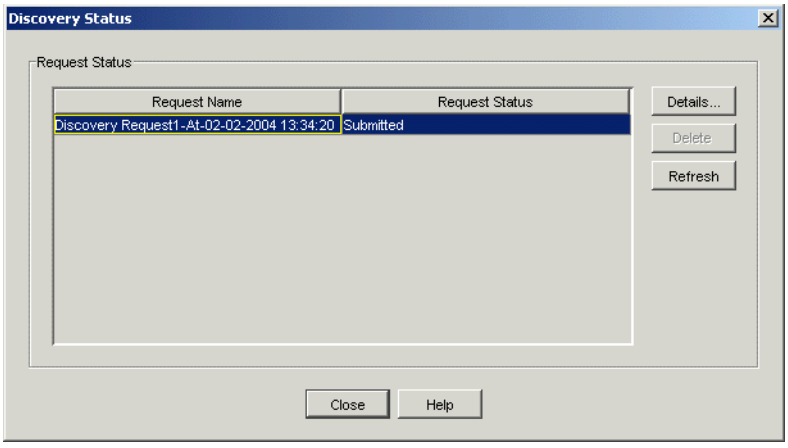
要求ステータスの確認

このオプションでは、送信済みの要求のステータスについて詳細が表示されます。要求のステータスレベルは次のいずれかです。

- [Pending]：要求が IPGROPER に送信されていません。
- [Submitted]：要求が IPGROPER に送信されました。
- [In Progress]：要求が IPGROPER によって処理されています。
- [Completed]：要求が IPGROPER によって処理されました。

要求のステータスを確認するには

1 [Discovery Console] で要求を選択し、[View Status] をクリックします。



次の操作を実行できます。

- [Details]：表で選択された要求の詳細を表示します。
- [Delete]：選択した要求を削除します。ステータスが［pending］の場合は、要求を削除できます。
- [Refresh]：要求の現在のステータスを表示します。

マップに反映される検出結果

管理サーバの Atlas Manager は、トポロジデータベースが作成されるとアトラスデータベースを作成し、Novell ConsoleOne のマップとして情報を表示します。［WAN］ページには、領域ページおよび接続されたルータがすべて表示されます。領域ページには、セグメントおよび接続されたルータが表示されます。

検出されたシステムは、接続されたルータまたはブリッジに基づき、アトラスの領域ページに配置されます。［Islands］ページには、ルータが検出されないセグメントが格納されます。接続されたルータが検出されると、Atlas Manager は適切なページにセグメントを再配置します。

マップに反映される検出結果の詳細については、次の節を参照してください。

- 860 ページの「ソースによる名前の優先度」
- 861 ページの「アトラスのシステム表示」

ソースによる名前の優先度

検出サイクルが進行し、より多くの情報が検出されると、マップに表示される名前が変更される場合があります。名前の情報ソースに応じて、異なる優先度が名前に与えられています。名前が検出されない場合は、ノードの IP/IPX アドレスがノード名として表示されます。

Atlas Manager では、検出されたオブジェクトの名前が、次のリストの順序に従って表示されます。

1. ユーザ定義名
2. DNS 名
3. Novell eDirectory 名
4. バインダリ名
5. SNMP 名

アトラスのシステム表示

システムがマップに表示される際に、Atlas Manager は次のリストの順序でサービスを参照します。最初のサービスがノードに関連付けられるとすぐに表示され、その他のサービスとの一致については確認されません。検出時に、より高い優先度のサービスが後から検出された場合は、アイコンが変更されることがあります。

優先順位	アイコン	説明
1.		Server Management Agent ソフトウェアを実行している NetWare サーバ
2.		Server Management Agent ソフトウェアを実行している Windows サーバ
3.		MS エンジンを実行している SFT III サーバ
4.		ファイルサーバソフトウェアを実行しているサーバ
5.		IP サービスを実行しているルータ
6.		IPX サービスを実行しているルータ
7.		スイッチまたはブリッジ
8.		検出プロセスを実行しているサーバ
9.		トポロジデータベースを実行しているサーバ
10.		トラフィック分析 (Traffic Analysis) エージェントソフトウェアを実行している NetWare サーバまたは Windows サーバ
11.		Remote Monitoring を実行しているサーバ
12.		Remote Monitoring II を実行しているサーバ

優先順位	アイコン	説明
13.		プリントサーバソフトウェアを実行しているサーバ
14.		IP ソフトウェアを実行しているサーバ
15.		NetWare Connect ソフトウェアを実行しているサーバ
16.		ルータ
17.		プリンタ
18.		IP ワークステーション
19.		IPX ワークステーション
20.		その他

システムに IPX または IP ルータサービスがある場合、Atlas Manager はそのシステムをルータと判断し、適切なページのセグメントに表示します。

検出のセットアップ

管理サーバの検出ソフトウェアは、ネットワーク上のノードを自動的に検出します。ネットワークノードとは、サーバ、デスクトップ、ルータ、ハブ、スイッチ、およびその他のネットワークデバイスです。サーバ上の Consolidator が、検出されたデータのデータベースを作成します。サーバ上の Atlas Manager が、このデータベースを読み取ってアトラスを作成します。

Novell ZENworks Server Management では、異なる 2 つの環境で検出を実行できます。

- ピュア IP 環境
- IP/IPX 環境

  Novell ConsoleOne と管理サーバ間で IP を有効にしておく必要があります。

検出を開始する前に、次の設定を確認して、検出システムが適切に設定されていることを確認してください。

- Novell ZENworks Server Management サーバに接続されているルータが、NXPCON でシードルータとして指定されていることを確認します。必要に応じて、IP ルータも追加して指定します。シードルータの指定と IP ルータの追加に関する詳細については、871 ページの「シードルータと追加 IP ルータの指定」を参照してください。
- 管理するすべてのデバイスに使用されるコミュニティ文字列がNXPCONで指定されていることを確認します。SNMP コミュニティ文字列の変更の詳細については、867 ページの「SNMP コミュニティ文字列の変更」を参照してください。
- 指定されたIPアドレスだけにアクセスが制限されるようにルータが設定されている場合、ネットワーク上のルータに照会する権利が Novell ZENworks Server Management サーバに与えられていることを確認します。IP ルータ検出の詳細については840 ページの「IP ネットワークだけの IP ルータ検出」を参照してください。
- IP または IPX 検出のスコープを制限する場合は、適切なスコープエントリを指定します。検出スコープの変更の詳細については、868 ページの「検出スコープの変更」を参照してください。
- DNS 設定ファイル sys:¥etc¥resolv.cfg に、有効な DNS サーバの IP アドレスが指定されていることを確認します。有効な DNS サーバが指定されていない場合は、ホストの DNS 名が検出されません。
- 有効な検出を実行するために、検出および管理する各ネットワークセグメントに Traffic Analysis Agent がインストールされ、実行されていることを確認します。これらのエージェントの名前とアドレスが、NXPCON で指定されていることも確認します。Traffic Analysis Agent の指定の詳細については、871 ページの「NXPLANZ によって照会される Traffic Analysis Agent の指定」を参照してください。
- MAC アドレスが異なるネットワーク番号に関連付けられている場合、そのようなネットワーク番号はすべて 1 つのセグメントに統合されます。統合されないようにするには、*installation_directory*¥mms¥mwserver¥bin¥consolidator.ini ファイルで、そのような MAC アドレスをすべて大文字で指定する必要があります。

  MAC アドレスは、consolidator.ini ファイルの［DuplicateMacAddress］で、キーと値のペアとして指定します。

  次に consolidator.ini の例を示します。

  ```
  [DuplicateMacAddress]

  mac1="00C04F59910D"

  mac2="00C04F5991AB"

  ...

  key_name=value
  ```

  キーは consolidator.ini 内で一意になるようにしてください。

  Novell ZENworks Management and Monitoring Services サーバを起動する前に、*zenworks_installation_directory*¥mms¥mwserver¥properties¥sloader.properties ファイルを編集して、TOPOLOGY MANAGER の下の ARGUMENTS 値にエントリ「-ini ″installation_directory¥mms¥mwserver¥bin¥consolidator.ini″」を追加してください。

次のタスクは、最初の検出時に実行され、組織のニーズに合わせて検出をカスタマイズする際に役立ちます。

- 864 ページの「検出の開始」
- 864 ページの「初期検出のステータスの確認」
- 865 ページの「検出結果の確認」
- 866 ページの「デフォルト設定の変更」
- 872 ページの「Java プロセスの設定」
- 874 ページの「管理サーバのアンロード」

検出の開始

検出ソフトウェアが管理サーバにロードされると、自動検出が開始されます。

自動検出を手動で開始し、バックエンドサービス (Management Site Services) をロードするには、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」の手順を参照してください。

管理サーバの再起動

管理サーバをメンテナンスなどで停止する場合、検出は再起動によって次の影響を受けます。

- 検出モジュールを再ロードするたびに、新しいバージョンの netexplor.dat が作成されます。
- 初期検出サイクルが再度開始されます。
- Novell ZENworks Server Management がネットワークを再検出すると、Consolidator はすべての検出データを再処理します。

検出モジュールをアンロードするには

1 NetExplorer サーバで「**unxp**」と入力します。

検出モジュールをロードするには

1 NetExplorer サーバで「**netxplor**」と入力します。

初期検出のステータスの確認

検出が進行すると、Novell ConsoleOne のトポロジマップに検出データが反映されます。ただし、大規模ネットワークでは、初期検出が終了するまでに 1 ～ 2 日かかる場合があります。

初期検出が終了したかどうかを簡単に判断するには、管理サーバで NXPCON ユーティリティを使用して、各 NetExplorer モジュールのステータスを確認します。マップ全体を表示するには、各モジュールが少なくとも 1 サイクルを終了している必要があります。

検出ステータスを知るには、NXPCON 画面の上部にある検出ステータスフィールドを確認します。この画面へのアクセス方法については、866 ページの「検出設定ユーティリティの使用」を参照してください。

NXPCON の主画面には、検出ステータスの監視に使用できる情報が表示されます。

次の情報が表示されます。

- **[NetExplorer Up Time]**：NetExplorer が実行を開始してからの時間が表示されます。
- **[NetExplorer System Status]**：全体的なステータスが表示されます。次の値のいずれかが表示されます。
  - [Waiting to start] - 1 つまたは複数の検出モジュールが起動を待機しています。
  - [Running] - 検出モジュールが実行中です。
- **[Module Status]**：各モジュールのステータスと各モジュールが終了したサイクル数が表示されます。次の値のいずれかが表示されます。
  - [Not Loaded] - モジュールがロードされていません。
  - [Waiting to Start] - モジュールはロードされていますが起動されていません。
  - [Running] - モジュールは実行中で、データを収集しています。
  - [Suspended] - モジュールは、実行スケジュールを終了したため、停止しています。
  - [Completed] - モジュールは検出サイクルを完了しています。
  - [Unknown] - NetExplorer がモジュールのステータスを取得できません（通常、これはモジュールがロードされていない場合に表示されます）。

検出結果の確認

初期検出後に、Consolidator によるデータベースの更新が終了したら、ネットワークトポロジがマップに正確に表示されているかどうかを確認します。

ノードがマップに表示されない場合は、NetExplorer がそのノードタイプを検出していない場合があります。ノードが正しいセグメントに表示されない場合は、NetExplorer がノードを正確に配置するのに十分な情報を取得していない場合があります。詳細については、847 ページの「検出されるネットワークオブジェクト」を参照してください。次の特性が認識されます。

- IP - IP ルータ、IP ホスト、および IP サービス（HTTP、Telnet、SMTP、DNS、FTP、および DHCP）の検出
- IPX - IPX ワークステーション、IPX ルータ、および IPX サービス（ファイル、印刷、その他の SAP（Service Advertising Protocol））の検出
- サブネットマスク
- サービス
- Novell eDirectory の名前とツリー
- DNS 名

管理サーバ上の Consolidator は、NetExplorer と通信してネットワーク検出データを取得します。Consolidator は、netexplor.dat ファイルを読み取ってデータベースを作成します。

重要： NETEXPLOR.DAT ファイルは、NetExplorer が再起動されるたびにリセットされます。

Consolidator は、Bridge エージェントと SN3 エージェントの 2 つの Java* コンポーネントと通信します。Bridge エージェントは、ネットワークに存在するブリッジと、ネットワークの関連トポロジを取得します。SN3 エージェントは、SLP を使用して NetWare 5.*x* サーバを検出し、検出された各 IP アドレスおよび IPX アドレスに対応する Novell eDirectory 名を取得します。

重要： NetExplorer と Consolidator は、管理サーバ上で互いに影響を及ぼすことなく実行できます。

NetWare 5.*x* は SLP (Service Location Protocol) をサポートしているため、NetWare 5.*x* サーバは他のサーバより短時間で検出されます。

検出完了の確認

IPX ワークステーションは、Management Agent ソフトウェアを実行している NetWare サーバにユーザがログインしているか、または接続している場合は、ユーザ名で検出されます。ネットワークの IPX デバイスと IPX ワークステーションのユーザ名が必ず検出されるようにするには、ユーザがログインするすべての NetWare サーバに Management Agent をインストールします。

NetExplorer が AppleTalk* デバイスを検出するようにするには、各セグメントのサーバに NetWare Traffic Analysis Agent をインストールする必要があります。

デフォルト設定の変更

検出ソフトウェアは、最適な環境で動作するように設計されたデフォルト設定でインストールされます。ただし、ネットワークまたはデータがデータベースに検出されない場合は、検出を再設定する必要があります。

詳細については、次の節を参照してください。

- 866 ページの「検出設定ユーティリティの使用」
- 867 ページの「ロードする検出モジュールの選択」
- 867 ページの「SNMP コミュニティ文字列の変更」
- 868 ページの「検出スコープの変更」
- 871 ページの「NXPLANZ によって照会される Traffic Analysis Agent の指定」
- 871 ページの「シードルータと追加 IP ルータの指定」

検出設定ユーティリティの使用

NXPCON ユーティリティを管理サーバで使用すると、検出の設定を変更できます。たとえば、検出スコープを変更したり、初期検出プロセスのステータスを確認したりできます。

NXPCON ユーティリティにアクセスするには

1. 管理サーバのサーバコンソールに、サーバプロンプトから直接、またはリモートでアクセスします。
2. 検出モジュールがすでにサーバにロードされている場合は、[Available Screens] ウィンドウで [NetExplorer Console Utility] オプションをクリックします。

   または

   検出モジュールがロードされていない場合は、サーバプロンプトで「**netxplor**」と入力します。

NetExplorer がロードされ、管理サーバでアクセスできるようになると、NXPCON が自動的にロードされます。

NXPCON が管理サーバにロードされない場合は、NetExplorer が実行されているかどうかを確認してください。NetExplorer が実行されている場合は、システムのコンソールプロンプトで「**load nxpcon**」と入力します。NetExplorer が実行されていない場合は、システムのコンソールプロンプトで「**netxplor**」と入力します。

ロードする検出モジュールの選択

デフォルトでは、Novell ZENworks Server Management をインストールすると、NXPCON ユーティリティがロードされ、すべてのモジュールが起動されます。ネットワークで IPX を使用していない場合は、NXIPX モジュールをロードしないように NXPCON を設定できます。

重要： TCP/IP が、サーバのネットワークボードのうち、少なくとも 1 つのボードにバインドされていることを確認してください。

ロードするモジュールを確認または変更するには

1. NXPCON で、[Configuration Options] > [NetExplorer Modules] の順にクリックします。
2. 変更するフィールドを選択し、(Enter) キーを押します。
3. モジュールをロードする場合は [Yes]、アンロードする場合は [No] を選択し、(Enter) キーを押します。
4. (Esc) キーを押して、[NetExplorer Modules] ダイアログボックスを終了します。
5. [Yes] をクリックします。

   IP ホスト検出またはファイルベース検出を有効にできます。次の手順で有効または無効にします。

   5a. [Configuration Options] > [IP Discovery] の順にクリックします。

   5b. [IP Host Discovery] または [File Based Discovery] を選択し、(Enter) キーを押します。検出オプションを有効にするには [Yes] を、無効にするには [No] を押します。
6. 管理サーバのプロンプトで「**unxp**」と入力し、NetExplorer をアンロードします。
7. 「**netxplor**」と入力し、NetExplorer モジュールを再ロードします。

SNMP コミュニティ文字列の変更

Novell ZENworks Server Management のデフォルトのコミュニケーション文字列は PUBLIC です。組織の SNMP コミュニケーション文字列が PUBLIC でない場合は、NXPCON で SNMP コミュニケーション文字列を再設定します。

注： ルータへの負荷を避けるため、組織の中には、制御レベルをもう 1 つ追加して、特定の IP アドレスだけがルータへの SNMP 照会を実行できるようにしているところもあります。この場合は、Novell ZENworks Server Management サーバに指定した IP アドレスが、ネットワークのルータに照会できることを確認してください。照会できない場合は、完全な検出結果が得られず、アトラスの [Islands] ページには不十分なネットワーク情報が表示されます。

IP および IPX 検出で使用するコミュニティ文字列などの SNMP 設定情報を表示、追加、変更または削除するには

1. NXPCON で、[Configuration Options] > [SNMP] の順にクリックします。
2. [SNMP] ダイアログボックスで、[Edit Community Name List] をクリックします。

3 コミュニティ文字列を追加するには、(Insert) キーを押します。

または

コミュニティ文字列を変更するには、コミュニティ文字列をクリックし、(Enter) キーを押します。

または

コミュニティ文字列を削除するには、コミュニティ文字列をクリックし、(Delete) キーを押します。

4 (Esc) キーを押し、[Configuration Options] ウィンドウから [Activate Changes] をクリックします。[Activate Changes] の詳細については、872 ページの「NetExplorer の SNMP 環境設定の自動更新」を参照してください。

5 表示されるメッセージに従います。

[SNMP] ウィンドウのその他の設定オプションについては、866 ページの「検出設定ユーティリティの使用」を参照するか、または Novell ConsoleOne のオンラインヘルプを参照してください。

検出スコープの変更

NXPCON は、デフォルトではすべての IPX ネットワークと IP ネットワークを検出するように設定されています。ただし、検出スコープは制限できます。

たとえば、IPX アドレスまたは IP サブネットアドレスが検出されるように制限できます。大規模ネットワークを管理する場合は、検出スコープを設定してネットワークの一部が検出されるように制限すると、ネットワークトラフィックが減少するためアトラスを管理しやすくなります。

検出スコープを正しく指定しないと、ターゲットデバイスを検出できません。そのため、検出するターゲットデバイスにつながるパスに存在するすべてのデバイスを、スコープに指定することは必須です。

次に例を挙げます。

検出サーバ D1 はネットワーク N1 に接続されています。ルータ R1 は、ネットワーク N2 を N1 と接続しています。ここでは、ネットワーク N2 を検出する必要があるとします。検出するには、次のエントリをスコープに指定する必要があります。

- サブネットマスク 255.255.255.255 の検出サーバ D1
- サブネットマスク 255.255.255.255 のルータ R1
- 適切なサブネットマスク番号のネットワーク N2

この例では、ネットワーク N2 はルータ R1 を介して検出サーバからアクセスされます。そのため、R1 がルーティングするネットワーク N1 に興味がない場合でも、R1 はスコープに指定する必要があります。

初期検出後に、ノードがネットワークから取り除かれても、データベースをリセットするまでそのノードはデータベース内に保持されます。

先に実行した検出によってすでにデータベースに存在しているデバイスは、検出スコープを変更しても影響を受けません。特に、より広いスコープ（またはスコープなし）で検出されたデバイスは、後から検出を実行する際にスコープを制限しても削除されません。スコープに指定したデバイスだけをアトラスに表示する場合は、データベースをリセットして、スコープの範囲外のセグメントとデバイスがアトラスに表示されないようにする必要があります。データベースをリセットすると、アラームやアラーム処理などのデータは、移動しておかない限り失われます。スコープの範囲外にあるデバイスの数が少ない場合は、Database Object Editor を使用してデバイスをデータベースから手動で削除することもできます。

検出するマスクフィールドで指定された IPX ネットワーク番号または IP アドレス範囲を入力して、IP または IPX 検出スコープを制限できます。IP または IPX スコープの制限を表示するには

1 NXPCON の［Configuration Options］ウィンドウで、［Discovery Scope］をクリックします。

2 ［IP Discovery Scope］または［IPX Discovery Scope］を選択します。

3 検出スコープを表示または設定するには、(Enter) キーを押します。

4 IP または IPX の新しい検出スコープエントリを追加するには、(Insert) キーを押します。

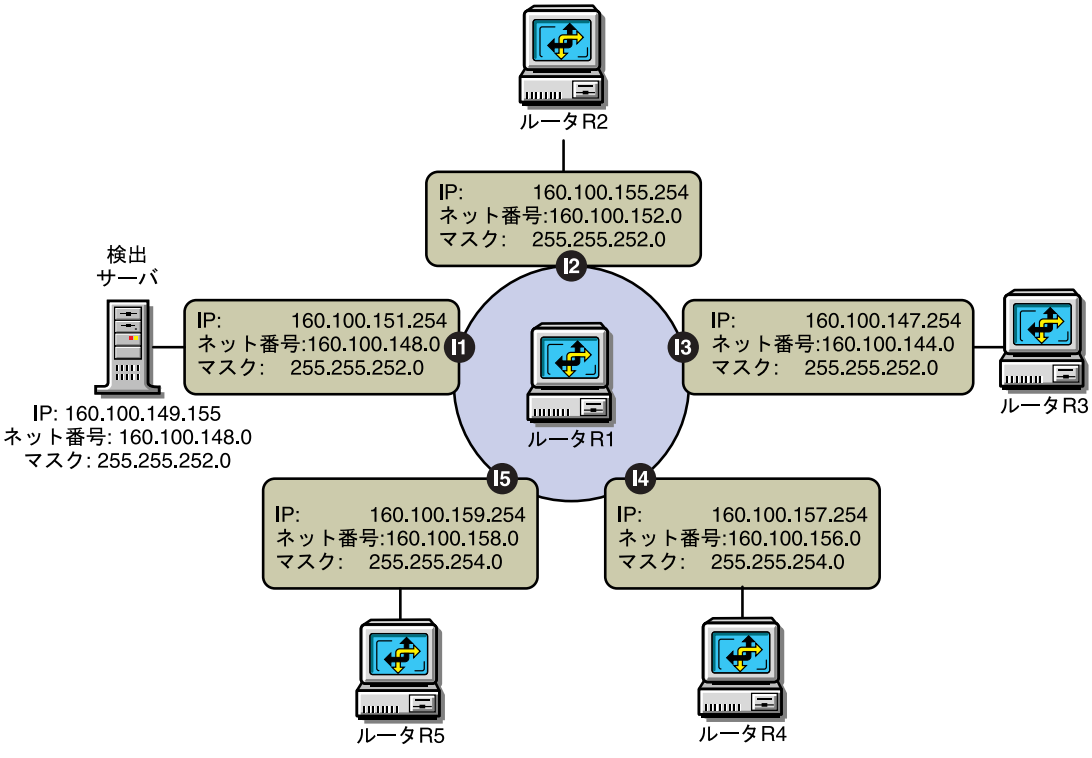
または

検出スコープエントリを変更するには、(Enter) キーを押します。

または

検出スコープエントリを削除するには、(Delete) キーを押します。

IP ネットワークの場合： 検索スコープはネットワーク番号にバインドされます。スコープは、次の図に示すように、特定のネットワークによって制限できます。



ケース 1: 160.100.148.0 を除外し、他の 4 つのネットワークを検出するには、スコープを次のように指定します。

160.100.149.155, 255.255.255.255

160.100.151.254, 255.255.255.255

160.100.144.0, 255.255.252.0

160.100.152.0, 255.255.252.0

160.100.156.0, 255.255.254.0

160.100.158.0, 255.255.254.0

ローカルネットワークの Novell ZENworks Server Management サーバとルータインタフェースのマスク 255.255.255.255 は、コンピュータ固有のスコープとして機能します。これにより、ネットワーク 160.100.148.0 の他のコンピュータは検出されなくなります。

ケース 2: ローカルネットワーク 160.100.148.0 だけを検出するには、スコープを次のように指定します。

160.100.148.0, 255.255.252.0

ネットワーク 160.100.148.0（マスク :255.255.252.0）の IP アドレス範囲は、160.100.148.1 から 160.100.151.254 までです。

ネットワーク上のすべての重要なサーバの IP アドレス範囲が 160.100.149.1 から 160.100.149.254 までの場合を考えます。次のスコープを指定する可能性があります。

160.100.149.0,255.255.255.0

このスコープは、検出システムによって許可されません。サブネットの一部だけを検出するスコープは設定できません。スコープにはサブネット全体を設定する必要があります。

ケース 3:160.100.156.0 と 160.100.158.0 だけを検出するには、スコープを次のように指定します。

160.100.149.155, 255.255.255.255

160.100.151.254, 255.255.255.255

160.100.156.0, 255.255.254.0

160.100.158.0, 255.255.254.0

最後の 2 つのスコープエントリを、1 つのエントリ 160.100.156.0, 255.255.252.0 と置き換えると、同じ効果を得ることができません。

2 つ以上のサブネットを含む 1 つのスコープエントリを作成することはできません。スコープはサブネットごとに作成する必要があります。

IPX ネットワークの場合： 1 つの IPX ネットワーク番号とマスクを入力することにより、検出される IPX ネットワークのスコープ制限します。

マスクは、一致する必要のあるネットワーク番号部分を示しています。マスクの F は対応する桁が一致している必要があり、0（ゼロ）は一致する必要がないことを意味しています。

たとえば、ネットワーク番号が 12340000 でマスクが FFFF0000 の場合は、1234 で始まるネットワーク番号と一致します。

ネットワーク番号が C00000FF でマスクが FF0000FF の場合は、C0 で始まり FF で終わるネットワーク番号 (C01234FF または C00000FF) と一致します。

5 検出スコープのアドレスとマスクを入力します。

6 (Esc) キーを押し、[Yes] をクリックして設定ファイルへの変更を保存します。

7 (Esc) キーを押して、[Discovery Scope] ウィンドウに戻ります。

8 NetExplorer をアンロードして再ロードするか、または管理サーバを再起動して、変更を反映します。

NXPLANZ によって照会される Traffic Analysis Agent の指定

ネットワークの Traffic Analysis Agent は、通常は NXPLANZ モジュールによって検出されます。ネットワーク上で SLP が無効になっているか、またはルータに SAP パケットのフィルタが適用されていると、NXPLANZ はネットワークの Traffic Analysis Agent をすべて検出できない場合があります。

Traffic Analysis Agent が NXPLANZ モジュールによって照会されるように設定するには

1 NXPCON で、[Configuration Options] > [NXPLANZ Discovery] の順にクリックします。

2 エージェントを追加するには、(Insert) キーを押します。

3 検出スコープのアドレスとマスクを入力します。

4 (Esc) キーを押し、[Yes] をクリックして設定ファイルへの変更を保存します。

5 NetExplorer をアンロードして再ロードするか、または管理サーバを再起動します。

6 エージェントを変更するには、エージェントを選択し、(Enter) キーを押します。必要な情報を変更します。

7 エージェントを削除するには、エージェントを選択し、(Delete) キーを押します。

シードルータと追加 IP ルータの指定

シードルータは、Novell ZENworks Server Management サーバが接続されているルータです。有効なルータ検出のために、NXPCON を使用してシードルータを常に指定し、Novell ZENworks Server Management サーバがシードルータに照会できるように、NXPCON で適切なコミュニティ名を指定してください。

ネットワークの一部を検出するときに、Novell ZENworks Server Management サーバが中間ルータの 1 つにアクセスできない場合は、追加 IP ルータを指定する必要があります。

シードルータまたは追加 IP ルータを指定するには

1 NXPCON で、[Configuration Options] > [IP Discovery] > [IP Router Discovery] の順にクリックします。

IP シードルータのデフォルトは <local> で、これは Novell ZENworks Server Management サーバです。

2 シードルータを追加するには、[IP Seed Router] を選択し、(Enter) キーを押します。

3 IP アドレスを入力します。

4 追加ルータを追加するには、[Additional IP Routers] を選択し、(Enter) キーを押します。

5 IP アドレスを入力します。

6 (Esc) キーを押し、[Yes] をクリックして設定ファイルへの変更を保存します。

7 NetExplorer をアンロードして再ロードするか、または管理サーバを再起動します。

NetExplorer の SNMP 環境設定の自動更新

NetExplorer の SNMP 環境設定 (SNMP のコミュニティ文字列など) を変更するときに、NetExplorer を再起動することなく自動的に更新することができます。NetExplorer を新しい設定で自動的に更新するには、NXPCON の [Options] ウィンドウで [Activate Changes] を選択します。

ただし、NXPCON の他の環境設定オプション (たとえば検出スコープなど) を変更した場合は、NetExplorer を再起動して変更を適用する必要があります。NetExplorer を再起動する方法については、873 ページの「検出 NLM ファイルの停止と起動」を参照してください。

Java プロセスの設定

検出システムの Java プロセスは次の 3 つです。

- Topology Manager
- Bridge Discovery
- SN3 Discovery

これらの Java プロセスは、Management Site Server の一部を構成し、*installation_path*¥novell zenworks¥mms¥mwserver¥properties ディレクトリの sloader.properties ファイル内のセクションとして存在します。これらは、次の形式で指定されます。

```
[Topology Manager]
Name = Topology Manager
Load Option = auto
Other options
```

Java プロセスを設定するには

1. Load Option の値を Auto から Manual に変更して、次にサーバで SLOADER コマンドを入力したときにプロセスが起動されないようにします。

   重要： Management Site Server の起動後に sloader.properties ファイルを変更した場合は、Management Site Server を再起動して変更を反映する必要があります。

2. sloader.properties ファイルの Load Properties オプションと Load Sequence オプションは変更しないでください。これらは、Management Site Server が正常に動作するために必要なオプションです。

検出の開始と停止のカスタマイズ

検出 NLM ファイルまたは Java 検出プロセスは、サイトサーバのその他のサービス（Alarm Manager サービスなど）に影響を与えずに、停止または起動できます。

検出 NLM ファイルの停止と起動

検出 NLM ファイルを停止するには、サーバコンソールで「**UNXP**」と入力します。

検出 NLM ファイルをすべて起動するには、サーバコンソールで「**NETXPLOR**」と入力します。

注： Java プロセスの実行中は検出 NLM ファイルを起動できません。Java プロセスを停止してから、サーバコンソールで「**NETXPLOR** 」と入力して、すべての検出 NLM ファイルを起動してください。

Java 検出サービスの停止と起動

検出 NLM ファイルを停止するには、サーバコンソールで「**STOPDIS**」と入力します。

検出 NLM ファイルをすべて起動するには、サーバコンソールで「**STARTDIS**」と入力します。

Java 検出プロセスの起動または停止は、どの時点でもカスタマイズできます。たとえば、Bridge Discovery を最初は実行せず、後から実行することにします。このような場合は、すべてのサービスを停止して再起動する必要はありません。

次の内容を含む、¥Novell ZENworks¥mms¥mwserver¥bin ディレクトリの startdis.ncf ファイルを編集します。

```
MWSETENV.NCF

java -Xbootclasspath/p:$mwxbpath -classpath
$MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.Start "Topology
Manager" "Bridge Discovery" "SN3 Discovery" <ip address of the server> sloader
```

このファイルでは、SN3 Discovery などの Java 検出プロセス名は、sloader.properties ファイルのセクションの名前と一致している必要があります。NCF ファイル内の名前を変更するだけで、Java 検出サービスを個別に停止および起動する同様の NCF ファイルを作成できます。たとえば、Bridge Discovery プロセスだけを起動するには、次の手順に従ってください。

1. 次の内容を持つ startbri.ncf ファイルを作成します。

   ```
   mwsetenv.ncf

   java -Xbootclasspath/p:$mwxbpath -classpath
   $MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.Start "Bridge
   Discovery" <ip address of the server> sloader
   ```

2. startbri.ncf file ファイルを ¥novell zenworks¥mms¥mwserver¥bin ディレクトリにコピーします。
3. startbri.ncf ファイルを実行して、Java 検出ブリッジサービスを起動します。

SN3 エージェントの Java 検出プロセスを停止するには、次の手順に従ってください。

1. 次の内容を持つ stopsn3.ncf ファイルを作成します。

   ```
   mwsetenv.ncf

   java -Xbootclasspath/p:$mwxbpath -classpath
   $MMSCP;$CLASSPATHcom.novell.utility.servicemanager.ui.Stop "SN3
   Discovery" <ip address of the server> sloader.
   ```

管理サーバのアンロード

管理サーバをアンロードするには

1 サーバを再起動できない場合は、すべての Service Loader プロセスが存在していることを確認します。サーバコンソールプロンプトで、次のように入力します。

stopService.ncf

このプロセスでは、サービスのアンロードに時間がかかる場合があります。

"com.novell.zfs.mms.utility.servicemanager.zfs_MMS_Services" および "com.novell.zfs.mms.utility.servicemanager.zfs_MMS_LanzSlpDis" のステータスを確認するには、サーバコンソールプロンプトで「**java - show**」と入力します。

その他の Java プロセスをすべて終了するには、「**java -exit**」を使用します。すべてのサービスが終了していない場合は、Java をアンロードします。

2 ネーミングサーバを使用する他の ZENworks 6.5 Server Management コンポーネントまたは ZENworks 6.5 Desktop Management コンポーネントを実行していない場合は、「**stopmms -n** 」と入力して、すべての ZENworks 6.5 Server Management コンポーネントをアンロードします。

3 (Ctrl)+(Esc) を押して Sybase* プロセスに切り替え、「**q**」と入力して Sybase データベースエンジンを終了します。

アトラスの管理

初期検出の終了後に、管理サーバで実行している検出を停止できます。ただし、Atlas Manager によるデータベースのアクセスは継続できます。検出サイクルは、次回の NetExplorer の起動時に、再度開始されます。データベースが Consolidator によって作成され、アトラスページが Atlas Manager によって自動的に更新されます。

ネットワークのサイズによって、初期検出時のデータの書き込みには数分から数日かかる場合があります。後続の検出サイクルがデータベースの更新に要する時間は、実質的には少なくなります。

- 874 ページの「アトラスの使用」
- 881 ページの「統合ビューの使用」

アトラスの使用

Novell ZENworks Server Management を最初にインストールすると、Atlas Manager のサーバモジュールが管理サーバに自動的にインストールされ、Atlas Manager のクライアントモジュールが Novell ConsoleOne にインストールされます。管理サーバ上の Atlas Manager は、システムアトラスを作成し、データベースのグラフィックビューをコンソールに提供します。

サーバ上の Atlas Manager は、データベースを読み取り、[Console] ビューと [Atlas] ビューの 2 つのデータベースビューを Novell ConsoleOne に提供します。両方のビューには、検出されたネットワークトポロジ、ノードの物理的な場所、ノード設定情報、およびアラーム情報が表示されます。

次の節では、アトラスの使用について説明します。

- 875 ページの「アトラスへのアクセス」
- 876 ページの「アトラス管理に役立つ役割の割り当て」
- 876 ページの「アトラスを使用したトラブルシューティング」
- 877 ページの「カスタムマップ」
- 880 ページの「ノード名の順序」

アトラスへのアクセス

Novell ZENworks Server Management のアトラスには Novell ConsoleOne からアクセスできます。Novell ConsoleOne を開き、Novell ZENworks Server Management のドメインネームスペースをダブルクリックして、ドメインを展開します。これにより、システムアトラスが表示されます。

次の表は、Novell ZENworks Server Management アトラスを構成する 3 つのページを示しています。

アトラスページ	アイコン	説明
[WAN] ページ		ネットワーク全体の概要を表示し、WAN 関連のネットワークトポロジを明確に示します。通常、アトラスに表示される [WAN] ページは 1 つだけです。
領域ページ		ネットワークのセグメントを表示します。アトラスには、複数の領域ページが表示される場合があります。たとえば、地理的な位置に基づいて、アトラスが分割される場合があります。サンノゼの企業がドイツに海外支店を持っている場合は、サンノゼのネットワークを Area1、ドイツのネットワークを Area2 として、ネットワークを分割できます。
[Islands] ページ		接続が決定されていないセグメントで構成されます。[Islands] ページは、検出時に完全に検出されていないネットワークオブジェクトのプレースホルダに相当します。アトラスに表示される [Islands] ページは 1 つだけです。

[Atlas] ビューのカスタマイズ

[Atlas] ビューは、次の 3 つの方法でカスタマイズできます。

- アトラスページの背景にカスタムビットマップを挿入する。
- アトラスページのノードの位置を、ドラッグして変更する。
- オブジェクトを代替名で表示する。

アトラス管理に役立つ役割の割り当て

Novell ZENworks Server Management では、アトラスを管理する役割を割り当てることができます。役割を割り当てることによって、ユーザによるオブジェクトへの特定の操作を制限できます。

ヒント： アトラスには、ネットワーク上の役割に基づくマップが表示されます。たとえば、セグメント A と B の特定のサーバを管理するように役割が制限されている場合、アトラスにはセグメント A と B のそのサーバのみが表示されます。

[Atlas] ビューが Novell ConsoleOne に表示されている場合は、アトラスページ（[WAN]、[Islands]、または領域ページ）で次のタスクを実行できます。

タスク	コメント
Open	ページを開く
Import	カスタムの壁紙を挿入する
Save	データベースの変更を更新する
Print	ページを印刷する
Rename	ページ名を変更する
Layout	異なる焦点でページを印刷する

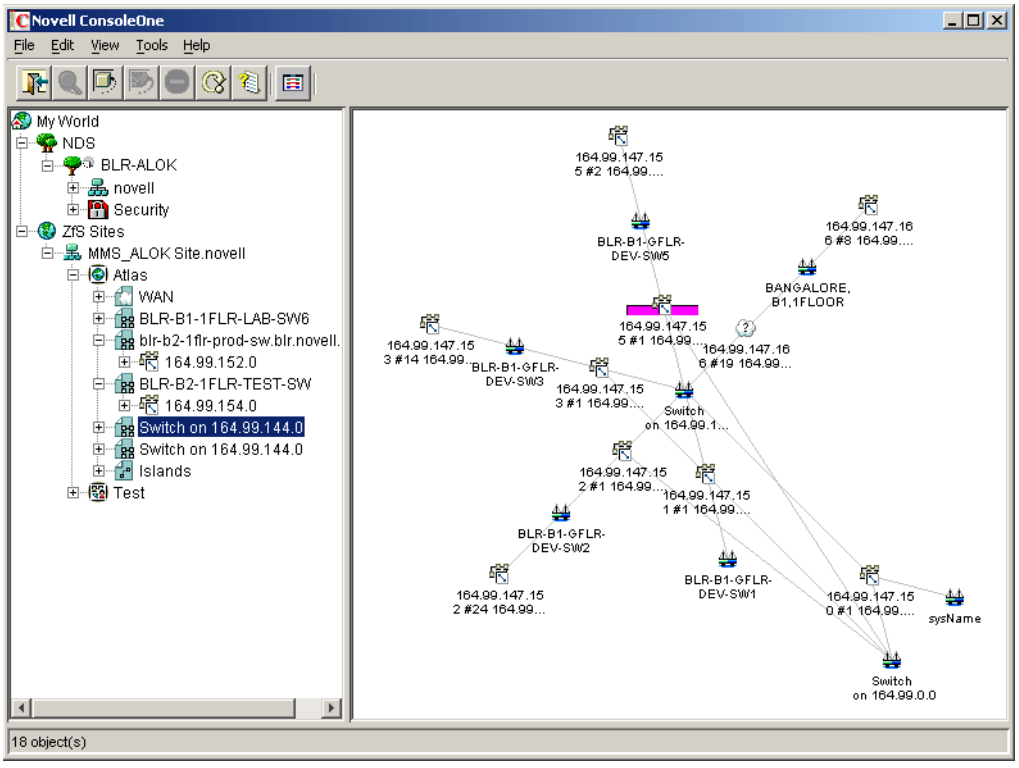
アトラスを使用したトラブルシューティング

アラーム処理を設定してデータベースにアラームを保存すると、Novell ZENworks Server Management マップで、ネットワークの状態を警告するアラームを表示できます。アラームの種類には、セグメントまたはノードに関する、重大なアラーム、メジャーアラーム、またはマイナーアラームがあります。これらのアラームが認識されると、アラームの重要度に応じて ConsoleOne のオブジェクトの上に次のような色が表示されます。

色	アラームの重要度
赤	重大
ピンク	メジャー
黄	マイナー

アラームステータスは階層構造の上に伝達されます。たとえば、サーバに重大なアラームが認識されると、対応するアラームアイコンがそのサーバを含むセグメントとページに表示されます。アラームについては、887 ページの「アラーム管理システムの管理」を参照してください。

次の図は、ConsoleOne の Atlas ネームスペースを示しています。



カスタムマップ

カスタムマップでは、カスタムアトラスとカスタムコンテナを作成および削除でき、ノードをコンテナにグループ化できます。アトラスのオブジェクトの階層を作成することもできます。アトラスには、カスタムコンテナを配置できます。カスタムコンテナ内にノードやサブコンテナを作成することもできます。ただし、ノードは［Atlas］の下に直接配置することはできません。

カスタムアトラスでは、次の操作を実行できます。

- 877 ページの「カスタムアトラスの作成」
- 878 ページの「カスタムコンテナの作成」
- 878 ページの「コンテナへのノードの追加」
- 879 ページの「カスタムアトラスオブジェクトの削除」
- 879 ページの「カスタムアトラスでのノードの検索」
- 879 ページの「存在するすべてのノードの検索」
- 880 ページの「カスタムコンテナへのノードのコピー」

カスタムアトラスの作成

1 カスタムアトラスを作成するサイトオブジェクトを右クリックし、［New］>［Atlas］の順にクリックします。

2 アトラスの名前を指定します。

3 ［OK］をクリックします。

カスタムコンテナの作成

新しいカスタムアトラス内にカスタムコンテナを作成できます。コンテナ内にサブコンテナを作成することもできます。

1 作成したカスタムアトラスを右クリックし、[New] > [Container] の順にクリックします。

または

Novell ConsoleOne の右のペインで、作成したカスタムコンテナを右クリックし、[New] > [Container] の順にクリックします。

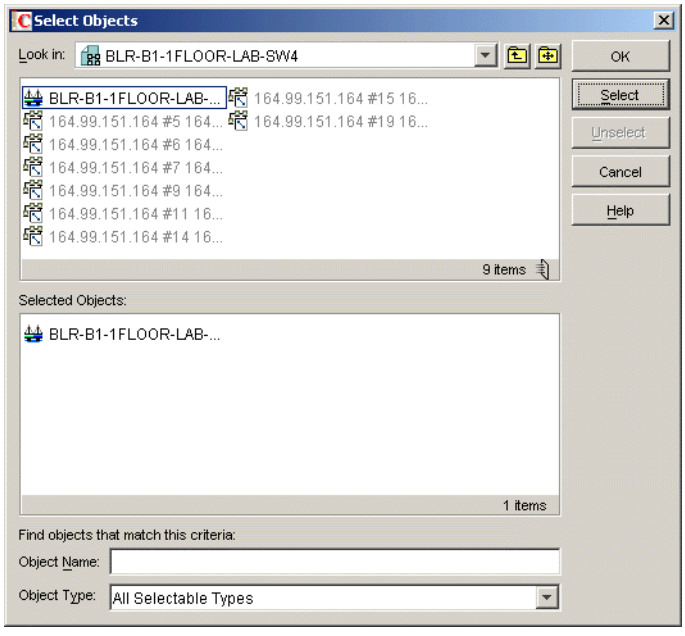
2 コンテナの名前を指定します。

3 [OK] をクリックします。

コンテナへのノードの追加

複数のノードを 1 つのコンテナに関連付けることができます。

1 作成したカスタムコンテナを右クリックし、[Add Nodes] をクリックします。



2 コンテナに追加するノードを選択します。

3 [Select] をクリックします。

選択したノードが [Selected Objects] リストに表示されます。

4 [OK] をクリックします。

カスタムアトラスオブジェクト名の変更

1 名前を変更するアトラスオブジェクトを選択します。

2 [Rename] をクリックします。

3 新しい名前を指定します。

4 [OK] をクリックします。

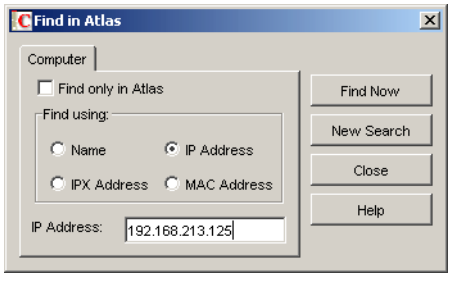
カスタムアトラスオブジェクトの削除

1 削除するアトラスオブジェクトを選択します。

2 [Delete] をクリックします。

カスタムアトラスでのノードの検索

特定のアトラス、または存在するアトラスすべてについて、特定のノードを検索できます。同じアトラスのノードを検索するには、[Find only in *atlasname*] チェックボックスを選択します。このチェックボックスを選択しない場合は、すべてのアトラスでノードが検索されます。



1 カスタムアトラスを右クリックし、[Find] をクリックします。

2 検索条件を指定します。

3 [Find Now] をクリックします。

カスタムアトラスのネットワークオブジェクトの場所が、[Find In Atlas] ダイアログボックスのリストに表示されます。

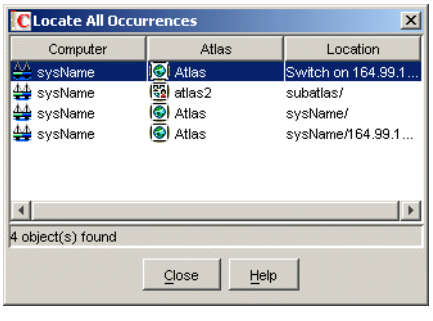
4 ノードの場所に移動するには、そのノードをダブルクリックします。

5 [Close] をクリックします。

存在するすべてのノードの検索

1 存在するすべてのノードを検索するには、検索するノードを右クリックし、[Locate All Occurrences] をクリックします。

存在するノードが、[Locate All Occurrences] ダイアログボックスに表示されます。



2 ノードの場所に移動するには、そのノードをダブルクリックします。

3 [Close] をクリックします。

カスタムコンテナへのノードのコピー

作成したカスタムコンテナにノードをコピーできます。

1 コピーするノードを選択し、右クリックして、[Copy to Container] を選択します。

2 [Select Objects] ダイアログボックスで、ノードをコピーするカスタムコンテナを指定します。

3 [OK] をクリックします。

ノード名の順序

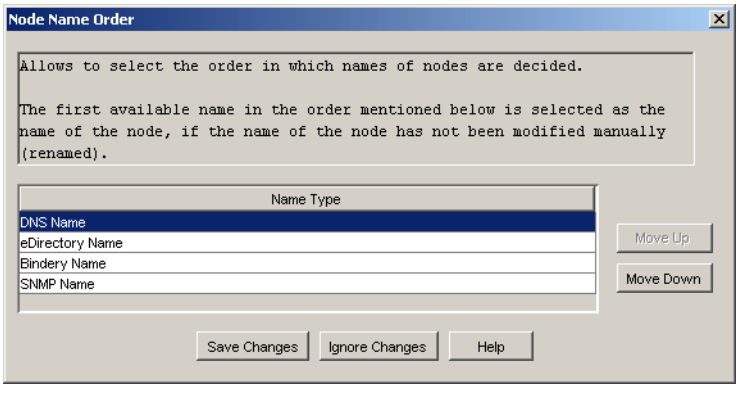
検出サイクルが進行し、より多くの情報が検出されると、マップに表示される名前が変更される場合があります。名前の情報ソースに応じて、異なる優先度が名前に与えられています。名前が検出されない場合は、ノードの IP/IPX アドレスがノード名として表示されます。

Atlas Manager では、検出されたオブジェクトの名前が、次のリストの順序に従って表示されます。

- ユーザ定義名
- DNS 名
- Novell eDirectory 名
- バインダリ名
- SNMP 名

表示順序を変更するには、[Node Name Order] ダイアログボックスを使用します。

1 [Atlas] レベルで、[File] > [Node Naming Order] の順にクリックします。



2 次のオプションを使用します。

- **[Move Up]** : ノード名の順序を変更します。
- **[Move Down]** : ノード名の順序を変更します。
- **[Save Changes]** : 変更を保存します。
- **[Ignore Changes]** : 変更を無視します。

統合ビューの使用

統合ビューサービスは、アトラスのフィルタとして機能するサービスです。統合ビューを使用すると、フィルタ機能によって、特定のタイプのデバイスまたはセグメントのリストを表示できます。統合ビューでは、特定のノードまたはセグメント上で最も重要度の高いアラームを確認する際に、簡単に移動して、すばやく操作できます。

統合ビューには、次の 2 つのタイプがあります。

- 881 ページの「Unified View for Devices」
- 882 ページの「Unified View for Segments」

Unified View for Devices

このビューでは、すべてのデバイス、管理可能なデバイス、または管理されないデバイスを表示できます。対応するデバイスタイプに関しては、デバイスによって実装される MIB のリストが、novell zenworks¥mms¥mwserver¥bin ディレクトリにある UnifiedView.ini ファイルの Manageability_definition プロパティを満たす場合、そのデバイスは管理可能と見なされます。Manageability_definition プロパティは、MIB 名の有効な論理式で更新できます。

次のデバイスタイプにフィルタを適用できます。

- すべて（すべてのデバイスタイプ）
- NetWare サーバ
- NCP プリントサーバ
- TCP サービス
- Printers
- IP ルータ
- スイッチ / ブリッジ
- IPX ルータ
- Windows サーバ

デバイスにフィルタを適用するには

1 アトラスで、[View] > [Unified View for Devices] の順にクリックします。

2 最初のドロップダウンリストから、[All] を選択してすべてのデバイスを表示します。

または

[Manageable] を選択して管理可能なデバイスを表示します。

または

[Unmanageable] を選択して、管理されないデバイスを表示します。

3 2 つ目のドロップダウンリストからデバイスタイプを選択します。

4 [Show] をクリックします。

統合ビューに、デバイスのリストが表示されます。統合ビューの表の列には、次の情報が表示されます。

- デバイスに関連付けられたアイコン。

- デバイスによって実装されたMIB。デバイスがMIBを実装しない場合は、そのデバイスの列に「No MIBs implemented」と指定されます。
- デバイスに対する最大重要度のアラーム。アラームの凡例を表示するには、ツールバの［Alarm Legend］ボタンを選択します。

Unified View for Segments

このビューでは、すべてのセグメント、管理可能なセグメント、または管理されないセグメントを表示できます。対応するセグメントタイプに関しては、セグメント内の少なくとも1つのデバイスによって実装されるMIBのリストが、UnifiedView.iniファイルのManageability_definitionプロパティを満たす場合、そのセグメントは管理可能と見なされます。Manageability_definitionプロパティは、MIB名の有効な論理式で更新できます。次のセグメントタイプにフィルタを適用できます。

- すべて（すべてのセグメントタイプ）
- Ethernet
- フレームリレー
- IPX互換モード
- トークンリング
- X.25
- PPP
- ATM
- FDDI

セグメントにフィルタを適用するには

1 ［Atlas］レベルで、［View］>［Unified View for Segments］の順にクリックします。

2 最初のドロップダウンリストから、［All］を選択してすべてのセグメントを表示します。

または

［Manageable］を選択して管理可能なセグメントを表示します。

または

［Unmanageable］を選択して、管理されないセグメントを表示します。

3 2つ目のドロップダウンリストからセグメントタイプを選択します。

4 ［Show］をクリックします。

統合ビューに、セグメントのリストが表示されます。統合ビューの表の列には、次の情報が表示されます。

- セグメントに関連付けられたアイコン。
- セグメントの名前。
- セグメントに対する最大重要度のアラーム。アラームの凡例を表示するには、ツールバの［Alarm Legend］ボタンを選択します。

24 アラーム管理の理解

Novell® ZENworks® Server Management のアラーム管理システムは、SNMP トラップ、しきい値アラーム、ネットワーク検出イベント、ping と接続テストのエラーなど、ネットワーク上で発生する重要なイベントをユーザに警告します。これにより、ネットワークの問題にすばやく対応したり、ネットワークで発生するイベントについて更新を受信したりできます。

アラームアイコンは Novell ConsoleOne® のオブジェクトに表示されます。アイコンは、重要度レベルを示す色に変わり、問題の発生を知らせます。イベントは［Active Alarm］ビューに報告され、各イベントは分類されて、対応するアラームアイコン付きで表示されます。

アラーム管理システムは、SNMP 標準トラップ通知をサポートするネットワーク上のすべてのデバイスを処理します。たとえば、NetWare 版 Management Agent がインストールされているすべての Novell NetWare® サーバでは、サーバの故障、過重負荷、および設定変更に関する通知が管理サーバに送られて処理され、ZENworks Server Management の ConsoleOne で表示できるようになります。

アラームを有効または無効にしたり、セグメントとサーバの基準統計に基づいたアラームしきい値（たとえば、使用率、および毎秒のパケット総数のセグメントアラーム）を設定して、統計のしきい値に達したときにアラームを発生するようにできます。アラームまたはイベントの発生時に実行されるアクションも設定できます。アラームまたはイベントに割り当てるアクションは、アラーム処理で指定します。

この節では、次のトピックについて説明します。

- 883 ページの「アラーム管理システムの理解」
- 887 ページの「アラーム管理システムの管理」
- 906 ページの「アラーム管理システムの維持」
- 906 ページの「アラーム管理システムのトラブルシューティング」

アラーム管理システムの理解

アラーム管理システムは、ネットワークの状態やイベントを警告します。この情報を使用、配布、および管理するツールとバックエンドサービスが用意されています。アラーム管理システムコンポーネントは、その他の Novell ZENworks Server Management コンポーネントと完全に統合されています。役割ベースサービス (Role-based Services) コンポーネントによるアクセス制御と、レポート機能によるレポート生成が提供されています。ネットワーク全体のデバイスとシステムによって生成されるイベントとアラームの処理と表示を一元管理できます。

Novell ConsoleOne で、アラーム管理システムが受信したアクティブアラームと過去のアラームの統計データを表形式で表示できます。これにより、アラームを簡単に扱えるようになり、ネットワークイベントと繰り返し発生するアラームの状態を追跡することもできます。ネットワークで発生したアラームは、次のものによってリアルタイムに通知されます。

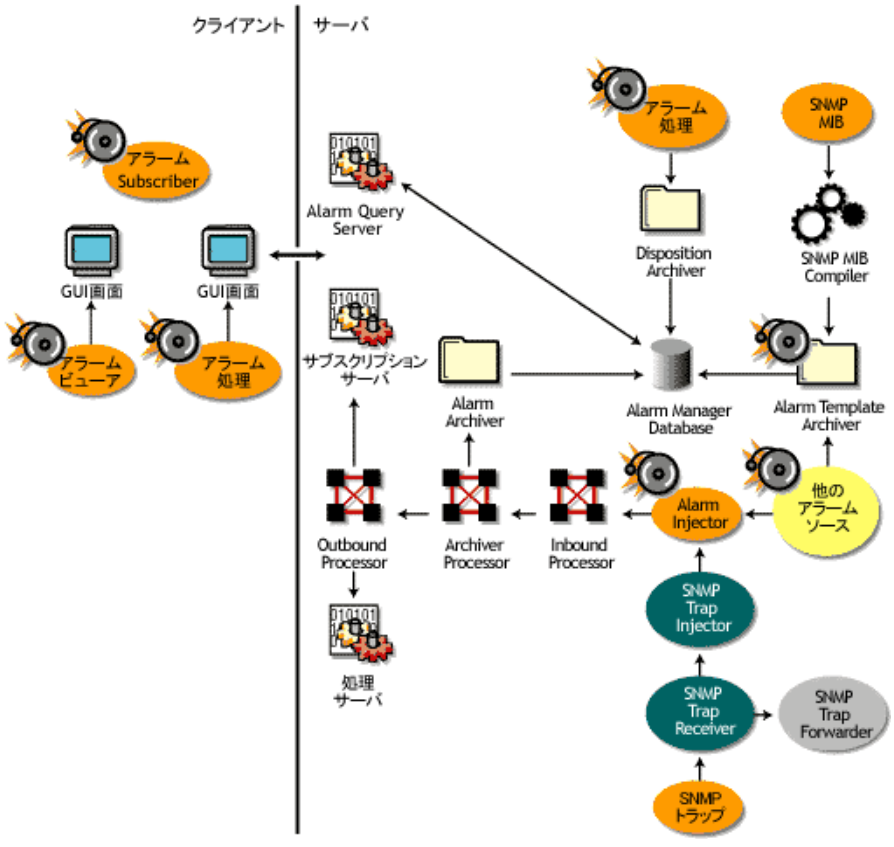
- 重要度レベル。アラームインジケータの色を変えて表示される。
- 音での通知
- ステータスバーに表示されるチッカーテープメッセージ

アラームの受信時にプログラムを自動で起動したり、イベントをリモートユーザに通知する電子メールメッセージを送信したりするアクションを割り当てることもできます。

アラーム管理システムのコンポーネント

アラーム管理システムは、アラームの処理、保存、および表示用の複数のコンポーネントで構成されています。アラーム管理システムが受信するすべてのアラームは、処理されてから、アラームに割り当てられているアプリケーションに送信されます。デフォルトでは、ConsoleOne がアラーム管理システムに割り当てられ、アラームの処理時に更新を受信します。HSN (Hierarchical Status Notification) もアラーム管理システムに割り当てられ、アトラスマップアイコンの色を状況に応じて変更します。

次の図は、アラーム管理システムコンポーネントを示しています。



アラーム管理システムを構成する主なコンポーネントを次に示します。

- 885 ページの「SNMP Trap Receiver」
- 885 ページの「SNMP Trap Forwarder」
- 885 ページの「SNMP Trap Injector」
- 885 ページの「Alarm Injector」
- 885 ページの「アラームプロセッサ」
- 885 ページの「Alarm Manager Database」
- 886 ページの「アーカイバ」
- 887 ページの「アラームビューア」

SNMP Trap Receiver

SNMP はネットワーク管理エージェントからトラップを受信し、SNMP Trap Forwarder と SNMP Trap Injector にトラップを渡します。

SNMP Trap Forwarder

SNMP Trap Forwarder は、トラップの受信後に Alarm Manager Database を調べて、そのトラップに SNMP トラップ転送処理があるかどうかを判断します。トラップに転送処理がある場合、SNMP Trap Forwarder はトラップを転送します。それ以外の場合、SNMP Trap Forwarder はトラップを無視します。

SNMP Trap Injector

SNMP Trap Injector はトラップをアラームに変換し、アラームを Alarm Injector に渡します。

Alarm Injector

Alarm injector は、SNMP Trap Injector およびその他のアプリケーションからアラームを受信して、Inbound Processor にアラームを渡します。

アラームプロセッサ

アラームプロセッサでは、アラームの受信、アーカイブ作成、および Subscriber への送信のためのプロセスが実行されます。Inbound Processor は、受信したアラームにアラームテンプレートを適用します。Inbound Processor の処理が終了すると、アラームは Archive Processor に送信されます。ここで、処理済みのアラームのログが作成され、Alarm Manager Database に格納されます。Archive Processor はアラームを Outbound Processor に送信し、ここからアラームがサブスクリプションサーバと処理サーバに順に送信されます。

Alarm Manager Database

Alarm Manager Database には、アラーム情報のリポジトリとして、次のものが格納されます。

- 886 ページの「処理済みのアラーム」
- 886 ページの「アラームテンプレート」
- 886 ページの「アラーム処理」

処理済みのアラーム

Alarm Manager Database に格納された処理済みのアラームデータは、Alarm Query Server を通じて Novell ConsoleOne に供給されます。アラームデータは、アラーム、およびアラーム概要表示とレポート生成に使用されます。

アラームテンプレート

テンプレートは、Inbound Processor が受信した各アラームに適用されます。アラームテンプレートは、MIB の SNMP トラップ定義、またはアラーム管理システムの管理基準および表示基準を処理するその他の独自の定義に基づいています。MIB をコンパイルすると、トラップ定義が使用され、アラームデータの表示方法と管理方法を提供するアラームテンプレートが作成されます。独自のアラームテンプレートは、独自の定義に基づいています。たとえば、ユーザが不正なパスワードでサーバにログインしようとすると、アラームが生成され、管理サーバに転送されます。管理サーバは、アラームを処理してトラップ OID（オブジェクト識別子）を識別し、関連付けるアラームテンプレートを割り当てます。

デフォルトテンプレートは、OID が認識されず、未定義のデバイスとして分類されたデバイスが送信する SNMP トラップに割り当てられています。トラップ OID がアラーム管理システムに認識されるようにするには、管理サーバでデバイスの MIB を MIB Pool にコンパイルする必要があります。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」を参照してください。

アラーム処理

アラーム処理では、各種の SNMP トラップまたは独自のアラームの処理方法を指定します。アラーム管理システムでのアラーム自動処理は、このアラーム処理で定義することによって設定できます。自動処理機能には、アラーム受信時に起動するアプリケーションの指定、電子メール通知の送信、他の Novell ZENworks Server Management 管理サーバへの処理済みアラームの転送、他のネットワーク管理システムへの SNMP トラップの転送などがあります。ビープ音など、アラームのオプションを設定することもできます。

アーカイバ

次の 3 つのアーカイバが Alarm Manager Database にデータを追加します。

- 886 ページの「Alarm Archiver」
- 886 ページの「Disposition Archiver」
- 887 ページの「Template Archiver」

Alarm Archiver

Alarm Archiver は、アラーム統計とデータをアラームデータベースに格納します。デフォルトでは、すべてのアラームがアーカイブされます。アラームをアーカイブしない場合は、アラーム処理を編集してアラームのアーカイブ作成を無効にできます。詳細については、904 ページの「アラーム統計のアーカイブ作成」を参照してください。

Disposition Archiver

Disposition Archiver は、Disposition Console からアラーム処理を受信して、Alarm Manager Database に保存します。

Template Archiver

Template Archiver は、MIB Compiler からアラームテンプレートを受信して、Alarm Manager Database に保存します。

アラームビューア

Novell ConsoleOne では、[Active Alarm] ビュー、[Historical Alarm] ビュー、および [Alarm Summary] ビューの 3 つのビューでアラームデータを表示できます。

[Active Alarm] ビューには、ネットワークで発生したイベントの統計が表示されます。[Active Alarm] ビューに表示されるアラームは、ユーザを所有者にすることも、グループに割り当てることもできます。このビューからアラームに実行できるタスクは、役割ベースサービスで許可されているアクセス権によって異なります。[Active Alarm] ビューでは、受信したアラームがリストに継続して追加されるため、常に最新のアラームが表示されます。アラームは処理されると、[Active Alarm] リストから削除されます。

[Alarm History] ビューには、アラームの割り当てと所有権に関する情報が表示されます。このビューを使用すると、アラーム管理システムが受信したアラームを追跡し、処理ステータスを確認できます。

[Alarm Summary] ビューは、受信したすべてのアラームをグラフ形式で表示します。

アラーム管理システムの管理

Novell ZENworks Server Management Novell ConsoleOne では、ネットワークの重大なイベントの監視、管理、および制御を一元管理できます。重要なシステムまたはイベントのエラーが通知されるようにアラーム管理システムを設定すると、ネットワークの維持に役立ちます。この節では、次のトピックについて説明します。

- 888 ページの「アラームインジケータの認識」
- 888 ページの「アラームの表示」
- 893 ページの「アラームの有効化と無効化」
- 893 ページの「アラームの解決」
- 896 ページの「アラームの削除」
- 897 ページの「アラームに関するアクションの実行」

アラームインジケータの認識

トポロジマップ、[Atlas] ビュー、[Active Alarm] ビュー、[Alarm History] ビュー、およびサーバ / ノード概要でノードを監視することにより、アラームでトリガされるイベントをネットワークで監視できます。次の表は、アラームインジケータと、関連付けられているアラームの種類を示しています。

アラームインジケータ	説明
影響を受けたオブジェクトに表示されるアラームアイコン	[Atlas] ビュー、[Console] ビュー、および Novell ConsoleOne の左ペインに、アラームがその重要度（重大、メジャー、マイナー）とともに表示されます。アラームアイコンは、そのオブジェクトに表示されたすべてのアラームを処理するまでセグメントオブジェクトまたはデバイスオブジェクトに表示されたままになります。アラームアイコンは、アラームの重要度レベルに基づいて変化します。アラームの重要度と関連アイコンについては、890 ページの「アラームの解釈」を参照してください。セグメントまたはデバイスに複数のアラームが記録されている場合、アラームアイコンには常に最高の重要度レベルが表示されます。
ステータスバーのチッカーテープメッセージ	アラーム管理システムでは、ステータスバーにアラームメッセージを自動的に表示できます。デフォルトでは、このオプションは有効になっています。各アラーム処理を個別に設定して、チッカーテープメッセージの表示を無効にできます。アラームでトリガされるイベントを認識すると、アラーム管理システムはステータスバーにアラームに関するメッセージを表示します。このオプションの設定については、902 ページの「チッカーテープメッセージの表示」を参照してください。
ビープ音	アラームの発生時に Novell ConsoleOne でビープ音が鳴るよう、アラーム管理システムを設定できます。デフォルトでは、このオプションは無効になっています。各アラーム処理を個別に設定して、音での通知を有効にできます。このオプションの設定については、903 ページの「ビープ音の発生」を参照してください。

アラームの表示

Novell ConsoleOne から、アクティブアラームおよび過去のアラームにアクセスできます。管理者は、役割ベースサービスを使用し、組織の役割に基づいてデータを細かく定義することにより、アラームデータと管理機能にアクセス制限を定義できます。

[Active Alarm] ビューと [Alarm History] ビューに表示されるアラームデータは、表示データへのフィルタの適用、列のレイアウトの変更、およびソート順の変更によって、表示方法を変更できます。表示方法を変更するすべてのオプションは、Novell ConsoleOne の [View] メニューから利用できます。

次の節では、アラームのさまざまな表示方法や使用方法について説明します。

- 889 ページの「アクティブアラームの表示」
- 889 ページの「過去のアラームの表示」
- 889 ページの「アラーム概要の表示」
- 890 ページの「アラームの解釈」
- 891 ページの「アラームのソート」
- 891 ページの「アラームへのフィルタの適用」

アクティブアラームの表示

Novell ZENworks Server Management Novell ConsoleOne の［Active Alarm］ビューには、管理ドメインごとに、セグメントまたはデバイスから受信した現在のアラームすべてに関するアラーム統計が表示されます。［Summary］ビューには、サーバまたはノードのすべてのアクティブアラームを示すリストが表示されます。

［Active Alarm］ビューと［Server Summary］ビューには、アクティブアラームの詳細情報を示す表が表示されます。これらのビューは、ネットワークに新しいアラームが発生してアーカイブされるたびに更新されます。新しいアラームがリストに追加されます。

［Active Alarm］ビューを表示するには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトをクリックします。

2 ［View］>［Active Alarms］の順にクリックします。

［Alarm History］ビューが表示されます。このビューから次のアクティビティを実行できます。

- 894 ページの「アラームの割り当て」
- 894 ページの「アラームの所有者の決定」
- 895 ページの「アラームの処理」
- 895 ページの「アラームへの注釈の追加」

過去のアラームの表示

［Alarm History］ビューには、各アラームの処理ステータスなど、アーカイブされたすべてのアラームに関する情報が表示されます。役割ベースサービスによってアクセスが許可されている場合のみ、このビューにアクセスできます。

［Alarm History］ビューを表示するには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトをクリックします。

2 ［View］>［Alarm History］の順にクリックします。

［Alarm History］ビューが表示されます。このビューから、次のアラーム処理アクティビティを実行できます。

- 894 ページの「アラームの割り当て」
- 894 ページの「アラームの所有者の決定」
- 896 ページの「アラームの削除」
- 895 ページの「アラームへの注釈の追加」

アラーム概要の表示

［Alarm Summary］ビューは、受信したアラームの概要をグラフ形式で表示します。このビューは、円グラフパネル、棒グラフパネル、トレンドパネルの 3 つの表示パネルに分割されます。これらのパネルに、指定した期間の情報を選択して表示できます。期間の範囲は、時間、日、週、月単位で指定します。

- 円グラフパネルには、重要度、カテゴリ、所有者、およびアラーム状態に基づくアラームの分布が示されます。

- 棒グラフパネルには、上位 N 個のアラームの種類、ソースアドレス、および影響を受けたノードが示されます。N 値は設定可能です。トレンドパネルには、アラームの受信率が表示されます。

円グラフおよび棒グラフの表示方法をカスタマイズして、カスタムデータが反映されるようにできます。

[Alarm Summary] ビューを表示するには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトをクリックします。

2 [View] > [Alarm Summary] の順にクリックします。

[Alarm Summary] ビューが表示されます。

円グラフと棒グラフの表示方法をカスタマイズするには

2a [Alarm Summary] ビューの [Customize] ボタンをクリックします。

[Customize Summary View] ダイアログボックスが表示されます。

デフォルトでは、このダイアログボックスのオプションはすべて選択されています。必要なオプションを選択すると、ビューをカスタマイズできます。

アラームの解釈

[Active Alarm] ビューと [Alarm History] ビューには、Alarm Manager Database にアーカイブされたアラームのリストが表示されます。アラームは表形式で表示されます。次の表は、データ種類と内容についての説明です。

データの種類（列）	内容
Severity	トラップに属する重要度レベルを示すアラームアイコン。次のアラームアイコンの色によって、アラームの重要度レベルが示されます。  赤 = 重大  赤紫 = メジャー  黄 = マイナー  青 = 情報  白 = 未定義
From	アラームをアラーム管理システムに送信したデバイスのネットワークアドレス。
Summary	イベントの概要。多くの場合、アラームによって影響を受けるオブジェクトの名前またはアドレスを含みます。
Owner	アラーム処理を担当するユーザまたはグループ。デフォルトの所有者は、SYSTEM です。
Received Time	アラーム管理システムがアラームを受け取った日時。

データの種類（列）	内容
Type	アラームの一般的な説明たとえば、ボリュームのディスク領域の不足など。
Category	トラップタイプオブジェクトに関連付けられた MIB で識別されるカテゴリ。

各ビューに表示された統計から、基準に基づいて、アラームビューに表示されるデータにフィルタを適用できます。詳細については、891 ページの「アラームへのフィルタの適用」を参照してください。アラームビューでアラームエントリを選択し、右クリックすると、操作を実行できます。

アラームのソート

[Active Alarm] ビューまたは [Alarm History] ビューでアラームをソートすると、アラームの表示順序を変更できます。デフォルトでは、アラームは受信した時間によって昇順にソートされます。

ソート設定を編集するには

1 [View] > [Settings] > [Sort] の順にクリックします。

2 アラームをソートする基準を選択します。次のカテゴリでソートできます。

- Type
- Severity
- Category
- Received time
- Summary
- Owner
- Affected Object

3 [Sort Order] ボックスから適切なラジオボタンを選択して、アラームを昇順（最古のアラートを先頭）にソートするか降順（最新のアラートを先頭）にソートするかを指定します。

4 [OK] をクリックします。

指定した基準に従ってアラームがソートされます。

アラームへのフィルタの適用

表形式ビューでは、フィルタ条件に基づいてアラームを表示できます。フィルタは現在の管理セッションにのみ適用され、Novell ConsoleOne の終了時に解除されます。

4 つのドロップダウンリストから条件を選択して、フィルタをセットアップします。1 行だけのシンプルなフィルタを使用することも、複数行または行グループで構成される複雑なフィルタを使用することもできます。複数行を使用してフィルタをセットアップする場合は、行または行グループ間の論理的関係を指定することも必要です。

フィルタをセットアップするには

1 フィルタを適用するビューを表示します。

2 [View] > [Settings] > [Filter] の順にクリックします。

[Alarm Filter] ダイアログボックスが表示されます。

3 最初のドロップダウンリストで、アラーム管理システムによってアラームにフィルタを適用する列を選択します。次の列を使用してアラームにフィルタを適用できます。

- **[Severity]**：アラームの重要度に基づいてアラームをフィルタ処理します。アラームの重要度は、アラームの種類に割り当てられます。
- **[Type]**：アラームの種類に基づいてアラームをフィルタ処理します。アラームの種類は、MIB で定義された SNMP トラップタイプまたは独自のアラーム定義によって設定されます。
- **[Category]**：アラームのカテゴリに基づいてアラームをフィルタ処理します。アラームカテゴリは、トラップタイプオブジェクトを定義する MIB に基づいています。
- **[Generator Type]**：アラームを生成するエージェントまたはシステムの種類に基づいてアラームをフィルタ処理します。

4 2 つ目のドロップダウンリストから演算子を選択します。

演算子は、選択した列を値に対してどのように制約するかを定義します。たとえば、選択したカテゴリが 3 つ目のドロップダウンリストで選択する値と等しい、等しくない、より大きい、より小さい、より大か等しい、より小か等しい、含む、またはその値で始まるように指定して、アラームを表示できます。使用できる演算子のリストは、選択した列によって異なります。

5 3 つ目のドロップダウンリストから値を選択します。

6 4 つ目のドロップダウンリストから値を選択して、このフィルタステートメントと、このほかに定義するステートメントとの関係を指定します。

- フィルタステートメントが 1 つだけの場合、またはグループの最後のステートメントの場合は、[End] を選択します。
- 現在のフィルタステートメントの下に 1 行追加する場合は、[New Row] を選択します。新しい行が追加されます。前の行と新しい行との論理的関係を定義する必要があります。アラームは、指定した論理的条件に基づいて表示されます。両方のフィルタ条件を満たすには、[And] を選択します。表示されるアラームにいずれかのフィルタ条件を適用するには、[Or] を選択します。
- 前の行と関係のない行を 1 つまたは複数追加する場合は、[New Group] を選択します。新しい行が追加されます。ドロップダウンリストが追加され、新しい行が前の行から分離されます。このドロップダウンリストから値を選択して、フィルタステートメント間の関係を指定します。両方のフィルタステートメントが満たされるようにするには、[And] を選択します。いずれかのグループのフィルタステートメントが 1 つだけ満たされるようにするには、[Or] を選択します。新しいグループを追加した場合は、4 つ目のドロップダウンリストで [End] を選択します。

7 フィルタを定義したら、[OK] をクリックします。

アラームリストが更新され、定義したフィルタ条件に一致するアラームのみが表示されます。

アラームの有効化と無効化

Novell ZENworks Server Management には、セグメントに接続されたステーションの Traffic Analysis Agent をホストする、NetWare および Windows 管理対象サーバとネットワークセグメントのためにデフォルトのしきい値が用意されています。アラームは、値がしきい値を超えた場合に生成されます。サーバしきい値アラームは、デフォルトでは、セグメントしきい値アラームが無効の場合に有効になります。受信するしきい値アラームを有効にする必要があります。

重要： セグメントのプロパティを変更するには、NetWare 版または Windows 版 Traffic Analysis Agent が、セグメントに接続されたステーションでホストされている必要があります。

セグメントしきい値アラームを有効または無効にするには

1 セグメントを右クリックし、[Properties] をクリックします。

2 [Segment Alarms] タブが表示されていない場合は、このタブを選択します。

3 有効または無効にするアラームを選択し、[Edit] をクリックします。

4 [Value] フィールドで、アラームを生成する基準になるしきい値を入力します。

5 [Sampling Interval] フィールドで、しきい値を超えてからアラーム生成に要する時間（秒）を入力します。

6 [Enable] チェックボックスを選択します。

7 [OK] をクリックします。

アラームの解決

ネットワークのセグメントおよびデバイスで発生するアラームは、Alarm Manager Database に追加され、[Active Alarm] ビューと [Alarm History] ビューに表示されます。Alarm Manager Database のエントリは、アラームが削除されるまでデータベース内に維持されます。最初にアラームを認識してから、グループまたはユーザにアラームを割り当て、アラームの所有者を決定し、最後に所有者が問題を解決してアラームがデータベースから削除されるまで、各アラームステータスがデータベースに記録されます。

アラームの解決操作は、アラームビューで 1 つまたは複数のエントリを右クリックし、次のアクションのいずれかをクリックすると表示されます。

- 894 ページの「アラームの割り当て」
- 894 ページの「アラームの所有者の決定」
- 895 ページの「アラームの処理」
- 895 ページの「アラームへの注釈の追加」
- 895 ページの「影響を受けたノードへの移動」

Novell ConsoleOne の [View] メニューからもアラームアクションのメニュー項目にアクセスできます。

1 つまたは複数のアラームの処理、割り当て、および所有者の決定を実行する順序は、組織によって異なります。アラームを処理すると、アラームは［Active Alarm］リストから削除され、［Alarm History］リストにのみ表示されます。アラームを解決する順序は、まずアラームをグループまたはチームメンバーに割り当てて、次にグループのメンバーにアラームの所有権を割り当てることをお勧めします。ネットワークの問題またはイベントが解決したら、チームメンバーはアラームを処理して［Active Alarms］リストから削除できます。このプロセスに従って、解決時のアラームステータスを追跡し、最後に［Alarm History］リストからアラームを削除できます。

アラームの割り当て

アラーム処理を担当するグループまたはユーザを指定できます。これにより、組織内にすでに存在するチーム割り当てを使用することができます。たとえば、NetWare サーバに関するすべてのアラーム処理をグループまたはチームメンバーに割り当てることができます。グループまたはユーザには、1 つまたは複数のアラームを割り当てることができます。ただし、アラームを割り当てるためのアクセス権が、役割ベースサービスによって付与されている必要があります。アラームフィルタを使用すると、特定のフィルタ条件に基づいたグループを決定できます。フィルタオプションについては、891 ページの「アラームへのフィルタの適用」を参照してください。

ヒント： これはオプションの機能で、アラーム解決のステータスを追跡するために用意されています。

アラームを割り当てるには

1 ［Active Alarm］リストまたは［Alarm History］リストから、割り当てるアラームを選択します。

2 ［View］>［Assign］の順にクリックします。

3 ［Username］フィールドで、アラームを割り当てるユーザまたはグループの名前を入力します。

入力する名前は、Novell eDirectory のユーザに関係なく、既存の組織構造を表すことができます。

4 ［OK］をクリックします。

アラームの所有者の決定

ユーザは、1 つまたは複数のアラームの所有権を得ることができます。ユーザが、ネットワークの問題の解決に割り当てられているグループのメンバーの場合、チームメンバーはそのアラームの所有権を得ることができ、最後にアラームを削除して、Alarm Manager Database からアラームを除去できます。

ヒント： これはオプションの機能で、アラーム解決のステータスを追跡するために用意されています。

アラームの所有権を得るには

1 ［Active Alarm］ビューまたは［Alarm History］ビューからアラームを選択します。

2 ［View］>［Own］の順にクリックします。

［Owner］フィールドの値が、ログイン時の Novell eDirectory 名に変更されます。このオプションはカスタマイズできません。このアクションの使用時は、Novell ConsoleOne にログインしたユーザが常にアラームの所有者になります。

アラームの処理

[Active Alarm] ビューには、未処理のアラームが表示されます。アラームは処理されると [Active Alarm] リストから削除され、Novell ConsoleOne のその他のビューに表示されるアラームインジケータも削除されます。アラームインジケータの種類については、888 ページの「アラームインジケータの認識」を参照してください。アラームは、[Alarm History] ビューには表示されています。

アラームを処理するには

1 [Active Alarm] リストからアラームを選択します。

2 [View] > [Handle] の順にクリックします。

アラームが [Active Alarm] リストから削除されます。[Alarm History] ビューに切り替えると、アラーム情報を表示できます。

アラームへの注釈の追加

[Active Alarm] ビューまたは [Alarm History] ビューに表示されるアラームに注釈を追加できます。注釈には、アラームに関する有用な情報を指定できます。

アラームを処理するには

1 [Active Alarm] ビューまたは [Alarm History] ビューからアラームを選択します。

2 [View] > [Note] の順にクリックします。

[Note] ダイアログボックスが表示されます。

アラームについての注釈を作成します。

3 [OK] をクリックします。

アラームアイコンに注釈アイコンが表示され、アラームに注釈が追加されていることが示されます。

アラームから注釈を削除する場合は、手順 2 を繰り返します。[Note] ダイアログボックスで作成した注釈を削除します。

[Apply] をクリックします。アラームの注釈が削除され、注釈アイコンも表示されなくなります。

影響を受けたノードへの移動

アラームがトリガされ、影響を受けたノードに移動して、そのノードの修正に必要なアクションを実行できます。

影響を受けたノードアラームに移動するには

1 [Active Alarm] ビューまたは [Alarm History] ビューからアラームを選択します。

2 [View] > [Jump to Affected Node] の順にクリックします。

[Console] ビューが表示され、アラームがトリガされたノードが強調表示されます。

アラームの削除

[Alarm History] ビューに表示されるアラームは、問題を解決した後にアラームリストから削除できます。1 つまたは複数のアラームエントリを削除して、リストからアラームを削除します。アラームを削除するには、[Alarm History] ビューを表示し、アラームを削除するためのアクセス権が、役割ベースサービスによって付与されている必要があります。

アラームを削除するには、次の 2 つの方法があります。

- [Alarm History] ビューからアラームを手動で削除できます。896 ページの「Novell ConsoleOne からのアラームの削除」を参照してください。
- アラーム管理システムの削除ユーティリティを使用して、アラームを自動的に削除できます。896 ページの「削除ユーティリティによるアラームの削除」を参照してください。

重要： 管理サーバ上の Alarm Manager Database は、アラーム管理システムが受信するすべてのアラームインスタンスのステータスを記録します。データベースが大量のディスクスペースを消費しないように、問題が解決したらアラームを削除するようにしてください。現在、Alarm Manager Database ではアラーム削除ユーティリティが使用され（デフォルト）、一定期間後、またはデータベースのサイズに基づいて、エントリが自動的に削除されます。

Novell ConsoleOne からのアラームの削除

Novell ConsoleOne からアラームを手動で削除できます。

アラームを削除するには

1 [Alarm History] リストから削除するアラームを選択します。

2 [View] > [Delete] の順にクリックします。

アラームが [Alarm History] ビューから削除されます。

削除ユーティリティによるアラームの削除

アラーム管理システムの削除ユーティリティを使用して、アラームを自動的に削除できます。このユーティリティを使用する前に、Alarm Manager Database をインストールしたサーバとボリュームのプロパティディレクトリに配置されたユーティリティ設定ファイル AMPURGE.PROPERTIES をセットアップする必要があります。次に、指定した日時で自動的に実行されるようにユーティリティのスケジュールを設定します。このユーティリティは、サーバコンソールから手動で実行することもできます。次の節では、アラーム管理システムの削除ユーティリティのセットアップと使用方法について説明します。

- 896 ページの「削除ユーティリティ設定ファイルのセットアップ」
- 897 ページの「自動実行のための削除ユーティリティのセットアップ」

削除ユーティリティ設定ファイルのセットアップ

アラーム管理システムの削除ユーティリティ設定ファイルの AMPURGE.PROPERTIES では、削除されるアラームを選択する基準と、プロセスを実行する日時が定義されます。このファイルは、Alarm Manager Database をインストールしたサーバとボリュームのプロパティディレクトリにあります。

削除ユーティリティを実行する前に、次の手順で設定ファイルをセットアップする必要があります。

1 AMPURGE.PROPERTIES ファイルをテキストエディタで開きます。

2 次の行の値を編集して、アラームを削除する基準を設定します。

- SeverityInformationalPurgeWait: 情報アラームが削除されるまでの日数。
- SeverityMinorPurgeWait: マイナーアラームが削除されるまでの日数。
- SeverityMajorPurgeWait: メジャーアラームが削除されるまでの日数。
- SeverityCriticalPurgeWait: 重大なアラームが削除されるまでの日数。
- SeverityUnknownPurgeWait: 未定義のアラームが削除されるまでの日数。

デフォルトでは、すべての重要度レベルのアラームは 7 日後に削除されます。

3 設定ファイルを保存します。

自動実行のための削除ユーティリティのセットアップ

削除ユーティリティが毎日実行されるようにスケジュールを設定して、Alarm Manager Database が大量のディスクスペースを消費しないようにできます。自動的に実行されるようにユーティリティをセットアップする前に、さまざまな重要度のアラームに関する削除設定をファイル内でセットアップする必要があります。896 ページの「削除ユーティリティ設定ファイルのセットアップ」を参照してください。

自動的に実行されるようにユーティリティをセットアップするには

1 AMPURGE.PROPERTIES ファイルをテキストエディタで開きます。

2 [PurgeStartTime] エントリを編集して、ユーティリティを実行する日時を設定します。

有効な値は 0 ～ 23 で、0 は深夜 12 時、23 は午後 11 時を意味します。削除ユーティリティはメモリ依存型のため、数分間サーバを占有する場合があります。したがって、ユーティリティはピーク時以外に実行するように設定してください。

3 ファイルを保存して閉じます。

4 ALARMMANAGER.PROPERTIES ファイルを開き、次の行が存在することを確認します。

AlarmPurgeService=yes

この行が存在しない場合は、ファイルの最後に追加します。

5 ファイルを保存して閉じます。

6 サーバを再起動します。

アラームに関するアクションの実行

アラームの発生時にアクションが自動的に実行されるようにアラームを設定できます。アラームを設定するには、各アラームテンプレートに関連付けられたアラーム処理を編集します。アラーム処理は、アラームテンプレートごとに Alarm Manager Database に作成され、デフォルト設定が割り当てられます。アラーム処理を編集して、次のアクションを有効にできます。

- 898 ページの「SMTP 電子メール通知の送信」
- 899 ページの「外部プログラムの起動」
- 900 ページの「他の管理システムへの SNMP トラップの転送」
- 901 ページの「他の管理サーバへのアラームの転送」
- 901 ページの「アラームの重要度と状態の変更」

- 902 ページの「チッカーテープメッセージの表示」
- 903 ページの「ビープ音の発生」
- 904 ページの「アラーム統計のアーカイブ作成」
- 904 ページの「アラームテンプレートのソート」
- 905 ページの「Novell ConsoleOne からのアラームテンプレートの削除」
- 905 ページの「アラーム処理の印刷」
- 905 ページの「ファイルへのアラーム処理のエクスポート」
- 906 ページの「Microsoft Excel へのアラームテンプレートのコピー」

SMTP 電子メール通知の送信

指定された電子メール通知受信者に SMTP メッセージを送信できます。デフォルトポート以外のポートで稼動している SMTP ポートサーバに SMTP 電子メール通知を送信することもできます。

SMTP 電子メール通知が自動送信されるようにアラーム処理を変更するには

1. Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。
2. [Alarm Disposition] タブをクリックします。
3. [Alarm Templates] リストから編集するアラームテンプレートを選択し、[Edit] をクリックします。

   [Edit Alarm Disposition] ダイアログボックスが表示されます。
4. [SMTP Mail Notification] タブをクリックします。
5. [Notify through SMTP Mail] チェックボックスを選択します。
6. [SMTP Host] フィールドに、受信および送信電子メールを処理する SMTP ホストサーバの IP アドレスとポート番号 (オプション) を入力します。

   ポート番号を指定する場合は、IP アドレスの後にコロン (:) を入力してから、ポート番号を指定してください。たとえば、SMTP ホストサーバの IP アドレスが 207.68.173.245 で、ポート番号が 12345 の場合は、207.68.173.245:12345 と指定します。
7. [From] フィールドに通知の送信者の名前を入力します。
8. [To] フィールドに受信者の電子メールアドレスを入力します。
9. [Subject] フィールドに電子メールの件名を入力します。
10. [Message] フィールドに、必要に応じて電子メールのメッセージを入力します。
11. [OK] をクリックします。

件名とメッセージのテキスト文字列には、次の表に示す変数を挿入できます。これらの変数を使用して、エラーまたはイベントが生成されたセグメントまたはデバイスの詳細情報をメッセージに追加できます。すべての変数の前にパーセント記号 (%) を付ける必要があります。たとえば、件名に %v 変数を追加してアラームの重要度を表示できます。変数に文字数を指定することもできます。%(*nnn*)X は、%X 値の長さを *nnn* 文字に制限します。X は書式指定子を表します。たとえば、%(10)a はアラーム ID を 10 文字まで表示します。

変数パラメータ	Name	説明
a	アラーム ID	データベースに保存されるときのアラームの識別番号。
c	影響を受けたクラス	アラームを送信した機器のクラス。これは、ネットワークのあらゆる部分に該当する可能性があり、データベース内で分類され、インデックスが作成されます。
o	影響を受けたオブジェクトの番号	アラームを生成したノードがデータベースに格納される際のノードの識別番号。
s	アラーム概要文字列	アラームを説明するメッセージ (これはステータスバーのチッカーテープメッセージと同じです)。
t	アラームの種類文字列	アラームの説明。これは［Alarm Summary］ウィンドウの［Alarm Type］列の記述と一致します。
v	重要度番号	アラームの重要度は次の番号で示されます。 4 = 重大 3 = メジャー 2 = マイナー 1 = 情報 これ以外はすべて未定義のアラームとして分類されます。
n	影響を受けるオブジェクトの名前	アラームによって影響を受けたノードの識別名。
p	ソースアドレス	アラームを生成したエージェントのソースアドレス。
-h	デフォルトヘッダの削除	SMTP メッセージの送信時に、デフォルトヘッダを切り捨てます。

外部プログラムの起動

アラーム処理を編集する際に、アラームの受信時に Novell ZENworks Server Management サーバのプログラムを自動的に起動するオプションを設定できます。たとえば、システム管理者のポケットベルにメッセージを送信するプログラムがアラームによって起動されるように指定できます。

プログラムの起動だけでなく、プログラムに渡す引数や変数も指定できます。

Novell ZENworks Server Management には、アプリケーションを起動する機能は用意されていますが、定義済みのプログラムは提供されていません。ただし、NLM を起動してスクリプトルーチンを実行することや、サードパーティのプログラムを使用することはできます。

アプリケーションの自動起動をセットアップするには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、［Properties］をクリックします。

2 ［Alarm Disposition］タブをクリックします。

3 ［Alarm Templates］リストから編集するアラームを選択し、［Edit］をクリックします。

［Edit Alarm Disposition］ダイアログボックスが表示されます。

4 [Launching Application] タブをクリックします。

5 [Launch Application] チェックボックスを選択します。

6 [Application Name] フィールドにアプリケーションのパスと名前を入力します。

7 [Argument] フィールドに必要な実行引数またはスクリプト変数を入力し、[OK] をクリックします。

引数はプログラムに直接渡されます。テキストは解析されず、リテラルテキスト文字列として読み込まれます。変数の前にパーセント記号 (%) を付ける必要があります。パーセント記号の次に、パラメータの長さを制限するフィールド (オプション) を追加できます。変数に文字数を指定することもできます。%(*nnn*)X は、%X 値の長さを *nnn* 文字に制限します。X は書式指定子を表します。たとえば、%(10)a はアラーム ID を 10 文字まで表示します。

次の表は、プログラムの起動時に使用できる変数の一覧です。

変数	Name	説明
a	アラーム ID	データベースに保存されるときのアラームの識別番号。
c	影響を受けたクラス	アラームを送信した機器のクラス。これは、ネットワークのあらゆる部分に該当する可能性があり、データベース内で分類され、インデックスが作成されます。
o	影響を受けたオブジェクトの番号	アラームを生成したノードがデータベースに格納される際のノードの識別番号。
s	アラーム概要文字列	アラームを説明するメッセージ (これはステータスバーのチッカーテープメッセージと同じです)。
t	アラームの種類文字列	アラームの説明。これは [Alarm Summary] ウィンドウの [Alarm Type] 列の記述と一致します。
n	影響を受けるオブジェクトの名前	アラームによって影響を受けたノードの識別名。
p	ソースアドレス	アラームを生成したエージェントのソースアドレス。
v	重要度番号	アラームの重要度は次の番号で示されます。 4 = 重大 3 = メジャー 2 = マイナー 1 = 情報 これ以外はすべて未定義のアラームとして分類されます。

他の管理システムへの SNMP トラップの転送

アラーム管理システムは、変更されていない SNMP トラップを転送するように設定できます。ターゲット管理ステーションまたはサーバの IP アドレスをアラーム処理で指定すると、トラップが自動的に転送されます。

SNMP トラップを転送するには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [SNMP Trap Forwarding] タブをクリックします。

5 [SNMP Target Address] フィールドにトラップを転送するサーバの IP アドレスとポート番号 (オプション) を入力し、[Add] をクリックします。

ポート番号を指定する場合は、IP アドレスの後にコロン (:) を入力してから、ポート番号を指定してください。たとえば、SMTP ホストサーバの IP アドレスが 207.68.173.245 で、ポート番号が 12345 の場合は、207.68.173.245:12345 と指定します。

サーバが [List of Targets] に追加されます。トラップを受信するすべてのサーバに対して、この手順を繰り返します。

6 [OK] をクリックします。

他の管理サーバへのアラームの転送

アラーム管理システムは、処理済みアラームを他の Novell ZENworks Server Management 管理サーバに転送するように設定できます。ターゲット管理サーバの IP アドレスまたはサーバ名をアラーム処理で指定すると、アラームが自動的に転送されます。

アラームを転送するには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [Alarm Forwarding] タブをクリックします。

5 アラームを受信するターゲットサーバを追加します。

5a [Site Name] フィールドで、アラームを転送する Novell ZENworks Server Management サイトを選択します。

5b [Site Host] フィールドで、アラームを転送する Novell ZENworks Server Management ホストを選択します。

5c [Add] をクリックします。

サーバが [List of Targets] に追加されます。アラームを転送するすべてのサーバに対して、この手順を繰り返します。

6 [OK] をクリックします。

アラームの重要度と状態の変更

アラーム処理のその他の設定により、アラームの重要度や状態を変更できます。アラームの重要度、状態、またはその両方を変更できます。受信したアラームには、変更された重要度と状態が表示されます。

アラームの重要度と状態を変更するには

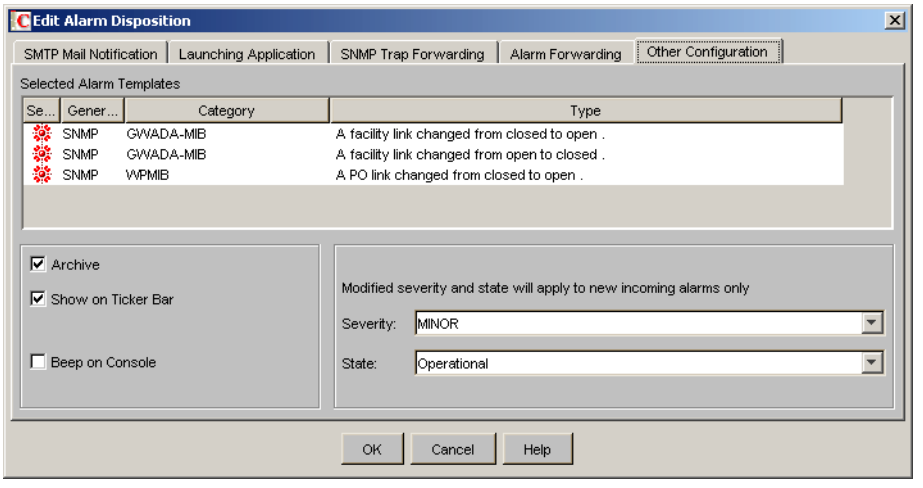
1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [Other Configuration] タブをクリックします。



5 アラームの重要度を変更するには、ドロップダウンリストから重要度を選択します。アラームの重要度は、次のいずれかに変更できます。

深刻
メジャー
マイナー
情報
不明

または

アラームの状態を変更するには、ドロップダウンリストから状態を選択します。アラームの状態は、次のいずれかに変更できます。

Operational
Unoperational
Degraded

6 [State] ドロップダウンリストからアラームの状態を選択します。

7 [OK] をクリックします。

チッカーテープメッセージの表示

アラーム処理のその他の設定により、Novell ConsoleOne のステータスバーにチッカーテープメッセージを表示できます。メッセージは、最新のアラームまたはネットワークイベントの概要を示します。

デフォルトでは、このオプションは有効になっています。アラーム処理を編集して、監視を必要とする重要なアラームだけがチッカーテープメッセージを表示するようにできます。

チッカーテープメッセージを無効または有効にするには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [Other Configuration] タブをクリックします。

5 チッカーテープメッセージを無効にするには、[Show on Ticker Bar] チェックボックスの選択を解除します。

または

チッカーテープメッセージを有効にするには、[Show on Ticker Bar] チェックボックスを選択します。

6 [OK] をクリックします。

ビープ音の発生

アラーム処理のその他の設定により、Novell ConsoleOne でビープ音を発生させることができます。音によって、アラームの発生をユーザに警告します。この機能は、次の場合に使用すると便利です。

- サーバの異常終了
- システム：ユーザによって停止されたサーバ
- ファイルシステムフル

デフォルトでは、このオプションは無効になっています。監視を必要とする重要なアラームについて、このオプションを有効にする必要があります。

ビープ音を有効または無効にするには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [Other Configuration] タブをクリックします。

5 ビープ音の機能を有効にするには、[Beep on Console] チェックボックスを選択します。

または

ビープ音の機能を無効にするには、[Beep on Console] チェックボックスの選択を解除します。

6 [OK] をクリックします。

アラーム統計のアーカイブ作成

アラーム管理システムシステムは、アラームとネットワークイベントの詳細情報を含むレポートを生成するレポートツールへデータを提供します。アーカイブオプションを有効にすると、アラームが管理サーバの Alarm Manager Database に格納されます。デフォルトではこのオプションが有効にされています。追跡および分析の必要がないアラームの種類のみ、このオプションを無効にする必要があります。

アラームのアーカイブ作成を有効または無効にするには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから編集するアラームを選択し、[Edit] をクリックします。

[Edit Alarm Disposition] ダイアログボックスが表示されます。

4 [Other Configuration] タブをクリックします。

5 アラームのアーカイブ作成を無効にするには、[Archive] チェックボックスの選択を解除します。

または

アラームのアーカイブ作成を有効にするには、[Archive] チェックボックスを選択します。

6 [OK] をクリックします。

アラームテンプレートのソート

アラーム管理システムシステムでは、さまざまな条件に基づいてアラームテンプレートをソートできます。デフォルトではこのオプションが有効にされています。テンプレートは、[Severity]、[Generator Type]、[Category]、または [Type] に基づいてソートできます。デフォルトでは、[Type] によってソートされます。[Sort Items By] オプションの下のドロップダウンリストから選択したフィールドに基づいてテンプレートをソートすることも、[Then By] オプションを使用して複数のフィールドを組み合わせてテンプレートをソートすることもできます。

アラームテンプレートをソートするには

1 Novell ConsoleOne の左側のフレームで、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Sort] ボタンをクリックします。

[Template Sorting] ダイアログボックスが表示されます。

4 [Sort Items By] ドロップダウンリストからフィールドを選択します。

5 [Then By] ドロップダウンリストからフィールドを選択します。

6 [Items By] ドロップダウンリストからフィールドを選択します。

7 [OK] をクリックします。

テンプレートは、[Sort Items By] オプションで選択したフィールドとこれらのオプションで選択した複数のフィールドに基づいてソートされます。たとえば、重要度、カテゴリ、生成者タイプに基づいてテンプレートをソートする場合は、[Sort Items By] リストで [Severity] を選択し、2 つの [Then By] リストで [Category] と [Generator Type] を選択します。テンプレートはまず重要度に基づいてソートされ、次にカテゴリ、生成者タイプの順に基づいてソートされます。

Novell ConsoleOne からのアラームテンプレートの削除

Novell ConsoleOne を使用して、[Alarm Templates] リストからアラームテンプレートを削除できます。削除したテンプレートに対応するアラームは、Alarm Manager によって処理されません。

Novell ConsoleOne を使用してアラームテンプレートを削除するには

1 Novell ConsoleOne で、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから削除するアラームテンプレートを選択し、[Delete] をクリックします。

アラーム処理の印刷

1 Novell ConsoleOne で、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストからアラームテンプレートを選択し、[Print] をクリックします。

4 [Print] ダイアログボックスでプロパティを選択し、[OK] をクリックします。

ファイルへのアラーム処理のエクスポート

アラーム処理情報を次のファイル形式にエクスポートできます。

- カンマ区切り (.csv)
- HTML (.html)
- タブ区切り (*.txt)
- 空白区切り (*.txt)

アラーム処理情報をファイルにエクスポートするには

1 Novell ConsoleOne で、Novell ZENworks Server Management のサイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Alarm Disposition] タブをクリックします。

3 [Alarm Templates] リストから印刷するアラームを選択し、[Print] > [Print to File] の順にクリックします。

4 アラーム処理情報のエクスポートに使用するファイル形式を選択します。

5 ファイル名を指定するか、[Browse] をクリックしてファイル名を選択します

6 [OK] をクリックします。

Microsoft Excel へのアラームテンプレートのコピー

Microsoft* Excel シートにアラームテンプレートをコピーできます。

1 コピーするアラームテンプレートを選択します。

2 (Ctrl)+(C) を押します。

3 Microsoft Excel シートで (Ctrl)+(V) を押します。

アラーム管理システムの維持

Novell ZENworks Server Management サーバの Alarm Manager Database のサイズは、アラーム管理システムがアラームのログを記録するたびに増加します。

重要： データベースのサイズは、管理しない限り管理サーバのハードディスクがいっぱいになるまで増加し続けます。

Alarm Manager Database のサイズを管理するには、解決済みのアラーム、または今後の参照やアクションに必要のないアラームを定期的に削除します。これにより、アラームレコードのインスタンスを Alarm Manager Database から削除して、データベースのサイズを管理します。

Novell ConsoleOne で、[View] メニューによって表示される [Alarm History] ビューからアラームを削除できます。詳細については、896 ページの「アラームの削除」を参照してください。

アラーム管理システムのトラブルシューティング

アラーム管理システムは、送信を要求していない SNMP トラップをエージェントから受信すると、デバイスの MIB で定義されたトラップタイプオブジェクトの適切なアラームテンプレートを探します。利用できるアラームテンプレートがない場合、アラーム管理システムは *installation_volume*¥*installation_directory*¥novell zenworks¥mms¥mwserver¥properties¥alarmmanager.properties ファイルの IgnoreUnknownTrap フラグを調べます。フラグの値が True の場合、アラームは無視されます。フラグの値が False の場合、アラームは未定義のトラップとしてデータベースにアーカイブされます。フラグの値が Yes の場合、アラームは無視されます。フラグの値が No の場合、アラームは未定義のトラップとしてデータベースにアーカイブされます。フラグのデフォルト値は Yes に設定されています。

この問題を解決するには、管理サーバの MIB Pool にデバイスの MIB を追加する必要があります。MIB には、デバイスから送信されるトラップのトラップ定義が含まれます。トラップタイプオブジェクトがアラーム管理システムで定義されていない場合は、トラップ OID（オブジェクト識別子）から受信したアラームの種類を解決できないため、未定義のアラームと見なされます。MIB のコンパイルと、MIB Pool への MIB の追加については、26 章 951 ページの「MIB ツールの使用」を参照してください。

新しいデバイスをネットワークに追加する場合は、MIB Pool に MIB を追加する必要があります。SNMP エージェントがステーション上でホストされるプロキシエージェントで、ソフトウェアが更新された場合は、MIB Pool の MIB を更新する必要があります。

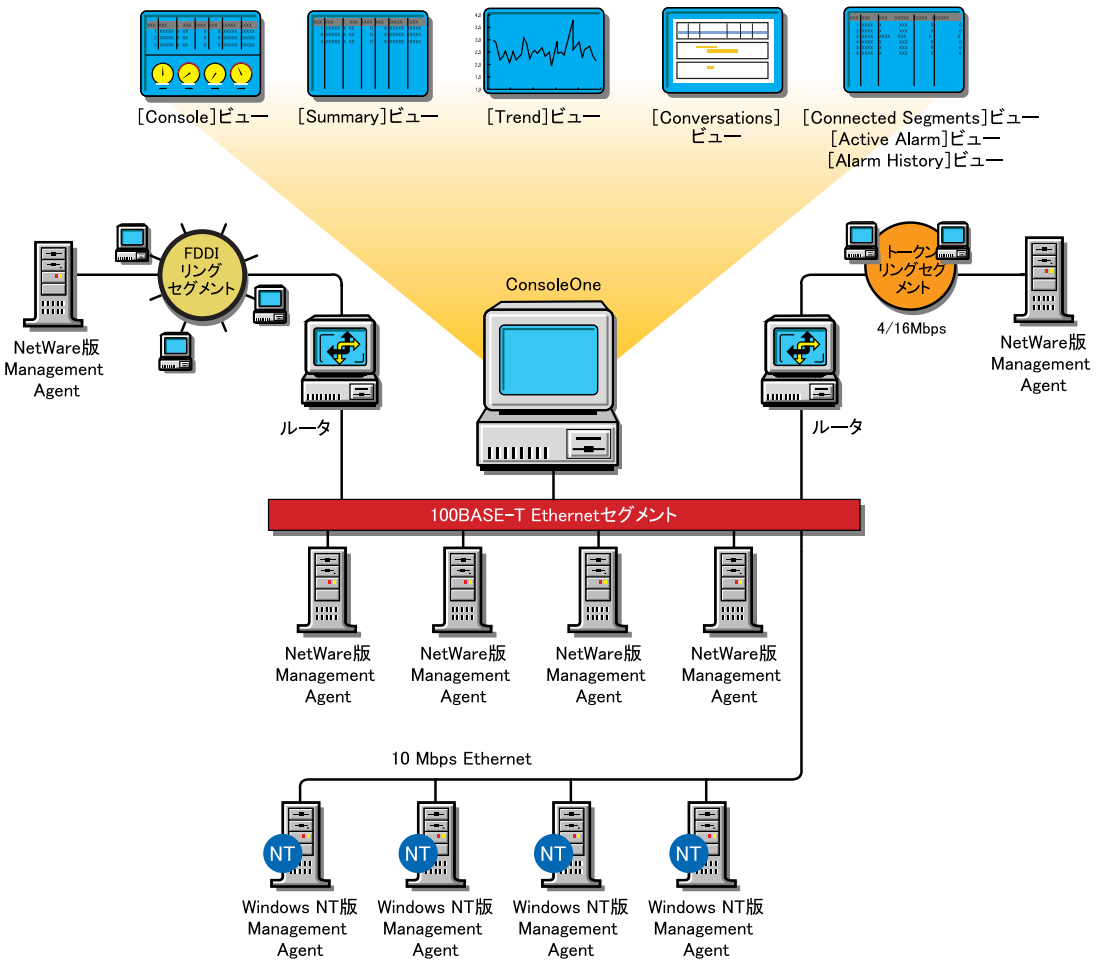
25 サーバ管理の理解

Novell ZENworks® Server Management のコンポーネントを使用することにより、ネットワーク上に存在する管理対象サーバとノードを監視、設定、および管理することができます。Novell NetWare® サーバおよび Windows サーバ用の SNMP ベースのサーバ管理エージェントは、リアルタイムのサーバパフォーマンスデータおよびサーバのアラームとイベントに関する情報をネットワーク管理コンソールに提供します。Novell ConsoleOne の左ペインにあるアトラスページマップまたは階層リストからサーバやノードを選択することにより、3 つの主要なビューの情報にアクセスすることができます。

- **[Console] ビュー：** 選択したサーバまたはノードに関する詳細情報を表示します。サーバ設定をドリルダウンすることにより、コンピュータで利用できるデバイス、オペレーティングシステム、およびサービスなど、コンピュータの内部コンポーネントに関する情報を表示することができます。
- **[Summary] ビュー：** サーバによって生成されたアラーム、CPU 使用率、および使用できるディスク容量など、サーバのパフォーマンスに関する詳細情報を表示します。サーバ設定をドリルダウンして、プロセッサ、スレッド、メモリ、ボリュームなどその他のコンポーネントに関する概要情報を表示することもできます。
- **[Trend] ビュー：** トレンドパラメータをグラフに表示し、さまざまな期間におけるサーバの状態を監視できるようにします。トレンドデータを使用することで、サーバの稼働状況を追跡することができます。この結果、潜在的な問題の発生を予測して、今後のサーバ構成の拡張計画を策定することができます。

サーバ管理コンポーネントを使用すると、ネットワーク上のサーバに関する情報を表示できるほか、管理対象の NetWare サーバを設定し、頻繁に使用するコマンドを Novell ConsoleOne から実行することができます。

次の図は、ZENworks Server Management コンポーネントの機能について示しています。NetWare 版 Management Agent と Windows 版 Management Agent がネットワーク全体に導入されています。



この節では次のトピックについて説明し、サーバ管理コンポーネントに関する詳細情報を提供します。

- 908 ページの「サーバ管理の理解」
- 910 ページの「サーバ管理の計画」
- 913 ページの「サーバ管理の最適化」
- 920 ページの「サーバの管理」
- 929 ページの「オブジェクトの階層構造とビューの詳細」

サーバ管理の理解

NetWare 版 Management Agent および Windows 版 Management Agent は、NetWare および Windows サーバソフトウェアのサーバ管理機能を上回るメリットを提供します。

この節では、次のトピックについて説明します。

- 909 ページの「SNMP ベースのサーバ管理」
- 910 ページの「SNMP エージェントの機能」

SNMP ベースのサーバ管理

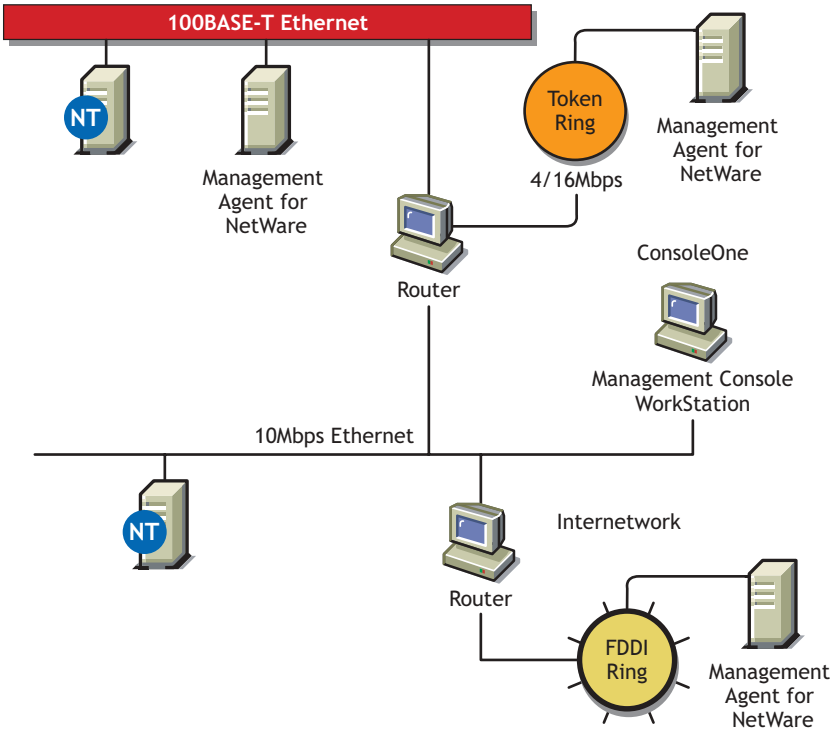
NetWare 版 Management Agent および Windows 版 Management Agent を使用する主なメリットは、これらのエージェントが業界標準の SNAP (Simple Network Management Protocol) をサポートしている点です。SNMP は、ネットワーク管理を制御するプロトコルであり、ネットワークデバイスとその機能を監視します。

Novell ZENworks Server Management SNMP エージェントは、パケット (データグラム) を送受信するのに UDP/IP、IPX™、および NCP™ の実装をサポートしています。この標準メカニズムの採用により、任意の SNMP コンソールまたはマネージャを使って、Novell ZENworks Server Management SNMP エージェントの情報を要求することができます。SNMP をサポートするすべてのコンソールを、SNMP コンソールとして使用することができます。Novell ZENworks Server Management Novell ConsoleOne は、SNMP v.1 による通信を完全にサポートしています。

SNMP エージェント

Novell ZENworks Server Management SNMP エージェントは、ネットワーク内の NetWare サーバと Windows サーバで稼働します。エージェントはサーバを監視し、Novell ConsoleOne のリクエストに応じて履歴データと動的データを収集します。管理者は、Novell ZENworks Server Management Novell ConsoleOne で、サーバで検出されたデバイス、オペレーティングシステム、またはサービスを表すアイコンをクリックするだけでデータを要求できます。

次の図は、NetWare 版 Management Agent と Windows 版 Management Agent、および ZENworks Server Management の ConsoleOne を使用したインターネットワークを示しています。



SNMP エージェントの機能

NetWare 版 Management Agent および Windows 版 Management Agent（NetWare および Windows サーバ向けの Novell SNMP ベースエージェント）の機能は、次のカテゴリに分類できます。

- 統計情報の収集
  - 監視：サーバを監視することにより、サーバのさまざまな監視要素に関する情報が即座に提供されます。こうした要素には、CPU 使用率、メモリ容量、キャッシュバッファ、接続しているユーザ、ボリューム、ディスク、各ユーザが使用しているディスク容量、ネットワークアダプタ、プリントキュー、プリントジョブ、および NetWare サーバまたは Windows サーバにロードされた NLM™(NetWare Loadable Module™) が含まれます。
  - トレンド分析：トレンドにより、さまざまなサーバオブジェクトに関する履歴データが提供され、SNMP コンソールのグラフに表示できます。トレンドはサーバ側に保存されるため、SNMP マネージャから継続的にポーリングを実行する必要はありません。このデータには、Novell ZENworks Server Management Novell ConsoleOne またはその他の SNMP ベースコンソールから SNMP を介してアクセスできます。
- アラーム通知：580 を超える種類のアラームまたはイベント (SNMP トラップ) を、任意の NetWare サーバから Novell ZENworks Server Management システムまたはその他の SNMP ベースコンソールに送信することができます。

  Windows システム、セキュリティ、またはアプリケーションに関するすべてのイベントは SNMP トラップに変換され、Novell ZENworks Server Management システムやその他の SNMP ベースコンソールに送信されます。

  イベントが発生した場合やしきい値を超えた場合、アラームにより管理者に通知されます。
- 設定管理：ネットワーク管理者は、NetWare 版 Management Agent を使って、リモートで NetWare サーバを設定することができます。NetWare サーバには、サーバパフォーマンスの調整に使用できる 187 個の SET パラメータが存在します。管理者は、Novell ZENworks Server Management Novell ConsoleOne で設定を表示して、すべてのパラメータを変更することができます。

SNMP エージェントは、管理対象になるすべてのサーバにインストールする必要があります。SNMP エージェントのインストールに関する詳細情報が必要な場合、または管理対象になるサーバにすでにエージェントソフトウェアをインストールしている場合は、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」を参照してください。

サーバ管理の計画

ネットワークサーバの通常のアクティビティを基準として定義できます。サーバアクティビティの基準ドキュメントを用意しておくと、アクティビティの異常を検出することができます。基準になるアクティビティを作成するには、サーバが正常に機能しているときに統計情報を収集する必要があります。

この節では、サーバ管理戦略を計画できるよう、次の情報について説明します。

- 911 ページの「通常のサーバアクティビティ基準の作成」
- 911 ページの「基準ドキュメントの使用」
- 911 ページの「サーバ基準ドキュメントに関するヒント」

通常のサーバアクティビティ基準の作成

CPU 使用率などのサーバに関する統計について、一定期間の情報をプロットしたトレンドグラフを作成する必要があります。統計サンプルのデータ収集期間が短い場合は、正確な統計値が得られないことがあります。サーバの設定を変更する場合、今後のアクティビティの比較対象になる別の基準を作成すると便利です。

基準ドキュメントの作成には 2 つの方法があります。1 つ目は、基準設定の対象になるさまざまなトレンドグラフを印刷することにより、手動で作成する方法です。もう 1 つは、サーバ管理のヘルスレポートを基準ドキュメントとして使用する方法です。ヘルスレポートの作成と生成に関する詳細については、1112 ページの「Server Management のヘルスレポートの管理」を参照してください。いずれのケースでも、収集されたデータをスプレッドシートなどのプログラムにエクスポートして、さらに詳しい分析を実行したり、レコードを長期間保存したりすることができます。

基準ドキュメントの使用

次の節では、基準ドキュメントの計画および使用に役立つ情報について説明します。

- 911 ページの「基準ドキュメントを使用してアラームしきい値を適切に設定する」
- 911 ページの「基準ドキュメントによるサーバの使用状況の追跡」
- 911 ページの「基準ドキュメントを使用したトラブルシューティング」

基準ドキュメントを使用してアラームしきい値を適切に設定する

SNMP エージェントソフトウェアの監視対象になるサーバの統計に対してアラームしきい値を設定する必要があります。このしきい値を超えると、Novell ConsoleOne に通知されます。サーバの統計に対してアラームしきい値を設定すると、ポーリングの対象になるサーバの統計情報を常に監視して、問題が発生していないかどうかを確認する必要はなくなります。

Server Management コンポーネントは、サーバの統計情報にデフォルトのしきい値を設定します。統計情報が変化してしきい値を超えると、アラームが生成されます。

基準ドキュメントによるサーバの使用状況の追跡

現在のサーバパフォーマンスの統計情報を、基準ドキュメントに記録されたパフォーマンスと比較することにより、サーバ設定の変更がパフォーマンスにどのような影響を及ぼしているのかを確認できます。この比較により、今後の負荷の増大を予測し、アップグレードや拡張を計画することもできます。リアルタイムのトレンドをグラフで表示したり、時間、日、週、月、および年単位の履歴データをグラフで表示したりできます。

基準ドキュメントを使用したトラブルシューティング

通常のサーバアクティビティを把握しておくことで、異常なアクティビティを認識し、問題の原因を特定することができます。

サーバ基準ドキュメントに関するヒント

各サーバ基準ドキュメントには、次に示す重要な情報を記載する必要があります。

- 912 ページの「CPU 使用率」
- 912 ページの「キャッシュバッファ」

- 912 ページの「ファイルの読み取りと書き込み」
- 912 ページの「ボリューム使用率」
- 912 ページの「Running Software」

CPU 使用率

CPU 使用率の統計情報は、マイクロプロセッサの使用状況を示します。CPU の使用率が高くなっている場合、ネットワークの応答に遅延が生じる可能性があります。使用率は、1 日のうちの特定の時間で高くなることがあります（たとえば、ユーザが朝にネットワークにログインするときや、電子メールにアクセスするとき）。また、特定の週や月で高くなることもあります。CPU 使用率を追跡すると、ピーク時やほとんど使用されていないときにサーバプロセッサにかかる負荷を把握することができます。この情報により、現在のシステムの性能およびアプリケーションプロセッサに求められるニーズの確認、およびパフォーマンスに与える影響の分析を実行することができます。

キャッシュバッファ

ほぼすべてのプロセッサが、処理の実行にサーバキャッシュを使用します。サーバキャッシュとは、ファイルが一時的に格納されるサーバメモリ（RAM）のブロックです。キャッシュバッファを使用すると、サーバのパフォーマンスは大きく向上し、ワークステーションはより高速にデータにアクセスできるようになります。これは、メモリに対する読み取り / 書き込み処理が、ディスクに対する読み取り / 書き込み処理に比べてきわめて高速に実行されるためです。最適なキャッシュバッファ容量は、サーバの総メモリ容量の 65% から 75% です（これ以上のキャッシュバッファを設定しても、パフォーマンスに悪影響を与えることはありません）。キャッシュバッファの容量が少ないと、サーバのパフォーマンスが低下して、異常終了する場合があります。サービスは、サーバの総メモリ容量の 45% に大幅に低下します。

ファイルの読み取りと書き込み

基準ドキュメントを使ってファイルの読み取りと書き込みに関するデータを追跡することにより、ボトルネックがディスク I/O チャネルによって発生しているのかどうかを確認できる場合があります。たとえば、ユーザに送信される ″サーバビジー″ パケットの数が増加し、ファイルの読み取りおよび書き込み数も増加した場合、ディスク I/O チャネルの速度低下やディスクアダプタドライバの障害によりボトルネックが発生することがあります。

ボリューム使用率

ボリューム使用率を追跡するのは、主に容量に関する計画を実行するためです。使用されるボリューム容量を長期にわたって追跡することにより、どのタイミングでストレージを増設する必要があるかを正確に予測できます。ボリューム使用率を追跡することにより、サーバでディスク容量の不足が発生しないようにすることもできます。

Running Software

実行中のソフトウェアに関する情報を基準ドキュメントに記載することにより、異なるサーバのソフトウェアを比較して、問題の発生しているアプリケーションをより簡単に特定することができます。各アプリケーションが使用するメモリ容量を基準ドキュメントに記載する方法も有効です。サーバですべてのメモリが使用されている場合に、どのアプリケーションが最も多くのメモリを使用しているのかを即座に確認できます。

サーバ管理の最適化

次の節に示す各設定オプションを確認し、どの機能を実行する必要があるかを決定します。

- 913 ページの「デフォルトのトレンドとしきい値の設定」
- 917 ページの「アラーム生成の管理」
- 919 ページの「SNMP アラームの受信先の定義」

デフォルトのトレンドとしきい値の設定

Novell ConsoleOne 内で、デフォルトのトレンド値およびしきい値を変更したり、NetWare 版 Management Agent または Windows 版 Management Agent ソフトウェアがインストールされているサーバのファイルを手動で変更したりすることができます。

サーバエージェントが最初にロードされたときに、ntrend.ini file（NetWare の場合）または n_nttren.ini file（Windows の場合）から、トレンドおよびしきい値の初期（デフォルト）値が読み取られます。初期値は、新しいトレンドファイルを作成するときにも必ず使用されます。新しいトレンドファイルは、監視対象になるオブジェクト（ボリューム、ディスク、インタフェースなど）のインスタンスがサーバで検出されたときに作成されます。

ntrend.ini ファイルから抜粋したサンプルを次に示します。

```
#-------------------------------------------------------
#                    | Sample |    Trend     |      Threshold      |
#Parameter            | Interval | Buckets Enbl | Rising Falling Enbl Type |
#-------------------------------------------------------
NUMBER_LOGGED_IN_USERS 5          60      1      100    90      1    rising
NUMBER_LOGGED_IN_USERS 7          8928    1      90     81      1    rising

NUMBER_CONNECTIONS     5          60      1      0      0       0    rising
NUMBER_CONNECTIONS     7          8928    1      0      0       0    rising

FILE_READS             5          60      1      0      0       0    rising
FILE_READS             7          8928    1      0      0       0    rising

FILE_WRITES            5          60      1      0      0       0    rising
FILE_WRITES            7          8928    1      0      0       0    rising

FILE_READ_KBYTES       5          60      1      0      0       0    rising
FILE_READ_KBYTES       7          8928    1      0      0       0    rising

FILE_WRITE_KBYTES      5          60      1      0      0       0    rising
FILE_WRITE_KBYTES      7          8928    1      0      0       0    rising

LSL_IN_PACKETS         5          60      1      0      0       0    rising
LSL_IN_PACKETS         7          8928    1      0      0       0    rising

LSL_OUT_PACKETS        5          60      1      0      0       0    rising
LSL_OUT_PACKETS        7          8928    1      0      0       0    rising

NCP_REQUESTS           5          60      1      0      0       0    rising
NCP_REQUESTS           7          8928    1      0      0       0    rising

CPU_UTILIZATION        5          60      1      90     81      1    rising
CPU_UTILIZATION        7          8928    1      80     72      1    rising

CACHE_BUFFERS          5          60      1      45     40      1    falling
CACHE_BUFFERS          7          8928    1      0      0       1    falling

CODE_DATA_MEMORY       5          60      1      0      0       0    rising
CODE_DATA_MEMORY       7          8928    1      0      0       0    rising
```

NetWare 版 Management Agent および Windows 版 Management Agent ソフトウェアの実行後、Novell ZENworks Server Management のしきい値設定機能を利用して、トレンド値およびしきい値を（Novell ConsoleOne を使って）変更することができます。サーバが停止した場合、サーバには、設定されていた最後のトレンドおよびしきい値の設定が保持されます。次のいずれかの状況が発生した場合、初期値はリセットされます。

- トレンドファイルが手動で削除された場合。

- たとえば、新しいボリューム、ディスク、またはインタフェースを追加することにより、サーバ構成が変更された場合。

重要： CD ボリュームのトレンドは保持されません。したがって、CD ボリュームのトレンドパラメータを変更しても効果はありません。

次の節では、初期のトレンド値およびしきい値を変更する場合に役立つ情報について説明します。

- 914 ページの「初期トレンド値の変更」
- 916 ページの「初期しきい値の変更」

初期トレンド値の変更

ntrend.ini ファイル（NetWare の場合）および n_nttren.ini ファイル（Windows の場合）に含まれるトレンド値により、特定のトレンドパラメータについてサンプルが取得される間隔（Sample Interval）、こうしたサンプルが保持される期間（Trend Buckets）、およびこのサンプル取得パラメータが有効かどうか（Enbl）が指定されます。ntrend.ini ファイルまたは n_nttren.ini ファイルの行で指定された各値に関するトレンドレコードが、個別のファイルとして sys:¥ntrend ディレクトリ（NetWare サーバの場合）または ¥trenfile ディレクトリ（Windows サーバの場合）に保存されます。

次の図は、ntrend.ini ファイルの NUMBER_LOGGED_IN_USERS トレンドパラメータに関する行を示しており、Sample Interval が 5、Trend Buckets が 60、および有効パラメータが 1（有効）に設定されています。

```
#-------------------------------------------------------
#                  | Sample | Trend          | Threshold
#  Parameter       | Interval | Buckets Enbl | Rising Falling Enbl Type |
#-------------------------------------------------------
NUMBER_LOGGED_IN_USERS  5       60      1      100    90     1    rising
```

次の節では、トレンドファイルで必須になる各パラメータを設定または変更する方法について説明します。

- 914 ページの「サンプル間隔の設定」
- 915 ページの「トレンドバケットの設定」
- 916 ページの「トレンドファイルの有効化 / 無効化」
- 916 ページの「トレンドデータのバックアップ」

ntrend.ini ファイルまたは n_nttren.ini ファイルに行を追加することにより、トレンドパラメータに対し複数のサンプル取得間隔および期間を指定することができます。

サンプル間隔の設定

指定したパラメータについて、トレンド分析ソフトウェアを使って、12 種類（5 秒から 1 日まで）の時間間隔（Sample Interval）の中からサンプルを収集することができます。

これらのサンプル間隔はそれぞれ、ntrend.ini ファイルおよび n_nttren.ini ファイル内のコード番号により指定されます。次の表は、使用できるサンプル間隔について、ntrend.ini および n_ntrend.ini ファイルで使用されるコードを示します。たとえば、特定のトレンドパラメータのサンプルを 1 時間ごとに収集する場合、コード 9 を使用します。

サンプル間隔	コード
5 秒	1
10 秒	2
15 秒	3
30 秒	4
1 分	5
5 分	6
15 分	7
30 分	8
1 時間	9
4 時間	10
8 時間	11
1 日	12

トレンドバケットの設定

サンプルを収集する間隔を決定したら、収集する期間を設定する必要があります。たとえば、特定のパラメータについて 1 時間のサンプル間隔を選択した場合、期間を 1 日、サンプル間隔を 1 時間に指定して、そのパラメータの状態を確認することができます。

指定したトレンドバケット数により、パラメータの収集期間が決定します。特定の期間で収集を実行するサンプルごとにトレンドバケットを指定する必要があります。たとえば、1 日の状態を 1 時間ごとに確認するには、24 個のトレンドバケット（1 時間ごと x24 時間）が必要になります。

特定の期間およびサンプル間隔で必要になるトレンドバケット数は簡単に計算できますが、実行可能なサンプル間隔で必要になるトレンドバケット数を簡単に参照できるよう、次の表を用意しました。期間については、1 時間から 1 年までの 7 つの種類を設定できます。

トレンド収集のサンプル間隔と期間を設定したら、トレンドファイルのサイズを計算することができます。特定のサンプル間隔および期間について、想定されるトレンドバケットの数、および KB 単位でのおよそのサイズ（括弧内に表示）も次の表で示しています。各トレンドバケットのサイズは、4 バイトにヘッダファイルの 512 バイトを加算した数値になります。たとえば、サンプル間隔が 5 秒で期間が 1 時間の場合、ファイルサイズは、720 個のトレンドバケット x4 バイト長（計算結果は、およそ 4KB）に 512 バイトを加算した数値になり、合計で 4.5KB になります。有効にされているトレンドと同じ数のトレンドファイルが常に存在します。

サンプル間隔	1 時間	1 日	1 週間	1ヶ月	3ヶ月
5 秒	720	17280	120960	535680	1607040
10 秒	360	8640	60480	267840	803520

サンプル間隔	1 時間	1 日	1 週間	1ヶ月	3ヶ月
15 秒	240	5760	40320	178560	535680
30 秒	120	2880	20160	89280	267840
1 分	60	1440	10080	44640	133920
5 分	12	288	2016	8929	26784
15 分	4	96	672	2975	8928
30 分	2	48	336	1488	4464
1 時間	1	24	168	744	2232
4 時間		6	42	186	558
8 時間		3	21	93	279
[1 Day]		1	7	31	93

指定した期間がファイルで経過した（トレンドバケットで満杯になった）後は、最新のサンプルによって最も古いサンプルが上書きされます。つまりファイルには、記録された期間における最新のサンプルが含まれます。たとえば期間を 24 時間とし、1 時間おきにサンプルを収集することを選択した場合（24 個のトレンドバケットを使用）、関連付けられたファイルには直近の 24 時間分のトレンドデータが含まれます。

トレンドファイルの有効化 / 無効化

ntrend.ini ファイルおよび n_nttren.ini ファイルの各行には、起動時にトレンドファイルの作成を開始するトレンド分析値の有効 / 無効を決定するパラメータが含まれています。トレンドファイルのデータ収集を有効にするには、このパラメータを 1 に設定します。起動時にトレンドファイルのデータ収集を無効にするには、このパラメータを 0 に設定します。

トレンドデータのバックアップ

トレンドデータが自動的にバックアップされることはありません。トレンドデータをバックアップする場合は、手動で実行する必要があります。

初期しきい値の変更

ntrend.ini ファイルおよび n_nttren.ini ファイルのデフォルトのしきい値により、いつトラップが生成されるかが指定されます。ユーザが定義した値は、トレンドファイルのヘッダに保存されます。パラメータが、設定されたしきい値を上回った場合は上昇トラップが、下回った場合は下降トラップが送信されます。

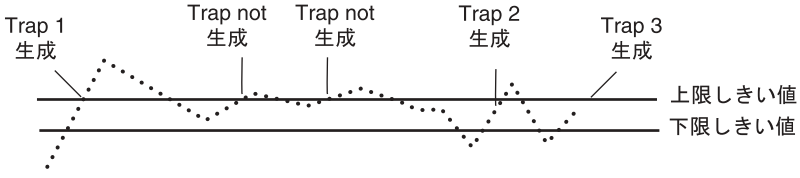
次の節では、しきい値で必要になる各パラメータを設定または変更する方法について説明します。

- 917 ページの「上限しきい値と下限しきい値の設定」
- 917 ページの「しきい値トラップの有効化 / 無効化」

上限しきい値と下限しきい値の設定

ntrend.ini ファイルおよび n_nttren.ini ファイルの各行には、上限しきい値と下限しきい値のパラメータが含まれます。各サンプル間隔で、指定したとおりの上昇トラップまたは下降トラップを生成できます。トラップの生成後、サンプル収集の対象になる値がこのしきい値を下回り、下限しきい値に達しない限り、このトラップが新たに生成されることはありません。

次の図の例は、上昇しきい値トラップを使ってこのプロセスを表しています。



この例で、Trap 1 が生成されるのは、パラメータの値が初めて上限しきい値を上回ったときです。この後、パラメータ値は 2 度上限しきい値を上回りますが、このときトラップが生成されることはありません。これは、パラメータが下限しきい値を下回っていないためです。Trap 2 および Trap 3 が生成されるのは、パラメータ値が下限しきい値を下回った後に、上限しきい値を上回ったためです。

しきい値トラップの有効化 / 無効化

ntrend.ini ファイルおよび n_nttren.ini ファイルの各行には、上限および下限しきい値に達した場合にトラップを送信する ntrend.nlm ソフトウェアを有効または無効にするパラメータが含まれています。このソフトウェアが、指定された値でトラップを送信できるようにするには、このパラメータを 1 に設定します。ソフトウェアがトラップを送信できないようにするには、このパラメータを 0 に設定します。

アラーム生成の管理

各管理対象サーバには、どのシステムイベントによってトラップが生成されるのかを指定するファイルが含まれています。NetWare では、nwtrap.cfg ファイルと ndstrap.cfg ファイルが sys:¥etc ディレクトリに保存されます。Windows NT では、nttrap.ini がこのファイルに該当し、mw¥ini ディレクトリに保存されます。

NetWare では、トラップ設定ファイルは nwtrap.nlm がロードされた場合にだけ読み取られます。したがって、トラップ設定ファイルへの変更は、次に nwtrap.nlm または ndstrap.nlm がロードされるまで有効になりません。

NetWare の .cfg ファイルには、サポートされるトラップの一覧が含まれます。次に示す項目を使って .cfg ファイルまたは nttrap.ini ファイルを変更できます。

- Novell ConsoleOne に転送されるアラームの種類
- SNMP トラップの送信に使用されるコミュニティ文字列
- マスクキーワードを使って無効にされるトラップの一覧
- 転送を禁止したい具体的なアラーム

環境設定ファイルは、キーワードおよびそれに関連付けられたデータ (大文字小文字の区別は無視されます) で構成されます。各キーワードは、それ自体で 1 行を構成する必要があります (マスクの値は除く。この値は複数の行にまたがる場合がある)。そしてキーワードの後には、1 行以上の関連付けられたデータが続きます。

ファイルの任意の場所にコメントを配置できます。キーワードとそれに関連付けられた情報との間にコメントを配置することもできます。コメントは、番号記号 (#) で始まり、その行の最後まで続きます。

次に示すのは、nwtrap.cfg ファイルの例です。

```
#
###################################
#NWTRAP.CFG
#
#NWTRAP Configuration File
#
#This file specifies information to be used by NWTRAP.NLM
#The file is read and the parameters set when NWTRAP is loaded. It must
#reside on volume SYS: in the directory SYS:\ETC and must be named
#NWTRAP.CFG to be found by NWTRAP. To change the parameters, first
#editthis file, then unload NWTRAP and load it again. Any changes to this
#file will not take effect until NWTRAP is next loaded. The parameters
#are specified by using a parameter keyword followed by the desired
#parameter value.
#
###############################################

Community
        Public
Time Interval
        10
Severity
        Warning

mask
#         "Memory: Short term alloc failed"
#          1

#         "FileSys: Directory write error (no vol)"
#          2

#         "FileSys: File write err, by server (no path)"
#          3

#         "FileSys: File write err, by user (no path)"
#          4
```

次の節では、アラーム生成の管理に役立つ情報について説明します。

- 918 ページの「時間間隔の設定 (NetWare 版 Management Agent のみ)」
- 919 ページの「アラーム重要度レベルの設定」

時間間隔の設定 (NetWare 版 Management Agent のみ)

同じパラメータまたはほとんど同じパラメータによってアラームが続けざまに (1 秒または 1 分につき数回) 発生することがあります。このような事態が発生した場合でも、時間間隔を指定することにより、間隔内で生成された 2 番目以降のアラームが最初のアラームとして解釈されることを回避できます。

ネットワークおよび Novell ConsoleOne に同じアラームが殺到する事態を回避するため、生成される各アラームに特定の時間間隔を指定することができます。最初のアラームと同じアラームがこの間隔内で発生した場合、そのアラームは破棄されます。

環境設定ファイルで、次のとおり時間間隔を定義できます。

Time Interval

n

n には、0 から 232 までの任意の値を指定することができます。この値は秒数を示し、この期間を経過しない限り、続けて発生する同様のアラームは破棄されます。

デフォルトの時間間隔は 10 秒です。

アラーム重要度レベルの設定

重要度キーワードを使って、アラームの重要度の最低レベルを設定し、それより重要度の低いアラームのトラップが送信されないようにします。

nwtrap.cfg および nttrap.ini ファイルで設定できる重要度レベルは、情報、警告、回復可能、重大、および致命的です。次の表は、NetWare の重要度レベルとそれに相当する SNMP および Novell ZENworks Server Management の重要度レベルを示しています

NetWare 重要度レベル	SNMP 重要度レベル	ZENworks Server Management 重要度レベル
0 - 情報	情報	情報
1 - 警告	マイナー	マイナー
2 - 回復可能	メジャー	メジャー
3 - 重大	重大	深刻
4 - 致命的	致命的	深刻
5 - 処理中止	致命的	深刻
回復不能	致命的	深刻

デフォルトのキーワードは警告です。デフォルトでは、警告以上の重要度レベルが設定されたすべてのアラームが転送されます。

SNMP アラームの受信先の定義

SNMP トラップ（アラーム）を Novell ZENworks Server Management サーバまたは他の管理ノードに送信するよう NetWare 版 Management Agent を設定することができます。

注： Windows サーバでトラップの送信先を設定する場合は、Microsoft Windows オペレーティングシステムソフトウェアに同梱されている、SNMP サービスに関するマニュアルを参照してください。

トラップの送信先を指定する手順については、次の節で説明します。

手動での traptarg.cfg ファイルの編集 (NetWare 版 Management Agent のみ)

トラップの受信先を手動で traptarg.cfg ファイルに追加することにより、こうした受信者を設定することができます。これは、トラップを Novell ZENworks Server Management サーバ以外のサードパーティ管理コンソールに送信する場合に役立ちます。

トラップの受信先のアドレスを traptarg.cfg ファイルで指定することにより、これらの受信先を手動で追加することができます。このファイルは、すべての NetWare サーバの sys:¥etc ディレクトリに配置されます。

traptarg.cfg は、SNMP トラップの受信先を定義します。このファイルにより、IPX および UDP/IP を使って送信する SNMP トラップの受信先を定義することができます。ファイルを IPX セクションと UDP/IP セクションに分割する方法、および受信先の IPX アドレスと IP アドレスを記述する方法を示すため、このファイルには必要な注釈がすべて付けられます。

traptarg.cfg ファイルは、SNMP がロードされた場合にのみ読み取られます。ほとんどの場合、SNMP がロードされるのは、サーバを停止して再起動したときです。これは、SNMP をロードする際には、さまざまなモジュールをアンロードして、再ロードする必要もあるためです。このように、traptarg.cfg ファイルに実行された変更は、次に nwtrap.nlm をロードするまで有効にはなりません。

重要： nwalarm.mib ファイルは、ホストリソース MIB (RFC1514.MIB) から記号をインポートします。このファイルは sys:novell zenworks¥mms¥mwserver¥mibcserver¥mibserverpool¥mibpool でも見つけることができます。

サーバの管理

NetWare 版 Management Agent ソフトウェアを NetWare サーバに、または Windows 版 Management Agent ソフトウェアを Windows サーバにインストールすると、管理対象サーバについて、データ収集を開始し、アラーム通知を受信できるようになります。さらに、設定をリモートで管理したり、レポートを生成したりすることもできるようになります。

Novell ZENworks Server Management で実行できるサーバ管理タスクは次のとおりです。

- 920 ページの「サーバ設定情報の表示」
- 921 ページの「概要データの表示」
- 922 ページの「トレンドデータの表示」
- 925 ページの「トレンドデータのサンプル収集の管理」
- 926 ページの「サーバのパラメータの設定」
- 927 ページの「サーバコマンドの実行」
- 928 ページの「Management Site Server のステータス」

サーバ設定情報の表示

サーバ設定データは、階層構造状のリストに整理されており、サーバオブジェクトから展開してドリルダウンすることができます。サーバの設定、メモリ使用率、アダプタ、ネットワークインタフェース、ディスクとディスクコントローラ、ボリューム、キュー、ユーザ、接続、開いているファイル、NLM ファイル (NetWare)、およびインストールされているソフトウェアに関する情報を表示できます。

サーバ設定情報を表示するには

1 展開したいサーバオブジェクトを特定します。

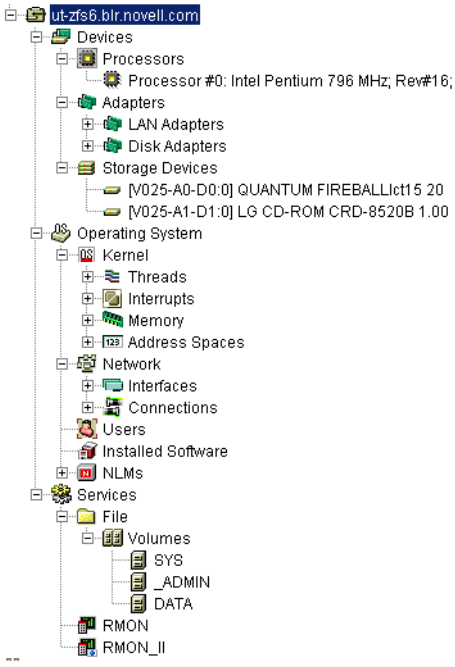
2 サーバオブジェクトの隣に表示されるプラス記号 (+) をクリックします。

左ペインの親オブジェクトの下にサーバオブジェクトが開き、サーバのコンテンツが表示されます。サーバデータは次の 3 つのカテゴリに分類されます。

-  Devices
-  オペレーティングシステム
-  サービス

3 つのカテゴリを表示できない場合、サーバオブジェクトでプローブの管理可能性を実行する必要があります。サーバオブジェクトを右クリックし、[Probe Manageability] を選択します。3 つのカテゴリが表示されます。

3 次の例で示すように、[Devices]、[Operating System]、[Services] の各オブジェクトの隣に表示されるプラス記号をクリックして、サーバ設定をさらにドリルダウンすることができます。



概要データの表示

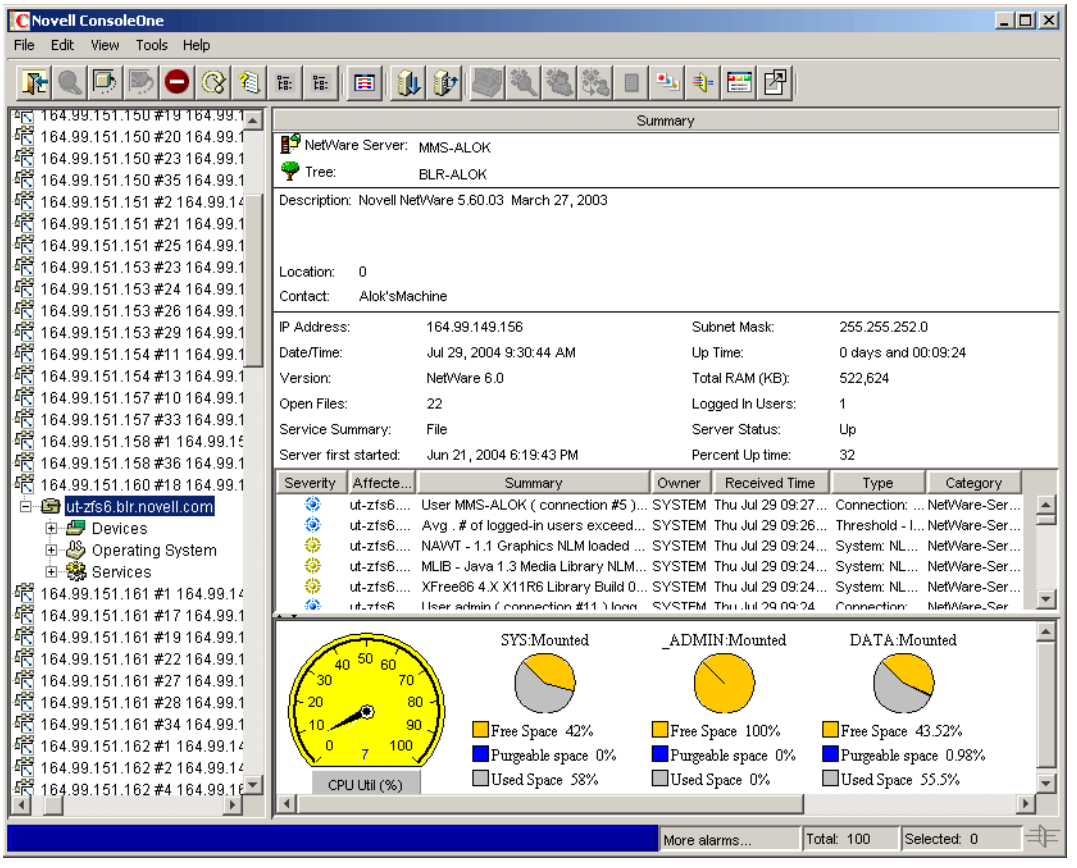
[Summary] ビューには、管理対象サーバでホストされている NetWare 版 Management Agent および Windows 版 Management Agent ソフトウェアに SNMP GET リクエストを実行して取得された統計表が表示されます。サーバは継続的にデータのポーリングを実行し、データに変化が発生した場合、統計は動的に更新されます。ポーリングを実行すると、SNMP GET および GET NEXT リクエストを利用して、データが更新されます。停止機能や再更新機能を使って、特定のオブジェクトのポーリングを制御することもできます。

サーバ、プロセッサ、LAN アダプタ、ディスクアダプタ、ストレージデバイス、スレッド、割り込み、メモリ、アドレス空間、インタフェース、接続、ユーザ、インストールされているソフトウェア、NLM ファイル (NetWare)、およびボリュームに関する概要データを表示することができます。具体的な [Summary] ビューに関する詳細については、929 ページの「オブジェクトの階層構造とビューの詳細」を参照してください。

概要情報を表示するには

1 概要データを表示するオブジェクトを右クリックし、[Views]、[Summary] の順にクリックします。

[Summary] ビューが表示されます。次の図は、サーバオブジェクトの [Summary] ビューを示しています。サーバの概要により、サーバの Novell eDirectory 名とツリー、IP アドレス、RAM、オペレーティングシステムとそのバージョン、IPX アドレス、サブネットワークマスク、稼働時間、ログインしているユーザ、開いているファイル、およびステータスなどの詳細情報が提供されます。さらにサーバの概要情報により、すべてのアラーム、影響を受けるオブジェクト、サマリ、オーナーとボリュームのディスク容量、キャッシュヒットとキャッシュバッファのトレンドグラフが示されます。[Summary] ビューにより、CPU 使用率がグラフ形式で示されます。CPU 使用率は、直前の 1 分間における CPU 処理時間の割合の平均値を表します。



トレンドデータの表示

NetWare 版 Management Agent または Windows 版 Management Agent によって管理されるサーバ上で、エージェントは CPU 使用率、メモリ使用率、およびネットワークインタフェースのトラフィックに関するトレンドデータを自動的に収集します。Novell ConsoleOne で、現在のトレンドデータや、時間、週、月、年単位の履歴トレンドデータを表示することができます。このビューでは、サンプルの収集を実行する時間間隔が x 軸に表示されます。y 軸にはサンプル期間におけるパラメータ値が割り当てられます。y 軸の値は、標準の省略形である K（キロ）、M（メガ）、および G（ギガ）を使用します。したがって、1K と表示された値は 1000 に相当します。同様に 1M と表示された値は 1,000,000 に相当します。

トレンドデータの監視は、トレンドアラームしきい値の設定、サーバの使用者の認識、サーバの使用負荷が高い時間帯の確認、問題のトラブルシューティング、複数のサーバ間での負荷の分散、リソースの計画などのタスクを実行する際に役立ちます。[Trend] ビューのデータを一般的なスプレッドシート形式にエクスポートして、他のユーザとデータを共有することもできます。

プロセッサ、LAN アダプタ、ストレージデバイス、メモリ、接続、ユーザ、およびボリュームに関するトレンドデータを表示できます。具体的な [Trend] ビューに関する詳細については、930 ページの「オブジェクトビューの詳細」を参照してください。

トレンド統計情報を表示するには

1 トレンドデータを表示するオブジェクトを右クリックし、[Views]、[Trend] の順にクリックします。

[Trend] ビューが表示されます。次の節では、[Trend] ビューを使って実行できるタスクについて説明します。

- 923 ページの「凡例の表示」
- 923 ページの「期間の変更」
- 924 ページの「[Trend] ビューの表示のカスタマイズ」
- 925 ページの「[Trend] ビュープロファイルの変更」

凡例の表示

[Trend] ビューの凡例を確認すれば、グラフで使用されている色がそれぞれ何を表しているのかがわかります。

凡例を表示するには

1 [Trend View] ツールバーの [Legend] ボタン  をクリックします。

期間の変更

[Trend] ビューの期間を指定すると、トレンドグラフに表示される時間の範囲が決まります。デフォルトでは、1 時間分の履歴が表示されます。

期間を変更するには

1 [Trend View] ツールバーのドロップダウンリストから期間を選択します。次に示す期間の中から選択できます。

- [1 Hour]
- [1 Day]
- [1 Week]
- [1 Month]
- [1 Year]

[Trend] ビューの表示のカスタマイズ

[Trend] ビューには、画面の表示方法をカスタマイズするための複数のオプションが用意されています。ビューをカスタマイズする場合、次のオプションから選択することができます。

- 924 ページの「グリッド線の表示」.
- 924 ページの「グラフの積み上げ / 積み上げ解除」.
- 924 ページの「Y 軸のサイズ変更」.

グリッド線の表示

デフォルトでは、トレンドグラフにグリッド線は表示されません。

水平および垂直方向のグリッド線を表示するには

1. 水平方向のグリッド線を表示するには、[Trend View] ツールバーの [Horizontal Grid]  ボタンを選択します。
2. 垂直方向のグリッド線を表示するには、[Trend View] ツールバーの [Vertical Grid]  ボタンを選択します。

   もう一度ボタンをクリックすると、水平および垂直方向のグリッド線を削除することができます。

グラフの積み上げ / 積み上げ解除

デフォルトでは、すべてのトレンドが、1 つの垂直軸を持つ 1 つのグラフに表示されます。しかしこのビューをカスタマイズして、各トレンドが個別のグラフに表示されるようにすることができます。

グラフの積み上げ / 積み上げ解除を実行するには

1. トレンドを個別のグラフに表示するには、[Trend View] ツールバーの [Strip Chart]  ボタンをクリックします。
2. トレンドを同じグラフに表示するには、[Trend View] ツールバーの [Stack Chart]  ボタンをクリックします。

Y 軸のサイズ変更

トレンドグラフ内の情報をより見やすくするのに、Y 軸のサイズを次のとおり変更することが必要になる場合があります。

1. Y 軸を拡大するには、[Increase Y Axis]  ボタンをクリックします。このボタンはグラフの左側に配置されています。
2. Y 軸を縮小するには、[Decrease Y Axis]  ボタンをクリックします。このボタンはグラフの左側に配置されています。
3. ウィンドウに合致するよう Y 軸のサイズを変更するには、[Trend View] ツールバーの [Scale to Fit]  ボタンをクリックします。

[Trend] ビュープロファイルの変更

[Trend] ビュープロファイルは、[Trend] ビューの起動時にグラフに表示されるパラメータセットを表します。プロファイルを編集することで、[Trend] ビューに表示されるパラメータを変更することができます。

プロファイルを編集するには

1 [Trend View] ツールバーの [Profile] ボタン  をクリックします。

[Profile] ダイアログボックスが表示されます。そのオブジェクトについて、現在 [Trend] ビューに表示されているパラメータが選択されています。

2 パラメータ名をクリックして、その選択を実行したり解除したりすることにより、プロファイルを編集します。

(Shift) キーを押しながらクリックすると、連続する複数のパラメータを選択できます。(Ctrl) キーを押しながらクリックすると、連続していない複数のパラメータを選択できます。

3 [OK] をクリックします。

トレンドデータのサンプル収集の管理

表示されるトレンドデータのパラメータを、次のオプションを使ってカスタマイズすることができます。

- 925 ページの「トレンドのサンプル収集と間隔の変更」.
- 926 ページの「アラームしきい値設定の変更」.

トレンドのサンプル収集と間隔の変更

サーバエージェントによってデータ収集される各トレンドについて、サンプル収集の間隔およびサーバに保存されるサンプル数を次のとおり設定できます。

1 オブジェクトを右クリックし、[Properties] をクリックします。

2 [Trend] タブをクリックします。

3 変更するトレンドパラメータを選択し、[Edit] をクリックします。

[Edit Trend] ダイアログボックスが表示されます。トレンドのサンプル収集および間隔に関する設定が、画面の [Sampling Parameters] セクションに表示されます。

4 サンプル収集のパラメータを有効または無効にするには、[State] ドロップダウンリストから適切な値を選択します。

5 トレンドパラメータのサンプル取得間隔 (Sample Interval) を変更するには、[Frequency] ドロップダウンリストから値を選択します。

5 秒から 1 日まで、12 ある時間間隔の中から選択することができます。

6 [Number of Samples] フィールドに値を入力することにより、サンプルの収集期間を指定します。

指定したサンプル (トレンドバケット) 数により、パラメータの収集期間が決まります。特定の期間で収集を実行するサンプルごとにトレンドバケットを指定する必要があります。必要なサンプル数の設定に関する詳細については、915 ページの「トレンドバケットの設定」を参照してください。

7 トレンドのサンプル収集と間隔の変更が終了したら [OK] をクリックします。

アラームしきい値設定の変更

NetWare 版 Management Agent および Windows 版 Management Agent を使ってデータを収集する各トレンドパラメータについてアラームしきい値を設定することができます。アラームしきい値を設定すると、NetWare 版 Management Agent はトレンドが設定済みのしきい値を超えた場合に Novell ConsoleOne にアラームを送信します。

NetWare 版 Management Agent は、アラームのしきい値を上回った場合、および下回った場合の両方を追跡します。各トレンドパラメータには、上限しきい値か下限しきい値のいずれかが関連付けられています。しきい値の種類を変更することはできません。

Novell ConsoleOne でアラームのしきい値を変更するには

1 オブジェクトを右クリックし、[Properties] をクリックします。

2 [Trend] タブをクリックします。

3 しきい値の設定を変更するトレンドパラメータを選択し、[Edit] をクリックします。

[Edit Trend] ダイアログボックスが表示されます。しきい値アラーム設定が、画面の [Rising Alarm Parameters] セクションに表示されます。

4 アラームパラメータを有効または無効にするには、[State] ドロップダウンリストから適切な値を選択します。

5 上限しきい値を設定または変更するには、[Rising Threshold] フィールドに値を入力します。

6 下限しきい値を設定または変更するには、[Falling Threshold] フィールドに値を入力します。

7 アラームしきい値設定の変更が完了したら、[OK] をクリックします。

サーバのパラメータの設定

アラーム条件の修正、サーバパフォーマンスの微調整、またはサーバで検出されるその他の問題の解決を実行するには、サーバの設定を変更する必要があります。サーバの設定は、NetWare 版 Management Agent をホストしている任意の NetWare サーバの Novell ConsoleOne から調整することができます。通常はサーバコンソールやリモートコンソールを使って設定される SET パラメータを、Novell ConsoleOne インタフェースから設定できます。Novell ConsoleOne で、現在の設定を表示して 1 つまたは複数の設定を変更した後、設定を確認してから、こうした調整をサーバに送信することができます。

パラメータの値と説明については、NetWare サーバのマニュアルを参照してください。この情報は、通常『Utilities Reference』マニュアルに掲載されています。

Novell ConsoleOne から NetWare の SET パラメータを表示または変更するには

1 サーバオブジェクトの隣に表示されるプラス記号 (+) をクリックすることにより、設定するサーバをドリルダウンします。

2 [Operating System] オブジェクトを右クリックし、[Properties] をクリックします。

[Set Parameters] タブが表示されます。このタブページには、NetWare の SET パラメータとそれぞれの現在の値が示されます。

3 [Set Parameters] タブの下向き矢印アイコンをクリックし、表示したい SET パラメータのカテゴリをクリックします。

[Communications]、[Directory Caching]、[Directory Services]、[Disk]、[Error Handling]、[File Caching]、[File System]、[Licensing Services]、[Locks]、[Memory]、[Miscellaneous]、[Multiprocessor]、[NCP]、[Service Location Protocol]、[Time]、[Transaction Tracking] のカテゴリの中から選択できます。

4 変更するパラメータを選択し、[Edit] をクリックします。

[Edit Parameters] ダイアログボックスが表示されます。

5 適切なフィールドに新しいパラメータ値を入力します。

6 パラメータの変更を有効にするタイミングを、[Apply Value] ボックスから適切なラジオボタンを選択して決定します。変更を適用するタイミングは、次の中から選択できます。

- [Now, until reboot]
- [Only after reboot]
- [Now, and after reboot]

7 [OK] をクリックします。

サーバコマンドの実行

次に示す、頻繁に使用される NetWare サーバのコマンドを Novell ConsoleOne から実行できます。

- 927 ページの「NLM のロードとアンロード」
- 927 ページの「ボリュームのマウントとマウント解除」
- 928 ページの「サーバ接続の切断」
- 928 ページの「Restarting a Server」
- 928 ページの「サーバのシャットダウン」

NLM のロードとアンロード

Novell ConsoleOne で NLM をロードまたはアンロードするには

1 NLM オブジェクトを右クリックし、メニューから次のコマンドを選択します。

- NLM をロードするには、[Load nlm] を選択します。
- NLM をアンロードするには、[Unload nlm] を選択します。

ボリュームのマウントとマウント解除

ボリュームをマウントまたはマウント解除するには

1 ボリュームオブジェクトを右クリックし、[Mount Volume] をクリックします。

または
ボリュームオブジェクトを右クリックし、[Dismount Volume] をクリックします。

確認ボックスが表示されます。

2 [OK] をクリックします。

サーバ接続の切断

サーバがクラッシュしてサーバ上のファイルが開いたままになっているとき、またはサーバを停止する前に、サーバ接続を切断することができます。これは、サーバコンソールから実行できる CLEAR STATION コマンドに相当します。

Novell ConsoleOne でサーバ接続を切断するには

1 次のオブジェクトを展開し、終了したい接続を特定します。[Server] > [Operating System] > [Network] > [Connections]

2 終了したい接続を右クリックし、[Clear Connection] をクリックします。

Restarting a Server

Novell ConsoleOne でサーバを再起動するには

1 サーバオブジェクトを右クリックし、[Restart Server] をクリックします。

サーバのシャットダウン

Novell ConsoleOne でサーバをシャットダウンするには

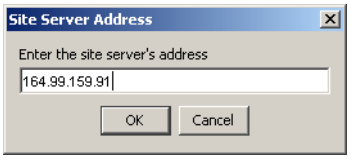
1 サーバオブジェクトを右クリックし、[Down Server] をクリックします。

Management Site Server のステータス

Management Site Server で現在実行中のすべての Management and Monitoring Services のステータスを表示できます。

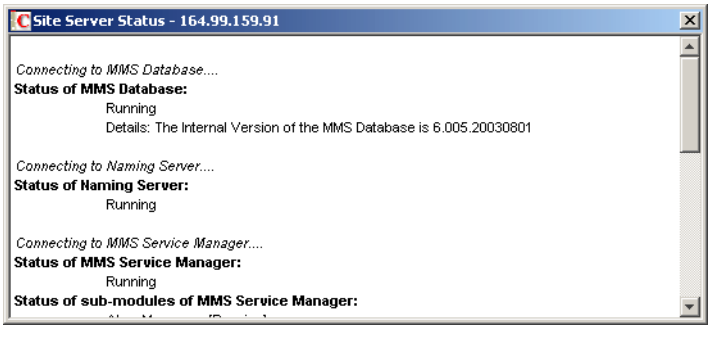
1 [Tools] > [Management Site Server Status] の順にクリックします。

2 Management Site Server の IP アドレスまたは DNS 名を指定します。



3 [OK] をクリックします。

[Management Site Server Status] ウィンドウに、Management Site Server のステータスが表示されます。



オブジェクトの階層構造とビューの詳細

管理対象のサーバオブジェクトを展開すると、そのサーバの内容に関する詳細情報を表示できます。次の節では、管理対象サーバで利用できるオブジェクトの詳細について説明し、各オブジェクトのビューで表示される統計データに関する情報を提供します。このトピックでは、次の情報について紹介します。

- 929 ページの「オブジェクトの階層構造」
- 930 ページの「オブジェクトビューの詳細」

オブジェクトの階層構造

次の表は、管理対象サーバで利用できるオブジェクトの階層構造と、オブジェクトに関連付けられたアイコンを示します。オブジェクトに関連付けられている、利用可能なビューに関する詳細については、対応するリンクを参照してください。

カテゴリコンテナ	サブカテゴリコンテナ	オブジェクトコンテナ	オブジェクト
 Devices	 931 ページの「Processors」		 プロセッサ
	 949 ページの「Printers」		 Printers
	 934 ページの「Adapters」	 LAN Adapters	 Adapter
		 Disk Adapters	 Adapter
	 932 ページの「Storage Devices」		 Storage Device
	 950 ページの「Other Devices」		 キーボード (Keyboard)
			 Mouse
	 950 ページの「Ports」		 Parallel Port
			 Serial Port

カテゴリコンテナ	サブカテゴリコンテナ	オブジェクトコンテナ	オブジェクト
オペレーティングシステム	Kernel	935 ページの「Threads」	Thread
		936 ページの「Interrupts」	Interrupt
		937 ページの「メモリ」	メモリ
		940 ページの「Address Spaces」	Address Space
	941 ページの「Network」	941 ページの「Interfaces」	Interface
		942 ページの「Connections」	Connection
	944 ページの「Users」		ユーザ
	945 ページの「Installed Software」		Software
	945 ページの「NLM」		NLM
サービス	File	946 ページの「Volumes」	Volume
	Print	948 ページの「Queues」	Queue

オブジェクトビューの詳細

次の節では、各オブジェクトビューで利用できる統計情報に関する詳細について説明します。

- 931 ページの「Processors」
- 932 ページの「Storage Devices」
- 934 ページの「Adapters」
- 935 ページの「Threads」
- 936 ページの「Interrupts」
- 937 ページの「メモリ」
- 940 ページの「Address Spaces」
- 941 ページの「Network」
- 941 ページの「Interfaces」
- 942 ページの「Connections」
- 944 ページの「Users」
- 945 ページの「Installed Software」
- 945 ページの「NLM」

- 946 ページの「Volumes」
- 948 ページの「Queues」
- 949 ページの「Printers」
- 950 ページの「Other Devices」
- 950 ページの「Ports」

Processors

プロセッサ速度を表示すると、サーバにかかる負荷の分析、およびサーバ間における負荷の分散に役立ちます。プロセッサ使用率に関するデータを表示すると、使用状況に関する問題を検出できます。さらに、サーバのバックアップなどのタスクを実行するのに適した、サーバに負荷がかかっていない時間帯を確認することができます。サーバのオペレーティングシステム (OS) によって、CPU の速度が自動的に確認され、OS のデータに基づいてレポートが生成されます。

プロセッサの速度は、サーバのパフォーマンスを決定する重要な要素です。したがって、サーバの負荷を分析し、複数のサーバ間で負荷を分散する場合、サーバのプロセッサ速度を把握することが重要になります。たとえば 1 台のサーバが、他のサーバの 2 倍の数のユーザを処理しているが、そのプロセッサが 2 倍の速度で処理を実行している場合、負荷は適切に分散されています。

サーバのプロセッサ使用率が通常より高くなったときに認識できるよう、サーバのプロセッサ使用率の基準を保持しておく必要があります。

管理対象サーバのプロセッサに関する情報を次のビューで表示できます。

- 931 ページの「Processors の［Summary］ビュー」
- 932 ページの「Processor の［Summary］ビュー」
- 932 ページの「Processors の［Trend］ビュー」

Processors の［Summary］ビュー

［Devices］>［Processors］の順にサーバオブジェクトを展開した後、Processors オブジェクトコンテナの［Summary］ビューにアクセスすることができます。このビューは、コンテナ内の各プロセッサオブジェクトに関する次の情報を表示します。

- **［Processor Number］：** プロセッサに割り当てられる一意の番号。
- **ステータス：** プロセッサのステータスは、オンライン、オフラインのいずれかです。

プロセッサがオンラインの場合にのみ、次の統計情報が表示されます。

- **［Utilization %］：** このプロセッサの直前における処理負荷を示します。割合 (%) で表されます。
- **［Interrupts Processed］：** このプロセッサで直前に発生した割り込みの数。
- **［Time Spent in Interrupts Last Second, in Microseconds］：** プロセッサが直前の割り込みの処理に費やした時間（マイクロ秒）。
- **［Number of Bound Threads］:** このプロセッサにバインドされているスレッドの数。プロセッサにバインドされているスレッドは、このプロセッサでのみ実行します。バインドされていないスレッドは、必要に応じて、別のプロセッサに移行できます。

Processor の [Summary] ビュー

[Devices] > [Processors] > [*processor #x*] の順にサーバオブジェクトを展開した後、個別のプロセッサに関する [Summary] ビューを選択できます。このビューには、次の情報が表示されます。

- **[Processor Number and Status]**：プロセッサに割り当てられる一意の番号とその現在のステータス。ステータスは、オンライン、オフラインのいずれかです。

プロセッサがオンラインの場合にのみ、次の統計情報が表示されます。

- **[Utilization %]**：このプロセッサの直前における処理負荷を示します。割合 (%) で表されます。
- **[Interrupts Processed]**：このプロセッサで直前に発生した割り込みの数。
- **[Time Spent in Interrupts Last Second, in Microseconds]**：プロセッサが直前の割り込みの処理に費やした時間 (マイクロ秒)。
- **[Number of Bound Threads]**: このプロセッサにバインドされているスレッドの数。プロセッサにバインドされているスレッドは、このプロセッサでのみ実行します。バインドされていないスレッドは、必要に応じて、別のプロセッサに移行できます。

Processors の [Trend] ビュー

[Devices] > [Processors] の順にサーバオブジェクトを展開した後、Processors オブジェクトコンテナの [Trend] ビューにアクセスできます。このビューには、各プロセッサに関する次のグラフが表示されます。

- **[CPU Utilization (avg.%)]**：プロセッサの直前における処理負荷を示します。割合 (%) で表されます。この情報は、プロセッサがオンラインの場合にのみ表示されます。

Storage Devices

ディスク容量 (MB 単位)、ディスクの種類、ブロックサイズなど、管理対象サーバのディスクドライブに関する詳細情報を取得できます。

各ディスクドライブのパーティション情報も表示できます。パーティション情報は特に重要です。これは、パーティション情報を利用することにより、パーティションに耐障害性が設定されているかどうか、ハードディスクがデータ整合性を失っていないかどうかを確認できるためです。

NetWare パーティションの耐障害性は、Novell ZENworks Server Management によって提供される詳細情報の一部です。ハードディスクがデータ整合性を失っていないかどうかを確認するには、リダクレクトされた領域を検査します。リダイレクトされた領域内の数は、データ整合性を維持するために Hot Fix Redirection Area にリダイレクトされたデータブロックの数を示します。リダイレクトされた領域内の数が多ければ多いほど、ハードディスクで障害の発生しているブロックの数も多くなります。期間内でリダイレクトされた領域の数が増大する場合、ハードディスクで障害が発生していることを示します。

NetWare 版 Management Agent によって管理される NetWare サーバ、または Novell ZENworks Server Management エージェントによって管理される Windows サーバで、エージェントは CPU 使用率、メモリ使用率、およびネットワークインタフェーストラフィックに関するトレンドデータを自動的に収集します。Novell ZENworks Server Management では、現在のトレンドデータを表示したり、時間、日、月、または年単位のトレンドデータの履歴を表示したりすることができます。トレンドデータを監視することにより、アラームしきい値の設定、サーバの使用者の割り出し、サーバに高い負荷がかかっているタイミングの確認、問題のトラブルシューティング、複数のサーバ間での負荷の分散、リソースのプランニングなどのタスクを実行できます。

管理対象サーバのストレージデバイスに関する情報を次のビューで表示できます。

- 933 ページの「Storage Devices の [Summary] ビュー」
- 933 ページの「Storage Device の [Summary] ビュー」
- 934 ページの「Storage Devices の [Trend] ビュー」

Storage Devices の [Summary] ビュー

[Devices] > [Storage Devices] の順にサーバオブジェクトを展開した後、Storage Devices コンテナオブジェクトの [Summary] ビューを選択することができます。このビューには、サーバの各ストレージデバイスに関する次の情報が表示されます。

- **[Disk Name]**：ディスクドライブ名。
- **[Size (KB)]**：ディスクドライブの合計サイズ (KB 単位)。
- **[Access]**：ディスクドライブが読み取り / 書き込み可能であるかどうか、または読み取りのみが可能かどうかを示します。
- **ステータス**：ディスクドライブが動作しているかどうかを表します。
- **[Type]**：メディアの種類。メディアの種類には、ハードディスク、フロッピーディスク、テープ、光ディスク (読み取り専用、読み取りは何度でも可能だが書き込みは一度だけ可能、読み取り / 書き込み可能)、RAM ディスクが含まれます。識別できない場合、このフィールドには [Other] または [Unkown] が表示されます。
- **[Driver Description]**：ディスクドライブが使用するドライバ名。
- **[Block Size]**：ディスクで使用するブロックの容量 (KB)。
- **[Heads]**：ディスクドライブ上の読み取り / 書き込みヘッドの数。
- **[Cylinders]**：ディスクドライブ上のシリンダの数。
- **[Sectors/Track]**：ディスクドライブ上のトラックあたりのセクタ数。
- **[SCSI Target ID]**：SCSI コントローラの場合にはターゲットアドレス、その他のデバイスの場合にはユニット番号。および SCSI デバイスの場合には論理ユニット番号、その他のデバイスの場合にはゼロ。

Storage Device の [Summary] ビュー

[Devices] > [Storage Devices] > [*storage_device_x*] の順にサーバオブジェクトを展開することにより、個別のストレージデバイスに関する [Summary] ビューを表示することができます。このビューには、次の情報が表示されます。

- **[Disk Name]**：ディスクドライブ名。
- **[Logical ID]**：論理パーティションに割り当てられた識別番号。
- **[Physical ID]**：物理パーティションに割り当てられた識別番号。

- [Type Partition]：DOS、NetWare、および UNIX* パーティションなど、パーティションの種類。
- [Size (KB)]：パーティションのサイズ (KB 単位)。
- [Redirection Area]：Hot Fix Redirection Area 全体のサイズ。
- [Redirected Area]：Hot Fix が検出した障害ブロックの数。
- [Reserved Area]：システム用に予約されている Hot Fix リダイレクションブロックの数。
- [Fault Tolerance]：使用される耐障害性機能の種類。使用できる耐障害性の機能の種類は、二重化とミラーリングです。耐障害性機能が存在しない場合、このフィールドには [None] という値が示されます。

Storage Devices の [Trend] ビュー

[Devices] > [Storage Devices] の順にサーバオブジェクトを展開した後、Storage Devices の [Trend] ビューを選択することができます。このビューには次の情報が表示されます。

- [File System Reads (#/min)]: 複数または単一のストレージデバイスで 1 分間に実行されるファイルシステムの読み取り数を示します。
- [File System Writes (#/min)]: 複数または単一のストレージデバイスで 1 分間に実行されるファイルシステムの書き込み数を示します。
- [File System Reads (KB/min)]: 複数または単一のストレージデバイスで実行される、KB ボリュームあたりのファイルシステムの読み取り数を示します。
- [File System Writes (KB/min)]：複数または単一のストレージデバイスで実行される、KB ボリュームあたりのファイルシステムの書き込み数を示します。
- [Free Redirection Area (%)]：ディスクリダイレクトに割り当てられる領域の、総ボリュームに対する割合 (%) を示します。

Adapters

I/O ポート、メモリアドレス、割り込み設定など、管理対象サーバのネットワークアダプタおよびディスクアダプタに関する詳細情報を取得できます。

同じアドレスや割り込みがサーバ内の 2 つのボードに設定された場合や、サーバのハードウェアのボードとコンポーネントに対して同じアドレスや割り込みが設定された場合など、設定に関する問題を検出するのにこのデータを使用することができます。2 つのボードで同じ I/O ポート、メモリアドレス、および割り込みを使用することはできません。

LAN アダプタで問題が発生した場合、サーバやワークステーションが通信できないなどのネットワーク問題が生じます。ネットワークボードで使用するフレームタイプに、サポートの対象になるプロトコルがバインドされているかどうかを、LAN アダプタに関する収集データを使って確認することができます (1 つのネットワークボードに複数のプロトコルがバインドされている場合があります)。問題が、ワークステーションで間違ったフレームタイプを使用しているなどの単純な原因により発生しているのかどうかを即座に確認できます (たとえば、サーバでは Ethernet_II フレームタイプ、ワークステーションでは Ethernet_802.2 フレームタイプを使用している場合)。

管理対象サーバのアダプタに関する情報を次のビューで表示できます。

- 935 ページの「Adapters の [Summary] ビュー」
- 935 ページの「Adapters の [Trend] ビュー」

Adapters の [Summary] ビュー

[Devices] > [Adapters] > [*adapter_x*] の順にサーバオブジェクトを展開した後、Adapters の [Summary] ビューを選択することができます。このビューには次の情報が表示されます。

- **説明：** アダプタハードウェアの種類。このフィールドには、メーカ、モデル、バージョンに関する情報が含まれます。ネットワークボードの場合、このフィールドにボードのショートネームとボードの焼き付けられた MAC アドレスが含まれることがあります。
- [Type] : アダプタの種類（たとえば、ネットワークカードまたはディスクストレージ）。
- [Devices Attached]: アダプタに関連付けられるデバイスの数（たとえば、ディスクコントローラに接続されるドライブの数）。
- [Driver Description] : このアダプタのドライバに関する説明。
- [Version] : ドライバソフトウェアのバージョン番号。
- [Interrupt Number] : アダプタが使用する一意の割り込み番号。
- [I/O Port] : アダプタが使用する一意の I/O ポートブロック。
- [Memory] : アダプタが使用する一意のメモリアドレス空間。
- [DMA] : アダプタが使用する DMA(Direct Memory Access) チャネル。
- [Slot] : アダプタが装着されるスロット。

Adapters の [Trend] ビュー

[Devices] > [Adapters] > [*adapter_ x*] の順にサーバオブジェクトを展開した後、Adapters の [Trend] ビューを選択することができます。このビューには次のグラフが表示されます。

- [LSL Packets Received] : アダプタが受け取る LSL パケットの数を表します。
- [LSL Packets Transmitted] : アダプタが伝送する LSL パケットの数を表します。
- [Packets Received] : アダプタが受け取るパケットの総数を表します。
- [Packets Transmitted] : アダプタが伝送するパケットの総数を表します。

Threads

管理対象サーバで現在実行中のすべてのスレッドに関する情報を表示できます。スレッドは、独立した実行単位として認識されます。

管理対象サーバのスレッドに関する情報を次のビューで表示できます。

- 935 ページの「Threads の [Summary] ビュー」

Threads の [Summary] ビュー

[Operating System] > [Kernel] > [Threads] の順にサーバオブジェクトを展開した後、Threads の [Summary] ビューを選択することができます。このビューには次の情報が表示されます。

- [Name] : アプリケーションスレッド名。
- [Share Group] : アプリケーションの共有グループ、およびグループに関連付けられたスレッドと共有。

- [Parent Module]：このスレッドに関連付けられているモジュール (NLM)。
- [State]：スレッドの状態。initializing(初期化中)、invalid(無効)、ready(準備完了)、running(実行中)、suspended(一時停止)、terminated(終了)、zombie(ゾンビ) のいずれかに該当します。
- [Suspended Due To]：スレッドが一時停止する理由。スレッドが一時停止状態にない場合、このフィールドは空白になります。
- [Execution Time, Microseconds]：直前にプロセッサがスレッドのコードを実行するのに要した時間。
- [Stack Size, Bytes]：スレッドのスタックのサイズ。
- [Soft Affinity]：スレッドが優先的に実行するプロセッサ。ただし必要に応じて、スレッドをプロセッサから移行できます。
- [Hard Affinity]：スレッドが、その実行中に特定のプロセッサに明示的にバインドされるかどうかを示します。スレッドが特定のプロセッサでのみ実行する場合には、そのプロセッサのキャッシュの状態を表示できます。スレッドが他の利用可能なプロセッサで実行できる場合、このフィールドの値はゼロになります。

Interrupts

管理対象サーバの登録済み割り込みに関する情報を表示することができます。マルチプロセッシングシステムでは、割り込み情報は、搭載されたすべてのプロセッサについて表示されるほか、各オンラインプロセッサについても個別に表示されます。

管理対象サーバの割り込みに関する情報を次のビューで表示できます。

- 936 ページの「Interrupts の [Summary] ビュー」
- 937 ページの「Interrupts の [Service Routines] ビュー」

Interrupts の [Summary] ビュー

[Operating System] > [Kernel] > [Interrupts] の順にサーバオブジェクトを展開した後、Interrupts の [Summary] ビューを選択することができます。このビューには次の情報が表示されます。

- [Name]：割り込みルーチンの名前。
- [Interrupt Number]：このサービスルーチンの番号。
- [Processor]：プロセッサの数。
- [Type]：割り込みサービスルーチンの種類。次のいずれかになります。
  - [Bus]：使用されるデバイス I/O 割り込み (たとえば、ディスクまたは LAN ドライバにより使用)。
  - [Local]：個別のプロセッサだけで使用されるハードウェアプラットフォーム固有の割り込み。
  - [System]：一意の割り込み要件を持つシステム用に予約される割り込みカテゴリ。
  - [Interprocessor]：1 つのプロセッサによって生成され、他のプロセッサに影響を及ぼす割り込み。
  - [Timer]：予防サポートのほかに、OS に対しタイマサービスを提供する割り込み (マルチプロセッシングシステムでは、タイマ割り込みは 1 つのプロセッサに限定されます)。

- [Service Routines]：この割り込みが発生したときに起動するサービスルーチンの数。
- [Interrupt Occurrences]：直前に発生した割り込みの処理に要した時間。
- [Execution Time]：直前にプロセッサがこの割り込みの処理に費やした時間。
- [Spurious Interrupts]：サーバの起動以降、発生するはずのない割り込みが発生した回数。

Interrupts の [Service Routines] ビュー

Interrupts の [Service Routines] ビューは、サーバで定義されているメモリアドレス空間に関する情報を提供します。

NetWare は、LAN ドライバ、ストレージデバイスドライバ、MONITOR、および Server Management Agent と共に、OS アドレス空間（カーネル）で稼働します。OS アドレス空間は、物理メモリによってサポートされます。

その他のすべてのアドレス空間はユーザ空間（ring 3）であり、仮想メモリによってサポートされます。アドレス空間で障害が発生した場合に、ユーザ空間で実行しているアプリケーションによってサーバが異常終了することはありません。

[Operating System] > [Kernel] > [Interrupts] の順にサーバオブジェクトを展開した後、[Service Routines] ビューを選択できます。このビューには次の情報が表示されます。

- [Name]：割り込みサービスルーチンの名前。
- [Service Routine Number]：このサービスルーチンに関連付けられたサービスルーチン番号。
- [Processor Number]：このルーチンが実行しているプロセッサの番号。
- [Interrupt Number]：このサービスルーチンに関連付けられている割り込み番号。
- [Interrupts Processed Last Second]：直前に ISR によって処理された割り込みの数。

メモリ

管理対象サーバのメモリに関する情報を次のビューで表示できます。

- 937 ページの「Memory の [Summary] ビュー」
- 938 ページの「Memory の [Trend] ビュー」
- 938 ページの「[Disk Cache] ビュー」
- 939 ページの「[Virtual Memory] ビュー」

Memory の [Summary] ビュー

[Operating System] > [Kernel] > [Memory] の順にサーバオブジェクトを展開した後、Memory の [Summary] ビューを選択することができます。このビューには次の情報が表示されます。

- [Type]：メモリの種類（たとえば、DOS、割り当てられたメモリ、キャッシュバッファ、またはコードおよびデータメモリ）。
- [Unit Size (bytes)]：メモリ割り当てのサイズ。
- [Total (KB)]：メモリユニット-ユニットサイズの数値。

- [Units Used]：割り当てられたメモリユニットの数。
- [Used (KB)]：割り当てられたメモリの容量 (KB)。

Memory の［Summary］ビューには、システムにおけるメモリの使用状況を表す円グラフも表示されます。

Memory の［Trend］ビュー

［Operating System］>［Kernel］>［Memory］の順にサーバオブジェクトを展開した後、Memory の［Trend］ビューを選択することができます。このビューには次のグラフが表示されます。

- [Cache Buffers (%)]：キャッシュバッファに割り当てられたメモリの割合 (%)。
- [Code and Data Memory (%)]: コードとデータに割り当てられたメモリの割合 (%)。
- [Allocated memory (%)]：割り当てられたメモリの容量。
- [Dirty Cache Buffers (%)]：ダーティキャッシュバッファメモリの容量。

［Disk Cache］ビュー

このビューは、ディスクキャッシュメモリの使用状況を表示します。キャッシュの使用状況に関する統計情報を活用して、キャッシュ用に RAM を増設する必要があるタイミングを決定します。［Operating System］>［Kernel］>［Memory］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- [Short Term Cache Hits %]：すでにキャッシュメモリに配置されたディスクブロックに対して、直前に実行されたリクエストの割合。リクエストされたデータがすでにメモリ内に存在する場合、ディスクの読み取りを実行する必要はありません。この値が 98% を下回る場合、キャッシュ用に RAM の増設を検討してください。また、［Long Term Cache Hits］との比較を実行してください。
- [Short Term Cache Dirty Hits %]：すでにキャッシュメモリに存在するが、ダーティであるディスクブロックに対して直前に実行されたリクエストの割合。ダーティキャッシュは、使用する前にディスクに書き込まれる必要があります。［Long Term Dirty Cache Hit］と［LRU Sitting Time］もチェックしてください。
- [Long Term Cache Hits %]: すでにキャッシュに存在するディスクブロックに対するリクエストの累積的な割合。リクエストされたデータがすでにメモリ内に存在する場合、ディスクの読み取りを実行する必要はありません。この累積的な割合を使って、全体的なディスクキャッシュの使用状況にアクセスします。この値が 90% を下回る場合、キャッシュ用に RAM を増設してください。
- [Long Term Cache Dirty Hits %]：キャッシュメモリにすでに存在するが、ダーティであるディスクブロックに対して実行されるリクエストの累積的な割合 (ダーティキャッシュを使用する前に、ダーティキャッシュをディスクに書き込む必要があります)。この累積的な割合を使って、全体的なディスクキャッシュの使用状況にアクセスします。このフィールドが高い値を示すか、安定して値が増加する場合、キャッシュ用に RAM を増設してください。［LRU Sitting Time］もチェックしてください。

- [Total Cache Blocks Allocated]: サーバを起動または再起動して以降、ディスクキャッシュブロックに対して実行されたリクエストの累積数。この値は、[Allocated from Available List] の値と [Allocated from Least Recently Used (LRU)] の値を合計したものです。[Allocated from Available List] の値がきわめて大きい場合、サーバで十分な容量の RAM がキャッシュ用に割り当てられています。[Allocated from LRU] の値が大きい場合、キャッシュ用に RAM を増設する必要があります。
- [Cache Blocks Allocated from Available List]: 利用可能リスト内のブロック（使用されていないブロック）によって実行される、ディスクキャッシュブロックに対するリクエストの数。利用できるブロックが存在しない場合、リクエストは、キャッシュブロックの LRU リストから実行されます。この値が [Allocated from LRU] の値よりもきわめて大きい場合、サーバにはキャッシュ用に十分な容量の RAM が設定されています。
- [Cache Blocks Allocated from LRU]: LRU キャッシュブロックのブロックによって実行される、ディスクキャッシュブロックに対するリクエストの数。一時停止中のリクエストが LRU キャッシュブロックからディスクに書き込まれ、現在のリクエストに対するブロックが解放されます。LRU キャッシュは、他のキャッシュが利用できない場合にのみ使用されるため、この数値が安定して増加するときには、RAM の増設が必要であることを示します。
- [Number of Times in Last 10 Minutes that the OS Had to Wait]: 直前の 10 分間で、OS がリクエストを実行するために LRU ブロックを待機した回数。この値が 7 を超える場合、キャッシュ用に RAM を増設する必要があります。
- [Number of Times OS Had to Wait]: リクエストを実行するために OS が LRU ブロックを待機した回数。
- [Total Number of Times the Write Request Was Delayed]: きわめて多くの書き込みを実行する必要があったため、またはディスクチャネルがビジー状態にあったため、書き込みリクエストで遅延が発生した回数。このフィールドに大きな値が示された場合、ディスクチャネルの I/O トラフィックが多すぎるか、キャッシュ用に RAM を増設する必要があることを示します。
- [Number of Times the Request Was Re-tried]: 対象になるブロックが使用されているため、ディスクキャッシュリクエストの再試行が必要となった回数。このフィールドが高い値を示すか、安定して値が増加する場合、キャッシュ用に RAM を増設してください。

[Virtual Memory] ビュー

このビューには、仮想メモリシステムに関する情報が表示されます。こうした統計情報を使って、サーバのメモリが効率よく使用されているかどうかを監視します。これらの値が一定の期間、きわめて安定しており、サーバのパフォーマンスが満足できる水準にある場合、サーバには、その負荷に対して適切な容量のメモリが搭載されています。たとえば、[Page Faults] の値が増加する場合、サーバのパフォーマンスは低下しています。逆に [Free Swap Pages] の値が増加する場合、サーバのパフォーマンスは向上しています。

[Operating System] > [Kernel] > [Memory] の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- [Total Page-In Requests]: サーバが起動して以降（サーバの稼働中）、仮想メモリをスワップファイルから移動するために実行されたリクエストの数。
- [Page-In Requests in Last 5 Seconds]: 4KB 仮想メモリページをスワップファイルから移動するために実行されたリクエストの数。

- [Total Page-Out Requests]: サーバが起動して以降（サーバの稼働中）、仮想メモリをスワップファイルに移動するために実行されたリクエストの数。
- [Page-Out Requests in Last 5 Seconds]: 4KB 仮想メモリページをスワップファイルに移動するために実行されたリクエストの数。
- [Total Swap Pages]: このサーバの仮想メモリシステム内の 4KB ページの数（メモリページ内のスワップファイルの数は、総バイト数を 4KB で除算した数値）。スワップファイルの数は、サーバの負荷に関するメモリ要件に合致するよう、大幅に増加したり、減少したりします。
- [Free Swap Pages] : 仮想メモリシステムが使用できる 4KB ページの数。
- [Reserved Swap Pages]: 仮想メモリシステムによって予約された 4KB ページの数。
- [Total Page Faults]: サーバが起動して以降（サーバの稼働中）、仮想メモリシステムがスワップファイルから取得した回数。
- [Page Faults in Last 5 Seconds]: 直前の 5 秒間で、仮想メモリシステムがスワップファイルから取得した回数（アクセスされたメモリは物理メモリによってサポートされなかったことを示す）。

Address Spaces

NetWare は、LAN ドライバ、ストレージデバイスドライブ、MONITOR、および Server Management Agent と共に OS アドレス空間（カーネル）で稼働します。OS アドレス空間は、物理メモリによってサポートされます。

その他のすべてのアドレス空間はユーザ空間 (ring 3) であり、仮想メモリによってサポートされます。アドレス空間で障害が発生した場合に、ユーザ空間で実行しているアプリケーションによってサーバが異常終了することはありません。

管理対象サーバのアドレス空間に関する情報を次のビューで表示できます。

- 940 ページの「Address Spaces の［Summary］ビュー」

Address Spaces の［Summary］ビュー

［Operating System］>［Kernel］>［Address Spaces］の順にサーバオブジェクトを展開した後、Address Spaces の［Summary］ビューを選択することができます。このビューには次の情報が表示されます。

- [Name] : このモジュールが実行する仮想メモリアドレス空間の名前。
- [Number of NLMs Loaded]: このアドレス空間にロードされる NLM プログラムの数。NetWare、LAN ドライバ、ストレージデバイスドライバ、MONITOR、および Server Management Agent は OS アドレス空間（カーネル）にロードされます。GroupWise®、Lotus Notes、または Oracle* データベースなどのサーバアプリケーションは、それぞれのアドレス空間（ユーザ空間または ring 3）にロードすることができます。
- [Mapped Pages] : このアドレス空間をサポートしている物理メモリページの総数。OS アドレス空間（カーネル）は、物理メモリによってサポートされる唯一のアドレス空間であることに注意してください。
- [Restarted] : このアドレス空間で障害が発生し、自動的に再起動した回数の合計。ゼロ (0) の値は、障害が発生していないことを示します。ゼロ以外の値は、アドレス空間で障害が発生したため回復が実行されたことを示します。アドレス空間のコアダンプに関する指示については、オンラインのトラブルシューティングマニュアルを参照してください。

- [Memory in Use, Bytes]：割り当てられているメモリで使用中の容量。
- [Memory Not in Use, Bytes]：割り当てられているメモリで使用されていない容量。
- [Memory As Overhead, Bytes]：割り当てプールの管理、およびメモリ断片化の容量の管理に使用するメモリ容量。
- [Total Blocks]：使用中であり、NLM のリクエストに利用できるメモリブロックの数。
- [Blocks in Use]：割り当てられて、使用されたメモリブロックの数。
- [Block Not Used]：割り当てられたが、使用されなかったメモリブロックの数。

Network

管理対象サーバのネットワークアクティビティに関する情報を次のビューで表示できます。

- 941 ページの「Network の [Trend] ビュー」

Network の [Trend] ビュー

[Operating System] > [Network] の順にサーバオブジェクトを展開した後、Network オブジェクトコンテナの [Trend] ビューにアクセスすることができます。このビューには、各ネットワークアダプタに関する次のグラフが表示されます。

- [Packets Received (KB/min)]：直前の 1 分間にアダプタが受け取ったパケット容量 (KB)。

Interfaces

管理対象サーバのネットワークインタフェースに関する情報を次のビューで表示できます。

- 941 ページの「Interfaces の [Summary] ビュー」
- 942 ページの「Interfaces の [Statistics] ビュー」

Interfaces の [Summary] ビュー

[Operating System] > [Network] > [Interfaces] の順にサーバオブジェクトを展開した後、Interfaces オブジェクトコンテナの [Summary] ビューにアクセスできます。

このビューには、次の情報が表示されます。

- [Frame Type]：この論理ボードにバインドされているフレームの種類。
- [MAC Address]：インタフェースの MAC アドレス。
- 説明：インタフェースボードを説明するテキスト。
- [Line Speed]：このボードを介して伝送される 1 秒あたりのビット数。
- [Type]：インタフェースの種類 (たとえば Ethernet CSMACD)。
- [Logical Board #]：この論理ボードに割り当てられた番号。
- [Logical Board Name]：この論理ボードに割り当てられた名前。
- [Protocol]：論理ボードにバインドされているプロトコル (たとえば、IP、ARP、または IPX)。

Interfaces の [Statistics] ビュー

[Operating System] > [Network] > [Interfaces] の順にサーバオブジェクトを展開した後、Interfaces オブジェクトコンテナの [Statistics] ビューにアクセスできます。

このビューには、次の情報が表示されます。

- [Frame Type] : この論理ボードにバインドされているフレームの種類。
- [MAC Address] : インタフェースの MAC アドレス。
- [MTU] : インタフェースで送受信できるデータグラムのサイズの最大値。
- [Admin Status] : インタフェースの望ましい状態。
- [Oper Status] : インタフェースの現在の稼働状況。
- [Bytes In] : インタフェースで受信したバイト数の合計。
- [Bytes Out] : インタフェースから伝送されたオクテットの合計数。
- [Ucast Packets In] : 上位階層のプロトコルに渡されたサブネットワークユニキャストパケットの数。
- [Ucast Packets Out] : 上位階層プロトコルがサブネットワークユニキャストアドレスに対して送信を要求したパケットの合計数。
- [Nucast Packets In] : 上位階層のプロトコルに渡された非ユニキャストパケットの数。
- [Nucast Packets Out] : 上位階層のプロトコルが非ユニキャストアドレスに対して送信を要求したパケットの合計数。
- [Discards In] : 上位階層のプロトコルに伝送できないエラーが検出されていないにもかかわらず、破棄するよう選択された着信パケットの数。
- [Discards Out] : 伝送できないエラーが発生していないにもかかわらず、破棄するよう選択された発信パケットの数。
- [Errors In] : 上位階層のプロトコルに伝送できないエラーが発生した着信パケットの数。
- [Errors Out] : エラーのため、伝送できなかった発信パケットの数。
- [Unknown Protocols In] : インタフェースを介して受信したが、未定義またはサポートされていないプロトコルが原因で破棄されたパケットの数。

このビューの [Clear Counters] ボタンを押すと、管理コンソールの値はリセットされますが、サーバの値はリセットされません。この操作を実行すると、ユーザはサーバから最新のデータを取得することができます。

Connections

管理対象サーバの接続に関する情報を次のビューで表示できます。

- 943 ページの「Connections の [Summary] ビュー」
- 944 ページの「Connections の [Trend] ビュー」
- 944 ページの「[Open Files] ビュー」

Connections の [Summary] ビュー

Connections の [Summary] ビューには、選択したサーバの接続に関する情報と統計が表示されます。たとえばこのビューには、サーバおよび他のクライアントが現在アクセスしているファイルの数が表示されます。Novell eDirectory をサポートする隠しファイルなど、特定のファイルが常に開いています。[Operating System] > [Network] > [Connections] > [*connection_x*] の順にサーバオブジェクトを展開した後、このビューを選択することができます。

このビューには次の情報が表示されます。

- **[Connection# Login Name]:** 接続番号とログイン名を示す文字列。接続 0（ゼロ）はシステムによって使用されることに注意してください。ログイン名は、適用できる場合、Novell eDirectory の完全識別名になります。
- **[Client Address] :**

  IP:*xxx.xxx.xxx.xxx:port number*
  IPX:*network:node:socket*
- **[Connection Time] :** 接続が確立した日付と時刻。
- **[Privileges] :** 接続には、次に示す 1 つ以上の権限を設定できます。
  - [Supervisor]
  - [Operator]
  - [Auditor]
  - [High_Privilege]
  - [Second_Authentication]
  - [Second_High_Privilege]
- **ステータス :** 次のいずれかのステータスが当てはまります。
  - [Not logged in]
  - [Logged in]
  - [Need security change]
  - [MacStation]
  - [Connection abort]
  - [Audited]
  - [Authenticated temporary]
  - [Audit connection recorded]
  - [DS audit connection recorded]
  - [Logout in progress]
- **[Read (bytes)] :** 接続の確立以降に読み取られたバイト数。
- **[Written (bytes)] :** 接続の確立以降に書き込まれたバイト数。
- **[NCP Requests] :** 接続の確立以降に実行された NCP リクエストの数。
- **[Open Files] :** 接続によって現在開かれているファイルの数。
- **[Locked Records] :** 接続により現在ロックされているファイルレコードの数。

Connections の［Trend］ビュー

［Operating System］>［Network］>［Connections］>［*connection_x*］の順にサーバオブジェクトを展開した後、Connections の［Trend］ビューを選択することができます。このビューには次のグラフが表示されます。

- **［Connections (avg.#)］**：直前のサンプル間隔における接続の平均数。

［Open Files］ビュー

Connection の［Open Files］ビューには、サーバの接続に関する情報と統計が表示されます。たとえばこのビューには、サーバおよび他のクライアントが現在アクセスしているファイルの数が表示されます。Novell eDirectory をサポートする隠しファイルなど、特定のファイルが常に開いています。［Operating System］>［Network］>［Connections］>［*connection_x*］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- **［Filename］**：ディレクトリパスを含む、開いているファイルの名前。
- **［Login Name］**：ファイルを開いたユーザ（存在する場合）の名前。ファイルが、システムまたは NLM によって開かれた場合、［Login Name］はゼロ長の文字列になります。
- **［Volume Name］**：開いているファイルを含む NetWare ボリュームの物理名。
- **［Directory Number］**：NetWare ボリューム内の開いているファイルを一意に識別する番号。
- **［Volume ID］**：NetWare ボリュームを一意に識別する番号。特定のボリュームに関するこのオブジェクトの値は、同じボリュームの nwVolID オブジェクトと同じ値になります。

Users

選択したサーバのユーザに関する情報を次のビューで表示できます。

- 944 ページの「Users の［Summary］ビュー」
- 945 ページの「Users の［Trend］ビュー」

Users の［Summary］ビュー

Users の［Summary］ビューには、選択したサーバにアクセスするユーザ情報が表示されます。［Operating System］>［Users］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには、各ユーザに関する次の情報が表示されます。

- **［Login Name］**：ユーザのログイン名。
- **［Disk Usage］**：ユーザが使用しているディスク容量。
- **［Last Login］**：ユーザが最後にサーバにログインした日付。
- **［Account Status］**：ユーザアカウントが有効かどうかを示します。
- **［Password］**：ユーザのパスワードが有効かどうかを示します。
- **［Real Name］**：ユーザの Novell eDirectory リアルネーム。
- **［Bad Login］**：ユーザが失敗したログイン試行の回数。このビューに 65535 が表示された場合、ログイン試行の最大数に達したことを示します。

- [Bad Login Address]：ユーザがログインに失敗した、実行元の場所のネットワークアドレス（存在する場合）。

Users の［Trend］ビュー

Users の［Trend］ビューには、選択したサーバにアクセスするユーザ情報が表示されます。［Operating System］>［Users］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次のグラフが表示されます。

- [Logged-In Users (avg.#)]：サーバにログインしたユーザの平均数を示します。

Installed Software

選択したサーバにインストールされているソフトウェアに関する情報を次のビューで表示できます。

- 945 ページの「Installed Software の［Summary］ビュー」

Installed Software の［Summary］ビュー

Installed Software の［Summary］ビューには、選択したサーバにインストールされたソフトウェアに関する情報が表示されます。［Operating System］>［Installed Software］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- [Name]：インストールされているソフトウェアモジュールの名前。
- [Type]：ソフトウェアの種類（たとえば、デバイスドライバ、アプリケーション、またはオペレーティングシステム）。
- [Date Installed]：ソフトウェアがインストールされた日付。

NLM

管理対象サーバのキューに関する情報を次のビューで表示できます。

- 945 ページの「NLM の［Summary］ビュー」
- 946 ページの「［Resource Tag］ビュー」

NLM の［Summary］ビュー

NLM の［Summary］ビューには、選択した NLM に関する情報が表示されます。［Operating System］>［NLMs］>［*nlm_x*］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- [Name]：NLM の名前。
- [Version]：NLM のバージョン番号。
- [Released]：NLM がリリースされた日付と時刻。
- [Memory (bytes)]：この NLM が使用するメモリ容量（バイト単位）。これは、NLM によって割り当てられた短期メモリ、半永久メモリ、および移動不可メモリの合計に、コードのサイズおよび NLM のこのインスタンスのデータセクションを加算した値です。
- 説明：NLM を説明するテキスト文字列。
- [Copyright]：NLM の著作権に関する文字列。

[Resource Tag] ビュー

[Operating System] > [NLMs] > [*nlm_x*] の順にサーバオブジェクトを展開した後、NLM の [Resource Tag] ビューを選択できます。このビューには次の情報が表示されます。

- **説明：** 所有モジュールがこのリソースタグに割り当てた名前。
- **[Number in Use]：** リソースタグのインスタンスの数。
- **[Resource Type]：** 追跡が実行されているリソースタグの種類（たとえば、セマフォやプロセッサ）。
- **[Address Space]：** リソースタグを所有するモジュールが実行しているアドレス空間の名前。

Volumes

NetWare サーバのディスクストレージ容量はボリュームに分割されます。サーバにマウントされたボリュームについて、さまざまなデータ（サイズ、空き容量、異なるディスク間にボリュームを配分する方法、容量を使用しているユーザなど）を表示することができます。個別のボリュームについて、設定、開いているファイル、セグメント、および使用状況に関するデータを表示できます。利用できるビューは次のとおりです。

- 946 ページの「Volume の [Summary] ビュー」
- 947 ページの「Volume の [Trend] ビュー」
- 947 ページの「[Open Files] ビュー」
- 947 ページの「Volume の [Segment] ビュー」
- 948 ページの「Volume の [Usage] ビュー」

Volume の [Summary] ビュー

Volume の [Summary] ビューには、単一のボリュームに関する詳細情報が表示されます。[Services] > [File] > [Volumes] > [*volume_x*] の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには次の情報が表示されます。

- **[Size (KB)]：** ボリュームのサイズ (KB 単位)。
- **[Free (KB)]：** ボリュームにおける空き容量 (KB 単位)。ファイルを追加または拡張すると、この数値はゼロに近づきます。円グラフにより、総容量のうちどのくらいが空き容量になっているのかを確認できます。
- **[Used (KB)]：** ボリュームの総容量からディスクの空き容量を差し引くことで計算される容量。
- **ステータス：** ボリュームがマウントされているかどうかを示します。ボリュームがマウントされていない場合、ボリューム名だけが示されます。
- **[Namespaces]：** ボリュームでサポートされるネームスペース。サポートされるネームスペースは、DOS、Macintosh*、NFS*、FTAM、および OS/2* です。
- **[Attributes]：** ボリュームの属性。使用できる属性は、ブロック細分割り当て、ファイル圧縮、データ移行、監査、および読み取り専用です。ボリュームには属性を組み合わせて使用することができます。たとえば、読み取り専用ボリュームにブロック細分割り当て属性を設定できます。
- **[# Logical Segment]：** このボリュームを構成しているセグメントの数。

- [DS Name]：ボリュームの Directory Services 完全識別名。適用できない場合はゼロ長の文字列。
- [Non-Purgable]：まだ消去期限が到来していない削除済みファイルによって占有されている容量（KB 単位）。この容量は、削除済みファイルを消去できるようになったときにはじめて空き容量として再利用できます。
- [Block Size]：ボリュームのブロックサイズ（バイト単位）。
- [Dir Slots]：ボリュームで利用できるディレクトリテーブルエントリの総数。
- [Used Dir Slots]：現在使用中のディレクトリテーブルエントリの数。
- [File System Name]：ボリュームのファイルシステムの種類がリモートであるかローカルであるかを示します。[File System Name] の値は、ボリュームがリモートの場合にのみ示されます。この場合、ファイルシステム名は、SITE1:/usr/x などのリモートマウントポイントになります。

Volume の [Trend] ビュー

[Services] > [File] > [Volumes] > [*volume_x*] の順にサーバオブジェクトを展開した後、Volume の [Trend] ビューを選択することができます。このビューには次のグラフが表示されます。

- [Volume % Free Space]：ボリュームでまだ利用することができる容量の割合。

[Open Files] ビュー

Volume の [Open Files] ビューにより、ボリュームで開いているすべてのファイルに関する表が表示されます。ファイルが複数の接続によって開いている場合、同じファイルについて複数のエントリが表内に表示されます。[Services] > [File] > [Volumes] > [*volume_x*] の順にサーバオブジェクトを展開した後、[Open Files] ビューを選択することができます。このビューには次の情報が表示されます。

- [Filename]：ディレクトリパスを含む、開いているファイルの名前。
- [Connection #]：ファイルを開いた接続の番号。
- [Login Name]：ファイルを開いたユーザ（存在する場合）の名前。ファイルが、システムまたは NLM によって開かれた場合、[Login Name] はゼロ長の文字列になります。
- [Directory Number]：NetWare ボリューム内の開いているファイルを一意に識別する番号。
- [Volume ID]：NetWare ボリュームを一意に識別する番号。

Volume の [Segment] ビュー

Volume の [Segment] ビューには、ボリューム上のセグメントに関する情報が表示されます。[Services] > [File] > [Volume] > [*volume_x*] の順にサーバオブジェクトを展開した後、このビューを選択することができます。Volume の [Segment] ビューが表示されている限り、サーバのデータは継続してポーリングされ、ビューは常にリアルタイム情報で更新されます。このビューには、選択したボリューム上の各セグメントに関する次の情報が表示されます。

- [ID]：ボリュームセグメントに割り当てられた識別番号。
- [Logical Partition ID]：論理パーティションに割り当てられた識別番号。
- [Physical Partition ID]：物理パーティションに割り当てられた識別番号。

- [Size]：セグメントのサイズ。
- [Fault Tolerance]：セグメントで使用されている障害対策の種類。使用できる種類は、二重化とミラーリングです。障害対策機能が設定されていない場合、この値は［None］になります。
- [Disk Drive]：セグメントが設定されているディスクドライブの名前。

Volume の［Usage］ビュー

Volume の［Usage］ビューには、各ユーザで使用されるボリュームの容量に関する情報が表示されます。Volume の［Usage］ビューが表示されている限り、サーバのデータは継続してポーリングされるため、ビューは常にリアルタイム情報で更新されます。［Services］>［File］>［Volumes］>［*volume_x*］の順にサーバオブジェクトを展開した後、このビューを選択することができます。このビューには、各ボリュームユーザに関する次の情報が表示されます。

- [Used KB]：現在使用している容量（KB 単位）。
- [Limit KB]：ユーザの制限容量（KB 単位）。
- [Username]：ユーザのログイン名。

Queues

管理対象サーバのキューに関する情報を次のビューで表示できます。

- 948 ページの「Queues の［Summary］ビュー」
- 948 ページの「Queue の［Summary］ビュー」
- 949 ページの「Queue の［Trend］ビュー」

Queues の［Summary］ビュー

Queues の［Summary］ビューには、管理対象サーバのプリントキューに関する次の情報が表示されます。

- [Queue Name]：キューの名前。
- [Type]：キューの種類（たとえば、アーカイブキュー、ジョブキュー、またはプリントキューなど）。
- [# Jobs]：現在キュー内に存在するプリントジョブの数。
- [# Print Servers]：このキューによってサービスされているプリントサーバの数。
- [Volume]：キューが設定されているボリューム。
- [Add Job State]：キューがジョブを追加できるかどうかを示します。
- [Attach State]：キューが追加できるかどうかを示します。

Queue の［Summary］ビュー

Queue の［Summary］ビューには、選択したキュー内のプリントジョブに関する次の情報が表示されます。

- [Job #]：プリントジョブに割り当てられた一意の番号。
- [Position]：プリントキュー内のプリントジョブの順序。
- [Bytes]：印刷されるバイト数。

- **説明：** プリントジョブに関する説明。
- [User]：ジョブを送信したユーザのユーザ名。
- [Entry Time]：ジョブがキューに追加された時刻。
- [Control Flags]：ジョブのコントロールフラグを表す値。たとえば、使用できるコントロールフラグとして、service auto start（サービス自動スタート）、execute（実行）、user hold（ユーザ待機）、operator hold（オペレータ待機）が挙げられます。
- [Target Time]：ジョブが印刷される日付と時刻。
- [Target Server]：ジョブのターゲットサーバ。
- [Actual Server]：現在ジョブを処理しているサーバの名前。

Queue の [Trend] ビュー

Queue の [Trend] ビューには、管理対象サーバの各キューに関する次のグラフが表示されます。

- [Wait Time of Next Ready Job (sec)]：次に用意されているジョブがキュー内で待機する平均時間。

Printers

プリンタ名、ポート、ドライバと説明、ステータス、エラー状況など、管理対象サーバにインストールされているプリンタに関する詳細情報を取得できます。管理対象サーバのプリンタに関する情報を次のビューに表示できます。

- 949 ページの「Printer の [Console] ビュー」
- 949 ページの「Printer の [Summary] ビュー」

Printer の [Console] ビュー

[Devices] > [Printers] の順にサーバオブジェクトを展開した後、Printers オブジェクトコンテナの [Console] ビューにアクセスすることができます。このビューには、コンテナ内の各プリンタオブジェクトに関する次の情報が表示されます。

- [Printer Name]：プリンタの名前。

Printer の [Summary] ビュー

[Devices] > [Printer] > [printer_x] の順にサーバオブジェクトを展開することにより、個別のプリンタに関する [Summary] ビューを表示できます。このビューには、次の情報が表示されます。

- [Printer Name]：プリンタの名前。
- [Printer Status]：このプリンタデバイスの現在のステータス。ステータスは、アイドル、印刷中、ウォームアップ、未定義の状態のいずれかです。
- [Error Condition]：lowPaper、noPaper、lowToner、noToner、doorOpen、jammed、offline、または serviceRequested で示されるエラー状況。

Other Devices

このビューからは、管理対象サーバにインストールされているキーボードやマウスなどの、その他のデバイスに関する情報を取得できます。

- 950 ページの「Other Devices の［Console］ビュー」

Other Devices の［Console］ビュー

このビューには、キーボードやマウスなどの、その他のデバイスが表示されます。

キーボードに関する情報は次のとおりです。

- ［Keyboard Name］
- ［Keyboard Type］
- ［Driver Name］
- ［Class］
- ［Bus Type］

マウスに関する情報は次のとおりです。

- ［Mouse Name］
- ［Mouse Type］
- ［Driver Name］
- ［Class］
- ［Bus Type］

Ports

このビューから、管理対象サーバにシリアルポートやパラレルポートをインストールできます。

- 950 ページの「Ports の［Console］ビュー」

Ports の［Console］ビュー

このビューには、COM ポートなどのシリアルポートや LPT ポートなどのパラレルポートに関する情報が表示されます。ポートに関する情報は次のとおりです。

- ［Port Name］
- ［Controller］
- ［Bus Type］

26 MIB ツールの使用

Novell ZENworks® Server Management では、ネットワーク上の SNMP (Simple Network Management Protocol) 対応デバイスを管理するためのツールを用意しています。この章では、MIB (Management Information Base) ツール、SNMP MIB Compiler、および SNMP MIB Browser について説明します。これらのツールの設定方法と使用方法についても説明します。詳細については、次の節を参照してください。

- 951 ページの「MIB ツールの理解」
- 961 ページの「MIB の設定と MIB ツールのセットアップ」
- 963 ページの「MIB Browser の使用」
- 973 ページの「MIB の保持」

MIB ツールの理解

次の節では、MIB Compiler と MIB Browser を使用して SNMP デバイスを管理する場合に必要なタスクについて説明します。

- 951 ページの「MIB について」
- 952 ページの「SNMP MIB Compiler の理解」
- 953 ページの「SNMP MIB Browser の理解」
- 955 ページの「MIB ツールを使ったデバイスの管理」
- 956 ページの「トラップの定義」

MIB について

デバイスを管理するには、デバイスがサポートする MIB のコピー (複数の場合もあり) を取得する必要があります。MIB は、厳格な形式で記述された ASCII 形式のテキストファイルであり、特定のデバイスクラスで利用することができる管理情報を説明します。たとえば、メーカ X のルータ XYZ を所有しており、このルータの管理に Novell ZENworks Server Management を使用することを検討している場合、メーカ X から XYZ ルータに関する MIB を取得する必要があります。Novell ZENworks Server Management では、多数の標準 MIB とベンダ固有 MIB を用意しています。これらの MIB は、MIB Server Pool フォルダ内の MIB Pool フォルダに存在します。Novell ZENworks Server Management はデフォルトで、これらの中から最も一般的に適用できる MIB をコンパイルします。

新しい MIB をコンパイルする場合、その MIB を MIB Server Pool フォルダ内の MIB Pool フォルダに保存する必要があります。コンソールユーザは、MIB Server Pool フォルダ内の MIB Pool フォルダにあるファイルを選択したり、削除したりすることができます。MIB Compiler は、MIB Server Pool フォルダ内の MIB Pool フォルダに示されているファイルをコンパイルします。

SNMP MIB Compiler の理解

MIB Compiler は次の項目を実行します。

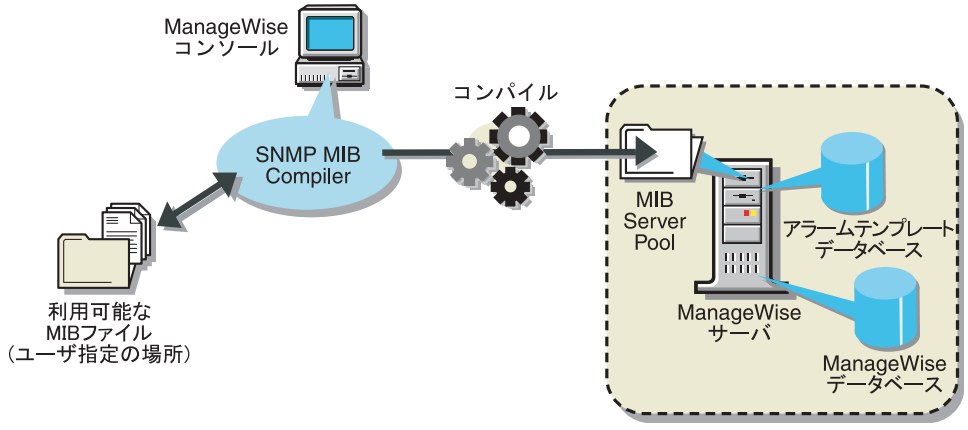
- ASN.1 および SNMP V1、V2 構文で記述されている、定義済みの SNMP MIB ファイルのセットを解析し、その構文を検証します。
- コンパイルしたファイルを Novell ZENworks Server Management データベースに保存します。このデータベースにより、すべてのユーザは一箇所に集められたコンパイル済みファイルにアクセスすることができます。

  MIB Server Pool フォルダに保存された MIB ファイルのコンパイルと保持を、コンソールを使って簡単に実行できます。MIB Pool フォルダに MIB ファイルを追加したり、MIB Pool フォルダから MIB ファイルを削除したりできます。
- アラームテンプレートデータベースのトラップ定義を更新します。

  MIB Compiler を使って、新しい SNMP アラームテンプレートを Novell ZENworks Server Management に導入できます。これにより、コンソールからアラームテンプレートにアクセスしたときに、これらのテンプレートをアラームとして認識し、解釈することができます。

  アラーム管理システムは、アラームに割り当てられる重要度レベルとデバイスステータスを設定するために、MIB 内のトラップ定義の注釈について解釈を実行します。Novell ZENworks Server Management に同梱される MIB ファイルにはすでに適切な注釈が付けられています。
- サイトサーバの MIB Pool に、RFC が含まれるようになりました。この RFC は、サードパーティベンダにより広範囲にわたって使用されます。
- MIB Pool に、Novell GroupWise、Novell BorderManager、Novell eDirectory、Novell Gateways、および Novell VPN のような Novell 独自の MIB が含まれるようになりました。
- コンパイル中に生成されたエラーコードに関するオンラインヘルプを［SNMP Compiler Results］ウィンドウから利用できるようになりました。このヘルプを利用して、こうしたエラーコードに関するすべてのトラブルシューティング情報を確認することができます。したがって、問題を即座に解決することが可能になります。
- ［SNMP Compiler Results］ウィンドウでエラーテキストが赤色で強調表示されるようになったため、エラーを認識しやすくなりました。
- MIB Compiler は、MIB 定義内の軽微なエラーを無視するようになりました。この結果、MIB Compiler は、より多くの MIB をコンパイルすることができます。
- すべての MIB の種類、カテゴリ、生成タイプ (TCG) が一意である必要はなくなりました。SNMP MIB Compiler は、TCG が同一であるすべてのトラップをキャプチャします。
- SNMP MIB Compiler は、アラーム管理システムと連携して機能するようになり、MIB Pool 内で利用可能なトラップ情報と同期した状態でアラーム情報を保持できます。SNMP MIB Compiler の処理速度は向上しています。

次の図は、MIB Compiler が MIB ファイルの情報をどのようにして Novell ZENworks Server Management データベースに組み込むのかを示しています。



Novell ZENworks Server Management をインストールする際、MIB Compiler を使って事前にコンパイルされる MIB ファイルもインストールされます。管理しようとしているすべての SNMP ノードの MIB を Novell ZENworks Server Management を使ってコンパイルする必要があります。サードパーティの MIB を統合することもできます。サードパーティベンダの MIB ファイル、または Novell ZENworks Server Management と共にインストールされなかった MIB ファイルを取得する場合は、MIB Compiler を使ってファイルをコンパイルする必要があります。

MIB Compiler による役割ベースのサービスの使用

Novell ZENworks Server Management が提供する役割ベースのサービスを使って、ネットワーク上のユーザにさまざま役割を割り当てることができます。自分の役割に Enable MIB Compiler タスクが割り当てられた場合、MIB Compiler を使用できます。

Novell ZENworks Server Management の役割ベースの管理に関する詳細については、795 ページの「役割ベース管理」を参照してください。

SNMP MIB Browser の理解

MIB Browser により、ネットワーク上の SNMP 対応デバイスを管理することができます。

このツールを使用するには、SNMP を理解し、MIB の構造を正しく把握している必要があります。MIB Browser を使用して、ターゲットノードにある MIB オブジェクトの値を設定することにより、ネットワーク上のノードを管理することができます。

SNMP MIB の構造についてよくご存知の場合は、MIB Browser を使って、SNMP 対応ノードからデータを取得することができます。

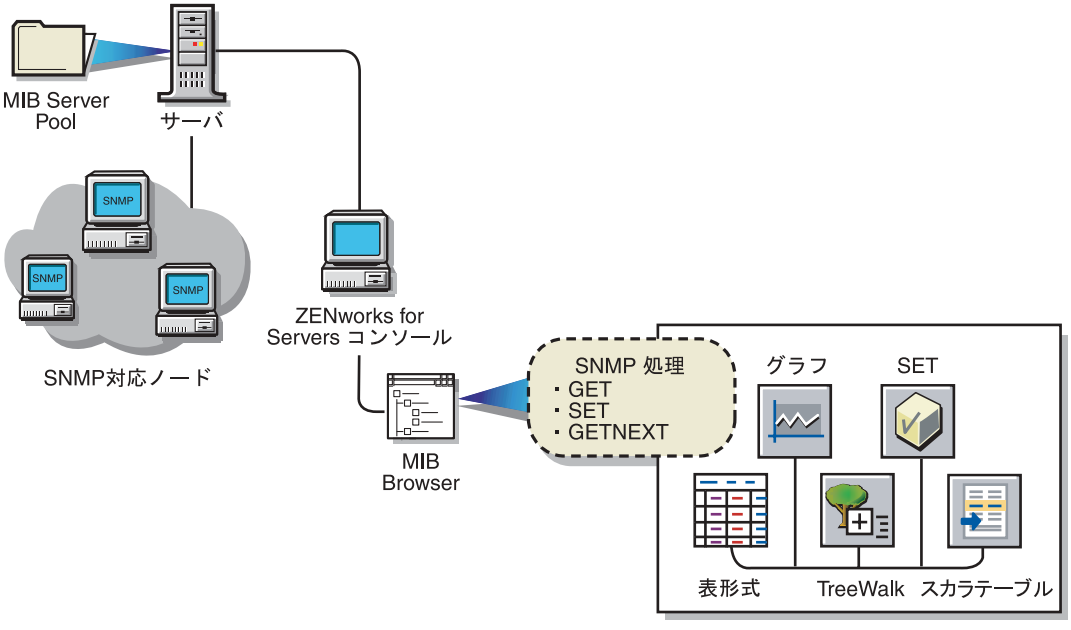
MIB Browser により、ネットワーク上の SNMP エージェントを介して、UDP(User Datagram Protocol) や IP(Internet Protocol) を使ったデータのやりとりをデバイスとの間で実行することができます。SNMP コマンドの結果は、[MIB Browser] ウィンドウに表示されます。

SNMP エージェントプログラムは、特定のネットワークデバイスに関する管理データにアクセスし、こうしたデータに対する SNMP Manager のリクエストに応答します。NetWare® Management Agent ソフトウェアは、NetWare サーバに設定される SNMP エージェントの一例です。SNMP エージェントは、ネットワーク上の各対応デバイスに設定します。

SNMP 対応ノードから取得したデータは多数の Novell ZENworks Server Management ウィンドウに表示されますが、取得するデータの種類の指定に MIB Browser の機能を使用することもできます。MIB Browser を使用することにより、Novell ZENworks Server Management ウィンドウに表示されない SNMP データを取得することもできます。

MIB Browser は、コンパイルされた MIB を取得し、ツリー形式でオブジェクトを表示します。MIB Browser を使用して、ツリー内を移動し、選択したオブジェクトの定義を検索することもできます。Novell ConsoleOne® と SNMP 対応ノード間の通信に使用されるコミュニティ文字列を設定して、デバイスを管理することができます。

次の図は、MIB Browser の機能について説明します。



MIB Browser には次の機能があります。

- MIB 情報をツリー形式で表します。

  MIB ツリーでオブジェクトを参照することができます。このツリーでは、すべてのコンパイル済み MIB の複合 OID（オブジェクト識別子）が表示されます。OID とは、ツリーのルートから各枝に至るまでパス内のすべてのオブジェクトに設定される一連の整数です。OID は、ツリー内のオブジェクトの位置も示します。たとえば、ツリー内の novell(23) オブジェクトは、1.3.6.1.4.1.23 として示されます。MIB ツリーの詳細については、964 ページの「MIB ツリーの参照」を参照してください。

- SNMP GET および GETNEXT コマンドを使用して、ノードに関する特定の情報を取得します。

  MIB 情報は次の形式で表示されます。

  - 表形式でのオブジェクトの表示

    表に新しい行を追加し、SNMP SET コマンドを発行して表内の列の値を更新することができます。詳細については、967 ページの「SNMP テーブルのインスタンスの変更」を参照してください。

- グラフ表示

  SNMP リクエストのグラフ作成を選択すると、1 つまたは複数の MIB オブジェクトのポーリングデータが［Graph］ウィンドウに表示されます。詳細については、971 ページの「SNMP リクエスト結果のグラフ表示」を参照してください。

- スカラテーブルの表示

  スカラオブジェクトを組み合わせることにより、スカラテーブルを作成できます。テーブルのスカラエントリを変更することができます。詳細については、970 ページの「スカラオブジェクトのテーブルの作成」を参照してください。

- TreeWalk 表示

  スカラおよび表形式のオブジェクトの OID 値を参照できます。詳細については、965 ページの「オブジェクトとその子ノードの値の表示」を参照してください。

- SNMP SET コマンドを使って、ターゲットノードの情報を変更します。

  コミュニティ文字列がターゲットノードと一致する場合、MIB オブジェクトの値を取得または変更することができます。ノードの変数をリモートで設定することを、ノードが許可している必要もあります。

- 表、スカラテーブル、またはグラフのプロパティを保存してプロファイルを作成します。

  プロファイルで指定したプロパティを使って、セグメント上の異なる SNMP 対応ノードに関する表、スカラテーブル、またはグラフを表示するにはプロファイルを開きます。詳細については、972 ページの「テーブルおよびグラフへのプロファイルの使用」を参照してください。

- スカラオブジェクト、テーブルとテーブルエントリオブジェクト、列オブジェクト、および MAXACCESS 値などについて新しいアイコンが採用され、認識しやすくなりました。

- 検索ユーティリティにより、MIB ツリー内で MIB 変数を検索できるようになりました。MIB 変数または MIB OID に基づいて検索することができます。

MIB Browser に関する詳細については、963 ページの「MIB Browser の使用」を参照してください。

MIB Browser による役割ベースのサービスの使用

Novell ZENworks Server Management が提供する役割ベースのサービスを使って、ネットワーク上のユーザにさまざま役割を割り当てることができます。自分の役割に Enable MIB Browser タスクが割り当てられた場合、MIB Browser を使用できます。

Novell ZENworks Server Management が提供する役割ベースの管理に関する詳細については、795 ページの「役割ベース管理」を参照してください。

MIB ツールを使ったデバイスの管理

Novell ZENworks Server Management を使って、ネットワーク上の任意の SNMP 対応デバイスを管理することができます。特に、次の項目を実行できます。

- SNMP 対応デバイスに関するアラーム（多くの場合、SNMP トラップと呼ばれる）を受信するためのアラームテンプレートの設定
- MIB Browser での、こうしたデバイスの値の表示と設定

MIB Browser を使用してデバイスの管理を行う前に、次の作業を実行する必要があります。

1. 必要な MIB を取得します。
2. 必要に応じて、トラップの注釈を追加します。
3. MIB Compiler を使用して MIB を追加または削除します。
4. MIB Compiler を実行して、Novell ZENworks Server Management に MIB をコンパイルします。

ASN.1 および SNMP V2 のサポート

MIB Compiler は、ASN.1 および SNMP V1、V2 構文で記述されたすべての MIB ファイルをサポートします。MIB Compiler では、ASN.1 構文に厳密な意味で準拠していない構文もサポートしています。

トラップの定義

一部の SNMP MIB は、ネットワークで異常なイベントが発生したときにデバイスが Novell ConsoleOne に送信できるトラップを定義しています。トラップを含む MIB をコンパイルすると、こうしたトラップに関する情報は Novell ZENworks Server Management アラームデータベースに追加されます。Novell ZENworks Server Management はトラップを受信すると、アラームデータベース内の情報を取得して使用し、アラーム概要文字列を生成して、アラームの種類、アラームの重要度、影響を受けるデバイスの状態、およびその他の詳細情報を判別します。

MIB ファイルのトラップ定義に注釈を追加すると、より詳しいアラーム情報を Novell ZENworks Server Management で表示することができます。こうした注釈はコメントとしてトラップ定義に追加されるため、この MIB をサードパーティ MIB コンパイラを使ってコンパイルすることができます。

すべての Novell® MIB には注釈が追加されます。他の MIB のトラップに注釈を付けないことを選択した場合、Novell ZENworks Server Management はアラームを表示しますが、表示される情報量は少なくなります。SNMP MIB は、TRAP-TYPE マクロを使用してトラップを定義します。

この節では、次のトピックについて説明します。

- 957 ページの「トラップ定義のキーワード」
- 957 ページの「テンプレートデータベース」
- 957 ページの「トラップ注釈のキーワード」
- 959 ページの「トラップ定義の例」
- 959 ページの「Novell ZENworks Server Management における注釈付きトラップの表示」
- 960 ページの「SUMMARY 文字列の書式設定」

トラップ定義のキーワード

次の表は、トラップの定義について説明しています。

キーワード	例	説明
TRAP-TYPE	dupIpxNetAddr	トラップの名前を指定します。たとえば、dupIpxNetAddr は IPX ネットワークアドレスが重複していることを表します。
ENTERPRISE	Novell NetWare-GA-alert-mib	ベンダのツリー内のノードの OBJECT 識別子を含みます。トラップを一意に識別するトラップ番号 (DESCRIPTION 句の後に付けられる ::=8) と一緒に使用されます。
VARIABLES	(osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer)	イベントの追加情報を提供するためにトラップのパラメータとして渡される MIB オブジェクトを、特定の順序で定義します。 たとえば osName は、トラップを送信しているサーバ名を指定するテキスト文字列です。osLOC は、サーバの位置を指定するテキスト文字列です。tiTrapTime は、イベントが発生した時刻を指定する整数です。
DESCRIPTION	"Two servers use the same IPX Internet address."	トラップのセマンティクスを説明するテキスト文字列を提供します。
Trap_number	: :=8	トラップを定義します。

テンプレートデータベース

MIB Compiler は、MIB ファイルのトラップ定義をアラームテンプレートデータベースに適用します。エージェントのすべてのトラップがデータベースに保存されます。

トラップ注釈のキーワード

次の表は、トラップに注釈を追加する場合に使用できるキーワードについて説明しています。

キーワード	説明
--#TYPE	アラームのショートネーム。この名前には、最大 40 文字を使用できます。この注釈が存在しない場合、SNMP トラップ名が使用されます。すべてのトラップには一意の種類を設定する必要があります。
--#SUMMARY	プレースホルダを含むアラームの説明、およびアラームで渡される実際のパラメータの書式情報。 詳細については、960 ページの「SUMMARY 文字列の書式設定」を参照してください。 この注釈が存在しない場合、アラーム概要文字列には、各 SNMP パラメータ名の後にその値が表示されます。
--#ARGUMENTS	SUMMARY 文字列に代入するパラメータのリスト。パラメータは、リストに表示された順序で代入されます。リストの各要素は、VARIABLES 句のパラメータのインデックス (ゼロベース) です。

キーワード	説明
--#SEVERITY	トラップに割り当てられるデフォルトの重要度。次のいずれかになります。 ◆ INFORMATIONAL ◆ MINOR ◆ MAJOR ◆ CRITICAL ◆ UNKNOWN この注釈が存在しない場合、重要度は UNKNOWN として表示されます。
--#TIMEINDEX	VARIABLES 句の変数のインデックス。このインデックスには、アラームが生成された時刻が含まれます。この時刻は、1970 年 1 月 1 日午前 0 時からの秒数で表される整数 (UNIX* 時刻) になります。こうした変数が VARIABLES 句に存在しない場合、VARIABLE 句の変数の総数よりも大きなインデックスを使用します。
--#HELP	このインデックスには、ヘルプファイルの名前が含まれています。
--#HELPTAG	このインデックスには、HELP インデックスで指定されているヘルプファイルの Help ID に対する参照が含まれています。
--#STATE	アラームが生成されたときのオブジェクトのデフォルトの状態。次のいずれかになります。 ◆ OPERATIONAL ◆ NONOPERATIONAL ◆ DEGRADED ◆ UNKNOWN この注釈が存在しない場合、状態は UNKNOWN になります。

トラップの注釈を追加する場合、次のルールに注意します。

- 各注釈がコメントとして組み込まれるようにする必要があります。先頭に二重ハイフンが付けられた行全体がコメントとして処理されます。
- 各注釈が個別の行になるよう設定する必要があります。
- 注釈は、956 ページの「トラップの定義」で説明されている順序で表示される必要があります。
- すべての注釈は、DESCRIPTION 句と ::= 句の間に挿入する必要があります。
- STATE および SEVERITY の値は、MIB を最初にコンパイルしたときにアラームデータベースに書き込まれます。アラームテンプレートの STATE および SEVERITY の値を変更する場合は、対応する MIB ファイルでこれらの値を変更してから、MIB Compiler を使って再コンパイルを実行します。

トラップ定義の例

次の節では、注釈を追加する前と追加した後の SNMP トラップの定義を示します。

- 959 ページの「注釈を追加する前のトラップ定義の例」
- 959 ページの「注釈を追加した後のトラップ定義の例」

注釈を追加する前のトラップ定義の例

```
dupIPXNetAddr      TRAP-TYPE
ENTERPRISE Novell NetWare-GA-alert-mib
VARIABLES{osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer}
DESCRIPTION"Two servers use the same IPX internetwork address."
::=8
```

注釈を追加した後のトラップ定義の例

```
dupIPXNetAddr      TRAP-TYPE
ENTERPRISE Novell NetWare-GA-alert-mib
VARIABLES{osName, osLoc, tiTrapTime, tiEventValue, tiEventSeverity, tiServer}
DESCRIPTION"Two servers use the same IPX internetwork address."
-- Trap annotations are as follows:
--#TYPE "Duplicate IPX address"
--#SUMMARY "%s at %s and %s are using the same IPX address"
--#ARGUMENTS {0,1,5}
--#SEVERITY CRITICAL
--#TIMEINDEX 2
--#HELP "MYHELP.HLP"
--#HELPTAG 60004
--#STATE DEGRADED
::=8
```

Novell ZENworks Server Management における注釈付きトラップの表示

Novell ZENworks Server Management が、957 ページの「トラップ定義のキーワード」で示した dupIpxNetAddr トラップを、次の変数が設定された状態で受け取ったと仮定します。

- osName = SJM-JACK
- osLoc = JACK's CORNER
- tiTrapTime = ~700000000
- tiServer = SJM-TIM

トラップを表示するには、[Active Alarm]、[Alarm History]、または [Alarm Detail] ウィンドウを使用します。次に、この例の結果を示します。

Receive Time:03/04/99 09:15:45

Alarm Type:Duplicate IPX address

Summary:SJM-JACK at JACK's Corner and SJM-TIM are using the same IPX address

Severity:Severe

State:Degraded

SUMMARY 文字列の書式設定

トラップ注釈内の SUMMARY キーワードは、アラーム概要に実際に表示される文字列を提供します。この文字列は、アラームが発生したときに Novell ZENworks Server Management によって使用されます。

文字列内のプレースホルダは、Novell ZENworks Server Management が文字列を表示する前に、トラップの実際のパラメータによって置換されます。各プレースホルダの書式設定文字列はパーセント記号 (%) で始まります。そしてこの文字列は、確定された文字列のプレースホルダに代入されるパラメータの書式設定方法を Novell ZENworks Server Management に通知します。

プレースフォルダの書式設定文字列は、ARGUMENTS キーワードで指定されているパラメータにより、順番に代入されます。ARGUMENTS キーワードは、VARIABLES 句で指定された各トラップパラメータのインデックス (ゼロベース) を一覧表示します。このインデックスは、SUMMARY 文字列に代入する順序で示されます。

Novell ZENworks Server Management は、SUMMARY 文字列に最大 140 文字を表示できます。こうした文字を使用して、該当するアラームについて最も関連性が高い情報を表示します。SUMMARY 文字列が長くなりすぎるため、MIB ファイルの行の長さを妥当な範囲に収めたい場合、複数の連続する SUMMARY 注釈を挿入することができます。この場合、文字列は連結されます。たとえば、次の注釈は同じ文字列を生成します。

ミ#SUMMARY "%s at %s and %s are using the same"

ミ#SUMMARY "IPX address"

ミ#SUMMARY "%s at %s"

ミ#SUMMARY "and %s are"

ミ#SUMMARY "using the same IPX address"

次の表は、書式設定文字列とパラメータの種類を示します。

パラメータの種類	書式設定文字列	表示形式
BOOLEAN	%s	True または False。
	%d	1 または 0。

パラメータの種類	書式設定文字列	表示形式
INTEGER	%x	16 進数。
	%d	10 進数。
	%t	整数または日付と時刻（グリニッジ標準時刻）を表示します。整数の場合、1970 年 1 月 1 日午前 0 時以降の秒数を表します。
OCTET STRING	%s	すべての制御文字を削除した状態でテキスト文字列を表示します。
	%m	ハイフンで区切られた MAC アドレスとしてデータの最初の 6 バイトを表示します。たとえば、00-00-07-00-07。
	%x	16 進数でオクテット文字列を表示します。たとえば、0000070007。
NULL	%d	数値 0 を表示します。
	%s	文字列 NULL を表示します。
OBJECT IDENTIFIER	%s	ドットで区切られた 10 進数の値を表示します。たとえば、1.3.6.5.4。
IP Address	%s	ドットで区切られた IP アドレスを表示します。たとえば、13.56.56.56。
	%x	長い 16 進数の値を表示します。
BIT STRING	%s	各バイトを 10 進数として表示します。

MIB の設定と MIB ツールのセットアップ

この節では、MIB の設定手順について説明するほか、個別のノードに対して SNMP 処理用のコミュニティ文字列をセットアップする手順について説明します。これらの手順を完了したら、MIB ツールを使って SNMP 処理を実行できます。

この節では、次のトピックについて説明します。

- 961 ページの「Novell ZENworks Server Management と統合するためのサードパーティ MIB の注釈付け」
- 962 ページの「SNMP 対応ノードの MIB のコンパイル」

Novell ZENworks Server Management と統合するためのサードパーティ MIB の注釈付け

SNMP トラップ（アラーム）が定義された MIB をコンパイルすると、こうしたトラップに関する情報が Novell ZENworks Server Management アラームデータベースに追加されます。この情報は、Novell ConsoleOne で表示することができます。

Novell ConsoleOne に詳しいアラーム情報を表示できるよう、すべての Novell MIB には注釈が付けられます。このアラーム情報には、アラーム、アラームの重要度、および影響を受けるノードの状態を示す概要が含まれます。サードパーティ MIB ファイルの場合、同じ情報が含まれるとは限りません。したがって、Novell ConsoleOne に表示されるサードパーティ MIB のトラップ情報が、Novell MIB の場合と比べて見劣りすることがあります。

サードパーティ MIB ファイルに注釈を追加してトラップを定義することにより、そのままの状態で MIB をコンパイルした場合に比べて、より多くのアラーム情報を Novell ZENworks Server Management に表示することができます。サードパーティ MIB の注釈はすべて、トラップ定義へのコメントとして追加されます。この処理により、こうした MIB を依然としてサードパーティ MIB コンパイラを使ってコンパイルすることができます。

サードパーティ MIB のトラップに注釈を付けない場合、Novell ZENworks Server Management はアラームを表示します。MIB Compiler は、見あたらない注釈について、ステータスディスプレイに警告を表示します。

サードパーティ MIB に注釈を追加するには

1 テキストエディタで MIB を開きます。

2 957 ページの「トラップ注釈のキーワード」で示されるいずれかの注釈を、次のルールに従って追加します。

- 注釈は、DESCRIPTION 句と "::=" 句の間にのみ入力します。
- 各注釈が個別の行になるよう設定する必要があります。
- 注釈は、957 ページの「トラップ注釈のキーワード」に示される順序で設定する必要があります。
- 各注釈をコメントとして埋め込みます。各注釈の先頭には、2 つのハイフンの後にシャープマーク (#) を付けます。

  例： --#Type "*type_description*"

  完全な例については、959 ページの「トラップ定義の例」を参照してください。

3 トラップ定義に対する注釈の追加を完了したら、変更を保存して、テキストファイルを閉じます。

962 ページの「SNMP 対応ノードの MIB のコンパイル」で示されているとおり、MIB をコンパイルします。

Novell ConsoleOne アラーム処理テーブルを使用して、SNMP MIB のデフォルト値からアラームの重要度レベルおよびアラームの状態に関する値を表示します。MIB のコンパイル後にアラームの重要度レベルまたは状態に関する値を変更した場合、これらの変更を有効にするには MIB を再コンパイルして、アラーム処理テーブルで実行した変更を上書きする必要があります。

SNMP 対応ノードの MIB のコンパイル

MIB Compiler を使用すると、MIB Server Pool の管理に加えて、MIB Server Pool に含まれる MIB ファイルのコンパイルを実行することができます。コンパイルされたファイルの情報は、Novell ZENworks Server Management サーバのデータベースに保存されます。このデータベースは MIB Browser と SNMP プロトコルデコーダによって使用されます。

MIB Compiler は、Novell ZENworks Server Management のアラーム管理システムが使用できるよう、トラップの定義をアラームテンプレートデータベースに追加したり、更新したりすることもできます。

MIB Server Pool には、MIB ファイルの一覧が含まれています。MIB ファイルを MIB Server Pool に追加したり、MIB Server Pool から削除したりすることができます。

MIB をコンパイルするには

1 Novell ConsoleOne で、Novell ZENworks Server Management サーバノードをクリックします。

2 ノードを右クリックし、[Properties]、[MIB Pool] タブの順にクリックします。

最新の MIB Pool には、データベース内に存在するコンパイル済み MIB ファイルの一覧が示されます。

3 オプションを選択します。

- MIB を追加するには、[Add] をクリックして .MIB ファイルを特定し、[MIB Pool] リストに .MIB ファイルを追加します。

  追加された MIB は、隣のリストボックスに表示されます。

  MIB を追加する際、そのトラップ情報を統合するか、除外するかを MIB のコンパイル中に選択します。トラップを MIB に統合しない場合、MIB のコンパイルが完了した時点で MIB 情報だけがデータベースに保存されます。トラップ情報を MIB に統合するには、[Advanced] をクリックして [Trap Integration] チェックボックスを選択します。

- [MIB Pool] リストからファイルを削除するには、リストの MIB を選択して、[Remove] をクリックします。

- ASN.1 構文に厳格に準拠していない MIB をコンパイルするには、[Advanced] をクリックして、[ASN.1 Syntax Relaxation] オプションを選択します。

4 [Compile] をクリックします。

MIB Compiler は、[MIB Pool] リスト内の .MIB 拡張子を持つすべてのファイルをコンパイルして、データベースを更新します。コンパイルプロセスは、[Results] ダイアログボックスを起動することにより開始されます。このダイアログボックスには、コンパイルに成功した MIB、コンパイルされなかった MIB と対応するエラーメッセージ、MIB コンパイル情報によるデータベース更新のステータス、アラームデータベース更新のステータスなど、MIB に関するステータス情報が表示されます。

重要： コンパイル中に [Results] ダイアログボックスを閉じることはできません。コンパイル中は、[Results] ダイアログボックスの [Close] ボタンを使用することができません。このダイアログボックスは、コンパイルが成功するか、失敗しないと閉じることができません。

5 [Close] をクリックします。

重要： SNMP MIB が正しく設定されていない場合、インポートされた RFC(Request for Comments) が MIB のコンパイル中に利用できない場合、または他の .MIB ファイルが利用できない場合、[MIB Compiler] ウィンドウにエラーメッセージが表示されます。必要な RFC または依存する MIB を追加してからコンパイルを実行します。

MIB Browser の使用

この節では、MIB Browser を使用した SNMP 対応ノードの管理方法について説明します。

この節では、次のトピックについて説明します。

- 964 ページの「MIB ツリーの参照」
- 965 ページの「オブジェクトとその子ノードの値の表示」
- 966 ページの「オブジェクト値のセットアップによるノードの設定」
- 967 ページの「SNMP 初期設定の変更」

- 967 ページの「SNMP テーブルのインスタンスの変更」
- 970 ページの「スカラオブジェクトのテーブルの作成」
- 971 ページの「SNMP リクエスト結果のグラフ表示」
- 972 ページの「テーブルおよびグラフへのプロファイルの使用」

MIB ツリーの参照

MIB Browser により、表示したいオブジェクトを選択することができます。選択すると、SNMP 照会がノードに送信され、要求したデータオブジェクトが取得されます。MIB Browser を使用して、SNMP 対応ノードの MIB に含まれる特定のオブジェクトに対して、GET、GETNEXT、および SET リクエストなどの SNMP 処理を実行することもできます。

MIB Browser は定期的にノードのポーリングを実行し、表示を常に更新します。スカラおよび表形式のデータオブジェクトの表示および変更を実行できます。

MIB Tree Browser

MIB Browser 内の MIB Tree Browser には、多数のオブジェクトで構成される管理データがアイコンを使って表示されます。

MIB Browser には、すべてのコンパイル済み MIB の複合 OID ツリーが表示されます。MIB Browser はファイルシステムとよく似ており、SNMP データオブジェクトであるリーフオブジェクトを示します。

MIB Browser は、選択したノードとそのサブツリーおよびリーフオブジェクトを表示し、MIB Tree Browser にオブジェクト名を表示します。ツリーの最上位レベルから参照して、リーフオブジェクトの値を表示することができます。

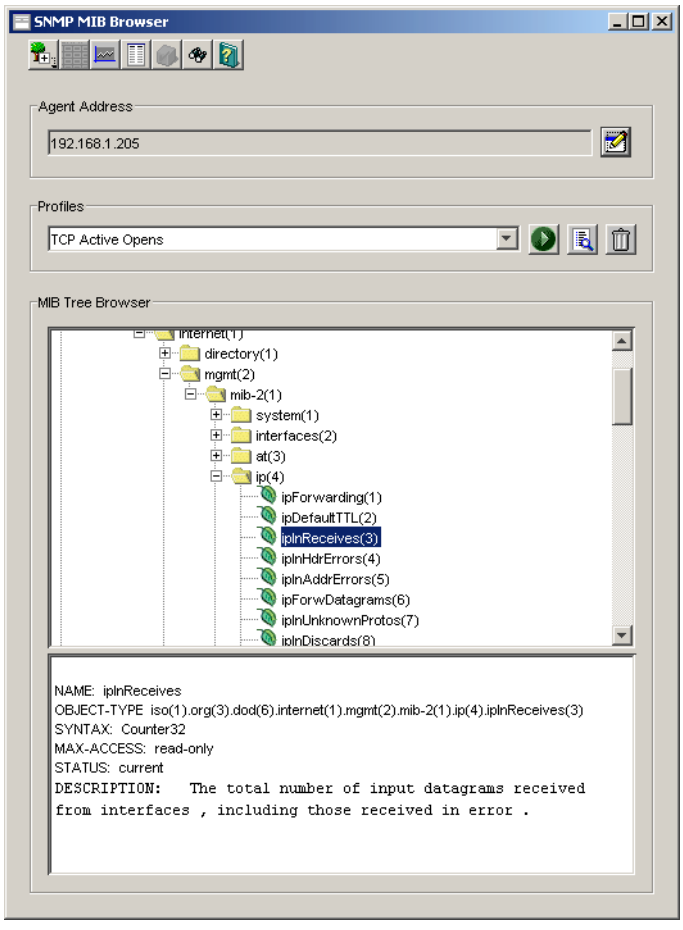
MIB Tree Browser の上のペインには、選択したオブジェクトを含むツリーが表示されます。各オブジェクトは、ファイルフォルダアイコンとして表示され、アイコンの後には SNMP 名と括弧で囲まれた SubID が示されます。オブジェクトがリーフノードではない場合、MIB Tree Browser にはその子も表示されます。

下のペインには、選択したオブジェクトに関する説明が示されます。この説明は、コンパイルした MIB ファイルから取得します。説明の書式は次のとおりです。オブジェクトに関するテキスト説明、完全な数値 OID とオブジェクト名、ASN.1 の種類、サイズ、テキストに関する規則、アクセス、Entry オブジェクトから抽出される Index 句、ステータス、および説明。

たとえば、子ノードを持つ内部ノード SYSTEM の場合、その子ノードは SYSTEM のプロパティを説明します。SYSTEM の OID は iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1) です。この OID を別の方法で表記すると 1.3.6.1.2.1.1 になります。この親ノードには情報が設定されておらず、子ノードにプロパティが設定されていることに注意してください。

SYSTEM の子ノードは sysDescr OID(1.3.6.1.2.1.1.1)、sysObjectID OID(1.3.6.1.2.1.1.2)、sysUpTime OID(1.3.6.1.2.1.1.3)、sysContact OID(1.3.6.1.2.1.1.4)、sysName OID(1.3.6.1.2.1.1.5)、sysLocation OID(1.3.6.1.2.1.1.6)、および sysServices OID(1.3.6.1.2.1.1.7) です。

次の図は［MIB Browser］ウィンドウを示しています。



MIB オブジェクトを参照するには

1 Novell ConsoleOne で、ターゲットになる SNMP 対応ノードをクリックします。

2 [File] > [Action] > [MIB Browser] の順にクリックします。

3 値を表示するオブジェクトを MIB Tree Browser でクリックします。

- オブジェクトを選択するには、MIB Browser のツリーで名前のテキストをクリックするか、アイコンをクリックします。
- ツリー表示の次のレベルを展開または折りたたむには、オブジェクトをダブルクリックします。

オブジェクトとその子ノードの値の表示

MIB Browser では、選択したノードとそのサブツリーおよびリーフオブジェクトを表示することができ、その値は [TreeWalk Query Results] ウィンドウに表示されます。スカラおよび表形式のオブジェクトの OID 値を参照できます。

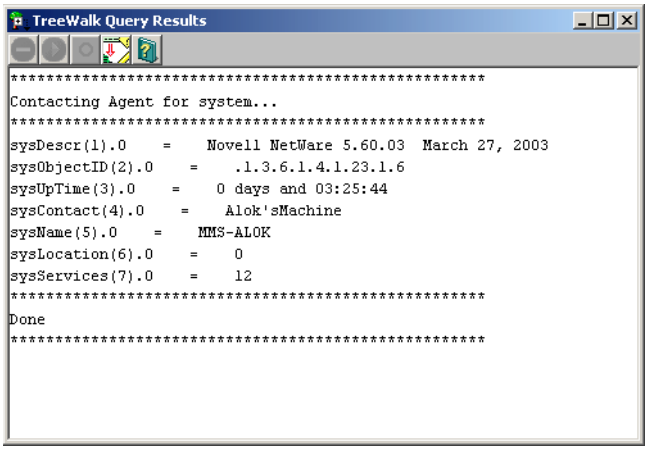
MIB オブジェクトのインスタンスの値を表示するには

1 Novell ConsoleOne で、ターゲットになる SNMP 対応ノードをクリックします。

2 [File] > [Action] > [MIB Browser] の順にクリックします。

3 オブジェクトをクリックし、[Perform TreeWalk for the node] ボタンをクリックします。

次の図は、[TreeWalk Query Results] ウィンドウを示します。



リーフオブジェクトを選択した場合、このオブジェクトの各インスタンスの値を表示できます。リーフオブジェクト以外のオブジェクトを選択した場合、このウィンドウには、そのオブジェクトの子ノードに関するすべての値が表示されます。たとえば、オブジェクト *system* の子ノードの値を表示したい場合は、親オブジェクト *system* をクリックします。

[Treewalk Query Results] ウィンドウの表示プロセスは、選択したオブジェクトのリーフオブジェクトを除くすべてについて再帰的に継続されます。ウィンドウ内のこの表示を一時停止して、再開することができます。

[TreeWalk Query Results] ウィンドウの表示のカスタマイズ

[TreeWalk Query Results] ウィンドウに表示される行数は、treewalk.properties ファイルの指定に基づきます。

このファイルは ¥novell consoleone¥*version*¥bin¥saved-views¥generic ディレクトリに存在し、次の設定を含みます。
MaximumNumberofLine=*number_of_lines_for_display*

number_of_lines_for_display には、一度に表示される行数が含まれます。デフォルトの設定は 10,000 行です。この設定は変更することができます。設定を適用するには、Novell ConsoleOne を再起動して、[TreeWalk Query Results] ウィンドウを表示する必要があります。テキストバッファが一杯になった場合に [TreeWalk Query Results] ウィンドウの表示を消去するには、[Clear] ボタンをクリックします。
treewalk.properties ファイルで大量の行を設定した場合、メモリ不足問題が発生することがあります。

オブジェクト値のセットアップによるノードの設定

適切な権限が付与されている場合、MIB Browser を使用して、SNMP SET コマンドを発行し、SNMP 対応ノードの情報を変更することができます。MIB Browser でスカラオブジェクトを選択して、その値を設定します。

整数、列挙された整数、オブジェクト識別子、文字列、および IP アドレスの各オブジェクトタイプの値を変更することができます。

スカラオブジェクトに対し SNMP SET コマンドを発行するには

1 Novell ConsoleOne で、ターゲットの SNMP 管理対象ノードをクリックします。

2 [File] > [Action] > [MIB Browser] の順にクリックします。

3 値を表示するスカラオブジェクトをクリックし、[Display Data As a Scalar Table] をクリックします。

4 スカラオブジェクトに対しオブジェクトの値を指定します。

5 [OK] をクリックします。

SNMP テーブルの列の値を変更するには、967 ページの「SNMP テーブルのインスタンスの変更」を参照してください。

SNMP 初期設定の変更

ターゲットデバイスと情報をやり取りするのに SNMP パラメータが使用されます。MIB Browser により、SNMP コミュニティ文字列を変更したり、新しいターゲットデバイスの伝送アドレスを指定したりすることができます。

SNMP 処理を実行する場合、こうした値を設定する必要があります。テーブルのポーリングなどの SNMP 処理を開始した後に、SNMP 初期設定を変更しても、その SNMP 処理に変更が適用されることはありません。

次のパラメータを変更できます。

[Agent Address]：SNMP リクエストの送信先になる SNMP 対応ノードの IP または内部 IPX アドレス、および DNS(Domain Name System) 名を指定することができます。このノードには、SNMP エージェントが設定されている必要があります。

[SET and GET Community Strings]：Novell ZENworks Server Management が使用するコミュニティ文字列は、管理対象ノードの SNMP エージェントが使用できるコミュニティ文字列と一致している必要があります。一致していない場合、SNMP 処理は失敗します。ノードの SNMP エージェントが、公開されている（デフォルト）文字列とは異なる SET および GET 処理用コミュニティ文字列を使用している場合、そのコミュニティ文字列を指定した後、デフォルトのコミュニティ文字列や以前に設定したコミュニティ文字列を無効にすることができます。コミュニティ文字列には、Unicode* または各国文字を使用できます。

SNMP の初期設定を変更するには

1 Novell ConsoleOne で、ターゲットになる SNMP 対応ノードをクリックします。

2 [File] > [Action] > [SNMP MIB Browser] の順にクリックします。

3 [Modify SNMP Preferences] をクリックします。

4 パラメータを指定し、[Close] をクリックします。

SNMP テーブルのインスタンスの変更

SNMP MIB 内のテーブルは、MIB の構造から抽出される SNMP コンストラクトです。テーブル内の各行は、SNMP テーブルの行に相当します。

MIB Browser の [Table Display] ウィンドウには、選択した表形式のオブジェクトが表示されます。このウィンドウでは、2 次元のグリッドに、SNMP テーブルからの 1 つ以上の行が表示され、SNMP のインデックスの順序に従って行が示されます。

このテーブルの列として、SNMP テーブルの各列が表示されます。各列の見出しは、SNMP テーブルの列から取得されます。[Table Display] ウィンドウには、選択した MIB の 1 つ以上の行の値を使って列が表示されます。

SNMP により、個別のテーブルエントリについてのみ処理を実行できます。OID によって、その列と行が識別されます。

MIB Browser から、次の処理を実行することができます。

- SNMP テーブルに行を追加します。

  詳細については、969 ページの「SNMP テーブルへの行の追加」を参照してください。

- 編集できるテーブルの行を変更します。

  行の追加または編集に関する詳細については、969 ページの「SNMP テーブルへの行の追加」を参照してください。

- テーブルをプロファイルとして保存します。

  テーブルをプロファイルとして保存する場合の詳細については、972 ページの「テーブルおよびグラフへのプロファイルの使用」を参照してください。

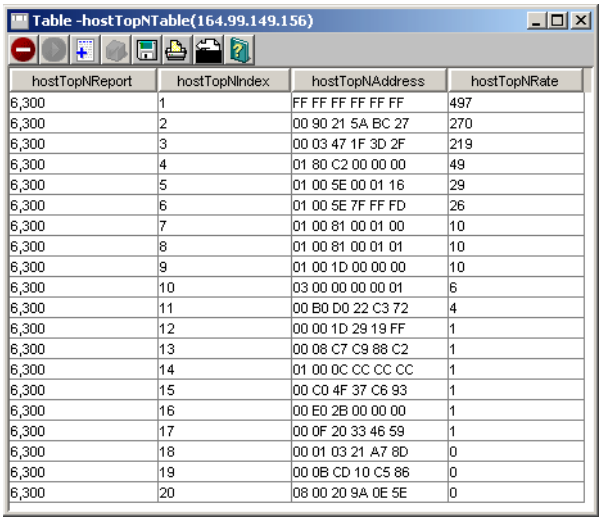
SNMP テーブルの表示

SNMP テーブルを表示するには

1. Novell ConsoleOne で、ターゲットになる SNMP 対応ノードをクリックします。
2. [File] > [Action] > [SNMP MIB Browser] の順にクリックします。
3. 値を表示する表形式オブジェクトをクリックし、[Display Data As a Table] をクリックします。

[Table Display] ウィンドウで、SNMP テーブルの行を追加したり、変更したりして、各列に値を入力することができます。SNMP テーブルにおける行の追加または変更に関する詳細については、969 ページの「SNMP テーブルへの行の追加」を参照してください。

次の図は、[MIB Browser Table Display] ウィンドウを示しています。



hostTopNReport	hostTopNIndex	hostTopNAddress	hostTopNRate
6,300	1	FF FF FF FF FF FF	497
6,300	2	00 90 21 5A BC 27	270
6,300	3	00 03 47 1F 3D 2F	219
6,300	4	01 80 C2 00 00 00	49
6,300	5	01 00 5E 00 01 16	29
6,300	6	01 00 5E 7F FF FD	26
6,300	7	01 00 81 00 01 00	10
6,300	8	01 00 81 00 01 01	10
6,300	9	01 00 1D 00 00 00	10
6,300	10	03 00 00 00 00 01	6
6,300	11	00 B0 D0 22 C3 72	4
6,300	12	00 00 1D 29 19 FF	1
6,300	13	00 08 C7 C9 88 C2	1
6,300	14	01 00 0C CC CC CC	1
6,300	15	00 C0 4F 37 C6 93	1
6,300	16	00 E0 2B 00 00 00	1
6,300	17	00 0F 20 33 46 59	1
6,300	18	00 01 03 21 A7 8D	0
6,300	19	00 0B CD 10 C5 86	0
6,300	20	08 00 20 9A 0E 5E	0

MIB Browser は SNMP 照会をノードに定期的に送信して、必要なデータオブジェクトを取得します。書き込み可能なオブジェクトに新しい値を設定すると、MIB Browser はこうした値をノードに書き込みます。MIB Browser は定期的にノードのポーリングを実行し、常に表示を更新します。SNMP のやり取りを中止したり、キャンセルしたりすることにより、ポーリングの間隔を変更することができます。

SNMP テーブルへの行の追加

SNMP テーブルに新しい行を追加すると、MIB Browser により SNMP SET リクエストが生成されます。

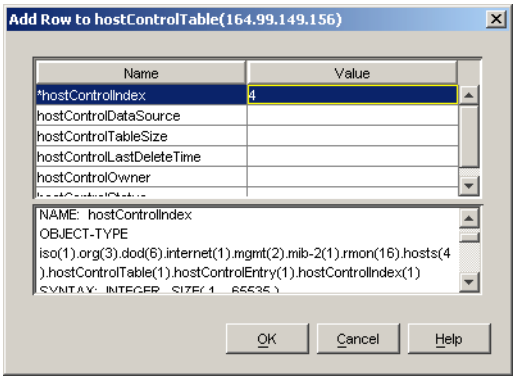
SNMP Set リクエストを生成する前に、MIB Browser は、MIB Browser テーブルで選択されたノードに GET コマンドを送信し、そのオブジェクトの値を取得します。指定された値を含む行をオブジェクトに追加する際、MIB Browser は複数の SNMP SET コマンドを発行し、SNMP テーブルを更新します。

SNMP テーブルに行を追加するには

1 [MIB Browser] ウィンドウのテーブルオブジェクトをクリックし、[Add a New Row to the Table] をクリックします。

テーブルオブジェクトの選択に関する詳細については、967 ページの「SNMP テーブルのインスタンスの変更」を参照してください。

次の図は、[Add Row to Table] ウィンドウを示しています。



2 行をダブルクリックします。

3 値を変更し、[OK] を 2 回クリックします。

SNMP テーブルに行を追加するには、アスタリスクで示されるすべてのインデックス行に値を入力する必要があります。

編集できるテーブルの行を変更するには

1 [Table] ウィンドウを開きます。

2 値を変更する行をクリックし、[Issue SNMP Set request for a column] ボタンをクリックします。

3 行をダブルクリックします。

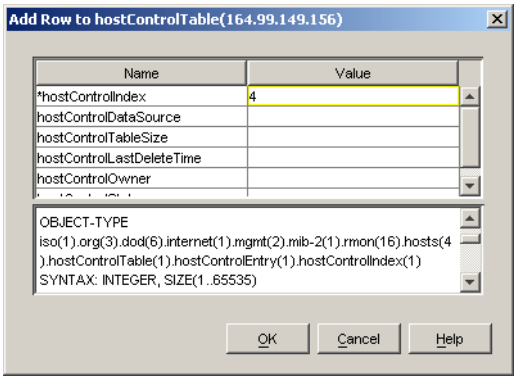
4 オブジェクトの値を変更し、[OK] を 2 回クリックします。

スカラオブジェクトのテーブルの作成

MIB Browser のスカラオブジェクトを組み合わせることにより、スカラテーブルを作成することができます。スカラテーブルとは、スカラオブジェクトエントリの名前と値が設定された 2 列のテーブルのことです。スカラテーブルを作成するには、スカラ子ノードを含むグループノードか、スカラオブジェクトのグループを選択します。たとえば、ipInDelivers や SysUpTime などの 1 つ以上のスカラオブジェクトを追加して、ipInDeliversTable という名前の新しいスカラテーブルを作成します。

作成したスカラテーブルを表示する場合は、スカラテーブルをプロファイルとして保存します。必要に応じて、スカラテーブルのプロファイルをロードすることができます。

次の図は、[Scalar Table] ウィンドウを示しています。



スカラオブジェクトを組み合わせてスカラテーブルを作成し、テーブルを表示するには

1 新しいスカラテーブルを作成します。
2 スカラエントリを追加したり、テーブルからエントリを削除したりして、既存のテーブルを変更します。
3 スカラテーブルをプロファイルとして保存します。
4 プロファイルを起動します。

新しいスカラテーブルを作成するには

1 Novell ConsoleOne で、ターゲットになる SNMP 対応ノードをクリックします。
2 [File] > [Action] > [SNMP MIB Browser] の順にクリックします。
3 スカラグループまたはスカラオブジェクトを右クリックし、[New]、[Scalar Table] の順にクリックします。

既存のテーブルにスカラエントリを追加したり、テーブルからスカラエントリを削除したりするには

1 既存のスカラテーブルを開きます。
2 [MIB Browser] ウィンドウに切り替え、[Add to] をクリックして、*Scalar_table_name* をクリックします。

   別の方法として、[MIB Browser] ウィンドウおよび [Scalar Table] ウィンドウのスカラエントリをクリックして、[Add Node Selected from Browser Window] をクリックします。

スカラエントリを削除するには、[Scalar Table] ウィンドウのスカラエントリをクリックし、[Remove the Node Selected in This Window] をクリックします。

SNMP リクエスト結果のグラフ表示

SNMP リクエストの結果を、MIB オブジェクトに関するポーリングデータを表示するグラフで表すことができます。ASN.1 タイプの Integer、Counter、Time Ticker、および Unsigned Integer の属性だけが、最新の絶対値としてグラフに表示されます。

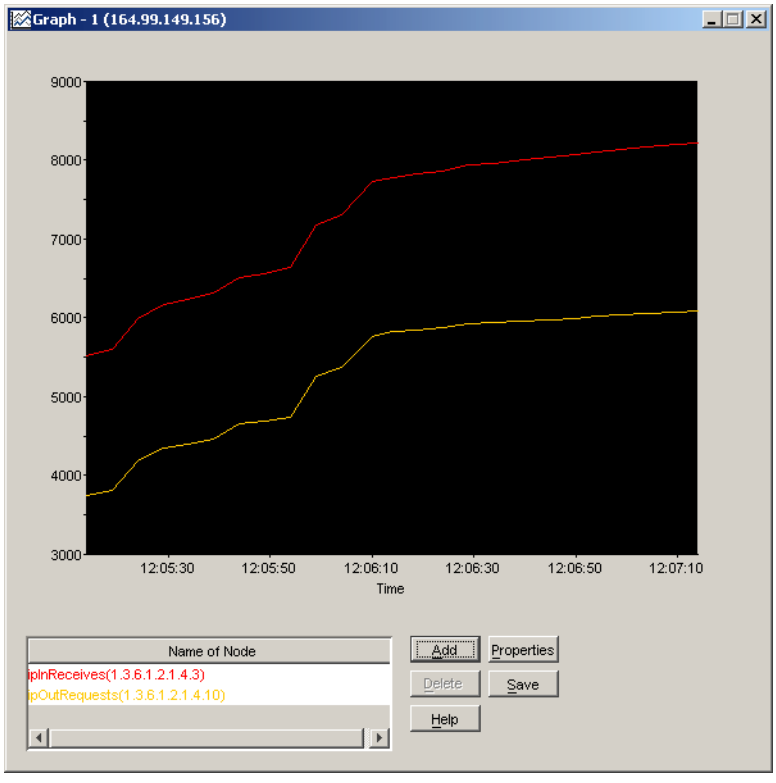
同じグラフに複数のオブジェクトを適用したり、さらに多くのオブジェクトを追加したり、既存のグラフから MIB オブジェクトを削除したりすることができます。作成したグラフを表示する場合は、グラフをプロファイルとして保存します。必要に応じて、このグラフプロファイルをロードすることができます。

1 つ以上のノードに関する SNMP リクエストの結果をグラフで表示するには

1. コンソールで、ターゲットになる SNMP 対応ノードをクリックします。
2. [File] > [Action] > [SNMP MIB Browser] の順にクリックします。
3. 値をグラフに表示する MIB オブジェクトをクリックします。
4. オブジェクトを右クリックし、[New]、[Graph] の順にクリックします。

MIB Browser は、選択されたオブジェクトとそのリーフオブジェクトの値を使用して、ウィンドウの [Graph] ペインに動的にグラフを作成します。

次の図は、[Graph] ウィンドウを示しています。



複数のオブジェクトの値をグラフに表示するには

1. [MIB Browser] ウィンドウに切り替えます。
2. グラフに表示する MIB オブジェクトをクリックし、[Add To]、[Graph] の順にクリックします。

   選択したオブジェクトが、表示先のアクティブなグラフウィンドウに追加されます。

別の方法として、[MIB Browser] ウィンドウから MIB オブジェクトをクリックし、MIB Browser Graph の [Add] ボタンをクリックすることもできます。リストからノードを選択し、[Delete] ボタンをクリックすることにより、不要なオブジェクトをリストから削除します。

[Graph] ウィンドウで、次の処理を実行することができます。

- グラフの Y 軸のサイズを変更します。
- 表示する期間を設定します。
- ポーリング間隔と表示の更新頻度を設定します。

  デフォルトでは、グラフに適用される値は絶対値です。sysUpTime に関して 1 秒ごとの値の変化率を表示する場合は、[Rate] オプションをクリックする必要があります。たとえば、ipInPackets をクリックし、[Rate] オプションを選択した場合、1 秒ごとの値を表示できます。

テーブルおよびグラフへのプロファイルの使用

プロファイルには、グラフ、テーブル、またはスカラテーブルのプロパティに関する情報が含まれます。表示方法 (テーブルまたはグラフ) やポーリング間隔などの情報を指定する場合に、プロファイルを使用します。

テーブル、スカラテーブル、グラフのプロパティをプロファイルとして保存して、プロファイルを作成します。プロファイルで指定されたのと同じプロパティを使って、セグメント上の異なる SNMP 対応ノードのテーブル、スカラテーブル、またはグラフを表示するには、そのプロファイルを開きます。プロファイルは変更したり、削除したりすることができます。

プロファイルを作成するには

1 表示ウィンドウのプロパティを保存します。

2 プロファイルを開きます。

3 必要に応じてプロファイルのプロパティを変更します。

プロファイルを保存するには

1 [Scalar table] ウィンドウ、[Graph] ウィンドウ、または [Table] ウィンドウで [Save] ボタンをクリックします。

2 プロファイルの詳細を入力します。

  オブジェクトの名前、説明、およびプロパティを指定します。

3 [OK] をクリックします。

プロファイルを開くには

1 [MIB Browser] ウィンドウのドロップダウンリストからプロファイルをクリックします。

2 [Launch This Profile] をクリックします。

選択したプロファイルを変更するには

1 [MIB Browser] ウィンドウで選択したプロファイルの [View/Edit Profile Contents] をクリックします。

選択したプロファイルを削除するには

1 [Delete This Profile] をクリックします。

MIB の保持

管理対象ノードについて MIB を追加する必要が生じた場合、MIB をコンパイルする必要があります。

Novell ZENworks Server Management から特定の MIB を削除するには、MIB Server Pool から該当する MIB テキストファイルを削除し、MIB Compiler のコンパイルを実行します。削除した MIB にトラップが含まれている場合、そのアラーム定義を削除してから、MIB Compiler のコンパイルを実行する必要があります。

MIB を追加する際、そのトラップ情報を統合するか、除外するかを MIB のコンパイル中に選択します。トラップと MIB の統合を許可しない場合、MIB のコンパイルが完了した時点で MIB 情報だけがデータベースに保存されます。

MIB の追加または削除の方法に関する詳細については、962 ページの「SNMP 対応ノードの MIB のコンパイル」を参照してください。

27 Monitoring Services

Novell ZENworks® Server Management を使用すると、ネットワークデバイス上のサービスの接続状況や可用性をテストできます。テストでは、診断用パケットを送信することによって応答を確認および測定します。また、サービスのステータスが変更したときにコンソールに通知されます。

この節では、テスト機能の概要や、ノードで監視できるサービスのリストを示し、テストのオプションについて説明します。詳細については、次の節を参照してください。

- 975 ページの「Monitoring Services の理解」
- 977 ページの「ターゲットノード上のサービスの監視」

Monitoring Services の理解

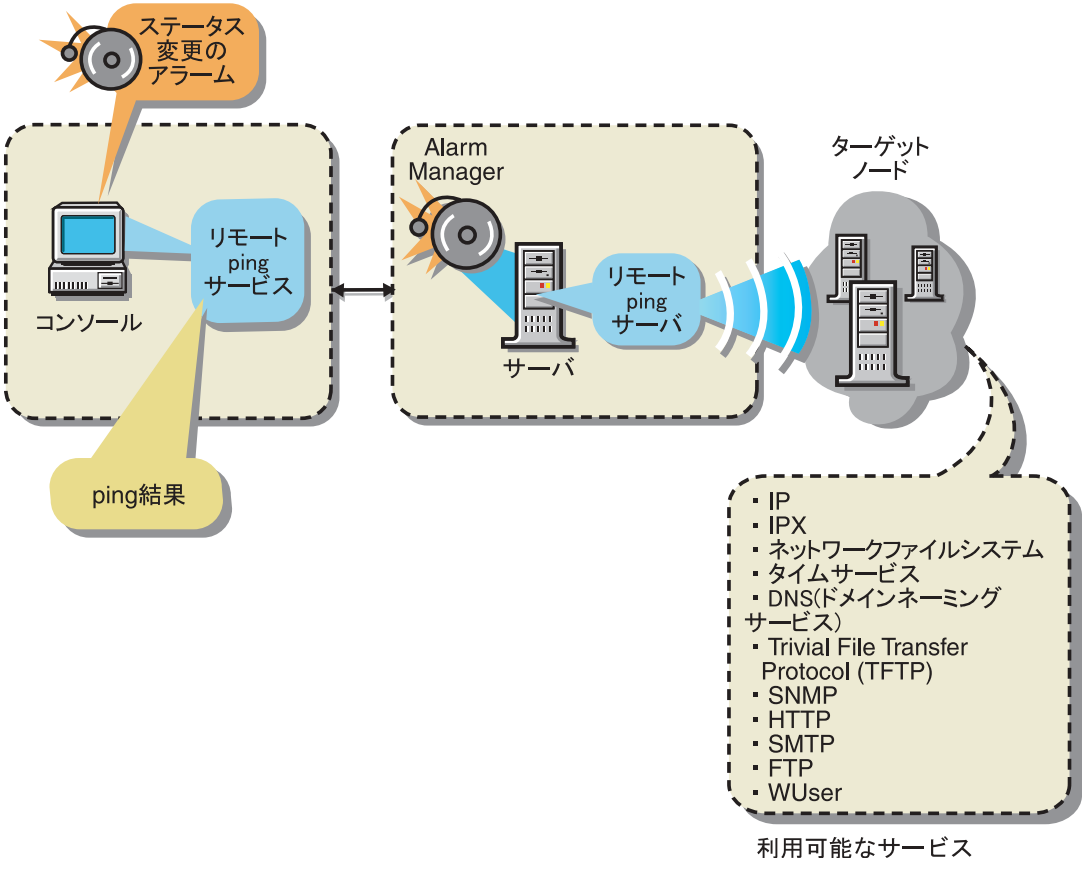
Monitoring Services 機能を使用すると、サーバやルータなどの 1 つまたは複数の重要なネットワークデバイスの接続状況をテストできます。たとえば、サービスを監視することによって、コンソールと重要なノードとの間の接続が切断されたときにすぐに通知されます。

このテスト機能では、次のサービスをテストできます。

- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- エコー
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- IPX™ (Internet Packet Exchange™)
- IP (Internet Protocol)
- NFS (Network File System)
- NNTP (Network News Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- タイムサービス
- TFTP (Trivial File Transfer Protocol)
- WUser

テスト機能は、Novell ZENworks Server Management サーバをリモート ping サーバとして使用します。テストの対象になるノード上のサービスを選択すると、コンソールが Novell ZENworks Server Management サーバ上のリモート ping サーバと対話し、テスト結果がコンソールに表示されます。

次の図は、Monitoring Services の概念図です。



ノードを監視するには、ノードを選択し、必要な期間だけ監視セッションを有効にします。

コンソールからサービスを監視するには、次の方法があります。

- 接続に問題があると思われる場合にノード上のサービスの接続状況を 1 回だけテストする。
- テスト機能を終了するまで、重要なノード上のサービスの接続状況を連続して監視する。
- セグメント上のノードのサービスを連続してポーリングする。たとえば、ターゲットノード上のサービスの接続テストは、監視を無効にするまで実行されます。監視を無効にしないと、コンソールを終了してもテスト機能は引き続き実行されます。

選択したターゲットノード上のサービスの接続状況をテストする場合、次のオプションを設定できます。

- 選択したターゲットノード上のサービスを指定する。

  TCP ベースのサービスをテストする必要がある場合は、そのサービスを既存のサービスのリストに追加します。

- テストを実行する間隔を定義する。
- タイムアウトの値を定義する。

  このタイムアウトの値により、ターゲットノードから応答を受け取るまでリモート ping サーバが待機する時間が決定されます。

接続状況を参照したり、往復遅延や、コンソールから送受信されたパケットの数などの診断情報を測定したりできます。

Monitoring Services の使用に関する役割ベースのサービス

役割ベースのサービス (Role-based Services) は、Monitoring Services のタスクをリモート ping の有効化として定義します。このタスクが役割に割り当てられているユーザは、Monitoring Services 機能を使用できます。

役割ベースのトラフィック分析タスク、Role-based Services の役割オブジェクトの作成、または Role-based Services の役割が実行できるタスクの指定に関する一般情報については、795 ページの「役割ベース管理」を参照してください。

ターゲットノード上のサービスの監視

この節では、Monitoring Services 機能の使用に関するタスクについて説明します。

コンソールを使用して、ネットワーク上の重要なノードを監視したり、ネットワークに影響が出る前に接続に関する潜在的な問題を管理したりできます。選択したノード上でテストするサービスを定義し、テスト結果や、リスト表示された各ターゲットノードの他のデータを表示します。テストを実行するには、次の一般的な手順に従います。

1. 監視するターゲットノードを定義します。

   ターゲットノード上のサービスの指定については、978 ページの「サービスを監視するターゲットノードの定義」を参照してください。

2. 個々のノードごとに、または複数のノードに対して、テストの間隔またはタイムアウトの値を変更します。

   これらのテストでは、ターゲットノードに対して実行されるテストの間隔のデフォルト値や、ターゲットノードから応答を受け取るまでリモート ping サーバが待機する時間を決定するデフォルト値が使用されます。これらのデフォルト値は変更できます。

   テストオプションの編集については、980 ページの「ノードのテストオプションの変更」を参照してください。

3. テスト結果を表示します。

   ノードは、定義されたテストの間隔で連続して監視されます。選択した Monitoring Services のテストに応じて、対応するテスト結果が表示されます。

   テスト結果のデータについては、979 ページの「テスト結果データの表示」を参照してください。

サービスを監視するターゲットノードの定義

Monitoring Services では、テストを実行するターゲットノードを指定する必要があります。次のテストオプションを選択できます。

- 978 ページの「ターゲットノード上のサービスを 1 回だけ実行する」
- 978 ページの「ターゲットノード上のサービスを連続して監視する」
- 978 ページの「テストを無効にするまでセグメント上のターゲットノードのサービスを連続してポーリングする」

注： サーバ上では、約 50 個の重要なサービスを同時に監視できます。50 個を超えるサービスを監視すると、サーバのメモリが大量に消費され、パフォーマンスが低下することがあります。

ターゲットノード上のサービスを 1 回だけ実行する

ネットワークのノードに問題があると思われる場合は、サービスを監視するノードに対して 1 回だけ ping を実行できます。サービスをテストするターゲットノードを選択し、IP または IPX アドレスを指定すると、ノードでテストされるサービスが決定します。たとえば、IPX アドレスを入力すると、デフォルトの IPX サービスがターゲットノード上でテストされます。

[Ping] ウィンドウに、ターゲットノードのステータスや、往復遅延の詳細などのテスト結果が表示されます。

ノード上のサービスを 1 回だけテストするには

1. Novell ConsoleOne で、選択したノードを右クリックし、[Ping] をクリックします。
2. ping を実行するターゲットノードの詳細を入力します。
3. [OK] をクリックします。

ターゲットノード上のサービスを連続して監視する

連続して監視するサービスを指定するには、ターゲットノードを追加し、ノード上のサービスと他のオプションを選択します。ターゲットノードは [Connectivity Test Results] ウィンドウのターゲットノードのリストに追加され、テスト結果のデータが表示されます。サービスの監視は、このウィンドウを閉じるまで実行されます。

ノード上のサービスをテストするためにターゲットノードを定義するには

1. Novell ConsoleOne で、[Action] をクリックし、[Connectivity Test] を選択します。
2. [Add] をクリックします。
3. [Add Ping Target] ダイアログボックスでターゲットノードの詳細を指定します。

   サービスの追加に関する詳細については、980 ページの「監視するサービスの追加」を参照してください。
4. [OK] をクリックします。

ターゲットノードが、[Connectivity Test Results] ウィンドウのターゲットノードのリストに追加されます。

テストを無効にするまでセグメント上のターゲットノードのサービスを連続してポーリングする

セグメントのノード上のサービスをポーリングするには、テストするサービスのリストを指定し、セグメント上のノードを選択します。[Monitor Tab Services] ウィンドウでテストを有効にし、[Polling] ビューにテスト結果を表示します。

テストを無効にしない場合は、コンソールを終了した後もサービスのポーリングが引き続き実行されます。

ポーリングを実行するノード上のサービスを定義するには

1 Novell ConsoleOne で、セグメントのノードを右クリックし、[Properties] をクリックして、[Monitor Services] タブをクリックします。

ノードが複数のセグメントに接続されている場合は、[List of Segment] ダイアログボックスに、複数のセグメント上にある同じノードの複数のアドレスが表示されます。追加するセグメント上のノードをクリックします。

2 [Monitor Services Tab] ウィンドウでターゲットノードに関する詳細を指定します。

サービスの追加に関する詳細については、980 ページの「監視するサービスの追加」を参照してください。

3 [OK] をクリックします。

テスト結果データの表示

ターゲットノード上でテストするサービスを定義すると、コンソールからテスト結果を表示できます。

選択したテストに応じたテスト結果が、該当するウィンドウに表示されます。

ノード上のサービスを 1 回だけテストすることを選択した場合は、テスト結果が [Ping] ウィンドウの [Ping Status] ウィンドウに表示されます。このターゲットノードは、[Connectivity Test Results] ウィンドウでテストされません。

サービスを連続して監視することを選択した場合は、ウィンドウを閉じるまでテストが実行されます。結果は、[Connectivity Test] ウィンドウに表示されます。

テストを無効にするまでサービスを連続してポーリングすることを選択した場合は、[Polling] ビューにテスト結果を表示できます。

ターゲットノード上のサービスを監視する場合は、次のテストデータが利用可能です。

[Ping Target]：サービスをテストするネットワークデバイスの名前またはアドレス (IP または IPX)

[Service]：ターゲットノード上でテストする監視対象サービス

[Port]：サービスが使用するポート番号

[Status of the Target]：[Up Status] は、サービスがノード上で利用可能であり、リモート ping サーバからアクセスできることを示します。[Down Status] は、サービスがダウンしており、サーバからアクセスできないことを示します。

[RoundTrip Delay]：リモート ping サーバがターゲットノードにテスト用パケットを送信してから、応答をターゲットノードから受け取るまでの時間 (ミリ秒)

[Packets Sent]：リモート ping サーバからターゲットノードに送信されたパケットの数

[Packets Received]：リモート ping サーバがターゲットノードから受信したパケットの数

[Packets Lost]：ターゲットノードのテスト中に失われたパケットの数および割合

Interval: 秒単位でテスト間隔の値を表示します。この値により、ターゲットノードに対して実行するテストの間隔が決定されます。

[Timeout]：ミリ秒単位でタイムアウトの値を表示します。この値により、ターゲットノードから応答を受け取るまでリモート ping サーバが待機する時間が決定されます。

[Connectivity Test Results] ウィンドウを表示するには

1 コンソールから [File] > [Action] > [Connectivity Test] の順にクリックします。

コンソールの右側のペインから 1 つまたは複数のターゲットノードを選択すると、接続テストを実行するノードのリストが [Connectivity Test Results] ウィンドウに表示されます。

ポーリングの結果を表示するには

1 コンソールでセグメントをクリックし、[View] > [Polling] の順にクリックします。結果は、[Atlas] レベルでも表示されます。任意のアトラスを選択して、[View] > [Polling] の順にクリックします。[Monitor Services] タブを使って追加したすべてのノードのステータスを、このオプションを使用して表示することができます。

注： [Polling] ビューのリストからターゲットノードを削除するには、ターゲットノードをクリックし、[Delete] をクリックします。

ノードのテストオプションの変更

個々のノードまたは複数のノードに対して以前に設定した、テスト間隔、タイムアウトオプションなどのテストオプションを変更できます。複数のノードを変更するには、[Connectivity Test Results] ウィンドウから複数のノードをクリックします。選択したすべてのターゲットノードにテストオプションが適用されます。

[Connectivity Test Results] ウィンドウを表示するには

1 [Connectivity Test Results] ウィンドウから対象となる行をクリックし、[Edit] ボタンをクリックします。

2 ping を実行する間隔とタイムアウトの値を入力します。

3 [OK] をクリックします。

デフォルト設定に戻す場合は、[Apply Defaults] をクリックします。

監視するサービスの追加

Monitoring Services により、ノード上のサービスをテストすることができます。デフォルトサービスリストに表示されていない TCP ベースのサービスをテストする必要がある場合は、ターゲットノードの追加時にそのサービスの詳細を追加します。

[Add Service] ダイアログボックスでサービスの名前を指定します。追加するサービス名は一意の名前にしてください。また、サービスのポート番号も指定する必要があります。

次の場合に、サービスの詳細を追加できます。

- 978 ページの「ターゲットノード上のサービスを連続して監視する」
- 978 ページの「テストを無効にするまでセグメント上のターゲットノードのサービスを連続してポーリングする」

追加するサービスは、サーバ上のファイルに保管されます。

28 トラフィック分析の理解

Novell ZENworks® Server Management には、ネットワークトラフィックの監視、データのキャプチャ、および監視対象のセグメントのノードやデバイスの主要な統計情報の収集を行うトラフィック分析ツールが用意されています。これらのツールを使用して、重要な情報を取得、評価、および分析し、LAN のトラブルシューティングや管理を効果的に行うことにより、ネットワークのパフォーマンスを最大に保つことができます。

この節では、次のトピックについて説明します。

- 981 ページの「トラフィック分析の理解」
- 995 ページの「セグメント監視の計画」
- 998 ページの「ネットワークトラフィックの分析の準備」
- 1000 ページの「ネットワークトラフィックの分析」
- 1034 ページの「トラフィック分析の最適化」
- 1045 ページの「Traffic Analysis Agent の理解」
- 1047 ページの「NetWare 版 Traffic Analysis Agent の使用」
- 1062 ページの「Windows 版 Traffic Analysis Agent の使用」

トラフィック分析の理解

この節では、トラフィック分析に関する基本的な情報を示し、Novell ZENworks Server Management トラフィック分析コンポーネントについて説明します。

- 981 ページの「トラフィック分析コンポーネント」
- 983 ページの「トラフィック分析コンポーネント間の通信」
- 984 ページの「トラフィック分析機能」
- 985 ページの「トラフィック分析の基礎知識」

トラフィック分析コンポーネント

Novell ZENworks Server Management トラフィック分析コンポーネントには、次のものが含まれます。

- 982 ページの「Management Server」
- 982 ページの「管理コンソール」
- 982 ページの「監視エージェントサーバ」

Management Server

管理サーバには、堅牢で高スケーラブルな Sybase* Adaptive Server Anywhere がインストールされており、ネットワーク内のノードおよびデバイスの名前やアドレスなどの静的情報が保管されます。管理サーバコンポーネントは、NetExplorer™、管理データベース、Consolidator、Atlas Manager などから構成されます。NetExplorer は、ネットワーク内のオブジェクトを検出し、オブジェクトを管理サーバに保管します。Consolidator は、NetExplorer によって検出されたネットワークオブジェクトに関する情報を取得し、管理データベースを構築します。NetExplorer の機能に関する詳細については、830 ページの「ネットワーク検出の理解」を参照してください。

管理データベースは、ネットワークトポロジを確立するために使用される CIM（Common Information Model）スキーマから構成されます。CIM スキーマ拡張機能により、データベース内の情報を整理し、この情報を使用してネットワークマップを表示します。Atlas Manager は、管理データベースから情報を取得し、Novell ConsoleOne 上にネットワークマップを表示します。

管理コンソール

Novell ConsoleOne® は、ディレクトリ対応で Java* ベースの Novell® のネットワーク管理ツールであり、管理コンソールコンポーネントです。Novell ZENworks Server Management は、Novell ConsoleOne のスナップインであり、メニューオプション、既存の Novell™ オブジェクトのプロパティページ、およびネットワークリソースを参照し整理する方法を追加することによって Novell ConsoleOne’の機能を拡張します。Novell ConsoleOne は、Novell ZENworks Server Management トラフィック分析を行うための直観的でグラフィカルなユーザインタフェースです。Novell ConsoleOne の機能に関する詳細については、874 ページの「アトラスの管理」を参照してください。

監視エージェントサーバ

ネットワーク上のセグメントまたはデバイスを分析する前に、それらが監視されていることを確認する必要があります。監視を有効にするには、ネットワーク監視エージェントソフトウェアが、ネットワーク内の管理サーバまたは独立したサーバのいずれかにインストールされていることを確認してください。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」を参照してください。ネットワーク監視エージェントは、ネットワークの監視に役立つ情報またはサービスを収集または提供します。

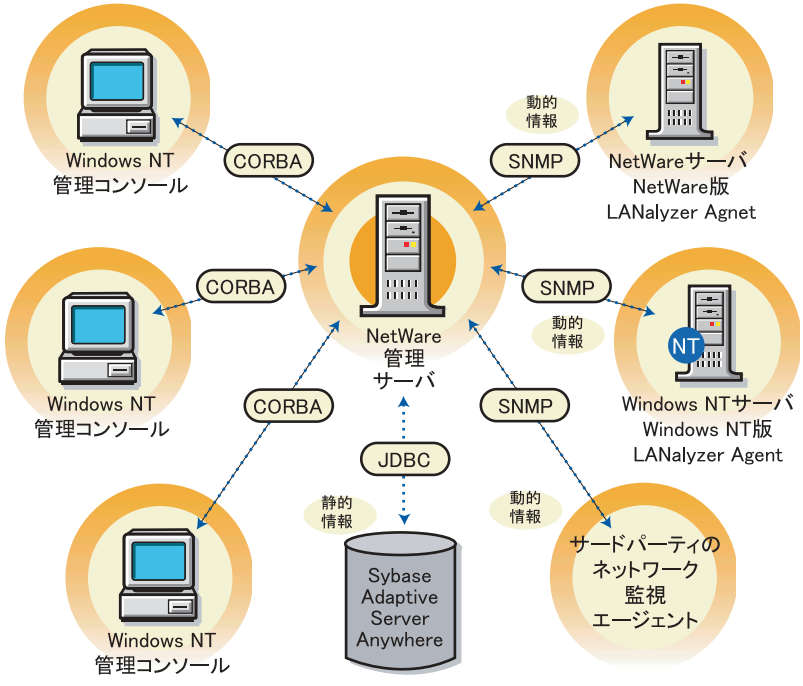
エージェントプログラムは、ユーザが指定したパラメータを使用して、ネットワークのすべてまたは一部を検索し、ユーザが要求した情報を収集し、ユーザが必要なときにその情報をユーザに提供します。エージェントによって収集された情報を使用して、ネットワーク上のトラフィックを分析できます。また、エージェントは Novell ConsoleOne に警告を送信することによって重複した IP アドレスなどの問題を通知するため、ネットワークパフォーマンスが影響を受ける前に問題を解決することができるようになります。アラームの管理に関する詳細については、887 ページの「アラーム管理システムの管理」を参照してください。

ネットワーク監視エージェントは、トラフィックを監視し、ネットワークの異常を検出するのに役立つネットワークオブジェクトや情報のデータベースを構築するためにフレームをキャプチャします。ネットワーク監視エージェントソフトウェアが各セグメントのサーバにインストールされている場合は、トラフィック分析ツールを使用して、ネットワーク上のトラフィックを監視し、ネットワークの問題の原因を特定し、最適なパフォーマンスを維持することができます。詳細については、985 ページの「ネットワーク監視エージェントについて」を参照してください。Novell NetWare® 版および Windows* 版 Traffic Analysis Agent は、Novell ZENworks Server Management のコンポーネントであり、Ethernet、FDDI、またはトークンリングネットワークを監視するために使用します。

トラフィック分析コンポーネント間の通信

Novell ConsoleOne は、CORBA (Common Object Request Broker Architecture) を使用して管理サーバと通信し、ネットワーク内のノードおよびデバイスに関する動的および静的情報を取得します。Novell ConsoleOne が管理サーバから静的情報を要求すると、管理サーバは JDBC (Java Database Connectivity) を使用して管理データベースと通信し、管理データベースから必要な静的情報を収集し、その情報を Novell ConsoleOne に提供します。Novell ConsoleOne が管理サーバから動的情報を要求すると、管理サーバは SNMP を使用してネットワーク監視エージェントと通信し、必要な動的情報を収集し、その情報を Novell ConsoleOne に提供します。

次の図は、このような通信に関する概念図です。



トラフィック分析機能

Novell ZENworks Server Management トラフィック分析コンポーネントは、次の機能を提供します。

- 984 ページの「セグメントによって生成されたトラフィックの分析」
- 984 ページの「セグメントに接続されたノードによって生成されたトラフィックの分析」
- 984 ページの「パケットの収集、収集したパケットのデコード、および収集した情報の表示」
- 984 ページの「プロトコルによって生成されたトラフィックの分析」
- 985 ページの「スイッチによって生成されたトラフィックの分析」

セグメントによって生成されたトラフィックの分析

トラフィック分析ツールを使用すると、現在および過去のセグメントの統計を収集し、リアルタイムで表示したり、保存して後で表示したり、データベース、スプレッドシート、または管理レポーティングシステムに転送したりできます。詳細については、1001 ページの「セグメントのトラフィックの分析」を参照してください。

セグメントに接続されたノードによって生成されたトラフィックの分析

トラフィック分析ツールを使用すると、監視対象の Ethernet、FDDI、またはトークンリングセグメント上のノードに関する統計情報を取得し、セグメント上の上位ノードを調べることができます。ノードがダウンしたときに警告するように無効ネットワーク内のノードのステータスを監視できます。また、事前に設定したしきい値のパラメータを超えると生成されるアラームを表示することもできます。すぐに通知する必要があるアラームは、電子メールを使用してリモートのユーザに転送できます。詳細については、1010 ページの「セグメントに接続されたノードのトラフィックの分析」を参照してください。

パケットの収集、収集したパケットのデコード、および収集した情報の表示

トラフィック分析ツールを使用すると、監視対象セグメント上のノード間のパケットをキャプチャできます。また、キャプチャするパケットの種類に基づいてキャプチャフィルタをすばやく定義できます。パケットがキャプチャされると、プロトコルがデコードされ、色で識別された概要、デコード、および 16 進のペインに表示されます。キャプチャしたパケットから取得された情報は、セグメント上のトラフィックを検査および分析するために使用されます。トラフィック分析ツールの分析機能および高度なプロトコルデコードを使用すると、ネットワークの異常を特定し、ネットワークパフォーマンスの問題を解決できます。詳細については、1017 ページの「パケットのキャプチャ」、995 ページの「Novell ZENworks Server Management によってサポートされているプロトコルデコードスイート」、および 1021 ページの「キャプチャされたパケットの表示」を参照してください。

プロトコルによって生成されたトラフィックの分析

トラフィック分析ツールを使用すると、ネットワークのネットワーク層、トランスポート層、およびアプリケーション層のプロトコルの配布を調べ、ネットワーク監視エージェントによって検出されたプロトコルの統計情報を取得できます。詳細については、1028 ページの「ネットワークのプロトコルによって生成されたトラフィックの分析」を参照してください。

スイッチによって生成されたトラフィックの分析

トラフィック分析ツールを使用すると、監視対象スイッチのポート統計を調べて、スイッチトラフィックを分析できます。詳細については、1032 ページの「スイッチ上のトラフィックの分析」を参照してください。

トラフィック分析の基礎知識

Novell ZENworks Server Management のツールを使用して、ネットワーク上のノードおよびデバイスに関する統計情報を取得できます。この情報を使用してネットワーク上のトラフィックのパフォーマンスを分析および管理することにより、ネットワークを円滑に運用できます。また、Novell ZENworks Server Management には、ノード間のパケットをキャプチャおよびデコードするツールも用意されています。キャプチャしたパケットから取得されたデコード済み情報を使用し、ノード間のトラフィックを分析できます。

セグメントと、セグメントに接続されたノードを分析するには、セグメントがネットワーク監視エージェントによって監視されていることを確認する必要があります。ネットワークの種類に基づいてエージェントを選択します。Novell ZENworks Server Management トラフィック分析ツールには、ネットワーク内のセグメントを監視するために使用できる NetWare 版 Traffic Analysis Agent および Windows 版 Traffic Analysis Agent が含まれます。NetWare 5.*x* は、Novell ZENworks Server Management の管理サーバです。NetWare 5.*x* に含まれる Novell eDirectory を Novell ConsoleOne と共に使用することにより、役割ベースの管理を実行できるようになります。

次の節には、Novell ZENworks Server Management トラフィック分析機能の理解に役立つ情報が記載されています。

- 985 ページの「ネットワーク監視エージェントについて」
- 993 ページの「役割ベースのトラフィック分析タスク」
- 995 ページの「Novell ZENworks Server Managementによってサポートされているプロトコルデコードスイート」

ネットワーク監視エージェントについて

ネットワーク監視エージェントには、SNMP を使用してネットワーク上のセグメントおよびデバイスをリモートから監視できる機能が用意されています。ネットワーク監視エージェントは、ネットワーク上のノードおよびデバイスに関する統計およびトレンド情報を収集および保管し、ネットワークのステータスに関する情報をリアルタイムで提供します。ネットワーク監視エージェントを使用すると、デスクトップから Ethernet、FDDI、またはトークンリングセグメントのトラブルシューティングおよび最適化を実行できます。

ネットワークの規模や種類に基づいて、RMON、RMON Lite、RMON Plus、RMON2、または Bridge エージェントを使用してトラフィックを監視できます。次の節には、エージェントの機能の理解に役立つ情報が記載されています。

- 986 ページの「RMON エージェントの機能」
- 987 ページの「RMON Lite エージェントの機能」
- 988 ページの「RMON Plus エージェントの機能」
- 989 ページの「RMON2 エージェントの機能」
- 991 ページの「Bridge エージェントの機能」
- 992 ページの「RMON に関する概要情報の表示」

RMON エージェントの機能

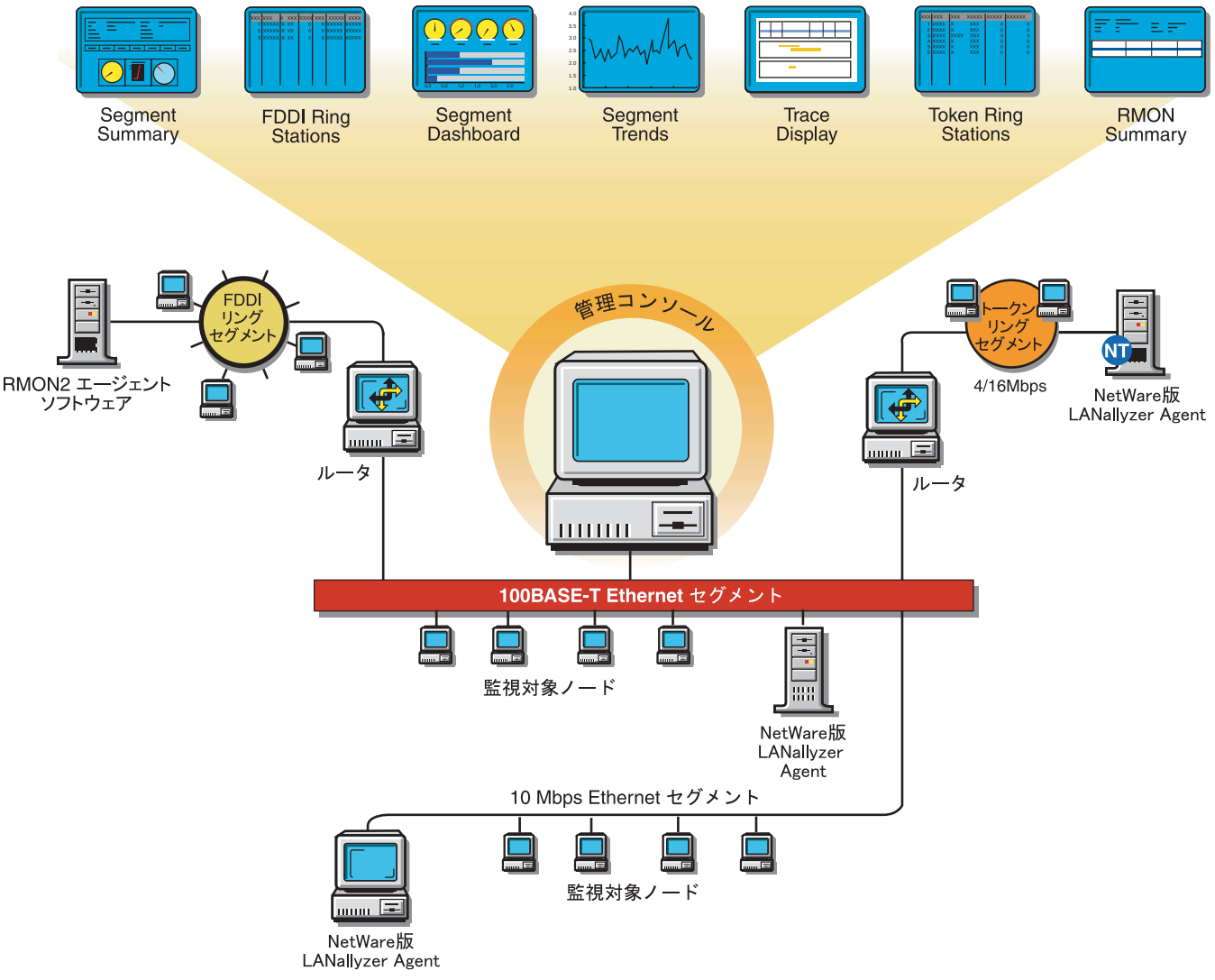
RMON エージェントは、標準的な監視機能の仕様に基づき、ネットワーク上のさまざまなノードおよびコンソールシステム間でネットワークデータを交換できます。このデータは、ネットワーク管理者が、分散する LAN のグループの監視、分析、およびトラブルシューティングを一元的に行うために使用します。RMON は、MIB の一部について説明している「RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)」で SNMP の拡張機能として指定されています。

RMON エージェントは、Ethernet、FDDI、またはトークンリングセグメントの監視に最適です。

RMON エージェントは、監視する要素の次の 9 つの RMON グループの情報を収集します。各グループは、ネットワーク監視要件を満たす特定のデータセットを提供します。詳細については、「RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)」を参照してください。

RMON グループ	説明
Statistics(統計情報)	エージェントが測定した、デバイスの各監視対象インタフェースに関する統計を含みます。
History	ネットワークから統計サンプルを定期的に記録し、後で取得できるように保管します。
Alarm	エージェントの変数から統計サンプルを定期的に取得し、以前に設定したしきい値と比較します。監視対象の変数がしきい値を超えると、イベントが生成されます。
Host	ネットワークで検出された各ホストに関連する統計を含みます。
HostTopN	ホストのいずれかの統計を基準にして順序付けられたリストの上位にあるホストに関するテーブルを作成します。
Matrix	2 つのノード間の通信に関する統計を保管します。デバイスが新しい通信を検出すると、テーブルに新しいエントリが作成されます。
Filters	パケットをフィルタの条件に一致させます。条件に一致したパケットは、キャプチャしたり、イベントを生成したりできるデータストリームになります。
Packet Capture	チャネルを通ったパケットをキャプチャできるようにします。
Events	デバイスからのイベントの生成および通知を制御します。

次の図は、RMON エージェントを使用してネットワーク上のノードおよびデバイスを監視するときに表示できる Novell ZENworks Server Management のビューを示しています。



RMON Lite エージェントの機能

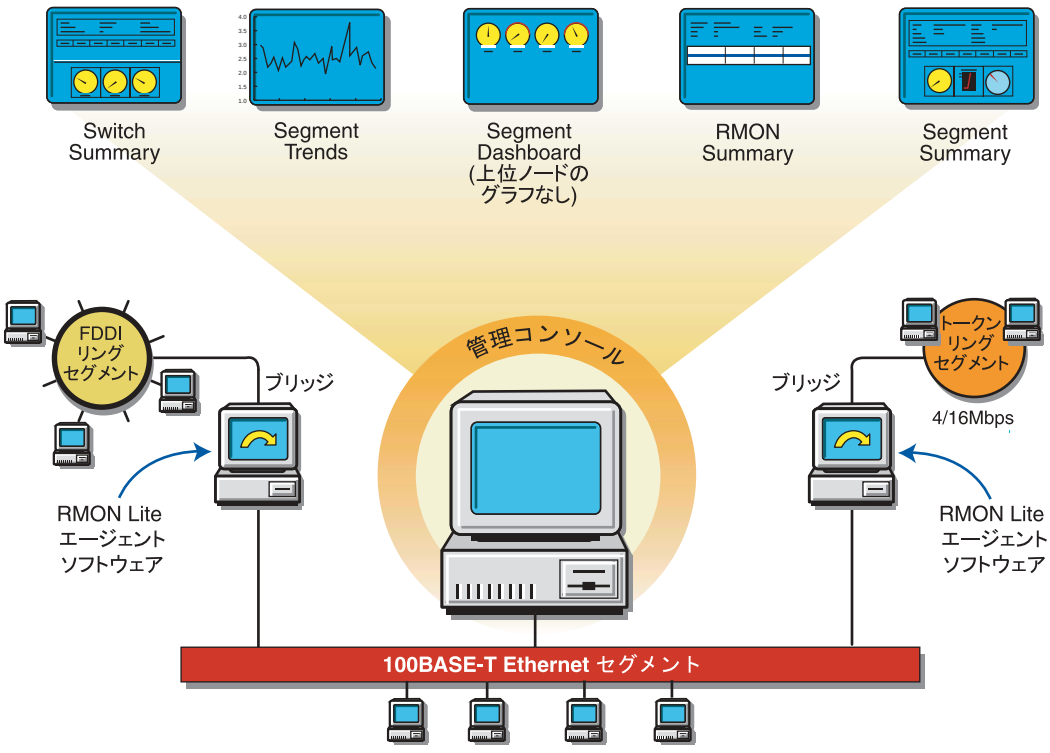
RMON Lite エージェントは、ネットワーク管理専用ではないデバイスの監視に最適です。たとえば、RMON Lite エージェントを使用して、ネットワーク内のスイッチを監視できます。

RMON Lite エージェントは、次の 4 つの RMON グループをサポートします。

- Statistics（統計情報）
- History
- Alarm
- イベント

各グループの簡単な説明については、986 ページの「RMON エージェントの機能」の表を参照してください。

次の図は、RMON Lite エージェントを使用してネットワーク上のノードおよびデバイスを監視するときに表示できる Novell ZENworks Server Management のビューを示しています。



RMON Plus エージェントの機能

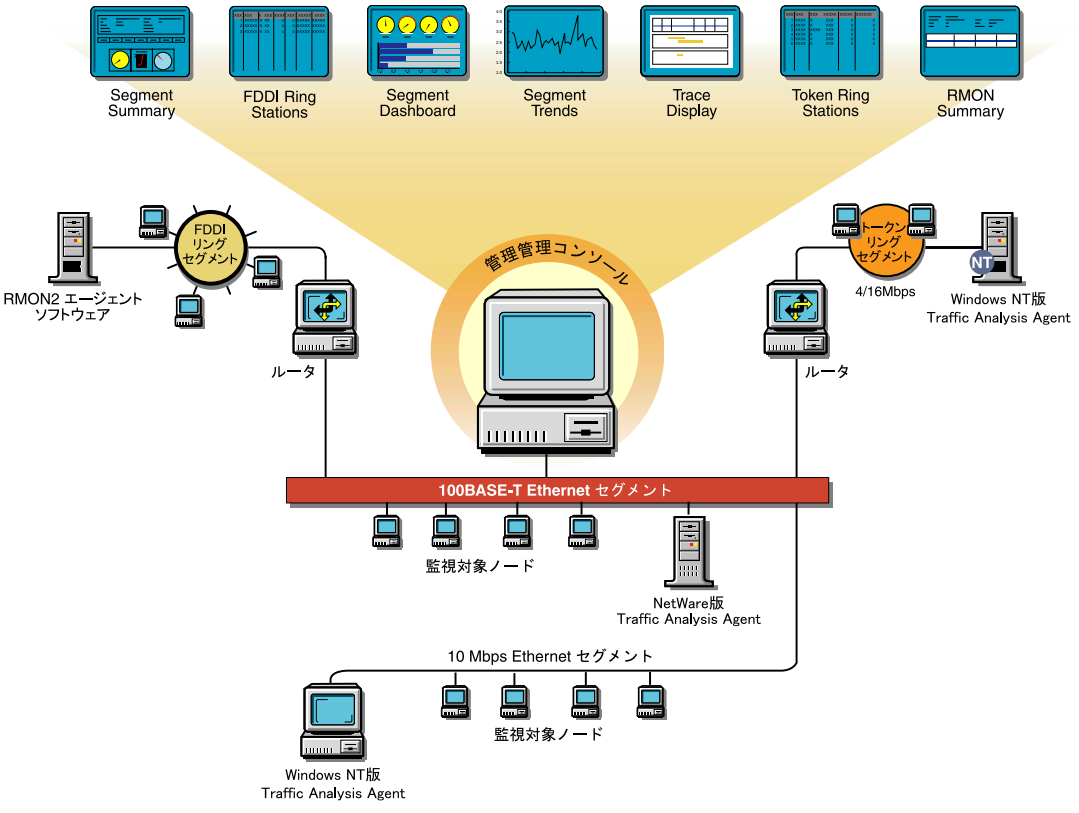
RMON Plus エージェントは、RMON エージェントから収集されたデータを提供することによって RMON エージェントの機能を拡張する独自のエージェントです。詳細については、986 ページの「RMON エージェントの機能」を参照してください。グループについては、次の表を参照してください。

RMON Plus グループ	説明
Buffer	バッファでキャプチャされたパケットのオクテット（フレームビットを除外し FCS（Frame Check Sequence）を含めます）の数を記録します。
Admin	バージョン番号などのエージェントに固有な情報を収集します。
HostMonitor	特定のホストテーブルのために一連のノードを監視し、ホストが稼働またはダウンしたときにトラップを設定します。
DuplicateIP	IP アドレスが重複する受信パケットのリストを記録および更新します。
MacToIP	個々のホストテーブルのためにホストアドレスに関連付けられた IP アドレスのレコードを保管します。
BoardStatus	RMON エージェントの各論理インタフェースのステータスを記録します。

RMON Plus は、Ethernet、FDDI、またはトークンリングセグメントの監視に最適です。ネットワーク上のトラフィックを監視するために使用される RMON Plus エージェントのバージョンに応じて、データを収集できるメディアの種類が異なります。RMON Plus エージェントの各バージョンでサポートされるメディアの種類については、次の表を参照してください。

RMON Plus エージェント	メディアサポート
NetWare 版 Traffic Analysis Agent1.1	Ethernet およびトークンリング
NetWare 版 Traffic Analysis Agent1.21 以降	Ethernet、FDDI、またはトークンリング
Windows 版 Traffic Analysis Agent（バージョン 1.30）	Ethernet、FDDI、またはトークンリング

次の図は、RMON Plus エージェントを使用してネットワーク上のノードおよびデバイスを監視するときに表示できる Novell ZENworks Server Management のビューを示しています。



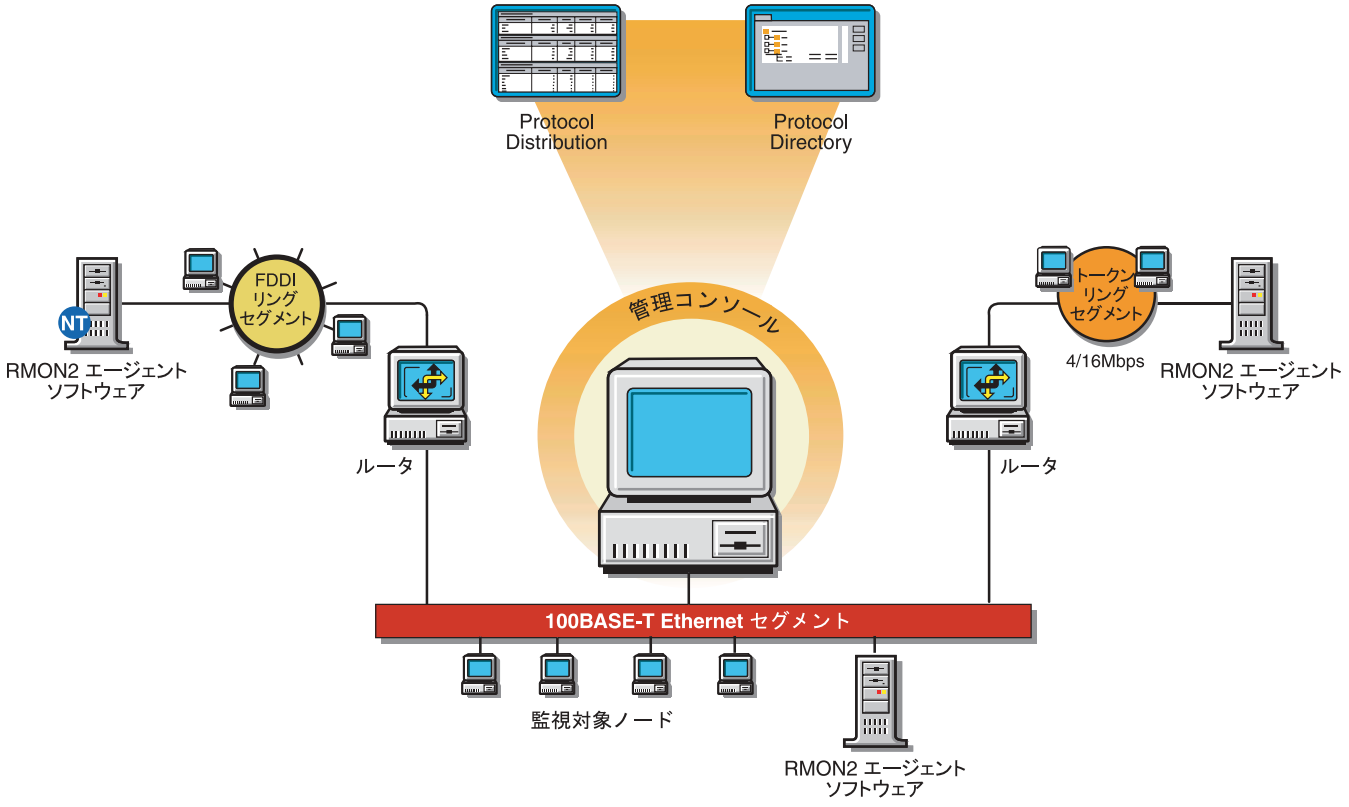
RMON2 エージェントの機能

RMON エージェントを使用すると、物理層およびデータリンク層のノードおよびデバイスからデータを収集できます。RMON2 エージェントを使用すると、ネットワークのネットワーク層およびアプリケーション層のノードおよびデバイスからデータを収集できます。また、RMON2 エージェントでは、ネットワークのノードで使用されているプロトコルおよびアプリケーションに基づいて、ネットワークの使用状況を調べることもできます。次の RMON2 グループを使用すると、データリンク層より上のトラフィックパターンを表示できます。詳細については、「RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)」を参照してください。

RMON2 グループ	説明
Protocol Directory	識別可能なすべてのプロトコルとその説明に関するテーブルを提供します。
Protocol Distribution	エージェントが追跡するように設定されている各プロトコルの統計情報を提供します。
Address Map	ネットワーク層アドレスを、対応する MAC (Media Access Control) アドレスにマッピングします。
Network-Layer Host	ネットワーク層アドレスごとに各ホストに関する統計情報を提供します。
Network-Layer Matrix	ネットワーク層アドレス間の各ネットワーク通信に関する統計情報を提供します。
Application-Layer Host	指定したアプリケーション層プロトコルについて、各ホストにより生成されたトラフィックに関する統計情報を提供します。プロトコルによって分割されたトラフィックは、Protocol Directory グループによって認識できます。
Application-Layer Matrix	指定したアプリケーション層プロトコルの、ネットワーク層アドレス間の通信に関する統計情報を提供します。プロトコルによって分割されたトラフィックは、Protocol Directory グループによって認識できます。
User History	指定した間隔で MIB オブジェクトの RMON2 データのサンプルを保存できるようになります。
Probe Configuration	リセット、ソフトウェア更新、IP アドレス変更、トラップ先などのエージェントパラメータを設定および照会するリモート機能を提供します。
RMON Conformance	グループのサポートのステータスに関する情報を管理ソフトウェアに提供します。

重要： コンソールは、Protocol Directory グループおよび Protocol Distribution グループのみサポートします。

次の図は、RMON2 エージェントを使用してネットワーク上のノードおよびデバイスを監視するときに表示できる Novell ZENworks Server Management のビューを示しています。



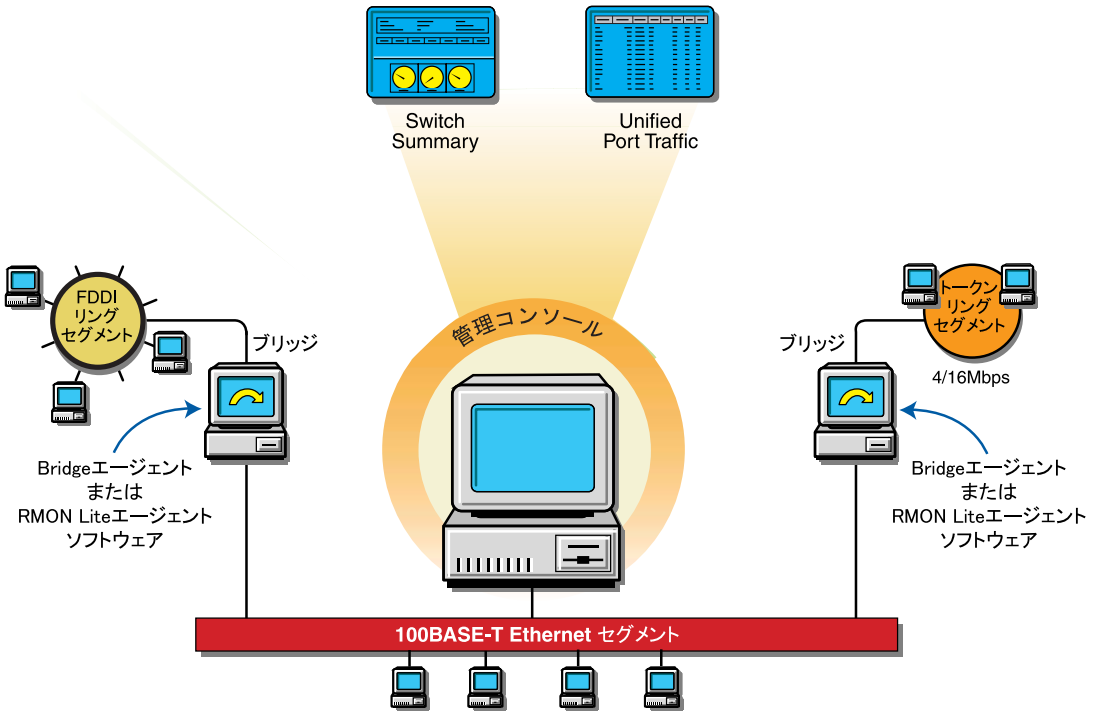
Bridge エージェントの機能

ブリッジは 、ネットワーク層以下の LAN セグメントに接続するために使用されます。ブリッジは、データリンクヘッダの情報に基づいてネットワーク間のパケットを転送することによって、2 つ以上の物理ネットワークを接続します。

Bridge エージェントは、次の 5 つの Bridge グループの情報を収集します。この情報を使用して、スイッチを使用したネットワークを監視できます。詳細については、「RFC 1493 (http://www.isi.edu/in-notes/rfc1493.txt)」を参照してください。

グループ	説明
Base	すべての種類のブリッジに適用可能なオブジェクトに関する情報を保管します。
Spanning Tree Protocol	スパンツリープロトコルを使用した場合の、ブリッジのステータスに関する情報を保管します。
Source Route Bridging	ソースルートブリッジを使用した場合の、デバイスのステータスに関する情報を提供します。
Transparent Bridging	トランスペアレントブリッジを使用した場合の、エンティティのステータスに関する情報を提供します。
スタティック	宛先アドレスフィルタリングを使用した場合の、エンティティのステータスに関する情報を収集します。

次の図は、Bridge エージェントを使用してネットワーク上のノードおよびデバイスを監視するときに表示できる Novell ZENworks Server Management のビューを示しています。



RMON に関する概要情報の表示

[RMON Summary] ビューには、選択したノード上の RMON サービスに関する概要情報が表示されます。RMON エージェントに関する静的情報や、ユーザによってエージェントから要求されたリソースの詳細が表示されます。[RMON Summary] ビューに表示されるリソース要求は、Packet Capture 要求および Host TopN 要求です。

RMON に関する概要情報を表示するには

1 ノード内で、[Services] の [RMON] をクリックします。

2 [View] > [RMON Summary] の順にクリックします。

次の表は、[RMON Summary] ビューに表示される静的情報について説明しています。

統計	説明
Agent Name	選択したセグメントを監視する RMON エージェントの名前
IP Address	RMON エージェントがインストールされているノードの IP アドレス
IPX™ Address	RMON エージェントがインストールされているノードの IPX (Internetwork Packet Exchange™) アドレス
Number of Interfaces	RMON エージェントがインストールされている管理サーバの論理インタフェースの数
Version	RMON Plus エージェントのバージョン番号
Type of RMON Service	RMON エージェントのタイプ :RMON、RMON Plus、または RMON2
Status of the Agent	RMON エージェントのステータス

[RMON Summary] ビューには、次の表で説明するリソース情報が表示されます。

統計	説明
Resource Name	要求したリソースの種類。次のいずれかになります。 ◆ Packet Capture ◆ Host TopN
Owner	行のコントロールインデックスに対応する所有者の名前
Index	Packet Capture リソースのチャネル、フィルタ、またはバッファコントロールインデックスおよび Host TopN リソースのコントロールインデックス

リソースを削除するには

1 Resource テーブルから行を選択します。

2 [Delete] をクリックします。

リソースを削除すると、選択した行に対応するエージェントのエントリが削除されます。

役割ベースのトラフィック分析タスク

Novell ZENworks Server Management を使用すると、役割に基づいて、次のトラフィック監視タスクを実行できます。

- ダウンしていないかどうかを監視するノードを追加する。

  詳細については 1015 ページの「停止していないかどうかノードを監視する」を参照してください。

- プロトコルディレクトリツリーにプロトコルを追加する。

  詳細については 1029 ページの「ネットワークで使用されているプロトコルのリストの表示」を参照してください。

- パケットをキャプチャする。

  詳細については 1017 ページの「パケットのキャプチャ」を参照してください。

- ノードがダウンしていないかどうかを監視することをやめる。

  詳細については 1015 ページの「停止していないかどうかノードを監視する」を参照してください。

- プロトコルディレクトリツリーからプロトコルを削除する。

  詳細については 1029 ページの「ネットワークで使用されているプロトコルのリストの表示」を参照してください。

- エージェントリソースを解放する。

  詳細については 992 ページの「RMON に関する概要情報の表示」を参照してください。

- セグメントアラームを設定する。

  詳細については、1041 ページの「[Set Alarm] ダイアログボックスでのアラームオプションの設定」を参照してください。

- 通信状況を表示する。

詳細については 1014 ページの「ノード間の通信状況（トラフィック）の表示」を参照してください。

- Traffic Analysis Agent を表示する。

  詳細については 998 ページの「優先 RMON エージェントの選択」を参照してください。

- プロトコルディレクトリを表示する。

  詳細については 1031 ページの「セグメントのプロトコルの配布状況を調べる」を参照してください。

- RMON に関する概要を表示する。

  詳細については 992 ページの「RMON に関する概要情報の表示」を参照してください。

- セグメントアラームを表示する。

  詳細については 1008 ページの「セグメントのアラーム統計の表示」を参照してください。

- セグメントダッシュボードを表示する。

  詳細については 1003 ページの「個々のセグメントのアプリケーションの決定」を参照してください。

- ダウンしていないかどうかを監視しているセグメントを表示する。

  詳細については 1015 ページの「停止していないかどうかノードを監視する」を参照してください。

- セグメントプロトコル配布を表示する。

  詳細については 1031 ページの「セグメントのプロトコルの配布状況を調べる」を参照してください。

- セグメントステーションを表示する。

  詳細については 1001 ページの「セグメントに関する統計のリストの表示」を参照してください。

- セグメントの概要を表示する。

  詳細については 1008 ページの「セグメントに関する概要情報の表示」を参照してください。

- セグメントのトレンドを表示する。

  詳細については 1001 ページの「セグメントのトラフィックの分析」を参照してください。

- スイッチまたはポートのトラフィックを表示する。

  詳細については 1032 ページの「スイッチのポートに関する統計の表示」を参照してください。

- スイッチの概要を表示する。

  詳細については 1033 ページの「スイッチに関する概要情報の表示」を参照してください。

役割ベースのサービスに関する詳細については、795 ページの「役割ベース管理」を参照してください。

Novell ZENworks Server Management によってサポートされているプロトコルデコードスイート

Novell ZENworks Server Management では、複数のプロトコルスイートをデコードできます。Novell ZENworks Server Management を使用すると、次のプロトコルスイートで発生する問題の分析およびトラブルシューティングを行えます。

- Novell NetWare プロトコルスイート
- NetWork File System プロトコルスイート
- Systems Network Architecture プロトコルスイート
- AppleTalk* プロトコルスイート
- TCP/IP プロトコルスイート

パケットキャプチャを設定し、[Trace Display] ウィンドウの結果内容を解釈するには、これらのプロトコルについて理解する必要があります。これらのプロトコルスイートおよびデコードのサポートに関する詳細については、1091 ページの付録 30、「Novell ZENworks Server Management でサポートされるプロトコルデコードスイート」を参照してください。

Novell ZENworks Server Management では、次のメディアで発生した問題の分析およびトラブルシューティングを行うこともできます。

- 標準的な Ethernet
- IEEE 802.3
- トークンリング
- FDDI

セグメント監視の計画

ネットワークの通常のアクティビティを基準として定義できます。セグメントのアクティビティの基準ドキュメントを用意しておくと、アクティビティの異常を見つけることができます。異常なアクティビティは、障害またはネットワークトラフィックの増加によって引き起こされます。基準となるアクティビティを作成するには、ネットワークが通常どおり機能しているときに統計情報を収集する必要があります。

次の節では、基準の作成および使用について説明します。

- 995 ページの「通常のセグメントアクティビティ基準の作成」
- 996 ページの「基準ドキュメントの使用」
- 997 ページの「セグメント基準ドキュメントに関するヒント」

通常のセグメントアクティビティ基準の作成

帯域幅の使用率などのセグメントに関する統計を取得するには、一定期間の情報をプロットしたトレンドグラフを作成してください。統計サンプルのデータ収集期間が短い場合は、正確な統計値が得られないことがあります。1 つまたは複数のネットワークコンポーネントを追加した場合は、将来のアクティビティを比較する他の基準を作成すると便利です。

Novell ZENworks Server Management で収集したデータは、スプレッドシートなどのプログラムにエクスポートし、詳細に分析したり、長期間保持したりできます。

基準ドキュメントの使用

基準ドキュメントは次の目的に使用できます。

- 996 ページの「基準ドキュメントを使用してアラームしきい値を適切に設定する」
- 996 ページの「基準ドキュメントを使用してネットワークトラフィックの増加とパフォーマンスへの影響を追跡する」
- 996 ページの「基準ドキュメントを使用して異常なセグメントアクティビティのトラブルシューティングを行う」

基準ドキュメントを使用してアラームしきい値を適切に設定する

Novell ZENworks Server Management では、ネットワーク監視エージェントソフトウェアによって監視されているセグメントに関する統計に対してアラームしきい値を設定できます。アラームしきい値を超えると、Novell ConsoleOne に通知されます。セグメントに関する統計に対してアラームしきい値を設定すると、問題が発生していないかどうかセグメントを頻繁に監視する必要がなくなります。

Novell ZENworks Server Management には、Ethernet、FDDI、およびトークンリングセグメントに対するさまざまなアラームしきい値のデフォルト値が用意されています。Novell ZENworks Server Management で追跡できるアラーム統計のリストについては、1041 ページの「[Set Alarm] ダイアログボックスでのアラームオプションの設定」の表を参照してください。セグメントのアクティビティの基準を作成することによって、デフォルト値がネットワークのセグメントに対して適切かどうかを判断できます。たとえば、セグメントの使用率を追跡した後で、通常よりも 5% ～ 10% 高い帯域幅使用率のアラームしきい値を設定します。このセグメントの使用率が通常よりも大きくなると、ユーザに通知されます。

重要： このアラーム通知機能を使用する場合は、セグメントアラームを有効にする必要があります。

基準ドキュメントを使用してネットワークトラフィックの増加とパフォーマンスへの影響を追跡する

現在のネットワークパフォーマンスを、基準ドキュメントに記録されたパフォーマンスと比較することにより、ネットワークの変化によってパフォーマンスがどのように影響を受けているのかを調べることができます。この比較によって、ネットワークトラフィックの増加を予測し、ネットワークのアップグレードや拡張を計画することもできます。また、Ethernet、FDDI、およびトークンリングのさまざまな統計に関するリアルタイムのトレンドグラフを表示できます。RMON2 エージェントがセグメントにインストールされている場合は、これらの統計の過去のトレンドを時間、日、週、月、および年単位で表示することもできます。セグメントパフォーマンスのトレンドの表示方法については、1004 ページの「セグメントに関するトレンドデータの分析」を参照してください。表示できるセグメントパフォーマンスのトレンドに関する統計のリストについては、1034 ページの「セグメント上のステーションを表示するオプションの選択」を参照してください。

基準ドキュメントを使用して異常なセグメントアクティビティのトラブルシューティングを行う

通常のネットワークアクティビティがわかっていると、異常なアクティビティを認識し、問題の原因を特定できます。

セグメント基準ドキュメントに関するヒント

各ネットワーク基準ドキュメントには、次の重要な情報を記載する必要があります。

- 997 ページの「帯域幅使用率」
- 997 ページの「パケット / 秒」
- 997 ページの「ネットワークエラーレート」
- 997 ページの「キロバイト / 秒」
- 998 ページの「セグメントの上位アクティブノード」

帯域幅使用率

帯域幅使用率の統計は、使用されているネットワーク帯域幅の割合を示します。帯域幅使用率は、特定の時間（たとえば、ユーザがネットワークにログインする朝など）、特定の週、または特定の月に高くなることがよくあります。帯域幅使用率を追跡すると、ネットワークセグメント、サーバ、およびルータの間でトラフィックの負荷を分散し、ネットワークをより効率的に運用できます。また、ネットワークトラフィックの増加がパフォーマンスに与える影響を調べることもできます。通常、新しいワークステーションやアプリケーションがネットワークに追加されると、帯域幅使用率は増加します。

パケット / 秒

ネットワーク回線上のパケットの数を監視すると、セグメントのトラフィックに関する情報を取得できます。ユーザが新しいアプリケーションを起動した後に、1 秒あたりのパケットの数の変化を確認することにより、アプリケーションを使用すると考えられるすべてのユーザがアプリケーションを使用したときの 1 秒あたりのパケット数の増加量を計算できます。1 秒あたりのパケット数は、帯域幅使用率とは異なります。帯域幅使用率はセグメント上の 1 秒あたりのキロバイト数に基づきますが、パケットのサイズはさまざまです。したがって、パケットのサイズまたは数が増加すると、帯域幅使用率も増加します。パケットの数が増加しても帯域幅使用率が増加しない場合は、パケットのサイズが小さいため、パケットの数が増加しても帯域幅使用率に影響を与えないことが考えられます。

ネットワークエラーレート

基準にエラーレートを含めることにより、いつネットワークのエラーレートが異常になったのかを調べることができます。ネットワークエラーレートを調べることは、ネットワークエラーによってネットワークがダウンすることがあるため重要です。エラーレートが高いと、ハードウェア障害が発生したり、ネットワークトラフィックが増加したりすることがあります。エラーが増加し帯域幅使用率が増加しない場合は、ネットワークボードやトランシーバの故障など、コンポーネントに問題がある場合があります。

キロバイト / 秒

1 秒あたりのキロバイト数を追跡すると、ネットワークのスループットを測定できます。この情報から、使用中の有効な帯域幅合計の割合を調べることができます。Ethernet ネットワークの最大有効帯域幅は 10Mbps です。トークンリングネットワークの最大有効帯域幅は、4Mbps または 16Mbps（ハードウェアに依存）です。

セグメントの上位アクティブノード

ネットワークの上位 3 つのサーバを追跡することにより、新しいユーザやアプリケーションを追加したときに、サーバ間で負荷を分散できます。監視対象のセグメントにある上位ノードのリストの表示方法については、1010 ページの「上位 20 のノード統計の表示」を参照してください。また、Request Being Processed パケットの数も監視します。これらのパケットの数が連続して増加する場合は、サーバの負荷が大きすぎることを示します。これらのパケットは、キャプチャおよびデコードすることによって監視できます。パケットのキャプチャ方法およびデコードされたパケットの表示方法については、1017 ページの「パケットのキャプチャ」および1021 ページの「キャプチャされたパケットの表示」を参照してください。

[Segment Trends] ビューでは、さまざまなセグメントの統計を表示し、他のアプリケーション (スプレッドシートなど) にそのデータをエクスポートして後で分析することができます。データは、表示するトレンドの統計値を保管するテキストファイルとして保存されます。トレンドデータをファイルにエクスポートするには、[Segment Trends] ビューのツールバーにある [Export] ボタンをクリックします。詳細については、1004 ページの「セグメントに関するトレンドデータの分析」を参照してください。

セグメントの現在の使用率は、[Segment Dashboard] ビューに表示されます。このビューにアクセスするには、[View] > [Segment Dashboard] の順にクリックします。詳細については、1003 ページの「個々のセグメントのアプリケーションの決定」を参照してください。

ネットワークトラフィックの分析の準備

Novell ZENworks Server Management ソフトウェアのコンポーネントには、NetWare 版 Traffic Analysis Agent と Windows 版 Traffic Analysis Agent が含まれています。ネットワーク監視エージェントは、管理サーバか、独立した NetWare または Windows サーバにインストールできます。エージェントは、接続されたセグメントのトラフィックを監視し、セグメントのノードやデバイスに関する情報を収集し、これらの情報を管理サーバに提供します。管理サーバは、これらの情報を Novell ConsoleOne に提供します。また、エージェントはトラップを管理サーバに送信し、このトラップは Novell ConsoleOne に転送されます。管理サーバと監視エージェントは、SNMP を使用して通信します。Novell ZENworks Server Management には、SNMP パラメータのデフォルト値が用意されています。

次の節では、セグメントのトラフィックを監視する優先エージェントの指定や、デフォルトの SNMP 設定の変更について説明します。

- 998 ページの「優先 RMON エージェントの選択」
- 999 ページの「SNMP パラメータの設定」

優先 RMON エージェントの選択

選択したセグメントに複数のリモート監視 (RMON) エージェントが存在する場合は、[RMON Agent] プロパティページからセグメントのノードを監視するエージェントを選択できます。このページには、RMON エージェントがインストールされているサーバのリストが表示されます。このリストから選択したエージェントが優先エージェントになります。優先エージェントは、セグメントを監視し、セグメントアクティビティを Novell ConsoleOne に送信するプライマリエージェントです。

[RMON Agent] プロパティページを表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [File] > [Properties] > [RMON Agent] タブの順にクリックします。

次の表は、[RMON Agent] プロパティページに表示される統計について説明しています。

統計	説明
Preferred	選択したサーバが優先 RMON エージェントサーバとして選択されている場合はチェックマークが表示されます。
Agent Name	RMON エージェントがインストールされているすべてのサーバのリストが表示されます。
Version	サーバにインストールされている RMON エージェントのバージョンが表示されます。 このバージョンは動的に取得されます。Novell ZENworks Server Management がリモートエージェントに接続できない場合、または選択したセグメントにサードパーティのエージェントがインストールされている場合、このフィールドは空白です。
Status	セグメントの RMON エージェントのステータスが表示されます。
MAC Address	ノードの物理 MAC (Media Access Control) アドレスが表示されます。
Interface Index	ネットワークボードを介してノードが接続できるセグメントと各インタフェースを対応付けるインタフェースインデックスの数が表示されます。
Available RMON Services	選択したエージェントから利用できる、RMON、RMON Plus、RMON2 などの RMON サービスのリストが表示されます。

RMON エージェントを優先エージェントとして選択するには

1 プロパティページに表示された名前のリストからサーバ名またはワークステーション名を選択します。

表示されるサーバ名およびワークステーション名は、RMON エージェントがインストールされたサーバおよびワークステーションの名前です。

2 [Apply] をクリックします。

SNMP パラメータの設定

動的情報を Novell ConsoleOne に表示するように要求した場合、ConsoleOne は管理サーバから情報を探します。管理サーバは、SNMP を使用してネットワーク監視エージェントと通信し、エージェントから必要な情報を取得し、Novell ConsoleOne に提供します。サーバとエージェント間の SNMP 通信は、Novell ZENworks Server Management によって提供されたデフォルトの SNMP 設定に基づきます。デフォルトの SNMP 設定は、[SNMP] ダイアログボックスを使用して変更できます。このダイアログボックスは、管理サーバが監視エージェントと通信中にエラーが発生した場合に Novell ConsoleOne に表示されます。

[SNMP] ダイアログボックスでは、コミュニティ文字列や SNMP 通信のセキュリティ設定を指定できます。また、サーバがエージェントと接続する場合のデフォルトのタイムアウト値を変更できます。サーバがエージェントと接続する前にデフォルトのタイムアウト値が経過した場合、またはサーバのコミュニティ文字列がエージェントのものと一致しない場合は、現在の設定で [SNMP] ダイアログボックスが Novell ConsoleOne に表示されます。このダイアログボックスでは、現在のタイムアウト値、コミュニティ文字列、および他の SNMP パラメータを変更できます。変更した値は、Novell ZENworks Server Management データベースに保存され、それ以降のすべてのトラフィック管理セッションに適用されます。

ネットワークのすべての監視エージェントに対する SNMP 設定を変更するには

1 Novell ConsoleOne で、Novell ZENworks Server Management ドメインを右クリックし、[Global SNMP Parameters] をクリックします。

特定のエージェントに対する SNMP 設定を変更するには

1 Novell ConsoleOne で、エージェントがインストールされたノードを右クリックし、[Properties] > [SNMP Settings] の順にクリックします。

次の表は、[SNMP Settings] プロパティページに表示される SNMP パラメータについて説明しています。

パラメータ	説明
Community String	エージェントから動的データを要求するノードのコミュニティ文字列
Timeout	エージェントからの応答を受け取るまでサーバが待機する必要がある最長時間
Retry	サーバがエージェントへの接続を試行する必要がある回数
Secure Set	管理サーバから監視エージェントに送信されるパケットを暗号化します。
Secure Get	監視エージェントから管理サーバに送信されるパケットを暗号化します。

ヒント： ネットワーク監視エージェントが NetWare 4.*x* で実行されていて、ネットワークが IPX に対応している場合は、IPX を使用しているエージェントと通信するために [SNMP] ダイアログボックスを使用します。この結果、Novell ZENworks Server Management トラフィック分析コンポーネントのパフォーマンスが大幅に向上します。

ネットワークトラフィックの分析

Novell ZENworks Server Management を使用すると、ネットワークを監視し、リアルタイムの統計の概要などの情報を収集して、ネットワークのパフォーマンスを調べたり、詳しいリアルタイムの統計を収集して、ネットワークのセグメントのパフォーマンスを調べたりできます。

表、ダイヤル、およびグラフを含むビューに、ネットワークのノードやセグメントのアクティビティに関する情報が表示されます。この情報を使用すると、通常のトラフィック負荷を特定し、ネットワーク障害を制御するためのネットワークに関する基準の確立などのさまざまなトラフィック管理タスクを実行したり、ネットワークセグメント、サーバ、およびルータの間でトラフィック負荷を分散するためにリアルタイムのパフォーマンスを分析したりできます。また、ノード情報を収集し、問題の原因と思われる特定のエンティティを重視することもできます。

次の節では、Novell ZENworks Server Management を使用してネットワーク監視アクティビティを管理する方法について詳しく説明します。

- 1001 ページの「セグメントのトラフィックの分析」
- 1010 ページの「セグメントに接続されたノードのトラフィックの分析」
- 1017 ページの「パケットのキャプチャ」
- 1021 ページの「キャプチャされたパケットの表示」
- 1028 ページの「ネットワークのプロトコルによって生成されたトラフィックの分析」
- 1032 ページの「スイッチ上のトラフィックの分析」

セグメントのトラフィックの分析

ネットワークのセグメントを監視すると、ネットワーク運用の費用対効果が大きくなり、安定的かつ円滑にネットワークを運用できます。取得する情報の種類に応じて、ネットワークのセグメントを監視するエージェントを選択できます。詳細については、985 ページの「ネットワーク監視エージェントについて」を参照してください。セグメントを監視するエージェントは、トラフィックデータを収集し、ユーザが必要なときにリアルタイムまたは過去の情報を提供します。

Novell ZENworks Server Management には、監視対象セグメントに関する統計情報を取得するために使用できるさまざまなビューが用意されています。ネットワークのすべてのセグメントに関する統計情報を表示するか、または個々のセグメントに関する統計情報を表示するかを選択できます。セグメントパフォーマンスのトレンドおよびセグメントに対して生成されたアラームのリストを表示できます。[Segment Summary] ビューには、セグメントパフォーマンスの概要が表示されます。

次の節では、ネットワークのセグメントのパフォーマンスを分析する方法について説明します。

- 1001 ページの「セグメントに関する統計のリストの表示」
- 1003 ページの「個々のセグメントのアプリケーションの決定」
- 1004 ページの「セグメントに関するトレンドデータの分析」
- 1008 ページの「セグメントのアラーム統計の表示」
- 1008 ページの「セグメントに関する概要情報の表示」

ヒント： リモート監視 (RMON) エージェントが実行されているサーバは、監視対象として選択したノードが停止したときにユーザに通知します。詳細については、1015 ページの「停止していないかどうかノードを監視する」を参照してください。保守のために RMON エージェントをネットワークから切り離す必要がある場合があります。セグメントを引き続き監視するには、セグメント上の別の RMON エージェントを選択します。詳細については、998 ページの「優先 RMON エージェントの選択」を参照してください。

セグメントに関する統計のリストの表示

[List Segments] ビューには、セグメントのリストと、ネットワークの各セグメントに関する統計情報が表示されます。統計は、ビューの表の列に表示されます。ビューには、Novell ConsoleOne で選択したオブジェクトまたはノードに関連付けられたセグメントのリストが表示されます。

Novell ZENworks Server Management を使用して個々のセグメントのノードに関する情報を取得する方法については、1010 ページの「セグメントに接続されたノードのトラフィックの分析」を参照してください。

すべてのセグメントの統計情報を参照するには

1 Novell ConsoleOne で、領域またはノードを選択します。

2 [View] > [List Segments] の順にクリックします。

領域を選択すると、[List Segments] ビューに、その領域内で見つかったすべてのセグメントに関する統計が表示されます。ノードを選択すると、そのノードに接続されたすべてのセグメントに関する統計が表示されます。

次の表は、表示される各セグメントに関する統計について説明しています。セグメントに関する統計のサンプル更新間隔は 15 秒です。

ヒント： セグメントの統計は、セグメントが NetWare 版 Traffic Analysis Agent または Windows 版 Traffic Analysis Agent によって監視された場合にのみ、[List Segments] ビューに表示されます。

統計	説明
セグメント名	セグメント名またはアドレス
Type	Ethernet、FDDI、トークンリング、PPP、未定義など、物理セグメントタイプ。未定義は、物理セグメントタイプがリストにないセグメントを示します。
Speed (Mbps)	セグメントの速度。この速度は、RMON エージェントをセグメントに接続するネットワークボードの速度や、セグメントのケーブルタイプなどの要因によって決まります。この列の値は、少なくとも 1 つの RMON エージェントがネットワーク上の少なくとも 1 つのサーバに接続されている場合にのみ表示されます。
Utilization%	セグメントのすべてのトラフィックで現在使用されている帯域幅の平均割合
Packets/s	セグメント上で現在伝送されている 1 秒あたりの平均パケット数
KBytes/s	セグメント上で現在伝送されている 1 秒あたりの平均キロバイト数
Errors/s	セグメントで現在発生している 1 秒あたりの平均エラー数
Message	セグメントの RMON エージェントのステータス詳細については、998 ページの「優先 RMON エージェントの選択」を参照してください。

Novell ZENworks Server Management はセグメントのポーリングを実行するため、[Messages] 列のメッセージはそれぞれ異なります。これらのメッセージは、セグメントの優先 RMON エージェントのステータスを示します。

優先 RMON エージェントは、セグメントに関する情報を Novell ConsoleOne に送信するために選択したノードです。この選択は、[RMON Agent] プロパティページから行えます。詳細については、998 ページの「優先 RMON エージェントの選択」を参照してください。

フィールドの表示、列の書式設定、項目のソートおよびグループ化、テキストフィールドのフォントの変更、またはテーブルビューへのグリッドラインの表示を行うためにビューを変更するには、[View] > [Settings] をクリックし、必要なオプションを選択します。詳細については、23 章 829 ページの「ネットワーク検出とアトラス管理の理解」を参照してください。

個々のセグメントのアプリケーションの決定

Novell ZENworks Server Management は、ネットワークの監視対象セグメントに関するリアルタイムの統計情報を提供します。この情報は、[Segment Dashboard] ビューに表示されます。セグメントのトラブルシューティングを行う場合は、このビューに表示される情報が役に立ちます。

[Segment Dashboard] ビューには、監視対象セグメントに関するリアルタイムの統計を示す 4 つのゲージが表示されます。ビューの下部には、ドロップダウンリストから選択した値に基づき、上位 8 つのノードのバーグラフが表示されます。デフォルトでは、1 秒あたりの送信パケット数が示されます。監視対象セグメントの上位アクティブノードのリストを表示する方法については、1010 ページの「上位 20 のノード統計の表示」を参照してください。

異なる統計に基づいた上位 8 つのノードを表示するには、[Segment Dashboard] ビューを設定します。また、上位ノードのグラフを表示するかまたは無効にするかを選択できます。詳細については、1034 ページの「セグメント上のステーションを表示するオプションの選択」を参照してください。

セグメントアラームに対して、[Segment Dashboard] ビューに表示される 1 秒あたりのパケット数、1 秒あたりのブロードキャスト数、および使用率の統計に関するアラームしきい値を設定できます。詳細については、1003 ページの「[Segment Dashboard] ビューに表示される統計に対するアラームしきい値の定義」を参照してください。

個々のセグメントの統計情報を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [View] > [Segment Dashboard] の順にクリックします。

[Segment Dashboard] ビューに、監視対象セグメントに関するリアルタイムの統計を示す 4 つのゲージが表示されます。ピーク値は、グラフの各バー上の線によって示されます。次の表は、[Segment Dashboard] ビューに表示される統計について説明しています。

統計	説明
Packets/s	セグメントで現在伝送されている 1 秒あたりのパケット数
Utilization%	セグメント上のパケットトラフィックによって現在使用されている最大ネットワーク容量の割合
Error/s	セグメントで現在伝送されている 1 秒あたりのエラーパケット数
Broadcasts/s	セグメントで現在伝送されている 1 秒あたりのブロードキャストパケット数（ブロードキャストパケットはセグメント上のすべてのアドレスに送信されます）

統計は 5 秒ごとに更新されます。各統計の数値は、ゲージに表示されます。

[Segment Dashboard] ビューに表示される統計に対するアラームしきい値の定義

[Segment Dashboard] ビューに表示される統計に対してアラームしきい値を設定するには

1 ゲージの回りの黒い輪をクリックします。

2 輪をドラッグしてデフォルト値を増減します。

輪をドラッグすると、輪の色が赤に変わります。

3 統計のしきい値として設定する値でマウスのボタンを離します。

輪の色は、選択したしきい値になるまで赤で表示されます。

監視対象セグメントに関する統計がしきい値を超えると、RMON エージェントが管理サーバにトラップを送信し、このトラップは Novell ConsoleOne に転送され、アラームが生成されます。

監視対象セグメント上にある上位ノードのグラフの表示

[Segment Dashboard] ビューの下部には、監視対象セグメントにある上位 8 つのノードのバーグラフが表示されます。グラフの基になるデフォルト統計は、1 秒あたりの送信パケット数で表示されます。グラフの基になる統計は変更できます。詳細については、1039 ページの「上位ノードグラフが表示される基になる統計の選択」を参照してください。また、上位ノードのグラフを表示するかまたは無効にするかを選択できます。詳細については、1039 ページの「上位ノードグラフを表示するオプションの選択」を参照してください。

グラフの統計は 5 秒ごとに更新されます。グラフは 60 秒ごとに再ソートされ、新しい上位ノードが表示されます。この時点で、新しいノードを追加し、既存のノードをリストから削除できます。

セグメントに関するトレンドデータの分析

Novell ZENworks Server Management では、監視対象セグメントのトラフィックパターンのトレンドを調べることができます。[Segment Trends] ビューからセグメントパフォーマンスのトレンドを表示できます。トレンド情報を使用して、セグメントに関する通常のアクティビティの基準を作成できます。基準を作成すると、セグメントアラームに適切なしきい値を設定し、保守アクティビティやバックアップを計画できます。また、セグメントで問題が発生した場合は、通常のトラフィックレベルを異常なトラフィックレベルと比較することによって、問題の原因を特定できます。詳細については、995 ページの「通常のセグメントアクティビティ基準の作成」を参照してください。

トレンドデータの分析については、次のトピックを参照してください。

- 1004 ページの「トレンドの表示の理解」
- 1005 ページの「トレンド統計の表示」

トレンドの表示の理解

セグメントのトレンドデータは、選択したセグメントを監視する RMON エージェントの種類や設定に応じて表示されます。

- RMON Plus がセグメントの優先 RMON エージェントである場合は、過去 1 時間の間 30 秒ごとに収集された現在のトレンドを表示したり、過去に表示されたトレンドを時間、日、週、月、および年単位で表示したりできます。

  重要： RMON エージェントがセグメントの複数のノードにインストールされている場合は、[RMON Agent] プロパティページでセグメントに関する情報を Novell ConsoleOne に送信するノードとして選択したノードが優先 RMON エージェントサーバになります。詳細については、998 ページの「優先 RMON エージェントの選択」を参照してください。

- RMON Plus がセグメントの優先 RMON エージェントとして選択されていない場合は、選択したセグメントの現在のトレンドのみを表示できます。現在のトレンドは、過去 1 時間の間 30 秒ごとに収集されたトレンドです。過去のトレンドを表示するには、RMON Plus エージェントを優先 RMON エージェントとして選択します。
- 優先RMONエージェントがNetWare版Traffic Analysis Agentバージョン1.30よりも前のバージョンである場合は、過去 1 時間の間収集された現在のトレンドと過去 1 日のトレンドを表示できます。
- リアルタイムのトレンドは、メモリの使用量が大きい場合、または RMON エージェントの設定が認められない場合は表示されません。
- RMON エージェントがダウン、または問題が発生している場合は、監視対象セグメントのトレンドが、分断されたグラフとして表示されます。
- 優先RMONエージェントがNovell Traffic Analysis Agent（バージョン1.30以降）またはリモートネットワーク監視用 MIB（RFC 1513）に対するトークンリング拡張機能を実装するサードパーティのエージェントである場合、セグメントの帯域幅使用率のグラフには、トークンリング［Segment］ビューのトレンドの実際の使用率よりも少し小さい値が表示されます。これは、MAC 層の統計が使用率の計算で考慮されないからです。

トレンド統計の表示

セグメントのトレンド統計を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 ［View］>［Segment Trends］の順にクリックします。

Ethernet、FDDI、およびトークンリングのセグメントに関するトレンドグラフが表示されます。デフォルトの統計は次のとおりです。これらの統計に基づいて 3 つの種類のセグメントに関するグラフが表示されます。

セグメントタイプ	デフォルト統計
Ethernet	パケット合計数、正常なパケット数、エラーパケット数
FDDI	パケット合計数
トークンリング	パケット合計数

ツールバーオプションを使用して、表示するトレンドの時間範囲を変更したり、表示するグラフの基となる統計を選択したり、データをファイルにエクスポートしたりできます。

次の表は、ツールバーオプションについて詳しく説明しています。

オプション		説明
Profile		[Profile] ダイアログボックスを表示します。[Profile] ダイアログボックスでは、デフォルトのプロファイルを選択できます。デフォルトのプロファイルによって、監視対象セグメントに関するパケット合計数、正常なパケット数、およびエラーパケット数の統計情報と共にトレンドが表示されます。 [Select Profile] リストに表示されたプロファイルを使用しないことを選択する場合は、[Select Statistics] リストから必要な統計を選択できます。選択した統計に基づいたセグメントのトレンドを表示する場合は、選択した統計を保存できます。デフォルトのプロファイルは、次回 [Segment Trends] ビューを表示したときに有効になります。
Legend		グラフの各色が何を表すのかを表示します。Legend のサイズは変更できます。
Stack		複数のトレンドを 1 つのグラフに重ねて表示します。このグラフは、縦軸が 1 つであり、選択したすべての統計を表します。
Unstack		トレンドを重ねないで表示し、統計ごとに別々の座標系としてグラフを表示します。
Horizontal Grid		[Segment Trend] ビューのグラフ領域に水平グリッド線を表示します。
Vertical Grid		[Segment Trends] ビューのグラフ領域に垂直グリッド線を表示します。
サイズの調整		ビューのグラフ領域にトレンドが完全に表示されるようにグラフを最大化または最小化します。
Export		[Segment Trends] ビューの情報をファイルにコピーします。ファイルには、トレンドで表示された統計値が保管されます。データを保存して後で分析できます。

オプション		説明
[Time Scale] ドロップダウンリスト		◆ [Real Time]：現在のトレンドグラフを表示します。このグラフのデフォルトのサンプル時間は 1 分ごとです。このグラフはリアルタイムで更新されます。 ◆ [One Hour]：選択したトレンドの過去 1 時間のグラフを表示します。 ◆ [One Day]：選択したトレンドの過去 1 日のグラフを表示します。 ◆ [One Week]：選択したトレンドの過去 1 週間のグラフを表示します。 ◆ [One Month]：選択したトレンドの過去 1ヶ月間のグラフを表示します。 ◆ [One Year]：選択したトレンドの過去 1 年間のグラフを表示します。 時間、週、月、および年単位の過去のトレンドは、NetWare 版 Traffic Analysis Agent バージョン 1.1 以降がセグメントの Traffic Analysis Agent サーバにインストールされている場合にのみ利用可能です。

[Segment Trends] ビューの [File] メニューから、現在のトレンドの統計情報を印刷したり、トレンドの統計情報をファイルにエクスポートしたり、データをテキスト形式で保存したりできます。また、後でスプレッドシートにファイルをインポートして分析できます。

以前または以降のトレンドを表示し、グラフのサイズを変更するには、次の表で示された、[Segment Trends] ビューのグラフ領域で利用可能なオプションを使用してください。

オプション		説明
Scale Up		クリックすると、グラフの Y 軸が 50 パーセント拡大します。
Scale Down		クリックすると、グラフの Y 軸が 50 パーセント縮小します。
Previous		選択したプロファイルまたは統計に基づいて以前のグラフを表示します。 過去のトレンドが表示された場合にのみ有効になります。
Next		以降のグラフを表示します。 過去のトレンドが表示された場合にのみ有効になります。

セグメントのアラーム統計の表示

Novell ZENworks Server Management は、セグメントのアラーム統計を追跡します。アラームは、セグメントに関する統計のしきい値を超えたときに生成されます。監視対象セグメントのすべてのアラームのリストは、[Segment Alarms] プロパティページに表示されます。

セグメントに関するアラーム統計を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [File] > [Properties] > [Segment Alarms] タブの順にクリックします。

Novell ZENworks Server Management には、さまざまなセグメントアラームのデフォルトしきい値が用意されています。監視対象セグメントのデフォルト値は有効または無効にすることができます。デフォルト値を使用しない場合は、[Set Alarm] ダイアログボックスでしきい値を設定します。セグメントアラームの設定方法に関する詳細については、1041 ページの「[Set Alarm] ダイアログボックスでのアラームオプションの設定」を参照してください。

セグメントに RMON エージェントが接続されていない場合は、エラーメッセージが表示されます。

セグメントに関する概要情報の表示

[Segment Summary] ビューには、ネットワークの監視対象セグメントに関する簡単な情報が表示されます。監視対象セグメントに関する静的情報、セグメントが監視対象であるかどうかについての情報、およびセグメントに対して生成されたアラームに関する情報が表示されます。監視対象セグメントのノードによるネットワーク容量の使用率、セグメントのノードによって伝送されたパケットに基づくトレンド、およびセグメント上のプロトコルの配布状況を簡単に確認できます。

セグメントの概要情報を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [View] > [Segment Summary] の順にクリックします。

次の表は、[Segment Summary] ビューに表示される静的情報について説明しています。

統計	説明
Name	セグメントの名前
Type	セグメントのメディアタイプ：イーサネット、FDDI、またはトークンリング
IP Address	セグメントの IP アドレス
IPX アドレス	セグメントの IPX アドレス
Primary Agent	セグメントのノードおよびトラフィックを監視する優先エージェントの名前
Agent Status	セグメントのノードおよびトラフィックを監視する優先エージェントのステータス
Nodes	セグメントのノードの数
IP Nodes	セグメントで IP アドレスが割り当てられているノードの数

統計	説明
IPX Nodes	セグメントで IPX アドレスが割り当てられているノードの数
Servers	セグメントの NetWare サーバの数
Workstations/Others	選択したセグメントに存在する、NetWare サーバ以外のノード数
Network Probes	選択したセグメントの監視エージェントの数
Switches	セグメントのスイッチの数
Routers	セグメントのノードおよびデバイスを接続するために使用するルータの数
Hubs	セグメントのハブの数

[Segment Summary] ビューには、次の表で説明するような、監視対象セグメントに対して生成されたアラームに関する情報が表示されます。

統計	説明
Severity	トラップに基づいた重要度レベル
From	アラームをアラーム管理システムに送信したデバイスのネットワークアドレス
Summary	イベントの概要。多くの場合、アラームによって影響を受けるオブジェクトの名前またはアドレスを含みます。
Owner	アラームによって影響を受けるセグメントまたはデバイス
Received Time	アラーム管理システムがアラームを受け取った日時
Type	アラームの一般的な説明（たとえば、ボリュームのディスク領域の不足など）
Category	トラップタイプオブジェクトを定義する MIB に基づいて、アラームのカテゴリを表示します。カテゴリは、管理サーバ MIB プールに含まれる MIB に直接関連します。たとえば、NetWare サーバのカテゴリは、NetWare Server Alarm MIB に基づきます。

[Segment Summary] ビューには、次の表で説明するような、監視対象セグメントに関する動的情報が表示されます。

統計	説明
Utilization%	セグメント上のパケットトラフィックによって使用されているネットワーク容量のリアルタイム値を示すダイヤルを表示します。
Packets	セグメントで伝送されているパケットに基づいたトレンドを表示します。RMON エージェントによって監視されているセグメントのリアルタイムのトレンドと、RMON Plus エージェントによって監視されているセグメントの日単位のトレンドを表示します。

統計	説明
Protocol Distribution	セグメントを監視するエージェントがデータを収集できるアプリケーション層プロトコルの配布状況を示す円グラフを表示します。各片はプロトコルスイートを表します。片をクリックすると、プロトコルの名前が表示されます。 選択したセグメントを監視するエージェントが RMON2 エージェントの場合に有効になります。

セグメントに接続されたノードのトラフィックの分析

Novell ZENworks Server Management には、ネットワークの監視対象セグメントに接続されたノードに関する情報を取得するために使用できるさまざまビューが用意されています。

次の節には、ネットワークのセグメントに接続されたノードのパフォーマンスを監視する場合に役に立つ情報が記載されています。

- 1010 ページの「上位 20 のノード統計の表示」
- 1011 ページの「FDDI セグメントのノードに関する統計の表示」
- 1012 ページの「トークンリングセグメントのノードに関する統計の表示」
- 1014 ページの「ノード間の通信状況（トラフィック）の表示」
- 1015 ページの「停止していないかどうかノードを監視する」

上位 20 のノード統計の表示

Novell ZENworks Server Management では、上位アクティブノードの統計を調べて、さまざまなパフォーマンス統計を取得できます。これは、特定の統計に基づいてトラフィックが最も大きいノードを見つける場合に役に立ちます。たとえば、ブロードキャストトラフィックが最も大きいノードを見つけることができます。

[Stations] ビューには、監視対象セグメントにあるすべてのノードのリストが表示されます。このビューでは、監視対象セグメントの上位 20 のノードを調べることができます。このビューには、1 秒あたりの送信パケット数を基準としてソートされた上位 20 のステーションのリストが表示されます。上位 20 のノードを表示する基になる異なる統計を選択できます。詳細については、1035 ページの「上位 20 のノードが表示される基になる統計の選択」を参照してください。上位ノードが 20 よりも少ない場合は、使用可能な数の上位ノードのみがリストに表示されます。

セグメントの上位 20 ノードの統計を表示するには

1. Novell ConsoleOne でセグメントを選択します。
2. [View] > [Stations] の順にクリックします。
3. [Stations] ビューで、[View] > [Show Top N Stations] の順にクリックします。

[Stations] ビューには、各ステーションの統計情報が示された列が表示されます。次の表は、[Stations] ビューに表示される統計について説明しています。

統計	説明
MAC Address	ノードの物理 MAC (Media Access Control) アドレス

統計	説明
ノード	ノードの名前（名前がデータベースにない場合はアドレス）
Util.%	ノードが送信したパケットによって使用される最大ネットワーク容量の割合
Packets/s In	ノードが受信した 1 秒あたりのパケット数
Packets/s Out	ノードが伝送した 1 秒あたりのパケット数
Bytes/s In	ノードが受信した 1 秒あたりのバイト数
Bytes/s Out	ノードが伝送した 1 秒あたりのバイト数
Errors/s	ノードが送信した 1 秒あたりのエラー数
Broadcasts/s	ノードが送信した 1 秒あたりのブロードキャストパケット数
Multicasts/s	ノードが送信した 1 秒あたりのマルチキャストパケット数（特定のノードグループに送信されたパケットの数）
Protocols	ノードが使用しているプロトコルの種類
First Transmit	Traffic Analysis Agent が起動されてからノードが初めてパケットを送信した日時
Last Transmit	Traffic Analysis Agent が起動されてからノードが最後にパケットを送信した日時

ステーションの統計は定期的に更新されます。テーブルは 60 秒ごとに再ソートされ、新しい上位ノードが表示されます。この時点で、新しいノードを追加し、既存のノードをリストから削除できます。

FDDI セグメントのノードに関する統計の表示

Novell ZENworks Server Management では、監視対象の FDDI リングセグメントのノードに関するデータを表示して、問題のトラブルシューティングを行うことができます。

[FDDI Ring Stations] ビューに、監視対象の FDDI リングセグメントにある個々のノードに関する統計が表示されます。このビューには、セグメントのノードのリストが表示され、リングの各ノードの順番と、アクティブモニタであるノードが示されます。

FDDI リングセグメントのノードの統計を表示するには

1 Novell ConsoleOne で、FDDI リングセグメントを選択します。

2 [View] > [FDDI Stations] の順にクリックします。

NetWare 版 Traffic Analysis Agent を最後に起動してから表示された各ノードに関する統計は累積され、次の表で説明されているように 10 秒ごとに更新されます。

統計	説明
Order	Traffic Analysis Agent からの、FDDI リングにあるノードの相対位置
Name	ノードの名前（名前がデータベースにない場合は、ノードの物理 (MAC) アドレス）

統計	説明
MAC Address	ノードの物理 (MAC) アドレス
Status	ノードのステータス： ◆ Onムノードは、リングのポーリングを頻繁に行っています。 ◆ Offムノードは、リングのポーリングを行っていません。
Duration	ノードのステータスが On または Off になってから経過した時間
UpStream Neighbor	論理リングでこのステーションのアップストリームにあるノードの MAC アドレス
DownStream Neighbor	論理リングでこのステーションのダウンストリームにあるノードの MAC アドレス
Last Entered Time	ノードが最後にリングに入った日時
Last Exit Time	ノードが最後にリングから出た日時
SMT Request Type	ノードが応答している SMT 要求。ノードが正常に要求に応答したかどうかを示します。失敗した場合は、理由を示す応答コードが表示されます。
SMT Response Type	SMT 要求を受信するノードによって生成された SMT 応答。ノードが応答できなかった場合は、理由を示す応答コードが表示されます。
Request Denied	ノードによって生成された要求拒否応答の累積数。要求拒否フレームは、応答するノードが要求元ノードの SMT バージョン番号をサポートしていない場合、セットが失敗した場合、またはノードからの帯域幅の同時割り当ての要求が拒否された場合に生成されます。
In CRC Error	このノードによって報告される CRC (Cyclic Redundancy Check) 回線エラーの合計数
Out CRC Error	このステーションのダウンストリームで最も近くにあるアクティブなノードによって報告され、プローブによって検出された CRC エラーの合計数
Lost Frames	ネットワーク上で受信した損失フレームエラーの合計数。損失フレームエラーは、フレームの終端デリミタがネットワークで失われたことを示します。
In Beacons	このステーションをアップストリームの近接したノードとして指定したプローブによって検出されたビーコンフレームの合計数
Out Beacons	このステーションによって送信され、プローブによって検出されたビーコンフレームの合計数
Insertions	このステーションがリングに挿入されたことをプローブが検出した回数

トークンリングセグメントのノードに関する統計の表示

[Token Ring Stations] ビューには、監視対象のトークンリングセグメントにある個々のノードに関する統計が表示されます。このビューには、セグメントのノードのリストが表示され、リングの各ノードの順番と、アクティブモニタであるノードが示されます。

トークンリングセグメントにあるノードの統計を表示するには

1 Novell ConsoleOne でトークンリングセグメントを選択します。

2 [View] > [Token Ring Stations] の順にクリックします。

ビューには、次の表で説明されるような統計情報が表示されます。RMON エージェントが起動されてからの統計が累積され、10 秒ごとに更新されます。

統計	説明
Order	RMON エージェントからの、トークンリングにあるノードの相対位置
Name	ノードの名前（名前がデータベースにない場合は、ノードの物理（MAC）アドレス）
MAC Address	ノードの物理（MAC）アドレス
Status	ノードのステータス： ◆ On␣ノードがリング上にあります。 ◆ Off␣ノードがリング上にありません。 ◆ On（Monitor）␣ノードはリング上にあり、アクティブモニタです。
Duration	このノードのステータスが On または Off である時間の長さ
Last Entered Time	ノードが最後にリングに入った日時
Last Exit Time	ノードが最後にリングから出た日時
Duplicate Address	他のノードが同じアドレスを使用していることをこのノードが検出したときに報告および生成される重複アドレスエラーの合計数
Soft Errors	このノードによって送信されたパケット内のソフトエラーの数
Inline Errors	このステーションによってリングエラーモニタに報告され、プローブによって検出されたエラー報告パケット内の回線エラーの合計数
Outline Errors	このステーションのダウンストリームで最も近くにあるアクティブなノードによって送信され、プローブによって検出されたエラー報告パケット内の回線エラーの合計数
Internal Errors	このノードが報告した内部エラーの数。一般的に、内部エラーは、ネットワークアダプタボードで発生した回復可能なエラーを示します。
In Burst Errors	リングエラーモニタに報告され、プローブによって検出されたバーストエラーの合計数
Out Burst Errors	このステーションのダウンストリームで最も近くにあるアクティブなノードによって報告され、プローブによって検出されたエラー報告パケット内のバーストエラーの合計数
AC Errors	リングプロセス時に、このノードが ARI（Address Recognized Indicator）と FCI（Frame Copied Indicator）を解釈できなかった回数
Abort Errors	ノードが中止シーケンスを送信した回数。通常、中止シーケンスは、ノードが現在送信しているフレームでエラーを検出したときに送信されます。
Lost Frame Errors	ノードがフレームを送信し、そのフレームを完全な状態で再び受信できなかった回数
Congestion Errors	ノードが、特定のアドレスに送信されたフレームを検出したが、そのフレームをコピーできなかった回数（通常、バッファの大きさが十分でないことが原因です）

統計	説明
Frame Copied Errors	ARI ビットおよび FCI ビットのいずれかまたは両方が 1 に設定された状態（他のノードが同じアドレスを使用していることを示します）で、ノードが、特定のアドレスに送信されたフレームを検出した回数
Frequency Errors	ノードの内部クックとリングのクロックが一致しなかった回数
Token Errors	トークンエラーの数。これらのエラーは、トークンが破損した場合、またはアクティブモニタが必要な長さの時間で伝送された新しいフレームを検出しない場合に発生します。このエラーは、アクティブモニタによってのみ報告されます。
In Beacon Errors	このステーションによって送信され、プローブによって検出されたビーコンフレームの合計数
Out Beacon Errors	このステーションによって送信され、プローブによって検出されたビーコンフレームの合計数
Insertions	このステーションがリングに挿入されたことをプローブが検出した回数
Last NAUN	NAUN (Next Active Upstream Neighbor) としてプローブが最後に指定したステーション

ノード間の通信状況（トラフィック）の表示

Novell ZENworks Server Management は、選択したノードとセグメントのそれ以外の 1 つまたは複数のノードとの間のすべてのネットワークトラフィックに関するリアルタイムのデータを提供します。このデータは、[Conversations] ビューから表示できます。このビューに表示されたデータを使用して、ノードの通信に関する特定の情報を調べることができます。たとえば、ルータまたはサーバと通信するノードを表示したり、サーバの負荷や、問題が報告されたノードの送受信トラフィックを調べたりできます。

ノード間の通信状況を表示するには

1 Novell ConsoleOne でノードを選択します。

2 [View] > [Conversations] の順にクリックします。

選択したノードが複数のセグメントに接続されている場合は、[Select Segment] ダイアログボックスが表示されます。

2a トラフィックを調べるノードが接続されているセグメントを選択し、[View] をクリックし、[Conversations] をクリックします。

[Conversations] ビューには、送信元ノードの負荷に対する送信先ノードのトラフィックの割合がリスト表示されます。ただし、サンプルの非対称性（サンプリングが同時に行われないこと）や統計値の丸め処理により、列の数字を足しても 100% にならないことがあります。

[Conversations] ビューに表示される統計は、5 秒ごとに更新されます。次の表は、[Conversations] ビューに表示される統計について説明しています。

統計	説明
ノード	送信元ノードが通信している送信先ノードの名前
% Pkt Load	送信先ノードと送信元ノード間のパケット負荷の割合

統計	説明
% Byte Load	送信元ノードと送信先ノード間のバイト負荷の割合
Pkts/s In	送信先ノードが送信元ノードから受信した 1 秒あたりのパケット数
Pkts/s Out	送信先ノードが送信元ノードに送信した 1 秒あたりのパケット数
Bytes/s In	送信先ノードが送信元ノードから受信した 1 秒あたりのバイト数
Bytes/s Out	送信先ノードが送信元ノードに送信した 1 秒あたりのバイト数
Pkts In	ビューを開いてから送信先ノードが送信元ノードから受信したパケット数
Pkts Out	ビューを開いてから送信先ノードが送信元ノードに送信したパケット数
KBytes In	ビューを開いてから送信先ノードが送信元ノードから受信した合計キロバイト数
KBytes Out	ビューを開いてから送信先ノードが送信元ノードに送信した合計キロバイト数
Protocols	この通信で送信先ノードが使用しているプロトコルパケットタイプ
First Transmit	Traffic Analysis Agent がロードされてから送信先ノードが初めてネットワークでデータを送信した日時
Last Transmit	Traffic Analysis Agent がロードされてから送信先ノードが最後にデータを送信した日時
MAC Address	送信先ノードの物理 (MAC) アドレス

停止していないかどうかノードを監視する

少なくとも 1 つの NetWare 版 Traffic Analysis Agent バージョン 1.0 以降がインストールされているセグメントの場合、監視するセグメントのノードを指定し、これらのノードが停止した場合に通知を受けることができます。この指定は、[Monitor Nodes for Inactivity] ビューで行います。

停止していないかどうかノードを監視することには、次の利点があります。

- セグメントのノードは、ノードが使用しているプロトコルに関係なく監視できます。
- ノードのステータスを取得するために Traffic Analysis Agent がノードに対してポーリングを実行しないため、この機能を使用してもネットワークトラフィックは影響を受けません。

停止していないかどうか監視するノードのリストを表示するには

1 ConsoleOne でセグメントを選択します。

2 [View] > [Monitor Nodes for Inactivity] の順にクリックします。

接続状況を監視する別の方法は、[Ping] ウィンドウでターゲットノードを指定し、指定したノードのステータスのテストを実行することです。[Connectivity Test] ウィンドウには、指定したターゲットノードのステータスに関する統計が表示されます。詳細については、27 章 975 ページの「Monitoring Services」を参照してください。

デフォルトでは、[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔はゼロ秒です。ビューを更新する頻度に基づいて、ポーリング間隔を設定してください。詳細については、1044 ページの「[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔の指定」を参照してください。また、エージェントがノードが停止していると見なす前にノードを検証する時間を変更することもできます。詳細については、1045 ページの「ノードが停止しているかどうかエージェントが判断するまでの時間を指定する」を参照してください。

重要： 監視を行うのは Novell ConsoleOne ではなく RMON エージェントであるため、ノードを監視するために [Monitor Nodes for Inactivity] ビューを開いたままにしたり、Novell ConsoleOne を実行したりする必要はありません。停止しているノードを Alarm Report で記録するために、Alarm Manager を実行してください。Novell ConsoleOne が実行されていない場合は、再起動後にアラームを確認してください。

停止していないかどうかノードを監視するには

1 ConsoleOne で、ノードを右クリックするか、ノードのリストが表示されたビューで、[Monitor Nodes for Inactivity] > [Add] の順にクリックします。

ノードが停止していないかどうか監視することをやめるには

1 ConsoleOne で、停止していないかどうか監視するノードを右クリックし、[Monitor Nodes for Inactivity]、[Delete] の順にクリックします。

重要： 停止しているノードの追加後にノードの NIC カードを変更した場合は、[Monitor Node for Inactivity] ビューにノードが表示されますが、MAC アドレスが変更されているためそのノードを削除することはできません。

次の表は、[Monitor Nodes for Inactivity] ビューに表示される統計について説明しています。

統計	説明
Name	停止していないかどうか監視するノードのリストを表示します。
MAC Address	ネットワークインタフェースの MAC アドレスを表示します。
Status	ノードのステータス（稼働または停止）を表示します。

Novell ConsoleOne が実行されている場合は、いつでも [Monitor Nodes for Inactivity] ビューを開いて、[Status] 列を確認できます。この操作を行うには、次の手順に従います。

1 ConsoleOne でセグメントを選択します。

2 [View] > [Monitor Nodes for Inactivity] の順にクリックします。

[Status] 列に、選択したノードが稼働しているか、または停止しているかが表示されます。

[Monitoring Nodes for Inactivity] の機能を使って、セグメントからノードの追加および監視を実行することができます。この操作を行うには、次の手順に従います。

1 ConsoleOne で、セグメントを右クリックし、[Monitor Nodes For Inactivity] ビューを選択します。

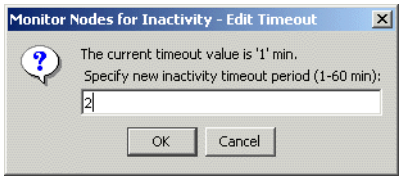
2  をクリックするか、[File] > [Actions] > [Add Node(s)] の順に選択します。

3 [Monitor Nodes for Inactivity - Add Node] ダイアログボックスで、追加するノードを選択します。

追加したノードは、ビュー内に表示されます。

[Monitor Nodes for Inactivity] モジュールは、監視対象のノードが Off のステータスまたは Timeout のステータスにある場合にアラームを送信します。[Monitor Nodes for Inactivity] ビューから、タイムアウト値を変更することもできます。

1  をクリックするか、[File] > [Actions] > [Edit Timeout] の順に選択します。



2 タイムアウト期間を指定します。

3 [OK] をクリックします。

パケットのキャプチャ

Novell ZENworks Server Management には、ネットワークアクティビティを分析し、ネットワーク障害の原因を特定するのに役に立つパケットキャプチャおよびデコードツールが用意されています。パケットをキャプチャしてデコードすると、セグメントの実際の状況に関する詳しい情報が得られるため、ネットワーク障害のトラブルシューティングを行うのに役立ちます。

Novell ConsoleOne は、任意の監視対象セグメントに対してパケットキャプチャを要求できます。各 RMON エージェントは、監視するセグメントのパケットをキャプチャし、ローカルのバッファに情報を保管します。

次の節では、パケットのキャプチャについて詳細に説明します。

- 1017 ページの「キャプチャフィルタの定義」
- 1020 ページの「パケットキャプチャの開始」
- 1020 ページの「同時パケットキャプチャの作成」
- 1020 ページの「パケットキャプチャの中止」
- 1020 ページの「中止されたパケットキャプチャの再開」
- 1021 ページの「キャプチャされたパケットの保存および表示」

キャプチャフィルタの定義

Novell ZENworks Server Management には、任意の Traffic Analysis Agent を使用してパケットをキャプチャする場合に使用できる、デフォルト値が設定されたキャプチャフィルタが用意されています。このデフォルト値は、フィルタを定義することによって変更できます。たとえば、あるノードから送信された NetWare パケットのみをキャプチャする場合は、これらのパケットのみをキャプチャするようにフィルタを定義できます。この結果、選択したパケットを保管するバッファの容量を節約できます。定義したフィルタ設定は、保存して後で使用することができます。

キャプチャフィルタを指定する場合、RMON エージェントのバッファにキャプチャする (含める) パケットを指定します。キャプチャしないパケットを指定しないでください。ノードとプロトコルの両方を指定すると、両方の基準を満たすパケットがキャプチャされます。複数のプロトコルファミリーを選択した場合は、いずれかのプロトコル基準を満たしたパケットがキャプチャされます。

キャプチャフィルタを定義するには

1 [File] > [Actions] > [Capture Packets] の順にクリックします。

2 デフォルトの名前を使用しない場合は、[Capture Name] テキストボックスに名前を入力します。

キャプチャ名を指定すると、同じセグメントに対する複数のキャプチャを簡単に追跡できます。

3 [Capture Using] ドロップダウンリストから、パケットをキャプチャするために使用する Traffic Analysis Agent を選択します。[Find In Atlas] をクリックすると、サイト上にある任意の Traffic Analysis Agent を選択できます。選択した Traffic Analysis Agent は保存され、次回に使用されます。

4 [Stations] ボックスで、送信元ノードおよび送信先ノードを入力または選択します。また、[Find Node] アイコンをクリックすると、[Find] ダイアログボックスからノードとアトラスコンポーネントを選択することもできます。

[Stations] ボックスには、ユーザがパケットをキャプチャできるセグメントのノードのリストが表示されます。Hardware、IP、または IPX ステーションから選択できます。

送信元ノードリストおよび送信先ノードリストの両方で [ANY] を選択した場合は、ノードが送受信したすべてのパケットキャプチャされます。

5 ノードのトラフィックフローの方向を選択します。

トラフィックフローの方向を指定するには、ドロップダウンリストから矢印オプションをクリックします。利用可能なノードおよびトラフィックフローの方向については、次の表を参照してください。

ノード	矢印	ノード	影響
node1	<==>	node2	node1 が node2 に送信するパケットと node2 が node1 に送信するパケットをキャプチャします。
node1	<==>	ANY	node1 が任意のノードに送信するパケットと node1 が任意のノードから受信するパケットをキャプチャします。これは、「ANY <==> node1」と同じです。
ANY	<==>	ANY	任意のノードが送受信したすべてのパケットをキャプチャします。
node1	==>	node2	node1 が node2 に送信したパケットをキャプチャします。これは、「node2 <== node1」と同じです。
node1	==>	ANY	node1 が他の任意のノードに送信したパケットをキャプチャします。これは、「ANY<== node1」と同じです。
node1	<==	node2	node2 が node1 に送信したパケットをキャプチャします。これは、「node2 ==> node1」と同じです。
node1	<==	ANY	任意のノードが node1 に送信したパケットをキャプチャします。これは、「ANY<== node1」と同じです。

6 使用されているプロトコルに基づいてフィルタリングを行う場合は、フィルタリングを行うプロトコルスイートを [Selected] リストボックスに追加します。

プロトコルを [Selected] リストボックスに追加するには、[Available] リストボックスからプロトコルを選択し、[Add] をクリックします。

または

プロトコルを［Selected］リストボックスから削除するには、削除するプロトコルを選択し、［Remove］をクリックします。

Novell ZENworks Server Management を最初に使用した場合は、デフォルトですべてのプロトコルが選択されます。プロトコルが［Selected］リストボックスに表示されていない場合は、すべてのプロトコルがキャプチャされます。

Novell ZENworks Server Management でサポートされているプロトコルデコードに関する詳細については、995 ページの「Novell ZENworks Server Management によってサポートされているプロトコルデコードスイート」を参照してください。

7 Ethernet、FDDI、またはトークンリングセグメントでキャプチャするパケットの種類を指定します。

次の表は、セグメントのデフォルト統計を示しています。

セグメントタイプ	利用可能な統計	デフォルト統計
Ethernet	正常なパケットのみ、エラーパケットのみ、または正常なパケットとエラーパケットの両方	正常なパケットおよびエラーパケット
FDDI リング	すべてのパケット、LLC パケット、MAC パケット、または SMT パケット	すべてのパケット
トークンリング	すべてのパケット、MAC パケット以外のパケット、または MAC パケット。MAC パケットは、トークンリングの運用を管理するために使用されます。	すべてのパケット

8 バッファがいっぱいの場合にパケットキャプチャを中止するかどうか、またはバッファ内の最も古いパケットを新しいパケットで上書きするかどうかを指定します。

パケットキャプチャを中止しないように指定した場合は、中止基準が存在しなくなり、すでにキャプチャされたパケットが新しいパケットで上書きされます。最も古いパケットを上書きするように選択した場合、パケットキャプチャは手動で中止する必要があります。

9 バッファサイズを指定します。

ドロップダウンリストからバッファサイズを選択するか、または必要なサイズを指定します。デフォルトのバッファサイズは 128KB です。

RMON エージェントは、要求されたバッファサイズを確保しようとします。バッファのサイズが大きいためサーバのメモリ領域が足りない場合、RMON エージェントは要求されたサイズのバッファを作成できません。

10 スライスサイズを選択します。

スライスは、バッファに保管する各パケットの最大バイト数を指定します。パケットのサイズはパケットヘッダから測定されます。スライスにより、簡単に、バッファ領域に保管するパケット数を最大にしたり、キャプチャされたパケットを処理する RMON エージェントの負荷を軽減したりできます。プロトコルヘッダ情報をデコードする場合は、100 ～ 150 バイト必要です。その他の情報は、通常、データの破損に関する問題が考えられる場合のみ必要なデータです。ただし、パケットが大きすぎる場合は、スライスによって情報が切り捨てられるため、デコードが正常に行われないことがあります。

キャプチャフィルタが設定されました。パケットをキャプチャしない場合は、[Cancel] ボタンをクリックしてください。

パケットキャプチャの開始

パケットキャプチャを開始するには

1. キャプチャフィルタを定義します。手順については、1017 ページの「キャプチャフィルタの定義」を参照してください。
2. セグメントの優先 RMON エージェントにフィルタ設定を適用するには、[OK] をクリックします。
3. [Capture Status] ダイアログボックスの [Start] をクリックします。

パケットキャプチャを開始すると、[Capture Status] ダイアログボックスの [Start] ボタンが [Stop] ボタンに切り替わり、キャプチャバッファ領域の状況がアクティビティインジケータに示されます。フィルタ基準を満たすパケットがキャプチャされると、キャプチャバッファにパケットデータが保管され、その下のボックスに、キャプチャされたパケットの数が表示されます。キャプチャバッファがいっぱいになると、ピンの回転が止まります。

同時パケットキャプチャの作成

キャプチャを最初に開始したときに行った手順を繰り返すことによって、同時パケットキャプチャを作成できます。これにより、異なるキャプチャ基準のキャプチャを設定および実行できます。

異なるキャプチャ基準のパケットキャプチャは、最大 20 個まで実行できます。

パケットキャプチャの中止

キャプチャフィルタを設定する場合は、キャプチャバッファがいっぱいになったときにパケットキャプチャを中止するかどうか、またはパケットのキャプチャを続行してバッファ内の最も古いパケットを上書きするかどうかを選択します。

デフォルトでは、キャプチャバッファがいっぱいになったときにパケットキャプチャが中止されます。バッファがいっぱいになったときに上書きするように選択した場合は、パケットキャプチャを手動で中止する必要があります。

パケットキャプチャを手動で中止するには、[Capture Status] ダイアログボックスの [Close] ボタンをクリックします。

重要： [Packet Capture Setup] ウィンドウからパケットキャプチャを再開すると、既存のバッファが削除および更新されます。

中止されたパケットキャプチャの再開

[Packet Capture Setup] ウィンドウが開いている場合は、[Capture Status] ダイアログボックスの [Start] ボタンまたは [Stop] ボタンをクリックしてパケットのキャプチャを開始または中止できます。[Start] ボタンと [Stop] ボタンは切り替わります。Novell ZENworks Server Management がパケットをキャプチャしているとき、ボタンは [Stop] と表示され、パケットをキャプチャしていないとき、ボタンは [Restart] と表示されます。RMON エージェントバッファの内容は、再開時に削除されます。

キャプチャされたパケットの保存および表示

キャプチャバッファを表示しているとき、または単独で、キャプチャされたパケットをファイルに保存し、必要な数のファイルを表示できます。

保存されたパケットキャプチャファイルを表示するには

1 [Tools] > [View Packet File] の順にクリックします。

[File Open] ダイアログボックスが表示されます。

2 パケットキャプチャファイルを参照して選択します。

.TR1 ファイル拡張子が自動的に付加されます。

キャプチャされたパケットの表示

[Capture Status] ダイアログボックスの [View] ボタンをクリックすると、[Trace Display] ウィンドウに、キャプチャバッファに保管されたデコード済みパケットが表示されます。パケットのキャプチャ中にこのウィンドウを表示すると、キャプチャが自動的に中止されます。

Novell ZENworks Server Management は、Novell ConsoleOne でデコードおよび表示するのに必要なパケットデータのみを RMON エージェントから取得します。これにより、RMON エージェントと Novell ZENworks Server Management の間で転送されるパケットデータ量が最小になります。キャプチャしたすべてのパケットを表示しない場合は、表示フィルタを作成して、キャプチャしたパケットの定義したグループのみを表示できます。詳細については、1024 ページの「表示フィルタの定義」を参照してください。

次の節では、キャプチャしたパケットの表示方法とトレース表示操作の実行方法について説明します。

- 1021 ページの「キャプチャされたパケットの表示」
- 1024 ページの「表示するパケットのフィルタ処理」
- 1024 ページの「表示フィルタの定義」
- 1026 ページの「異なるパケットの選択およびデコード」
- 1026 ページの「プロトコルフィールドおよび 16 進形式のバイトの強調表示」
- 1027 ページの「パケットファイルの保存」
- 1028 ページの「パケットファイルを開く」
- 1028 ページの「パケットの印刷」

Novell ZENworks Server Management には、キャプチャされたパケットが [Trace Display] ウィンドウに表示される際に適用されるデフォルト値が用意されています。このデフォルト値を変更するには、1041 ページの「キャプチャされたパケットを表示するオプションの選択」を参照してください。

キャプチャされたパケットの表示

デコードされたキャプチャ情報、16 進形式のパケットデータ、およびキャプチャされたパケットに関する概要を表示するには、[Trace Display] ビューを使用します。

キャプチャされたパケットを表示するには

1 Novell ConsoleOne で、ノードまたはセグメントを選択します。

2 [File] > [Actions] > [Capture Packet] の順にクリックします。

3 選択したキャプチャフィルタを使用してパケットをキャプチャします。詳細については、1017 ページの「キャプチャフィルタの定義」を参照してください。

4 [Capture Status] ダイアログボックスの [View] ボタンをクリックします。

次の節で説明されているように、[Trace Display] ウィンドウには、キャプチャおよびデコードされたパケットが表示された 3 つのペインが含まれます。

- 1022 ページの「パケットデコードの表示」
- 1022 ページの「16 進形式のパケットデータの表示」
- 1023 ページの「キャプチャされたパケットに関する概要の表示」

パケットを最初に表示する場合は、[Summary] ペイン内の最初のパケットが強調表示され選択されています。このパケットの内容は、[Decode] ペインに表示されます。[Summary] ペインで異なるパケットを選択した場合は、そのパケットが強調表示され、そのパケットのデコードされた内容が [Decode] ペインに表示されます。

[Trace Display] ペインのサイズを変更するには、ウィンドウ間の境界線をドラッグしてください。

パケットデコードの表示

選択したパケットの内容に関する詳細情報は、[Decode] ペインに表示されます。パケットの内容は、プロトコルフィールドによって解釈（デコード）および表示されます。

デフォルトでは、完全にデコードされたパケットデータが [Decode] ペインに表示されます。[Trace Display] ウィンドウでは、デコードされたパケットを完全なプロトコルデコードとして表示するか、または 1 つのプロトコル層に対して 1 行単位で表示するかを設定できます。デフォルト設定の変更方法に関する詳細については、1041 ページの「キャプチャされたパケットを表示するオプションの選択」を参照してください。

16 進形式のパケットデータの表示

16 進形式の未解釈のパケットデータは、[Hexadecimal] ペインに表示されます。[Hexadecimal] ペイン（右側）の ASCII または EBCDIC 領域では、ASCII 文字または EBCDIC 文字に該当しない 16 進形式の各バイトはドットで表示されます。

[Hexadecimal] ペインの最初の列は、16 進形式のバイトのオフセットを示します。オフセットは、ヘッダの先頭からカウントされたバイトの数です。たとえば、最初の 3 行には、次のオフセットが示されています。

- Hexadecimal 0 ゼロオフセットを示します。
- Hexadecimal 10 16進形式の16オフセットを示します(これより前に16バイトあります)。
- Hexadecimal 20 16進形式の32オフセットを示します(これより前に32バイトあります)。

[Decode] ペインで 1 行単位のデコードされたパケットを表示することを選択したか、または完全にデコードされたパケットを表示することを選択したかに関係なく、すべてのパケットが [Hexadecimal] ペインに表示されます。[Hexadecimal] ペインと強調表示ツールは、パケットの特定のバイトにプロトコルを関連付けるときに完全なデコード表示を行う際に特に役に立ちます。詳細については、1026 ページの「プロトコルフィールドおよび 16 進形式のバイトの強調表示」を参照してください。

キャプチャされたパケットに関する概要の表示

送信元ノードと送信先ノード間の通信に関する概要は、[Summary] ペインに表示されます。[Summary] ペインでデコードを引き続き行うパケットを選択し、他のペインにその情報を表示できます。[Summary] ペインは水平方向にスクロールでき、ペインの列のサイズや位置を変更できます。

次の表は、[Summary] ペインに表示されたキャプチャ済みパケットに関する統計情報について説明しています。

統計	説明
No.	Traffic Analysis Agent で受信した順番に並べられたパケットの数。
Source	パケットを送信したノードの IP アドレス、IPX アドレス、または物理 (MAC) アドレス。 名前はデータベースに保管されます。名前がデータベースに存在する場合は、MAC アドレスが表示されます。
Destination	パケットの送信先ノード。ノードは、ノードの IP アドレス、IPX アドレス、または物理 (MAC) アドレスとして表示されます。
Layer	パケットの最上位プロトコル層の略語。NCP は NetWare Core Protocol™ (NCP™) ソフトウェア、ether は Ethernet データリング層、RTMP は AppleTalk Routing Table Maintenance Protocol 層、802.2 は IEEE 802.2 Logical Link Control 層を表します。完全なデコードオプションを選択した場合は、プロトコル層の完全な名前とそのすべてのフィールドが [Decode] ペインに表示されます。[Hexadecimal] ペインには完全なパケットが表示されます。
Summary	最上位プロトコル層の内容に関する簡単な説明。
Error	パケットのエラーの種類 (存在する場合)。この列は、Ethernet メディアに対してのみ表示されます。
Size	パケットのバイト数。パケットサイズには、プレアンブルと CRC は含まれません。
Absolute Time	パケットを受信したときの、コンピュータに設定された時計の時刻。
Interpacket Time	前のパケットを受信し終わってから現在のパケットを受信し終わるまでの時間。
Relative Time	まだバッファに保管されている最初のパケットを受信してから経過した時間。

表示するパケットのフィルタ処理

パケットをキャプチャした後で、キャプチャバッファに表示フィルタを適用し、必要なパケットのみを表示できます。フィルタ処理は、ノードの名前またはアドレス、プロトコルファミリーまたはプロトコル層、あるいは選択したフィールドの内容を使用して行うことができます。これは、パケットをキャプチャした後で、特定のワークステーションで問題が発生し、そのワークステーションが送受信したパケットのみを表示する場合などに役に立ちます。

表示フィルタ処理を行うには、RMON エージェントからキャプチャしたパケットの一部を Novell ConsoleOne に転送する必要があります。キャプチャする量が多い場合は、転送時間が長くなり、ネットワーク帯域幅が大量に消費されます。表示中にフィルタ処理を行うのではなく、詳細なキャプチャフィルタを定義することをお勧めします。ただし、同じキャプチャのフィルタ処理を再度行う場合は、データがすでに Novell ConsoleOne に転送されているので、Traffic Analysis Agent からデータを再び転送する必要はありません。したがって、同じパケットキャプチャのフィルタ処理をすばやく行うことができます。

表示フィルタは、表示にのみ影響を与えます。キャプチャバッファは変更されません。キャプチャされたすべてのパケットは、キャプチャバッファに保管されたままであり、異なる表示フィルタを使用して、または表示フィルタを使用せずに表示できます。

表示フィルタを定義するには次の 2 つの方法があります。

- [Trace Display] ウィンドウで、[View] > [Filter] の順にクリックします。

  [Display Filter] ダイアログボックスが表示されます。詳細については、1024 ページの「表示フィルタの定義」を参照してください。

- [Summary] ペインでパケットをダブルクリックするか、または [Decode] ペインまたは [Hexadecimal] ペインで、選択されているプロトコル層またはフィールドをダブルクリックします。

  フィルタは、選択した内容に基づいて設定されます。また、必要に応じてフィルタ情報を変更することもできます。詳細については、1025 ページの「ポイントクリックフィルタ処理」を参照してください。

表示フィルタの定義

選択したキャプチャフィルタを使用してパケットをキャプチャします。詳細については、1017 ページの「キャプチャフィルタの定義」を参照してください。表示フィルタを定義するには、次の手順に従います。

1. Novell ConsoleOne でセグメントを選択します。
2. [File] > [Actions] > [Packet Capture] の順にクリックします。
3. [Capture Status] ダイアログボックスの [View] ボタンをクリックします。
4. 表示されアクティブな [Trace Display] ウィンドウで、[View] > [Filter] の順にクリックします。
5. ドロップダウンリストからノードを選択します。IP、IPX、または MAC アドレスから選択します。

   あるいは、いずれかまたは両方のドロップダウンリストに、ANY の代わりにノード名またはアドレスを入力します。
6. ドロップダウンリストで利用可能な矢印オプションからトラフィックフローの方向を選択します。

7 特定のプロトコル層のすべてのパケットを表示するには

7a プロトコルのリストからプロトコルスイートの名前をダブルクリックし、プロトコルスイートのすべてのプロトコルが示されたリストを表示します。

7b リストをスクロールし、必要なプロトコルを探します。

7c プロトコルを選択します。

8 特定のフィールド内の内容が同じであるパケットをすべて表示するには

8a 16 進形式のバイト数単位でオフセットを入力します。

パケットがデコードされている場合は、[Hexadecimal] ペインでオフセット列を使用してオフセットをカウントできます。詳細については、1022 ページの「16 進形式のパケットデータの表示」を参照してください。

8b オフセットをパケットの先頭からカウントするか、またはプロトコル層の先頭からカウントするかを指定します。

プロトコル層オプションを選択した場合は、[Protocol] ボックスで特定のプロトコルを選択する必要があります。

8c フィルタに含めるデータを入力します。

8d データを表示する形式を指定します。16 進、ASCII、または EBCDIC 形式オプションから選択します。

また、ポイントクリックフィルタ処理を使用して、値を入力することもできます。1025 ページの「ポイントクリックフィルタ処理」を参照してください。

9 [OK] をクリックします。

ダイアログボックスが閉じられ、Novell ZENworks Server Management によってキャプチャバッファから必要なパケットが選択されます。

キャプチャバッファが大きい場合は、フィルタを通過した最初のパケットが表示されます。これらのパケットを調べている間、フィルタ処理はバックグラウンドで引き続き実行されます。

[Summary] ペインには、表示フィルタの基準を満たすフィルタされたパケットのリストが表示されます。この節の前半で説明したように、これらのパケットは表示およびデコードできます。

ポイントクリックフィルタ処理

ポイントクリック方法を使用して表示フィルタを定義するには、[Trace Display] ウィンドウでフィールドをダブルクリックします。

ポイントクリック方法を使用して表示フィルタを定義するには

1 1 つの通信（たとえば 1 つのノードと 1 つのサーバ間の通信）のパケットのみを表示するには、[Summary] ペインで該当する通信のパケットをダブルクリックします。

[Display Filter] ダイアログボックスには、選択したパケットの送信元と送信先が表示されます。また、必要に応じてアドレスを変更することもできます。たとえば、送信先アドレスを ANY、ブロードキャストアドレス、または特定のノードアドレスに変更できます。

または

特定のプロトコル層を含むすべてのパケットを表示するには、[Decode] ペインで、該当するプロトコルの行をダブルクリックします。

[Display Filter] ダイアログボックスには、選択したプロトコルが表示されます。

または

特定のフィールドと同じ内容のすべてのパケットを表示するには、[Decode] ペインで、該当するフィールドをダブルクリックします。

[Display Filter] ダイアログボックスには、フィールド、データ、および選択したフィールドのデータの種類が表示されます。

または

特定のオフセットと同じ内容のすべてのパケットを表示するには、[Hexadecimal] ペインで、該当するフィールドをクリックします。

[Display Filter] ダイアログボックスには、選択したフォールドの オフセットとデータの種類が表示されます。

2 [OK] をクリックします。

ダイアログボックスが閉じられ、Novell ZENworks Server Management によってキャプチャバッファからパケットが選択されます。

[Summary] ペインには、表示フィルタの基準を満たすパケットのリストが表示されます。

異なるパケットの選択およびデコード

異なるパケットを選択しデコードするには

1 [View] > [Go To] の順にクリックします。

また、キーボードの矢印キーを使用して、異なるパケットを強調表示することもできます。

2 パケット数を入力します。

指定したパケット数がキャプチャされたパケットの合計数よりも大きい場合は、エラーメッセージが表示されます。表示フィルタが設定され、指定したパケットがフィルタを通過しない場合は、指定したパケットに最も類似したパケットが表示されます。

パケットは、[Summary] ペインでマウスまたは矢印キーを使用してパケットのヘッダを選択したときに RMON エージェントから取得されます。[Go To] ダイアログボックスを使用すると、RMON エージェントから不必要なパケットデータを転送することを避けることができます。同様に、デコード概要の作成時に、スクロールボタンを使用して [Summary] ペインをスクロールすることによってパケットヘッダデータのみ取得できます。矢印キーを使用すると、すべてのパケットデータが取得されます。

プロトコルフィールドおよび 16 進形式のバイトの強調表示

Novell ZENworks Server Management には、プロトコルフィールドと 16 進形式のバイトを関連付けるのに便利な強調表示ツールが用意されています。強調表示ツールは、プロトコルデコードについて初めて学習するネットワークマネージャに役に立つトレーニングツールです。

このツールの使用方法は次のとおりです。

- [Decode] ペインでプロトコル層を強調表示します。

  [Hexadecimal] ペインの選択されたプロトコル層ですべてのバイトが強調表示されます。

- [Decode] ペインのいずれかのプロトコル層のフィールドをクリックします。

  関連付けられたバイトが [Hexadecimal] ペインで強調表示されます。

- [Hexadecimal] ペインで 16 進形式のバイトをクリックします。

  [Hexadecimal] ペインにあるこのフィールドのすべての 16 進形式のバイトと、ASCII バイトまたは EBCDIC バイトが強調表示され、関連付けられたフィールドが [Decode] ペインで強調表示されます。

- [Hexadecimal] ペインの ASCII または EBCDIC テキストをクリックします。

  フィールドに属するすべての 16 進形式のバイトと、ASCII バイトまたは EBCDIC バイトは、[Hexadecimal] ペインで強調表示され、関連付けられたフィールドは [Decode] ペインで強調表示されます。

パケットファイルの保存

キャプチャされたパケットをファイルに保存し、ファイルを後で開いて分析または印刷できます。ファイルにパケットを保存するときに、指定した名前のバイナリファイルが作成されます。次の場合に、ファイルにパケットを保存できます。

- 他のシステムにパケットを転送する場合、またはパケットを送信して分析を行う場合。
- 必要なパケットのみを表示するために、デコードされたキャプチャ済みパケットに表示フィルタを適用する場合。表示フィルタの適用後は、フィルタ処理されたパケットをファイルに保存できます。
- バッファから保存されたパケットを他のパケットと比較する場合。他のパケットを保存するか、またはキャプチャバッファからそれらのパケットを表示できます。1 度に表示できるアクティブなキャプチャバッファの数は 1 つだけです。ただし、ファイルにパケットを保存した後は、必要な数のファイルを開いたり、必要に応じてキャプチャバッファを同時に表示したりできます。

パケットファイルは、Windows 版 Traffic Analysis Agent および以前のバージョンの ManageWise® と互換性があります。したがって、Windows 版 Traffic Analysis Agent を使用してキャプチャおよび保存したパケットは、Novell ZENworks Server Management を使用して表示できます。

キャプチャバッファの表示中に、キャプチャされたパケットをファイルに保存するには

1 [File] > [Save As] の順にクリックします。

  パケットのフィルタ処理を行ったかどうかに応じて、[Save Filtered Packets or Save Unfiltered Packets] ダイアログボックスが表示されます。

2 [Filename] テキストボックスに名前を入力します。

  .TR1 ファイル拡張子が自動的に付加されます。

3 [OK] をクリックします。

  重要： 保存するキャプチャされたパケットをフィルタ処理します。(1024 ページの「表示するパケットのフィルタ処理」を参照してください)。パケットを保存する場合、表示フィルタを通過したパケットのみを保存します。表示フィルタ処理を行わない場合は、すべてのパケットが保存されます。

パケットファイルを開く

パケットファイルを開くには

1 Novell ConsoleOne のメインメニューから、[Tools] > [View Packet File] の順にクリックします。

2 開くファイルをダブルクリックします。

パケットの印刷

パケットを印刷するには

1 パケットをキャプチャするか、またはパケットファイルを開くことによって、[Trace Display] ウィンドウを開きます。

2 [File] > [Print] の順にクリックします。

3 必要な印刷オプションを選択します。

印刷先、形式、および印刷するパケットを選択できます。

- デフォルトプリンタに印刷するかまたはファイルに出力するかを選択します。ファイルを選択する場合は、ファイル名を入力し、ファイルを現在のパケットデータで上書きするか、または現在のパケットデータをファイルに追加するかを指定します。
- パケット情報の概要、16 進形式の情報のみ、完全なデコード、または簡単なデコードのいずれを表示するか選択します。これらの形式は、1021 ページの「キャプチャされたパケットの表示」で説明されている 3 つのペインに対応します。
- すべてのパケットを印刷するか、ある範囲のパケットを印刷するか、またはフィルタ処理されたパケットのみを印刷するかを選択します。

4 [OK] をクリックします。

ネットワークのプロトコルによって生成されたトラフィックの分析

Novell ZENworks Server Management では、ネットワークのプロトコルの配布状況を調べて、ネットワーク層、トランスポート層、およびアプリケーション層で RMON2 エージェントが検出したプロトコルの統計情報を取得できます。また、サポートされたカスタムプロトコルをネットワークに追加することもできます。サポートされたプロトコルは、RMON2 エージェントによってデコード可能であり、プロトコルを使用してネットワークに伝送されたパケットの数をカウントします。カスタムプロトコルは、RMON2 エージェントによってサポートされていませんが、ネットワークのノードによって使用されます。

次の節では、Novell ZENworks Server Management を使用してネットワーク内のプロトコルを管理する方法について説明します。

- 1029 ページの「ネットワークで使用されているプロトコルのリストの表示」
- 1031 ページの「セグメントのプロトコルの配布状況を調べる」

ネットワークで使用されているプロトコルのリストの表示

ネットワークのネットワーク層、トランスポート層、およびアプリケーション層で使用されているサポートされたカスタムプロトコルの階層関係を表示するには、[Protocol Directory] プロパティページを使用します。デフォルトでは、このページに、プロトコルの展開されたリストを示すプロトコルディレクトリツリーが表示されます。データリンク層で使用されているプロトコルは、最上位に表示されます。各プロトコルを展開すると、選択されたプロトコルの下にサポートされたカスタムプロトコルのリストが表示されます。

また、[Protocol Directory] プロパティページで、RMON2 エージェントによってサポートされているプロトコルを追加または削除することもできます。詳細については、1029 ページの「プロトコルディレクトリツリーへのサポートされたプロトコルの追加」を参照してください。また、RMON2 の制限された拡張機能を使用すると、ネットワークのノードによって使用され RMON2 エージェントによってサポートされていないカスタムプロトコルを追加することもできます。詳細については、1030 ページの「サポートされたプロトコルツリーへのカスタムプロトコルの追加」を参照してください。制限された拡張機能に関する詳細については、「RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)」を参照してください。

選択されたプロトコルに関して、RMON2 エージェントでサポートする RMON2 グループを指定できます。これにより、指定した、エージェントでサポートするグループの RMON2 の詳細を取得できます。プロトコルの追加中に、Host グループ、Matrix グループ、および Address Map グループに対するエージェントサポートを有効にすることができます。プロパティページの下部にある [Groups Supported] ボックスには、選択されたプロトコルに対して、ネットワーク層およびアプリケーション層の Host グループおよび Matrix グループのエージェントサポートと Address Map グループのサポートが有効であるかどうか、このサポートが無効であるかどうか、またはこれらのグループがサポートされていないかどうかが示されます。[Groups Supported] ボックスに表示された値は設定できます。

[Add] ボタンおよび [Remove] ボタンは、プロトコルディレクトリツリーでプロトコルを選択した場合にのみ有効になります。

重要： NetWare 版 Traffic Analysis Agent および Windows 版 Traffic Analysis Agent は、プロトコルディレクトリのプロトコルに対する Address Map、Host、および Matrix グループの有効化をサポートしません。

[Protocol Directory] プロパティページを開くには

1 Novell ConsoleOne で、ノード内の [Service] の [RMON2] をクリックします。

2 [File] > [Properties] > [Protocol Directory] タブの順にクリックします。

次の節を参照してください。

- 1029 ページの「プロトコルディレクトリツリーへのサポートされたプロトコルの追加」
- 1030 ページの「サポートされたプロトコルツリーへのカスタムプロトコルの追加」

プロトコルディレクトリツリーへのサポートされたプロトコルの追加

サポートされたプロトコルは、RMON2 エージェントによってデコード可能であり、プロトコルを使用してネットワークに伝送されたパケットの数をカウントします。

RMON2 エージェントによってサポートされているプロトコルのパラメータにはデフォルト値が用意されています。プロトコルの名前を入力すると、プロトコルがサポートされている場合はデフォルト値が表示されます。

プロトコルディレクトリツリーにプロトコルを追加するには

1 [Protocol Directory] プロパティページを開きます。

2 プロトコルディレクトリツリーからプロトコルを選択します。

3 [Add] をクリックします。

次の表は、選択されたプロトコルのパラメータについて説明しています。

重要： Protocol Name パラメータは設定できません。選択されたプロトコルのポート番号またはプロトコルコードを設定する場合は、選択されたプロトコルのすべての子プロトコルが削除されます。

パラメータ	説明
Protocol Name	プロトコルの名前を表示します。
Protocol ID	プロトコルの ID を表示します。アプリケーション層プロトコルのポート番号または他の層のプロトコルに対するプロトコルコードを表示します。プロトコル ID は、必ず 10 進形式の値で表示されます。
Description	選択したプロトコルの簡単な説明が表示されます。
Groups Supported	Address Map グループ、Host グループ、または Matrix グループのエージェントサポートが、選択したプロトコルに対して有効になっているかどうかを表示します。

[Protocol Name] リストから入力または選択したプロトコル名が RMON2 エージェントによってサポートされていると、プロトコルのデフォルトパラメータが [Add Protocol] ダイアログボックスの適切なフィールドに表示されます。デフォルト値を使用しない場合は、プロトコルの追加後にパラメータを編集できません。

4 [OK] をクリックします。

新しいプロトコルは、選択したプロトコルの子プロトコルとして追加されます。追加したプロトコルのパラメータは編集できません。パラメータを変更する場合は、プロトコルを削除し、プロトコルを再度追加する必要があります。

サポートされたプロトコルツリーへのカスタムプロトコルの追加

カスタムプロトコルは、RMON2 エージェントによってサポートされていませんが、ネットワークのノードによって使用されます。RMON2 エージェントが、選択されたプロトコルに対して、RMON2 の制限された拡張機能をサポートする場合は、選択されたプロトコルにカスタムプロトコルを追加できます。詳細については、「RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)」を参照してください。RMON2 エージェントがプロトコルに対して制限された拡張機能をサポートしない場合は、そのプロトコルにカスタムプロトコルを追加できます。カスタムプロトコルは子プロトコルを持つことができません。

カスタムプロトコルにはデフォルト値が用意されていないため、RMON2 エージェントによってサポートされていないプロトコルを追加する場合は、適切な値を入力する必要があります。

カスタムプロトコルをプロトコルディレクトリツリーに追加するには

1 プロトコルディレクトリツリーから、サポートされているプロトコルを選択します。

2 [Add] をクリックします。

3 [Protocol Name] フィールドで、プロトコルの名前を入力します。

4 [Protocol ID] フィールドで、アプリケーション層プロトコルのポート番号、または他の層のプロトコルのプロトコルコードを入力します。

重要： ポート番号またはプロトコルコードは、10 進形式の値で入力してください。

5 [Groups Supported] ボックスから、プロトコルに対して RMON2 エージェントがサポートするグループを選択します。

カスタムプロトコルは、サポートされたプロトコルの子プロトコルとして追加されます。

プロトコルディレクトリツリーからプロトコルを削除するには

1 プロトコルディレクトリツリーからプロトコルを選択します。

2 [Remove] をクリックします。

重要： 子プロトコルを持つプロトコルを削除すると、すべての子プロトコルもプロトコルディレクトリツリーから削除されます。

セグメントのプロトコルの配布状況を調べる

Novell ZENworks Server Management では、RMON2 エージェントによって検出されたプロトコルの配布状況を調べることができます。このビューに表示された情報を使用して、ネットワークのトラフィックを分析し、ネットワーク障害のトラブルシューティングを行うことができます。プロトコルの追加、削除、または編集を行うには、[Protocol Directory] プロパティページを使用します。詳細については、1029 ページの「プロトコルディレクトリツリーへのサポートされたプロトコルの追加」と 1030 ページの「サポートされたプロトコルツリーへのカスタムプロトコルの追加」を参照してください。

RMON2 エージェントによって検出されたプロトコルの配布状況は、プロトコルが検出された層に基づいて、[Protocol Distribution] ビューに表示されます。

選択されたセグメントのプロトコルの配布状況を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [View] > [Protocol Distribution] の順にクリックします。

ビューには、ネットワークで検出されたプロトコルがリストされた次の 3 つのテーブルが表示されます。

- ネットワーク層テーブル
- トランスポート層テーブル
- アプリケーション層テーブル

RMON2 エージェントによって検出されたプロトコルは、検出された層に応じて、[Protocol Distribution] ビューの適切なテーブルに表示されます。各テーブルには、15 秒ごとに更新されたプロトコルの統計が表示されます。

次の表は、[Protocol Distribution] ビューに表示されるプロトコルの統計について説明しています。

統計	説明
Protocol Name	プロトコルの名前
Packets/s	監視対象セグメント上のエージェントによって検出されたプロトコルを使用して伝送された 1 秒あたりの平均パケット数

統計	説明
Bytes/s	監視対象セグメント上のエージェントによって検出されたプロトコルを使用して伝送された 1 秒あたりの平均バイト数
Packet Rate %	このプロトコルを使用して伝送されたパケットの割合。これは、エージェントによって検出されたすべてのプロトコルを使用して伝送されたパケットの合計に対する割合です。
Byte Rate %	このプロトコルを使用して伝送されたバイトの割合。これは、エージェントによって検出されたすべてのプロトコルを使用して伝送されたバイトの合計に対する割合です。

重要： 各プロトコルの 1 つのエントリのみが［Protocol Distribution］ビューに表示されます。複数のプロトコルスイートでサポートされているプロトコルには、統合された統計が表示されます。

スイッチ上のトラフィックの分析

Novell ZENworks Server Management では、監視対象スイッチのポートに関する統計情報と、スイッチを使用しているネットワークの各ポートに接続されているノードのリストが提供されます。この情報は、［Unified Port Traffic］ビューに表示されます。このビューでは、スイッチを使用しているネットワークのデスクトップスイッチおよびワークグループスイッチ上の負荷を調べることができます。スイッチの各ポートに 1 つのノードしか接続できない場合、スイッチはデスクトップスイッチと呼ばれます。スイッチの 1 つのポートが、複数のノードが接続されている接続デバイスに接続されている場合、スイッチはワークグループスイッチと呼ばれます。

スイッチのポートに接続されているポートおよびノードは、組み込みの RMON エージェントまたは外部 RMON エージェントを使用して監視できます。組み込みの RMON エージェントは、スイッチのポートにインストールされます。外部 RMON エージェントは、スイッチに接続されたノードにインストールされます。

次の節では、スイッチポートと、スイッチを使用しているネットワークのポートに接続されたノードに関する情報の取得方法について説明します。

- 1032 ページの「スイッチのポートに関する統計の表示」
- 1033 ページの「スイッチに関する概要情報の表示」

スイッチのポートに関する統計の表示

ネットワークのスイッチポートに関する統計情報を取得するには、［Unified Port Traffic］ビューを使用します。このビューには、各ポートに接続されたノードのドロップダウンリストも表示されます。このビューに表示された情報は、ポートのトラブルシューティングを行うときに役に立ちます。

［Unified Port Traffic］ビューには、スイッチのポートに接続されたノードのリストと、各ポートに関する統計が表示されます。スイッチの Ethernet ポートに関する Ethernet 固有の統計を表示できます。FDDI およびトークンリングポートに固有な統計は、このバージョンの Novell ZENworks Server Management では表示されません。ただし、メディアの種類に関係なく、スイッチのすべてのポートに関する一般的なポートの統計は表示されます。すべての統計を表示するか、または［Unified Port Traffic］ビューを設定して、選択した統計を表示するかを選択できます。詳細については、1040 ページの「［Unified Port Traffic］ビューで表示する統計を選択する」を参照してください。

スイッチのポートの統計を表示するには

1 Novell ConsoleOne で、スイッチ内の［Services］の［Switch/Bridge］を選択します。

2［View］>［Port Traffic］の順にクリックします。

スイッチに関する概要情報の表示

［Switch Summary］ビューには、選択したスイッチに関する簡単な情報が表示されます。選択したスイッチに関する情報と、スイッチで生成されたアラームに関する静的情報を表示できます。また、スイッチが受信した 1 秒あたりのパケット数およびブロードキャスト数を調べることもできます。

スイッチの概要情報を表示するには

1 Novell ConsoleOne で、スイッチ内の［Services］の［Switch/Bridge］を選択します。

2［View］>［Switch Summary］の順にクリックします。

［Switch Summary］ビューには、次の表で説明するような、選択したスイッチに関する静的情報が表示されます。

統計	説明
Vendor	スイッチベンダの名前
Switch Type	スイッチの種類：トランスペアレントまたはソースルート
Number of Ports Active	スイッチでアクティブなポートの数
Forwarding Table Overflow Count	転送テーブルが容量を超えた回数
Up Time	スイッチを最後に再起動してから経過した時間
Number of Ports Present	選択したスイッチに存在するポートの数
Number of MAC Addresses Learned	スイッチによって動的に検出された MAC アドレスの数

［Switch Summary］ビューには、次の表で説明するように、選択したスイッチで生成されたアラームに関する情報が表示されます。

統計	説明
Severity	トラップに基づいた重要度レベル
From	アラームをアラーム管理システムに送信したデバイスのネットワークアドレス
Owner	アラームによって影響を受けるセグメントまたはデバイス
Summary	イベントの概要。多くの場合、アラームによって影響を受けるオブジェクトの名前またはアドレスを含みます。

統計	説明
Received Time	アラーム管理システムがアラームを受け取った日時
Type	アラームの一般的な説明（たとえば、「ボリュームのディスク領域が不足しています」など）
Category	トラップタイプオブジェクトを定義する MIB に基づいて、アラームのカテゴリを表示します。カテゴリは、管理サーバ MIB プールに含まれる MIB に直接関連します。たとえば、NetWare サーバのカテゴリは、NetWare Server Alarm MIB に基づきます。

[Switch Summary] ビューには、次の表で説明するような、選択したスイッチに関する動的情報が表示されます。

Statistics（統計情報）	説明
Switch Load (pkts/sec)	スイッチが受信した 1 秒あたりのパケット数に基づくスイッチの負荷
Frames Dropped/sec	受信時に破棄されたパケットの 1 分あたりの数
Broadcasts/sec	スイッチのポートに接続されたノードからスイッチが受信したブロードキャストの数

トラフィック分析の最適化

ネットワークパフォーマンスを分析するために Novell ZENworks Server Management によって提供されるツールには、デフォルト設定が用意されています。必要な情報のみを表示するために、さまざまなビューのデフォルト設定を変更できます。

次の節では、ネットワーク環境に適合するように、Novell ZENworks Server Management ツールを設定する方法について説明します。

- 1034 ページの「セグメント上のステーションを表示するオプションの選択」
- 1036 ページの「トレンド統計を表示するオプションの選択」
- 1039 ページの「上位ノードグラフを表示するオプションの選択」
- 1040 ページの「[Unified Port Traffic] ビューで表示する統計を選択する」
- 1041 ページの「キャプチャされたパケットを表示するオプションの選択」
- 1041 ページの「[Set Alarm] ダイアログボックスでのアラームオプションの設定」
- 1044 ページの「[Monitor Nodes for Inactivity] ビューの設定」

セグメント上のステーションを表示するオプションの選択

[Stations] ビューを設定して、監視対象セグメント上の上位 20 のノードのみまたはすべてのノードを表示できます。上位 20 のノードを表示する基になる統計を選択することもできます。

次の設定オプションが利用可能です。

- 1035 ページの「セグメント上のすべてのノードに関する統計の表示」

- 1035 ページの「セグメント上の上位 20 のノードに関する統計の表示」
- 1035 ページの「上位 20 のノードが表示される基になる統計の選択」

セグメント上のすべてのノードに関する統計の表示

セグメント上のすべてのノードに関する統計を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [View] > [Stations] の順にクリックします。

セグメント上のすべてのノードを表示するには、しばらく時間がかかり、ネットワークトラフィックが増加します。

3 [Stations] ビューで、[View] > [Show All Stations] の順にクリックします。

セグメント上の上位 20 のノードに関する統計の表示

セグメント上の上位 20 のノードに関する統計を表示するには

1 Novell ConsoleOne でセグメントを選択します。

2 [View] > [Stations] の順にクリックします。

3 [Stations] ビューで、[View] > [Show Top N Stations] の順にクリックします。

上位 20 のノードが表示される基になる統計の選択

1 秒あたりの送信パケット数は、デフォルト統計であり、この値を基にして上位 20 のノードが [Stations] ビューに表示されます。上位 20 のノードを表示する基になる異なる統計を選択するには、次の操作を行います。

- [Stations] ビューから、[View] をクリックして [Show Top N Stations] を選択し、表示された統計のリストから該当する統計を選択します。
- [Stations] ビューのツールバーの [Top Nodes Statistics] ドロップダウンボックスをクリックし、表示された統計から該当する統計を選択します。

次の表は、利用可能な統計について説明しています。

統計	説明
Packets/s In	ノードが受信した 1 秒あたりのパケット数
Packets/s Out	ノードが伝送した 1 秒あたりのパケット数
Bytes/s In	ノードが受信した 1 秒あたりのバイト数
Bytes/s Out	ノードが伝送した 1 秒あたりのバイト数
Errors/s	ノードが送信した 1 秒あたりのエラー数
Broadcasts/s	ノードが送信した 1 秒あたりのブロードキャストパケット数
Multicasts/s	ノードが送信した 1 秒あたりのマルチキャストパケット数 (特定のノードグループに送信されたパケットの数)

デフォルト設定を変更した後で［Stations］ビューを閉じると、デフォルト設定の変更の保存を促すメッセージが表示されます。選択した統計に基づいて［Stations］ビューを表示する場合は、設定を保存します。次回、Novell ConsoleOne を開き、［Stations］ビューを表示したときに、指定した統計に基づいて監視対象セグメント上のノードを表示できます。

トレンド統計を表示するオプションの選択

セグメントパフォーマンストレンドが［Segment Trends］ビューに表示される際の基になるデフォルト設定を変更できます。

次の設定オプションが利用可能です。

- 1036 ページの「トレンド表示の基になる統計の選択」
- 1038 ページの「タイムスケールオプションの設定」

トレンド表示の基になる統計の選択

セグメントパフォーマンスが表示される際の基になる統計を変更するには

1 ［Segment Trends］ツールバーの［Profile］ボタンをクリックします。

2 ［Select Profile］リストからプロファイルを選択します。

デフォルトのプロファイルによって、監視対象セグメント上のパケット合計数、正常なパケット数、およびエラーパケット数の統計情報と共にトレンドが表示されます。

［Select Profile］リストに表示されたプロファイルを使用しないことを選択する場合は、［Select Statistics］リストから必要な統計を選択できます。

統計リストでは、次の表で説明するように、Ethernet、FDDI、およびトークンリングの統計を調べることができます。

統計	メディアサポート	説明
Abort Delimiter Errors/s	トークンリング	検出された 1 秒あたりの平均中止デリミタエラー数。このエラーはノードが伝送を中止したことを示します。
AC Errors/s	トークンリング	検出された 1 秒あたりの平均 AC エラー数。このエラーは、パケットの受信先がパケットを受信済みとマークするのに失敗した場合、またはパケットエラーフラグを設定した場合に報告されます。
Beacons	FDDI およびトークンリング	サンプリング間隔で検出された 1 秒あたりの平均ビーコン数。ステーションは、アップストリームでハード障害を検出したときにこれらのパケットを伝送します。
Broadcast Packets/s	Ethernet、FDDI、トークンリング	1 秒あたりのブロードキャストパケット数
Burst Errors/s	トークンリング	検出された 1 秒あたりの平均バーストエラー数。このエラーは、必要な時間、ノードが転送を検出しなかったことを示します。

統計	メディアサポート	説明
Claim Tokens/s	FDDI リング	リングが通常のリング状態またはリングパージ状態からクレームトークン状態になる 1 秒あたりの平均回数
CRC/Alignment Errors/s	Ethernet および FDDI リング	1 秒あたりの CRC (Cyclic Redundancy Check)/整列エラー数
Echo Pkts/s	FDDI リング	ネットワークで受信された 1 秒あたりの平均エコーフレーム数
Elasticity Buffer Errors/s	FDDI リング	このステーションによって報告された 1 秒あたりの平均弾力性バッファオーバーフローエラー数。これは、送信側と受信側のステーション間でクロック周波数が異なるため発生します。
Error Packets/s	Ethernet	1 秒あたりのエラーパケット数
Fragments/s	Ethernet	1 秒あたりのフラグメント数
Frame Copied Errors/s	FDDI リング	ステーションによって報告された 1 秒あたりの平均フレームコピーエラーフレーム数
Frequency Errors/s	トークンリング	検出された 1 秒あたりの平均周波数エラー数。このエラーは、ノードのトークンリングクロックがアクティブモニタのクロックと非常に異なることを示します。
Good Packets/s	Ethernet	1 秒あたりの正常なパケット数
Internal Errors/s	トークンリング	検出された 1 秒あたりの平均内部エラー数。通常、これらのエラーは、ネットワークボードの障害を示します。
Jabbers/s	Ethernet	1 秒あたりの超過送信の数
Line Errors/s	トークンリング	検出された 1 秒あたりの平均回線エラー数。これらのパケットは、有効なサイズですが、FCS (Frame Check Sequence) エラーがあり、8 ビットの範囲内に収まりません。
Lost Frames/s	FDDI およびトークンリング	ネットワークで検出された 1 秒あたりの平均損失フレームエラー数
Monitor Contentions/s	トークンリング	検出された 1 秒あたりの平均モニタ競合数。これらのパケットは、アクティブモニタがリングで検出されない場合にすべてのアクティブノードによって伝送されます。
Multicast Packets/s	Ethernet、FDDI、およびトークンリング	1 秒あたりのマルチキャストパケット数
Oversize Packets/s	Ethernet	1 秒あたりの超過サイズパケット数
Packets	FDDI およびトークンリング	サンプリング間隔で検出された 1 秒あたりの平均パケット数

統計	メディアサポート	説明
Receive Congestion Errors/s	トークンリング	検出された 1 秒あたりの平均受信混雑エラー数。このエラーは、ノードがそのアドレスに送信されたフレームを認識し、利用可能なバッファ領域がないことを示します。
Ring Wraps/s	FDDI リング	このインタフェースでラップアラウンド状態が検出された 1 秒あたりの平均回数。このエントリは、リングが実際にラップアラウンドした回数を示しません。このエントリは、リングがこの物理パスをラップアラウンドしたことを示します。
Token Errors/s	トークンリング	検出された 1 秒あたりの平均トークンエラー数。このエラーは、トークンが破損しているか、またはアクティブモニタが必要な時間内に新しいフレームを検出しなかったことを示します。
Total Bytes/s	Ethernet	1 秒あたりの平均合計バイト数
Total Packets/s	Ethernet	1 秒あたりの平均合計パケット数
Undersize Packets/s	Ethernet	1 秒あたりの未満サイズパケット数
Unicast Packets/s	Ethernet	1 秒あたりのユニキャストパケット数
Utilization%	Ethernet、FDDI、およびトークンリング	サンプリング間隔ですべてのパケットによって使用される最大ネットワーク容量に対する割合

トレンドが表示される基になるデフォルト統計を変更した後で [Segment Trends] ビューを閉じると、デフォルト設定の変更の保存を促すメッセージが表示されます。セグメントパフォーマンストレンドを、選択したプロファイルまたは統計に基づいて表示する場合は、定義した設定を保存します。次回、Novell ConsoleOne を開いて、[Segment Trends] ビューを表示したときに、定義したプロファイルまたは統計に基づいたトレンドを表示できます。

タイムスケールオプションの設定

セグメントパフォーマンストレンドは、1 分ごとに更新されます。グラフを更新する基になる異なるタイムスケールを設定できます。次のタイムスケールオプションから選択してください。

- Real Time（リアルタイム）
- One Hour（1 時間）
- One Day（1 日）
- One Week（1 週間）
- One Month（1ヶ月）
- One Year（1 年）

ヒント： トレンド表示の基になるデフォルトのタイムスケールオプションを変更した後で［Segment Trends］ビューを閉じると、デフォルト設定の変更の保存を促すメッセージが表示されます。トレンドをリアルタイムで更新しない場合は、選択したタイムスケール設定を保存します。次回、Novell ConsoleOne を開いて、［Segment Trends］ビューを開いたときに、選択したタイムスケールオプションに基づいてトレンドが更新されます。

上位ノードグラフを表示するオプションの選択

［Segment Dashboard］ビューを使用して、上位ノードのグラフを表示するまたは無効にすることができます。詳細については、1004 ページの「監視対象セグメント上にある上位ノードのグラフの表示」を参照してください。上位ノードグラフは、［Segment Dashboard］ビューの下部に表示されます。1 秒あたりの送信パケット数は、グラフが表示される基になるデフォルト統計です。グラフを表示する基になる異なる統計を選択できます。

次の設定オプションが利用可能です。

- 1039 ページの「［Segment Dashboard］ビューへの上位ノードグラフの表示」
- 1039 ページの「上位ノードグラフが表示される基になる統計の選択」
- 1040 ページの「［Segment Dashboard］ビューで上位ノードグラフを無効にする」

［Segment Dashboard］ビューへの上位ノードグラフの表示

［Segment Dashboard］ビューに上位ノードグラフを表示するには

1 ［Segment Dashboard］ビューで、［View］＞［Show Top N Graph］の順にクリックします。

上位ノードグラフが表示される基になる統計の選択

異なる統計に基づく上位ノードグラフを表示するには、［Segment Dashboard］ビューで次の操作を行います。

- ［View］＞［Show Top N Graph］をクリックし、統計を選択します。
- ［Segment Dashboard］ビューのツールバーの［Top Nodes Statistics］ドロップダウンボックスをクリックし、統計を選択します。

  次の表は、これらの統計について説明しています。

統計	説明
Broadcasts/min	ノードが伝送した 1 分あたりのブロードキャストパケット数
Bytes/s in	ノードが受信した 1 秒あたりのバイト数
Bytes/s out	ノードが伝送した 1 秒あたりのバイト数
Errors/min	ノードが伝送した 1 分あたりのエラー数
Packets/s in	ノードが受信した 1 秒あたりのパケット数
Packets/s out	ノードが伝送した 1 秒あたりのパケット数
Multicasts/min	ノードが伝送した 1 分あたりのマルチキャストパケット数

重要： 1 分あたりのエラー数、1 分あたりのブロードキャスト数、および 1 分あたりのマルチキャスト数は、5 秒ごとではなく 60 秒ごとに更新されます。

[Segment Dashboard] ビューで上位ノードグラフを無効にする

[Segment Dashboard] ビューに上位ノードグラフを表示するには

1 [Segment Dashboard] ビューで、[View] > [Disable Top N Graph] の順にクリックします。

[Unified Port Traffic] ビューで表示する統計を選択する

Novell ZENworks Server Management では、スイッチの各ポートに関する統計が提供されます。[Unified Port Traffic] ビューを使用して、ポート統計や、各ポートに接続されているノードのリストを表示できます。スイッチの Ethernet ポートに関する Ethernet 固有の統計を表示できます。FDDI およびトークンリングポートに固有な統計はこのバージョンの Novell ZENworks Server Management では表示されませんが、メディアの種類に関係なく、スイッチのすべてのポートに関する一般的なポートの統計は表示されます。詳細については、1032 ページの「スイッチのポートに関する統計の表示」を参照してください。[Unified Port Traffic] ビューでは、選択した統計のみを表示するように選択できます。

[Unified Port Traffic] ビューで表示する統計を選択するには

1 [Unified Port Traffic] ビューで、[View] > [Settings] の順にクリックします。

2 [Available Columns] リストから統計をクリックし、[Add] をクリックします。

次の表は、ポートに関して表示される一般的なポート統計について説明しています。ポートのメディアタイプは関係ありません。

統計	説明
Frames In/sec	ポートが受信した 1 秒あたりのフレーム数
Frames Out/sec	ポートが送信した 1 秒あたりのフレーム数
Port Link Status	ポートがアクティブであるか、または非アクティブであるかを示します。ポートがアクティブの場合、ポートはパケットを送受信できます。
Speed	ポートがパケットを送受信する速度
Media Type	選択したポートのメディアタイプ
Local Traffic	同じポートのノードに送信されたトラフィックレート

次の表は、前の表に示された一般的なポート統計以外の、Ethernet ポートに対して表示された Ethernet 固有の統計について説明しています。

統計	説明
Collisions/sec	1 秒あたりの衝突数
Utilization	ポート上のパケットトラフィックによって現在使用されている最大ネットワーク容量の割合
Broadcasts/sec	ポートが現在送受信している 1 秒あたりのブロードキャストパケット数
Multicasts/sec	ポートが送受信した 1 秒あたりのマルチキャストパケット数
Packets/sec	ポートが送受信した 1 秒あたりのパケット数

統計	説明
CRC Align Error	ポートによって報告された回線エラーの合計数
Oversize Pkts	ポートが送受信した超過サイズパケット数

キャプチャされたパケットを表示するオプションの選択

Novell ZENworks Server Management には、[Trace Display] ウィンドウにキャプチャされたパケットを表示するデフォルト設定が用意されています。

デフォルト設定を変更し、異なったトレースを表示するには

1 [Trace Display] ウィンドウを開きます。

2 [Trace Display] メニューで、[View] > [Options] の順にクリックします。

3 デコードされたパケットをどのように表示するかを選択します。

- [Full Protocol Decode] : 選択したパケットの各プロトコル層の各フィールドに関する情報を提供します。これはデフォルトのデコードです。
- [One Line Per Protocol Layer]: 選択したパケットの各プロトコル層に対して 1 行の情報を提供します。

4 最初の強調表示位置を表示するレベルを選択します。

- [At Highest Protocol Layer]: パケットの最上位プロトコル層を最初に強調表示します。これはデフォルトの設定です。
- [At Packet Header] : パケットヘッダを最初に強調表示します。

5 デコードされたパケットを表示する形式を選択します。

- [ASCII] :16 進データを ASCII 形式で表示します。これはデフォルトの設定です。
- [EBCDIC] :16 進データを EBCDIC 形式で表示します。

[Set Alarm] ダイアログボックスでのアラームオプションの設定

Novell ZENworks Server Management には、セグメントのデフォルトアラームしきい値が用意されています。Ethernet、FDDI、およびトークンリングセグメントにさまざまなエラー状況のしきい値を設定することにより、セグメントを頻繁に監視する必要がなくなります。

セグメントアラームを有効にすると、RMON エージェントがアラームしきい値設定に基づいてセグメントを監視します。設定されたしきい値を超えると、RMON エージェントがトラップを管理サーバに送信し、管理サーバはトラップを Novell ConsoleOne に転送します。

必要に応じてアラームしきい値のデフォルト値を変更してください。[Segment Trends] ビューを使用してネットワークの平均およびピークトラフィックレベルを測定することにより、適切な値を調べることができます。詳細については、1004 ページの「セグメントに関するトレンドデータの分析」を参照してください。これは、ネットワークでの通常のセグメントアクティビティの基準を作成する場合に行うことができます。

セグメントのアラームしきい値を設定するには

1 Novell ConsoleOne でセグメントを選択します。

2 [File] > [Properties] > [Segment Alarms] タブの順にクリックします。

3 セグメント統計を選択し、[Edit] をクリックします。

4 監視対象セグメントに設定されたアラームを有効にするには [Enable] をクリックします。

[Enable] をクリックすると、テキストフィールドと [Default] ボタンが有効になります。ただし、デフォルトしきい値が見つからない場合は、[Default] ボタンは有効になりません。

5 しきい値を入力します。

6 サンプリング間隔を指定します。

RMON エージェントは、統計の平均を計算するためにサンプリング間隔を使用して、アラームしきい値設定を超えたかどうかを調べます。

ヒント： また、[Segment Dashboard] ビューを使用して、セグメント統計のアラームしきい値を定義することもできます。詳細については、1003 ページの「[Segment Dashboard] ビューに表示される統計に対するアラームしきい値の定義」を参照してください。

次の表は、Novell ZENworks Server Management が Ethernet、FDDI、およびトークンリングセグメントに対して追跡するアラーム統計について説明しています。

統計	メディアサポート	説明
Abort Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均中止エラー数。これらのエラーは回線エラーに似ていますが、伝送中に発生します。
AC Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均アドレス認識（およびフレームコピー）エラー数。このエラーは、パケットの受信先がパケットを受信済みとマークするのに失敗した場合、またはパケットエラーフラグを設定した場合に報告されます。
Beacons	FDDI およびトークンリング	サンプリング間隔で検出された 1 秒あたりの平均ビーコン数。ステーションは、アップストリームでハード障害を検出したときにこれらのパケットを伝送します。
Broadcasts	Ethernet、FDDI、およびトークンリング	ブロードキャストアドレス FF-FF-FF-FF-FF-FF に送信された 1 秒あたりの平均パケット数。通常、ブロードキャストメッセージは、すべてのステーションに対する、情報の一般的な要求またはステータス情報の伝送から構成されます。
Burst Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均バーストエラー数。バーストエラーは、ステーション間で信号が短時間転送されないことによって発生します。
Claim Tokens	FDDI リング	リングが通常のリング状態またはリングパージ状態からクレームトークン状態になる 1 秒あたりの平均回数
Congestion Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均混雑エラー数。受信側ステーションのバッファ領域が不足しているため、パケットを保管できません。
CRC Errors	Ethernet および FDDI リング	サンプリング間隔で検出された 1 秒あたりの平均 CRC エラー数。これらのパケットは有効なサイズですが、FCS エラーがあります。

統計	メディアサポート	説明
Echo Pkts	FDDI リング	ネットワークで受信された 1 秒あたりの平均エコーフレーム数
Elasticity Buffer Errors/s	FDDI リング	このステーションによって報告された 1 秒あたりの平均弾力性バッファオーバーフローエラー数。これは、送信側と受信側のステーション間でクロック周波数が異なるため発生します。
Fragments	Ethernet	サンプリング間隔で検出された 1 秒あたりの平均フラグメント数。フラグメントは、64 バイトよりも小さく、FCS エラーがあるパケットです。通常、フラグメントは衝突の結果発生します。
Frame Copied Errors	FDDI およびトークンリング	サンプリング間隔で検出された 1 秒あたりの平均フレームコピーエラー数。このエラーは、他のステーションが最初のステーションに送信されたパケットを受信したことをステーションが検出したことを示します。
Frequency Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均周波数エラー数。このエラーは、ステーションのトークンリングクロックがアクティブモニタのクロックと異なることを示します。
Internal Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均内部エラー数。通常、これらのエラーは、ネットワークアダプタボードの障害を示します。
超過送信	Ethernet	サンプリング間隔で検出された 1 秒あたりの平均超過送信パケット数。超過送信は、1518 バイトを超える、FCS エラーがあるパケットから構成されます。
Line Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均回線エラー数。これらのパケットは、有効なサイズですが、FCS エラーがあり、8 ビットの範囲内に収まりません。
Lost Frames	FDDI およびトークンリング	ネットワーク上で受信した損失フレームエラーの合計数。損失フレームエラーは、フレームの終端デリミタがネットワークで失われたことを示します。
Monitor Contentions	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均モニタ競合数。これらのパケットは、アクティブモニタがリングで検出されない場合に伝送されます。
Multicasts	Ethernet、FDDI、およびトークンリング	マルチキャストアドレスに送信された 1 秒あたりの平均パケット数
Oversize	Ethernet	サンプリング間隔で検出された 1 秒あたりの平均超過サイズパケット数。超過サイズパケットは、サイズが 1518 バイトを超え、FCS を含みます。
Packets	Ethernet、FDDI、およびトークンリング	サンプリング間隔で検出された 1 秒あたりの合計パケット数
Ring Wraps/s	FDDI リング	このインタフェースでラップアラウンド状態が検出された 1 秒あたりの平均回数。このエントリは、リングが実際にラップアラウンドした回数を示しません。このエントリは、リングがこの物理パスをラップアラウンドしたことを示します。

統計	メディアサポート	説明
Token Errors	トークンリング	サンプリング間隔で検出された 1 秒あたりの平均トークンエラー数。このエラーは、トークンが破損しているか、またはアクティブモニタが現在のサンプリング間隔中に伝送された新しいフレームを検出しなかったことを示します。
Undersize	Ethernet	サンプリング間隔で検出された 1 秒あたり平均の未満サイズパケットの数。未満サイズエラーは、64 バイト未満の場合に発生します。
Utilization(%)	Ethernet、FDDI、およびトークンリング	サンプリング間隔ですべてのパケットによって使用される最大ネットワーク容量に対する割合

ネットワークのセグメントに対して適切なしきい値を設定した場合、[Segment Alarms] プロパティページ上の [Save As Default] ボタンをクリックすると、デフォルト値として定義した値が保存されます。ただし、Novell ZENworks Server Management によって提供されたデフォルトしきい値は、新しい値の適用後に利用できなくなります。

[Monitor Nodes for Inactivity] ビューの設定

デフォルトでは、[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔はゼロ秒です。更新するビューに基づいて、ポーリング間隔を設定できます。監視対象セグメント上のノードを監視しているエージェントは、指定された時間ノードを検証した後で、ノードが停止していると見なします。エージェントがノードが停止していると見なす前にノードを検証する時間は変更できます。

次の設定オプションが利用可能です。

- 1044 ページの「[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔の指定」
- 1045 ページの「ノードが停止しているかどうかエージェントが判断するまでの時間を指定する」

[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔の指定

lsmparameters.propertie ファイルの PollInterval パラメータを変更して、[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔を指定できます。

[Monitor Nodes for Inactivity] ビューを更新するポーリング間隔を指定するには

1 *operating_system_drive*¥install¥novell consoleone¥bin ディレクトリにある lsmparameters.properties ファイルを開きます。

2 PollInterval パラメータの値を指定します。

PollInterval 値は、秒単位の正の値である必要があります。デフォルト値は、ゼロ (0) 秒です。

ノードが停止しているかどうかエージェントが判断するまでの時間を指定する

選択されたノードが停止した場合、ノードを監視しているエージェントは、ノードが停止していると見なす前にノードの状態を 1 分間検証します。lsmparameters.properties ファイルの HostTimeOut パラメータを変更することによって、エージェントがノードが停止していると見なすまでの、選択されたノードを検証する時間を変更できます。エージェントは、ノードが停止していると見なす前に、指定された時間、停止しているノードを検証します。

ノードが停止しているかどうかエージェントがノードを検証する時間を変更するには

1 *operating_system_drive*¥install¥novell consoleone¥bin ディレクトリにある lsmparameters.properties ファイルを開きます。

2 HostTimeOut パラメータの値を指定します。

HostTimeOut 値は、分単位の正の値である必要があります。デフォルト値は 1 分間です。

Traffic Analysis Agent の理解

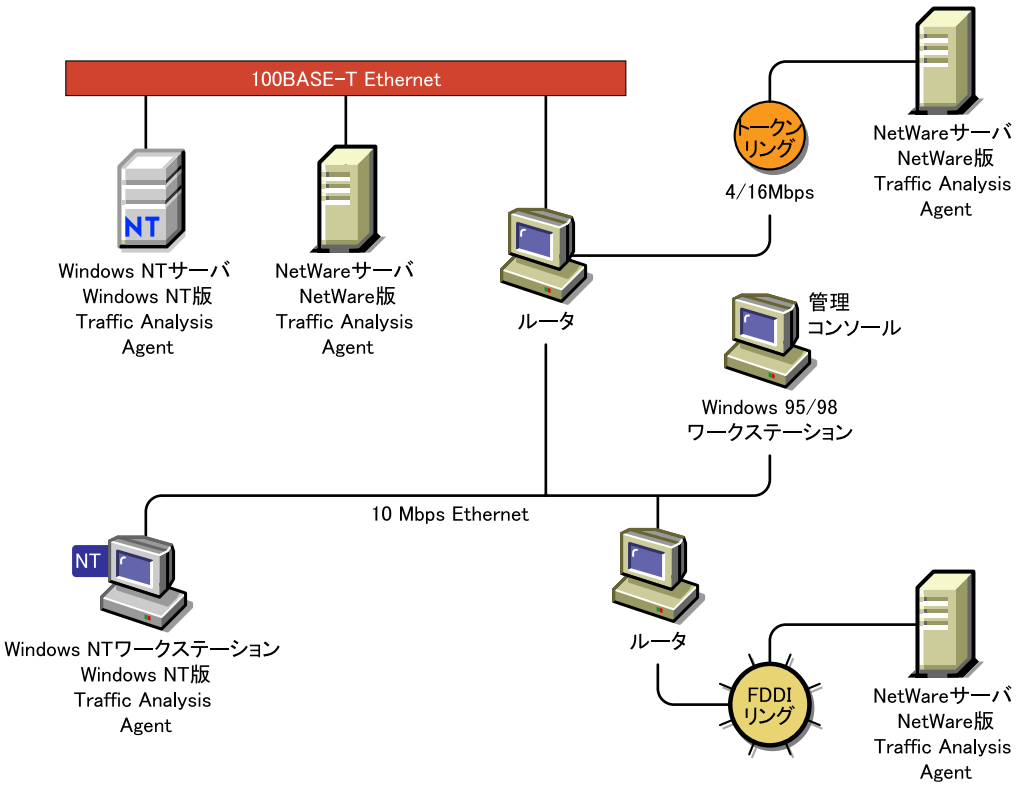
Traffic Analysis Agent を使用すると、使用しやすい Novell ZENworks Server Management インタフェースから、Ethernet、FDDI、およびトークンリングセグメントで構成される異種 LAN 環境を監視できます。

Traffic Analysis Agent は、NetWare サーバ、Windows サーバ、または Windows ワークステーションで実行できる RMON エージェントです。Traffic Analysis Agent は、RMON MIB (RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)) によって定義された一連の機能を実装します。これらのエージェントは、ネットワークのアクティビティに関する情報を収集します。この情報は、SNMP を使用して Novell ConsoleOne から利用できます。

Traffic Analysis Agent は、次の機能を提供します。

- セグメントのパフォーマンスを監視し、重要なネットワーク統計情報を Novell ConsoleOne に提供する。
- アラームしきい値を簡単に設定し、積極的なネットワーク管理を行えるようにする。
- 監視対象ネットワーク上の問題を診断および解決するためにすべてのパケットまたは選択したパケットをキャプチャする。
- SMP (Symmetric Multi-Processing) アーキテクチャを含む複数のネットワークセグメントを監視する。
- 高いネットワーク使用率や通信エラーなどの問題が発生していないかどうかネットワークセグメントを監視する。
- DHCP サーバからネットワークのノードへの動的な IP アドレスの割り当てを追跡する。
- 合計バイト数、合計パケット数、正常なパケット数、エラーパケット数などの統計を求めるために、リアルタイムトレンド (時間単位) および過去のトレンド (日単位、週単位、月単位、および年単位) を表示するデータを保管する。
- 停止していないかどうかノードを監視し、監視対象ノードが停止した場合にはユーザに通知する。

次の図は、Traffic Analysis Agent の機能を示しています。



Novell ZENworks Server Management には、次の Traffic Analysis Agent が含まれています。

- NetWare 版 Traffic Analysis Agent。

  詳細については 1047 ページの「NetWare 版 Traffic Analysis Agent の使用」を参照してください。

- Windows 版 Traffic Analysis Agent。

  詳細については 1062 ページの「Windows 版 Traffic Analysis Agent の使用」を参照してください。

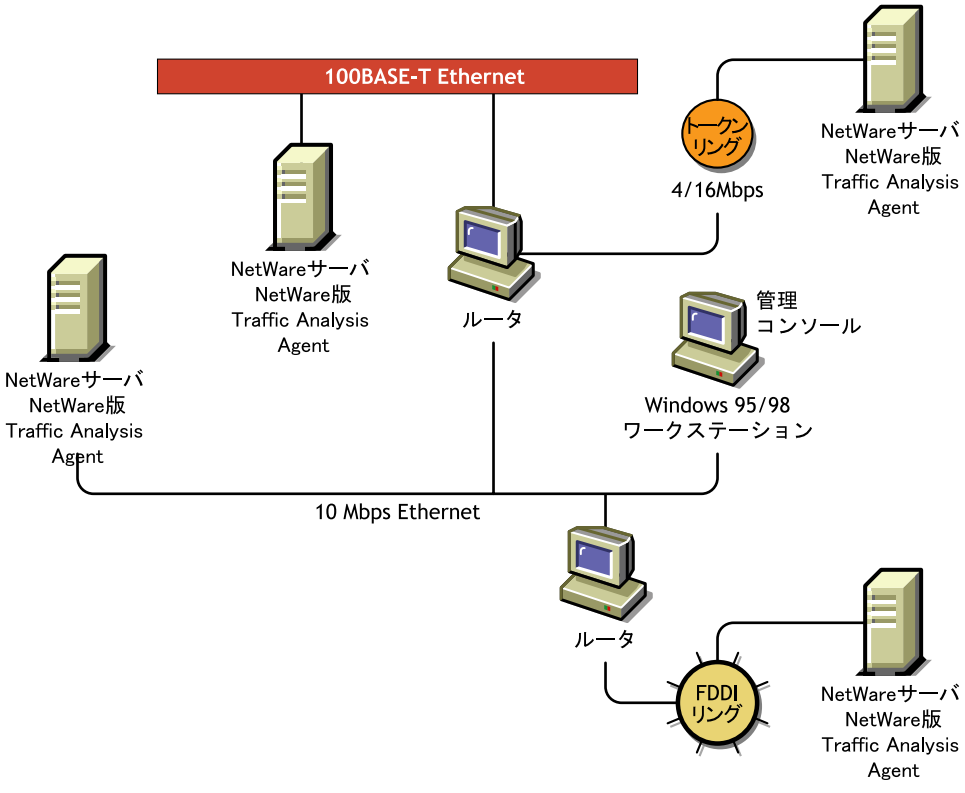
Novell ZENworks Server Management の Traffic Analysis Agent は RMON Plus エージェントです。詳細については、988 ページの「RMON Plus エージェントの機能」を参照してください。また、これらのエージェントは、最初の 2 つの RMON2 グループも実装します。最初の RMON2 グループは、Protocol Directory グループであり、エージェントが統計を監視および更新するプロトコルのテーブルを提供します。2 つ目の RMON2 グループは、Protocol Distribution グループであり、ディレクトリの各プロトコルに関する統計のテーブル提供します。詳細については、989 ページの「RMON2 エージェントの機能」を参照してください。

NetWare 版 Traffic Analysis Agent の使用

NetWare 版 Traffic Analysis Agent (NLA 1.30) は、NetWare サーバ上で実行します。これは、Ethernet、FDDI、またはトークンリングセグメントのトラフィックを NetWare で監視するための NLM プログラム群です。

NetWare 版 Traffic Analysis Agent は、トークンリングメディアに対する RMON MIB (RFC 1513 (http://www.isi.edu/in-notes/rfc1513.txt)) のトークンリング拡張機能、FDDI メディアに対する Novell 固有 MIB、および Ethernet メディアに対する RMON (RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)) を実装します。また、NetWare 版 Traffic Analysis Agent は、RMON2 (RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)) の最初の 2 つのグループを実装します。

次の図は、NetWare 版 Traffic Analysis Agent の機能を示しています。



次の節では、NetWare 版 Traffic Analysis Agent の最適化および使用について説明します。

- 1048 ページの「NetWare 版 Traffic Analysis Agent のインストール計画」
- 1048 ページの「NetWare 版 Traffic Analysis Agent のパフォーマンスの最適化」
- 1056 ページの「NetWare 版 Traffic Analysis Agent のコンソールユーティリティの使用」

NetWare 版 Traffic Analysis Agent のインストール計画

NetWare 版 Traffic Analysis Agent を NetWare サーバにインストールするには、サーバが、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」で指定されたシステム要件を満たす必要があります。

33 章 1119 ページの「SNMP コミュニティ文字列の使用」で説明されているように、NetWare SNMP パラメータを設定してください。これにより、NetWare 版 Traffic Analysis Agent をサーバに円滑にインストールできます。

注： 以前のバージョンの Traffic Analysis Agent(Novell ZENworks Server Management では、Traffic Analysis Agent と呼ばれます）をアンインストールすることをお勧めします。ただし、これは必須ではありません。以前のバージョンの Traffic Analysis Agent をアンインストールしない場合は、アップグレードされた NetWare サーバで新しい Traffic Analysis Agent が実行されていることを確認してください。

NetWare 版 Traffic Analysis Agent のパフォーマンスの最適化

次の節では、NetWare サーバ版 Traffic Analysis Agent のパフォーマンスを向上させる方法について説明します。

次の節で説明されている NetWare 版 Traffic Analysis Agent の機能を設定するには、lanz.ncf ファイルのパラメータを設定します。

- 1048 ページの「LANZ.NCF ファイルの内容」
- 1052 ページの「LANZ.NCF ファイルの内容の変更」

LANZ.NCF ファイルの内容

lanz.ncf ファイルによって、NetWare 版 Traffic Analysis Agent を実行するために必要なすべての NLM ソフトウェアがロードされます。lanz.ncf ファイルは、sys:¥zfs_agnt¥lanz ディレクトリに存在します。

次の例は、デフォルトの lanz.ncf ファイルの完全な内容です。

```
#

# Novell NetWare Traffic Analysis Agent

# Version 1.3

#

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

# LANZ.NCF:Novell NetWare Traffic Analysis Agent Load File

#

# This NCF file is created by the Novell NetWare Traffic Analysis Agent
install program.

# It is used to load the Novell NetWare Loadable Module files that make up
Novell NetWare

# Traffic Analysis Agent.

# WARNING:You should not modify this file unless you need to change one of

# the configuration parameters documented below.Other changes to this

# file are not recommended.Should you damage this file, you must reinstall
```

```
# Novell NetWare Traffic Analysis Agent.

#

# NOTE:To enable or disable the monitoring of network adapters by

# Novell NetWare Traffic Analysis Agent, use the LANZCON utility as described
in the

# Novell NetWare Traffic Analysis Agent Installation and Administration
guide.

#

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

# Load Parameter Descriptions

#

# load LANZSU debug=1

#

# debug=1    Turns on the LANZ Control screen to see the transactional

# messages from the Novell NetWare Traffic Analysis Agent.

#

# load LANZMEM bound=KB age=HHH

#

# bound=KB   This is the upper limit on memory that can be allocated

# dynamically by the Novell NetWare Traffic Analysis Agent.

#

# Increasing this number allows you to create larger packet

# capture buffers and maintain data for inactive stations

# for a longer period of time.

#

# Decreasing this value reduces the amount of memory that

# can be used by Novell NetWare Traffic Analysis Agent.This leaves more

# memory for the other server tasks.

#

# Novell NetWare Traffic Analysis Agent automatically purges data for

# inactive stations as the memory boundary is approached.

# This allows Novell NetWare Traffic Analysis Agent to adjust to

#

# the memory that is available to it dynamically.

#

# If the boundary is low, purging occurs frequently, saving
```

```
# only data for stations that have been recently active on
# the network.If this happens, a message appears on the
# system console indicating that not enough memory has been
# allocated to Novell NetWare Traffic Analysis Agent.
#
# KB is the memory boundary in kilobytes.
#
# Initial value:Set by the installation program
# based on memory usage
#
# Minimum recommended value:      512
#
# Maximum recommended value:75% of free server memory
# when NLM files are loaded
#
# Default value:If bound=KB is not specified,
# it defaults to 3072.
#
# age=HHH    Novell NetWare Traffic Analysis Agent purges data for stations
that have
# not been active on the network recently.This parameter
# controls how long data for inactive stations is maintained.
#
# Memory that is used by the station table is not available
# for other uses, such as capturing packets.Reducing the
# AGE value tends to increase the amount of memory
# available for capturing packets.
#
# If you cannot allocate capture buffers that are large,
# you may need to reduce the AGE value.
#
# HHH is the inactivity period, in hours, before station data
# is purged.
#
# Minimum recommended value:      1
#
```

```
# Default value:If age=HHH is not specified,
# it defaults to 168 (1 week)
#
# load LANZDI level=1
#
# level=1    It indicates that the LANZDI will stop receiving packets
# when CPU utilization gets high.
#
# Default is OFF.LANZDI will continue to receive packets even
# when CPU utilization gets high.
#
# load LANZSM topn=N
#
# topn=N     The number of concurrent sorts of top N nodes that
#
# Novell NetWare Traffic Analysis Agent supports for each network adapter.
#
# Recommended value: 4
# Minimum value:     2
# Maximum value:     10
#
# load LANZTR poll = 1
#
# poll=1     Polls token ring source-routed bridges.
#
# load LANZCTL trapreg=1
#
# trapreg=1 Causes SNMP traps to be sent to management consoles
# advertising themselves on the network, as well as stations
# listed in SYS:\ETC\TRAPTARG.CFG. Omitting this parameter
# or setting it to 0 causes traps to be sent only to those
# stations listed in the SYS:\ETC\TRAPTARG.CFG file.
#
# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
load gtrend.nlm
```

```
load lanzsu.nlm

load lanzmem.nlm bound = 3072 AGE = 168

load lanzlib.nlm

load lanzdi.nlm

load lanzael.nlm

load lanzhis.nlm

load lanzfcb.nlm

load lanzsm.nlm topn = 4

load lanztr.nlm

load lanzfddi.nlm

load lanzctl.nlm trapreg = 1
```

LANZ.NCF ファイルの内容の変更

次の節では、NetWare 版 Traffic Analysis Agent の機能を設定するために、lanz.ncf ファイルでコマンドのパラメータを変更する方法について説明します。

- 1052 ページの「LANZ 制御画面を有効にする」
- 1053 ページの「パケットキャプチャを無効にする」
- 1053 ページの「重複 IP アドレスアラームの生成を無効にする」
- 1053 ページの「パケットフロー制御の設定」
- 1053 ページの「利用可能メモリの上限の設定」
- 1054 ページの「サーバメモリからのデータの削除」
- 1054 ページの「上位ステーションの同時ソート」
- 1055 ページの「Management Site Server へのアラームの自動送信」
- 1055 ページの「ソースルートブリッジのポーリング」
- 1055 ページの「LANZ.NCF ファイルの変更内容を有効にする」

lanz.ncf ファイルで変更を行い、NetWare 版 Traffic Analysis Agent の設定を変更するには

1. テキストエディタで lanz.ncf ファイルを開きます。
2. 表示された適切なパラメータを挿入または変更し、ファイルを保存します。
3. 1055 ページの「LANZ.NCF ファイルの変更内容を有効にする」で説明されているように、NetWare 版 Traffic Analysis Agent をアンロードおよび再ロードします。

LANZ 制御画面を有効にする

LANZ 制御画面は、NetWare 版 Traffic Analysis Agent の重大なイベントを報告します。

LANZ 制御画面を有効にするには、次に示すように、LOAD LANZSU.NLM ステートメントに DEBUG パラメータを挿入します。

```
LOAD LANZSU.NLM DEBUG=1
```

デフォルトでは無効に設定されています。

パケットキャプチャを無効にする

パケットキャプチャを無効にすると、ネットワークセグメントで送信されたパケットでキャプチャされた機密データを他のユーザが見ることができなくなります。

パケットキャプチャを無効にするには、次に示すように、LOAD LANZFCB ステートメントにコメントマーク (#) を挿入します。

```
LOAD LANZFCB.NLM
```

また、パケットキャプチャを完全に無効にするのではなく、高レベルのトラフィックの場合にだけパケットキャプチャを制御することもできます。詳細については、1053 ページの「パケットフロー制御の設定」を参照してください。

重複 IP アドレスアラームの生成を無効にする

DHCP 環境では、DHCP クライアントをシャットダウンすると、IP アドレスが DHCP サーバに解放されます。IP アドレスを DHCP サーバに解放するときに、クライアントは DHCPRELEASE パケットを送信します。このパケットがエージェントに届かない場合、間違った重複 IP アドレスアラームが生成されます。

重複 IP アドレスアラームの生成を無効にするには、次に示すように、DUPIP パラメータの値にゼロ (0) を指定します。

```
LOAD LANZSM DUPIP=0
```

DUPIP パラメータにゼロ以外の値が指定された場合、またはパラメータが指定されなかった場合は、重複 IP アドレスアラームが生成されます。

パケットフロー制御の設定

NetWare 版 Traffic Analysis Agent は、通常、無差別モードで動作し、ネットワーク上のすべてのパケットを受信します。ただし、サーバ使用率が高く、パフォーマンスが低下している場合は、LEVEL パラメータを 1 に設定します。この設定により、サーバのトラフィックレベルが高いときにエージェントが一時停止し、トラフィックレベルが正常に戻ったときに自動的に無差別モードで再び動作します。

デフォルトでは、LEVEL パラメータが指定されないため、エージェントは無差別モードで連続して動作します。

パケットフロー制御を設定するには、次に示すように、LEVEL パラメータ設定を使用します。

```
LOAD LANZDI LEVEL=1
```

利用可能メモリの上限の設定

BOUND パラメータは、NetWare 版 Traffic Analysis Agent に動的に割り当てることができる利用可能メモリ領域の上限を設定します。

BOUND パラメータの値の単位はキロバイト (KB) です。デフォルト値は 3072KB です。最小推奨値は 512KB です。最大推奨値は、すべての NLM ファイルがロードされた後で利用可能なメモリ領域の 75% です。

次のような場合は、「Insufficient memory available for the Traffic Analysis Agent for NetWare」というメッセージが表示されることがあります。

- サーバの空きメモリ領域が少ない場合
- サーバの空きメモリ領域は十分にあるが、NetWare 版 Traffic Analysis Agent が利用できるメモリ領域が存在しない場合
- 非常に大きいパケットキャプチャバッファを要求したが、要求したよりも小さいメモリ領域がエージェントによって割り当てられた場合

このような場合は、BOUND パラメータの値を増やして、NetWare サーバに RAM を追加してください。

利用可能なメモリ領域の上限を変更するには、次に示すように、BOUND パラメータに適切な値を指定します。

```
LOAD LANZMEM BOUND=3072 AGE=168
```

サーバメモリからのデータの削除

NetWare 版 Traffic Analysis Agent はサーバメモリにデータを保持します。AGE パラメータの値を設定することにより、メモリに保持されたデータの量を制御できます。データが保持されてからパラメータで指定された時間が経過すると、データがメモリから削除されます。AGE パラメータは、特に大規模なブリッジネットワークの場合に役に立ちます。

AGE パラメータの値の単位は時間です。デフォルト値は 168 時間、すなわち 1 週間です。最小推奨値は 1 時間です。

エージェントに十分なメモリを割り当てているにもかかわらず、「Insufficient memory available for the Traffic Analysis Agent for NetWare」というメッセージが表示される場合は、AGE パラメータの値を減少させてください。

メモリが十分ではない場合でも、エージェントまたはサーバは影響を受けません。NetWare 版 Traffic Analysis Agent は、割り当てられたメモリが十分ではない場合でも、問題なく稼働します。

サーバメモリに保持されたデータの量を変更するには、次に示すように、AGE パラメータの値を変更します。

```
LOAD LANZMEM BOUND=3072 AGE=168
```

上位ステーションの同時ソート

NetWare 版 Traffic Analysis Agent は、[Segment Dashboard] ビュー、[Stations] ビュー、またはその両方のビューの上位 8 つのグラフが Novell ConsoleOne によって表示されたときに、ステーションをソートします。ソートは、それぞれ独立しており、異なる統計に基づいて計算されます。

それぞれのソート計算でサーバの CPU サイクルが使用されるため、同時計算の数を制限します。

ネットワークアダプタごとに同時ソート計算の数を設定するには、次に示すように、TOPN パラメータを設定します。

```
LOAD LANZSM TOPN=n
```

デフォルト値は 4、最小値は 2、最大値は 10 です。

Management Site Server へのアラームの自動送信

NetWare 版 Traffic Analysis Agent は、SNMP アラーム（SNMP トラップと呼ばれることもあります）を、ネットワーク内にある次の設定の Management Site Server または他のノードに自動的に送信できます。

- NetWare 版 Traffic Analysis Agent は､Management Site Server から送信された SAP パケットを受信します。
- Management Site Server または他のノードは､サーバの TRAPTARG.CFG ファイルに指定されています。このファイルを編集し、他のトラップターゲットを追加できます。

traptarg.cfg ファイルは、sys:¥etc ディレクトリに保管されます。このファイルには、その使用に関する指示が記載されています。このファイルは、ASCII テキストエディタを使用して編集できます。

アラームを自動的に送信するには、次に示すように、TRAPREG パラメータ設定を追加します。

```
LOAD LANZCTL TRAPREG=1
```

デフォルト値は 1 です。TRAPREG パラメータを省略した場合、またはパラメータ値をゼロ (0) に設定した場合、エージェントは traptarg.cfg ファイルで指定された管理コンソールにのみアラームを送信します。

ソースルートブリッジのポーリング

トークンリングネットワークでのソースルートブリッジのポーリングを制御するには、次に示すように、POLL パラメータを使用します。

```
LOAD LANZTR POLL=1
```

1 = On and 0 = Off.

POLL パラメータを 1 に設定すると、1 秒ごとにソースルートブリッジがポーリングされます。ポーリング間隔は変更できません。デフォルトでは有効に設定されています。

この機能を無効にするには、次に示すように、POLL パラメータをゼロ (0) に設定します。

```
LOAD LANZTR POLL=0
```

デフォルトでは、POLL パラメータは省略されます。また、トークンリングアダプタがインストールされていないシステムに対しては、LOAD LANZTR ステートメントがコメントアウトされています。

LANZ.NCF ファイルの変更内容を有効にする

lanz.ncf ファイルで行った変更の内容を有効にするには

1 LANZNCF ファイルを保存します。

2 サーバのプロンプトで「**ULANZ**」と入力し、エージェントをアンロードします。

3「**LANZ**」と入力し、エージェントを再ロードします。

NetWare 版 Traffic Analysis Agent のコンソールユーティリティの使用

NetWare 版 Traffic Analysis Agent 1.3 には、次の 3 つのタスクを実行するコンソールユーティリティ（lanzcon.nlm）が用意されています。

- 選択したネットワークアダプタによるネットワーク監視を有効または無効にする。
- 詳しいトラブルシューティング情報のソースを提供する。
- 残留エントリ（たとえば、異常終了した管理コンソールによって作成された Host TopN エントリ）を解決する。

NetWare 版 Traffic Analysis Agent をインストールすると、lanzcon.nlm は、sys:¥zfs_agnt¥lanz ディレクトリに自動的にインストールされます。

この節では、次のトピックに関して詳細に説明します。

- 1056 ページの「NetWare 版 Traffic Analysis Agent のコンソールユーティリティのロード」
- 1057 ページの「ネットワークアダプタの監視を有効または無効にする」
- 1057 ページの「ネットワークアダプタ情報の表示」
- 1058 ページの「エージェントアイテムステータスの表示」
- 1059 ページの「各アイテムに関する詳細情報へのアクセス」
- 1061 ページの「トレンドファイルの移行」

NetWare 版 Traffic Analysis Agent のコンソールユーティリティのロード

lanzcon.nlm を使用するには、NetWare のコンソールプロンプトで次のコマンドを入力します。

LOAD LANZCON CONTROLCOMMUNITY = *<control community string>*

重要： コマンドライン引数を指定せずに LANZCON を起動した場合、デフォルトの制御コミュニティ文字列は PUBLIC です。

lanzcon.nlm がロードされ、サーバに現在インストールされているネットワークアダプタに関する概要情報と共にネットワークアダプタのリストが表示されます。

各ネットワークアダプタに関する次の情報が表示されます。

- **Number (#):** ネットワークインタフェーステーブルのネットワークアダプタエントリ番号
- **説明：** ネットワークアダプタの簡単な説明
- **Media Type:**Ethernet、FDDI、トークンリングなど、ネットワークアダプタに接続されたネットワークの種類
- **Adapter Address:** ネットワークアダプタの物理アドレス

ネットワークアダプタの監視を有効または無効にする

選択したネットワークアダプタの監視を有効または無効にするには

1 [Network Adapters] 画面で適切なアダプタを選択し、(F3) キーを押します。

- 選択したアダプタが現在Ethernetまたはトークンリングネットワークを監視している場合、コンソールには [Adapter Is Monitoring] 画面が表示されます。
- 選択したアダプタがEthernetまたはトークンリングネットワークを監視していない場合、コンソールには [Adapter Is Not Monitoring] 画面が表示されます。

2 [Yes] または [No] をクリックし、監視を有効または無効にします。

監視を無効にすると、選択したアダプタのすべての LAN 分析データが削除されます。

LANZCON を使用している場合は、FDDI アダプタを無効にできません。FDDI アダプタを無効にするには、次の手順に従います。

1 LANZCON をアンロードします (ロードされている場合)。

2 LANZ をアンロードします (ロードされている場合)。

3 sys:¥zfs_agnt¥lanz ディレクトリにある lanz.ncf を編集するために開きます。

4 このステートメントの先頭に # 記号を入力し、ステートメント LOAD lanzfddi.nlm をコメントアウトします。

5 lanz.ncf を保存し閉じます。

6 LANZ を再ロードします。

ネットワークアダプタ情報の表示

ネットワークアダプタのアイテムに関する詳細情報を表示するには

1 [Network Adapters] 画面でアダプタを選択し、(Enter) キーを押します。

2 [Select Information to View] 画面で、[Show Adapter Items] を選択します。

LANZCON ユーティリティによって、選択したアダプタに関連するすべてのアイテムがリスト表示された [Network Adapter Items] 画面が表示されます。

トークンリングアダプタに関するこの画面には、Novell Token Ring RMON MIB からの情報が表示されます。詳細については、1058 ページの「エージェントアイテムステータスの表示」を参照してください。

[Select Information to View] メニューに戻るには、(Esc) キーを押します。

選択したアダプタに関する次の情報が表示されます。

- **Item:** 選択したアダプタによって現在監視されているアイテムの種類。[Network Adapter Items] 画面には、トークンリング、Statistics、History、Host、Matrix、および Host TopN から構成される一般的なアイテムが表示されます。NetWare 版 Traffic Analysis Agent は、デフォルトでこれらのアイテムを監視します。[Network Adapter Items] 画面では、トラフィックが最も多いノードのリストを示す Host TopN アイテムがユーザによって追加されています。設定に応じて、Novell ConsoleOne を使用しこの画面に他のアイテムを追加できます。

アイテムを選択し、各トピックに関する詳しい情報を表示できます。選択したアイテムの値を表示するには、必要なアイテムを選択し、(Enter) キーを押します。画面のその他の情報については、次のセクションを参照してください。

- **Index:** 同じ種類のすべてのアイテムのリストにある、表示されたアイテムのエントリ番号。関連するテーブルは、このインデックスによって識別されます。
- **説明：** エントリの説明。この列は、アイテムを作成したソフトウェア会社またはユーザを示します。NetWare 版 Traffic Analysis Agent によって自動的に監視されたアイテムは、モニタによって示されます。

  トークンリングネットワークエントリの場合、この列にはメディア速度およびローカルリング番号が表示されます。

エージェントアイテムステータスの表示

[Select Information to View] メニュー > [Show Agent Items] をクリックすると、NetWare 版 Traffic Analysis Agent が監視している各ネットワークアダプタのすべてのアイテムが LANZCON によって表示されます。

選択したエージェントのエージェントアイテムステータスを表示するには

1 [Network Adapters] 画面でアダプタを選択し、(Enter) キーを押します。

2 [Select Information to View] 画面で、[Show Agent Items] を選択します。

[All Novell NetWare Traffic Analysis Agent Items] 画面には、セグメントを監視しているエージェントに関連するすべてのアイテムが表示されます。たとえば、複数のネットワークセグメントを監視するために複数のアダプタを使用する場合は、エージェントによって監視されているすべてのアイテムが表示されます。

エントリ (トークンリングネットワークエントリを除く) を削除するには、エントリを選択し、[Delete] をクリックして、[Yes] をクリックします。

[Network Adapter Items] 画面に戻るには、(Esc) キーを押します。

エージェントに関する次の情報が表示されます。

- **Item:** 利用可能なアイテムの種類。[All Novell NetWare Traffic Analysis Agent Items] 画面には、Statistics、History、Host、Matrix、および Host TopN から構成される一般的なアイテムが表示されます。設定に応じて、その他のアイテムを表示できます。

  アイテムを選択し、各トピックに関する詳しい情報を表示できます。アイテムの値を表示するには、必要なアイテムを選択し、(Enter) キーを押します。画面のその他の情報については、次のセクションを参照してください。
- **Index:** 同じ種類のすべてのアイテムのリストにある、表示されたアイテムのエントリ番号。関連するテーブルは、このインデックスによって識別されます。
- **説明：** エントリの説明。この列は、アイテムテーブルを作成したソフトウェア会社またはユーザを示します。NetWare 版 Traffic Analysis Agent によって自動的に監視されたアイテムは、モニタによって示されます。

  トークンリングネットワークエントリの場合、この列にはメディア速度およびローカルリング番号が表示されます。

各アイテムに関する詳細情報へのアクセス

この節では、選択したアダプタと NetWare 版 Traffic Analysis Agent の両方で利用できる主要な情報について説明します。次のトピックについて説明します。

- 1059 ページの「トークンリング RMON MIB 情報の表示」
- 1059 ページの「FDDI リング RMON MIB 情報の表示」
- 1059 ページの「統計情報の表示」
- 1059 ページの「履歴情報の表示」
- 1060 ページの「ホスト情報の表示」
- 1061 ページの「マトリックス情報の表示」

トークンリング RMON MIB 情報の表示

トークンリング RMON MIB 情報を表示するには

1 [Network Adapter Items] 画面でトークンリングアイテムを選択し、(Enter) キーを押します。

2 [Select Information to View] 画面で [Show Adapter Items] を選択し、(Enter) キーを押します。

3 この画面を閉じるには (Esc) キーを押します。

FDDI リング RMON MIB 情報の表示

FDDI リング RMON MIB 情報を表示するには

1 [Network Adapter Items] 画面で FDDI リングアイテムを選択し、(Enter) キーを押します。

2 [Select Information to View] 画面で [Show Adapter Items] を選択し、(Enter) キーを押します。

統計情報の表示

統計情報は、セグメントごとの各監視対象アダプタに関する基本的な統計を示します。

統計情報を表示するには

1 [Network Adapter Items] 画面で [Statistics] をクリックします。

2 (Enter) キーを押します。

Ethernet ネットワークエントリの場合、LANZCON ユーティリティによって、[Statistics Information] 画面が表示されます。

この画面には、選択したネットワークアダプタの統計値が表示されます。この画面は、各フィールドの最新の値で定期的に更新されます。

3 この画面を閉じるには、(Esc) キーを押します。

履歴情報の表示

履歴情報によって、監視されているネットワークのサンプリング機能が定義されます。History Control テーブルによって、特定のネットワークアダプタに対する特定のサンプリング間隔で一連のサンプルが定義されます。

履歴情報を表示するには

1 [Network Adapter Items] 画面で [History] をクリックし、(Enter) キーを押します。

2 この画面を閉じるには、(Esc) キーを押します。

フィールドの説明は次のとおりです。

- **Index:** History Control テーブルの行を一意に識別する整数値
- **Data Source:** ネットワークアダプタや、このオブジェクトによって定義されたエントリのデータソースである Ethernet、FDDI、またはトークンリングセグメントを識別します。
- **Buckets Requested:** このエントリに関連付けられたメディア固有のテーブルの一部にデータが保存される離散サンプリング間隔の要求された数。
- **Buckets Granted:** データが保存される離散サンプリング間隔の実際の数。
- **Interval:** 各バケットに対するデータのサンプリングが行われる間隔 (秒単位)。この間隔には、1 から 3,600 (1 時間) までの数を設定できます。過去 1 時間のデフォルトの間隔は 1 つのサンプルあたり 30 秒であり、過去 1 日のデフォルトの間隔は 1 つのサンプルあたり 30 分 (すなわち、1,800 秒) です。

  サンプリングスキームは、割り当てられたバケットと制御間隔によって決定されます。
- **Owner:** アイテムを作成したエンティティ。「Monitor」は、アイテムが NetWare 版 Traffic Analysis Agent によって作成されたことを示します。
- **ステータス :** Valid のステータスは、エージェントが、テーブルによって提供された指示に従って、正常に稼働していることを示します。

ホスト情報の表示

ホストグループは、LAN 上の特定のホストまたはノードに関する統計を収集します。NetWare 版 Traffic Analysis Agent は、正常なパケットの送信元 MAC アドレスおよび送信先 MAC アドレスを調べることによって、LAN 上の新しいノードを認識します。エージェントに認識された各ノードに対して、一連の統計が保持されます。

ホスト (ノード) 情報を表示するには

1 [Network Adapter Items] 画面で [Host] をクリックし、(Enter) キーを押します。

ホストグループは、2 つのデータテーブルおよび 1 つの制御テーブルの 3 つのテーブルから構成されます。2 つのデータテーブルは、hostTable と hostTimeTable です。制御テーブル hostControlTable には、2 つのオブジェクトが含まれ、このオブジェクトは [Host Information] 画面に表示されたフィールドに対応します。

- **Index:** hostControlTable の行を一意に識別する整数値。制御テーブルの各行は、一意のネットワークアダプタおよび一意のセグメントを示します。
- **Data Source:** ネットワークアダプタや、このオブジェクトによって定義されたエントリのデータソースである Ethernet、FDDI、またはトークンリングセグメントを識別します。
- **Table Size:** この行に関連付けられた hostTable の行の番号。
- **Last Delete Time:** この行に関連付けられた hostTable の一部からエントリが最後に削除された時刻に対応する sysUpTime MIB オブジェクトの値。削除が行われなかった場合、この値はゼロ (0) になります。

- **Owner:** アイテムを作成したエンティティまたはユーザを示します。「Monitor」は、アイテムが NetWare 版 Traffic Analysis Agent によって作成されたことを示します。
- **ステータス：** Valid のステータスは、エージェントが、テーブルによって提供された指示に従って、正常に稼働していることを示します。

マトリックス情報の表示

マトリックスグループは、ネットワークセグメント上のノード間の通信に関する情報を記録します。情報は、マトリックス形式で保存されます。マトリックス形式で保存すると、サーバを最も頻繁に使用しているノードに関する情報などの、特定の組み合わせのトラフィック情報を簡単に取得できます。

マトリックス情報を表示するには

1 [Network Adapter Items] 画面で [Matrix] をクリックし、(Enter) キーを押します。

マトリックスグループは、2 つのデータテーブルおよび 1 つの制御テーブルの 3 つのテーブルから構成されます。データテーブルは、matrixSDTable と matrixDSTable です。制御テーブル matrixControlTable には、2 つのオブジェクトが含まれ、このオブジェクトは [Matrix Information] 画面に表示されたフィールドに対応します。

- **Index:** matrixControlTable の行を一意に識別する整数値。制御テーブルの各行は、特定のネットワーク上の通信を検出し、2 つのデータテーブルにそれらの通信に関する統計を保管する機能を定義します。
- **Data Source:** ネットワークアダプタや、このオブジェクトによって定義されたエントリのデータソースである Ethernet、FDDI、またはトークンリングセグメントを識別します。
- **Table Size:** この行に関連付けられた matrixTable の行の番号。
- **Last Delete Time:** この行に関連付けられた matrixTable の一部からエントリが最後に削除された時刻に対応する sysUpTime オブジェクトの値。削除が行われなかった場合、この値はゼロ (0) になります。
- **Owner:** アイテムを作成したエンティティまたはユーザを示します。「Monitor」は、アイテムが NetWare 版 Traffic Analysis Agent によって作成されたことを示します。
- **ステータス：** Valid のステータスは、エージェントが、テーブルによって提供された指示に従って、正常に稼働していることを示します。

トレンドファイルの移行

Novell ConsoleOne では、監視対象の Ethernet、FDDI、およびトークンリングセグメントに関するトラフィックパターンのトレンドを表示できます。トレンドデータを使用すると、セグメントのトラフィックを分析できます。詳細については、1004 ページの「セグメントに関するトレンドデータの分析」を参照してください。

以前のバージョンの NetWare 版 Traffic Analysis Agent (1.20 および 1.21) は、1 分ごとにサンプリングが行われたトレンドデータを収集しました。Novell ZENworks Server Management に付属の NetWare 版 Traffic Analysis Agent 1.30 は、1 分、1 時間、および 1 日ごとにサンプリングが行われたトレンドデータを収集します。NetWare 版 Traffic Analysis Agent バージョン 1.30 のこの機能により、エージェントと Novell ConsoleOne との間の通信量が最小限に抑えられ、ネットワークトラフィックを削減できます。

移行ツール (gtrend.exe) を使用すると、NetWare 版 Traffic Analysis Agent の以前のバージョンによって収集されたトレンドデータを、NetWare 版 Traffic Analysis Agent バージョン 1.30 および Novell ConsoleOne によって使用できるトレンドデータに変換できます。

NetWare 版 Traffic Analysis Agent バージョン 1.20 または 1.21 によって収集されたトレンドファイルを移行するには

1 インストール CD の gtrend.exe を 32 ビット Windows コンピュータの TEMP フォルダにコピーします。

2 以前のバージョンの NetWare 版 Traffic Analysis Agent によって収集されたトレンドデータファイルを TEMP フォルダにコピーします。

3 gtrend.exe を実行します。

この結果、既存の 1 分間のトレンドファイルが、NetWare 版 Traffic Analysis Agent バージョン 1.30 で使用できる、対応する 1 時間および 1 日のトレンドファイルに移行されます。

4 移行されたトレンドファイルを NetWare サーバの sys:¥gtrend¥ フォルダにコピーし、同じサーバで NetWare 版 Traffic Analysis Agent バージョン 1.30 を実行します。

注： 移行ツールでは、NetWare 版 Traffic Analysis Agent バージョン 1.20 または 1.21 によって収集された古いトークンリングトレンドデータを移行できません。これは、古いエージェントが、1 分ごとにサンプリングが行われたトレンドデータを収集するために固有の Token Ring MIB を実装しているからです。NetWare 版 Traffic Analysis Agent バージョン 1.3 は、過去のトレンド (1 分間、1 時間、および 1 日) をサポートする標準の Token Ring MIB を実装しています。

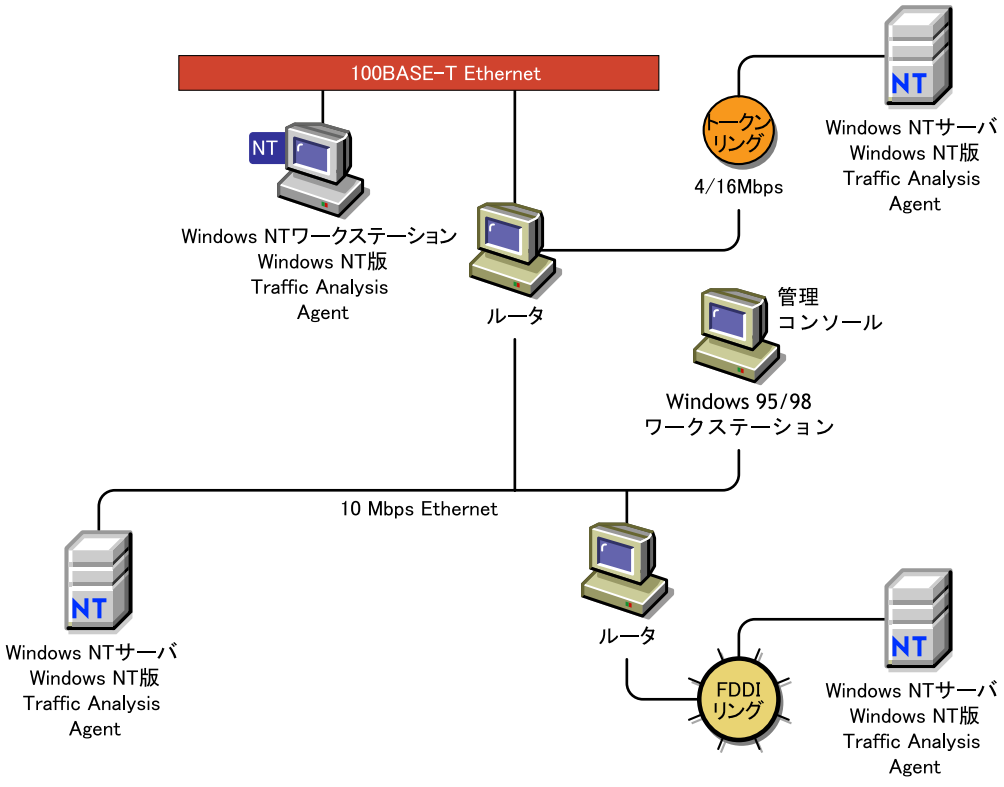
Windows 版 Traffic Analysis Agent の使用

Windows 版 Traffic Analysis Agent (バージョン 1.30) は、Windows サーバまたは Windows ワークステーションで実行されます。Windows 版 Traffic Analysis Agent は、Ethernet、FDDI、またはトークンリングセグメントのトラフィックを監視します。

Windows 版 Traffic Analysis Agent は、RMON MIB によって定義された機能を実装する RMON エージェントです。Windows 版 Traffic Analysis Agent は、トークンリングメディアに対する RMON (RFC 1513 (http://www.isi.edu/in-notes/rfc1513.txt)) のトークンリング拡張機能、FDDI メディアに対する Novell 固有 MIB、および Ethernet メディアに対する RMON (RFC 1757 (http://www.isi.edu/in-notes/rfc1757.txt)) を実装します。

これらのエージェントは、ネットワークのアクティビティに関する情報を収集します。この情報は、SNMP を使用して Novell ConsoleOne から利用できます。また、Windows 版 Traffic Analysis Agent は、RMON2 (RFC 2021 (http://www.isi.edu/in-notes/rfc2021.txt)) の最初の 2 つのグループを実装します。

次の図は、Windows 版 Traffic Analysis Agent の機能を示しています。



インストール時の変更

Windows 版 Traffic Analysis Agent をインストールすると、次のファイルが Windows にコピーされます。

ファイル名	場所	説明
lanzndis.sys	¥WINNT¥SYSTEM32¥DRIVERS	カーネルモードドライバインタフェース
lanzctl.dll	¥WINNT¥SYSTEM32	コントロールモジュール
lanzmem.dll	¥WINNT¥SYSTEM32	メモリマネージャモジュール
lanzlib.dll	¥WINNT¥SYSTEM32	ライブラリモジュール
lanzdi.dll	¥WINNT¥SYSTEM32	ユーザモードドライバインタフェース
lanzsm.dll	¥WINNT¥SYSTEM32	モニタモジュール
lanzhis.dll	¥WINNT¥SYSTEM32	履歴モジュール
lanzael.dll	¥WINNT¥SYSTEM32	アラーム、イベント、およびログモジュール
lanzfcb.dll	¥WINNT¥SYSTEM32	フィルタキャプチャ、バッファモジュール
lanztr.dll	¥WINNT¥SYSTEM32	トークンリングマネージャモジュール
lanzfddi.dll	¥WINNT¥SYSTEM32	FDDI マネージャモジュール

ファイル名	場所	説明
gtrend.dll	¥WINNT¥SYSTEM32	トレンドモジュール
lanzcon.exe	¥LANZNT	エージェントコンソールアプリケーション
lanzcon.chm	¥LANZNT	エージェントコンソールヘルプ
gtrend.exe	¥ZFS_AGNT¥LANZCON	古いエージェントからトレンドデータを移行するツール
mgmtapi.dll	¥ZFS_AGNT¥LANZCON	SNMP アプリケーションファイル
msvcp50.dll	¥ZFS_AGNT¥LANZCON	LANZCON に必要な MFC API
lanzctl.dll	¥ZFS_AGNT¥LANZCON	LANZCON に必要
msflxgrd.ocx	%SystemRoot%¥System32	LANZCON で ActiveX* コントロールを有効にします。

重要： LANZCON アプリケーションのデフォルトディレクトリの場所は、zfs_agnt¥lanzcon です。LANZCON の場所は、インストール時に変更できます。

次の節では、Windows 版 Traffic Analysis Agent の最適化および使用について説明します。

- 1064 ページの「Windows 版 Traffic Analysis Agent のインストール計画」
- 1067 ページの「Windows 版 Traffic Analysis Agent の最適化」
- 1070 ページの「LANZCON の使用」

Windows 版 Traffic Analysis Agent のインストール計画

Windows 版 Traffic Analysis Agent をインストールするには、Windows SNMP サービスを設定する必要があります。

Windows SNMP サービスのインストールと設定

Novell ZENworks Server Management エージェントをインストールする前に、Windows SNMP サービスをインストールおよび設定する必要があります。これは管理サーバとの通信を有効にするために必要となります。

SNMP を Windows にインストールおよび設定するには

1 SNMP サービスをインストールします。

1a コントロールパネルで、[ネットワーク] > [サービス] > [追加] の順にクリックします。

1b [ネットワークサービスの選択] ダイアログボックスから SNMP サービスを選択します。

1c [OK] をクリックします。

1d Windows 配布ファイルのフルパスを入力します。

1e [続行] をクリックします。

2 SNMP が自動的に起動するように設定します。

2a コントロールパネルで［サービス］をダブルクリックします。

2b［SNMP］>［スタートアップ］の順にクリックします。

2c［スタートアップの種類］オプションで、［自動］を選択します。

3 SNMP トラップサービスを自動的に開始するよう設定します。

3a コントロールパネルで［サービス］をダブルクリックします。

3b［SNMP Trap Service］>［スタートアップ］の順にクリックします。

3c［スタートアップの種類］オプションで、［自動］を選択します。

4 エージェントがトラップを管理サーバに送信できるよう、トラップのコミュニティ名と送信先アドレスを指定します。

4a コントロールパネルで［ネットワーク］をダブルクリックします。

4b［サービス］タブをクリックし、［SNMP Service］を選択します。

4c［プロパティ］をクリックします。

4d［トラップ］タブをクリックします。

4e［コミュニティ名］ボックスから名前を選択し、［追加］をクリックします。

利用可能なコミュニティ名がない場合、［追加］ボタンは無効になります。

4f パブリックコミュニティ名が存在しない場合は、「**public**」と入力します。

4g［追加］をクリックします。

4h トラップを受け取る必要のあるワークステーションやサーバのループバック IP アドレスの他に、別の DNS 名と IP アドレスを追加するには［トラップ送信先］ボックスを使用します。

4i［OK］をクリックします。

5 エージェントがすべてのホストからの SNMP パケットを受け付けるよう、SNMP セキュリティオプションのトラップコミュニティ名を設定します。

5a コントロールパネルで［ネットワーク］をダブルクリックします。

5b［サービス］タブをクリックし、［SNMP Service］を選択します。

5c［プロパティ］をクリックします。

5d［セキュリティ］タブをクリックします。

5e［受け付けるコミュニティ名］ボックスの［追加］をクリックします。

5f［コミュニティ名］ボックスで、「**public**」と入力します。

［受け付けるコミュニティ名］リストには、Windows が要求を受け入れるコミュニティ名が表示されます。

5g［追加］をクリックします。

5h［すべてのホストから SNMP パケットを受け付ける］を選択し、［OK］をクリックします。

Windows 2000 SNMP サービスのインストールおよび設定

Novell ZENworks Server Management エージェントをインストールする前に、Windows 2000 SNMP サービスをインストールおよび設定する必要があります。これは管理サーバとの通信を有効にするために必要となります。

SNMP を Windows 2000 にインストールおよび設定するには

1 SNMP サービスをインストールします。

1a コントロールパネルで、[管理ツール] を選択し、[Configure Your Server] を選択します。

1b [Application Server] オプションで、[Terminal Services] を選択します。

1c [Start] をクリックします。

1d Windows コンポーネントウィザードで、[管理とモニタ ツール] をダブルクリックします。

1e [簡易ネットワーク管理プロトコル] を選択します。

1f [OK] をクリックします。

1g [次へ] をクリックします。

インストール後、SNMP が自動的に開始されます。

2 SNMP トラップサービスを自動的に開始するよう設定します。

2a コントロールパネルで、[管理ツール] > [サービス] の順にクリックします。

2b [SNMP Trap Service] > [スタートアップ] の順にクリックします。

2c [スタートアップの種類] オプションで、[自動] を選択します。

3 エージェントがトラップを管理サーバに送信できるよう、トラップのコミュニティ名と送信先アドレスを指定します。

3a コントロールパネルで、[管理ツール] > [サービス] の順に選択します。

3b [SNMP サービス] をダブルクリックします。

3c [プロパティ] をクリックします。

3d [トラップ] タブをクリックします。

3e [コミュニティ名] ボックスから名前を選択し、[追加] をクリックします。

利用可能なコミュニティ名がない場合、[追加] ボタンは無効になります。

3f パブリックコミュニティ名が存在しない場合は、「**public**」と入力します。

3g [追加] をクリックします。

3h トラップを受け取る必要のあるワークステーションやサーバのループバック IP アドレスの他に、別の DNS 名と IP アドレスを追加するには [トラップ送信先] ボックスを使用します。

3i [OK] をクリックします。

4 エージェントがすべてのホストからの SNMP パケットを受け付けるよう、SNMP セキュリティオプションのトラップコミュニティ名を設定します。

4a コントロールパネルで、[管理ツール] > [サービス] の順にクリックします。

4b [SNMP サービス] をダブルクリックします。

4c［プロパティ］をクリックします。

4d［セキュリティ］タブをクリックします。

4e［受け付けるコミュニティ名］ボックスの［追加］をクリックします。

4f［コミュニティ名］ボックスから名前を選択します。

［受け付けるコミュニティ名］リストには、Windows 2000 が要求を受け入れるコミュニティ名が表示されます。

4g［追加］をクリックします。

4h［すべてのホストから SNMP パケットを受け付ける］を選択し、［OK］をクリックします。

重要： SNMP サービスのインストール後は、サービスパックを再インストールしてください。

Windows 版 Traffic Analysis Agent の最適化

Windows 版 Traffic Analysis Agent のパラメータを設定して、Windows のパフォーマンスを最適化できます。エージェントのパフォーマンスを、ネットワーク環境に応じて最適化できます。

この節では、Windows 用のエージェントコンソール (LANZCON) を使用して、エージェントを最適化し、Windows 版 Traffic Analysis Agent 機能を監視する方法について説明します。詳細については、1070 ページの「LANZCON の使用」を参照してください。

次の節では、Windows 版 Traffic Analysis Agent の設定オプションについて説明します。

- 1067 ページの「Windows 版 Traffic Analysis Agent の設定」
- 1068 ページの「Windows 版 Traffic Analysis Agent のモジュールの設定」
- 1068 ページの「Windows 版 Traffic Analysis Agent のパラメータの設定」
- 1069 ページの「SNMP サービスによってエージェントが自動的にロードされる」

Windows 版 Traffic Analysis Agent の設定

Windows 版 Traffic Analysis Agent には、モジュールやパラメータのデフォルト値が用意されています。デフォルト値を変更して、Windows 版 Traffic Analysis Agent のパフォーマンスを最適化できます。

Windows 版 Traffic Analysis Agent の次のモジュールを設定できます。

- Packet Capture
- Station Monitor
- Token Ring Manager
- FDDI Manager

詳細については 1068 ページの「Windows 版 Traffic Analysis Agent のモジュールの設定」を参照してください。

Windows 版 Traffic Analysis Agent の次のパラメータを設定できます。

- Memory Bound
- Memory Age

- Top N Station
- Generate Duplicate IP Address Alarms
- Trend Files Location

詳細については1068 ページの「Windows 版 Traffic Analysis Agent のパラメータの設定」を参照してください。

Windows 版 Traffic Analysis Agent のモジュールの設定

デフォルトでは、すべてのエージェントモジュールがロードされるように設定されています。モジュールを無効にすることを選択できます。

Windows 版 Traffic Analysis Agent のモジュールを無効にするには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Modules] > [Disable] の順にクリックします。

2 エージェントが監視するモジュールを選択解除します。

3 [OK] をクリックします。

Windows 版 Traffic Analysis Agent のパラメータの設定

Windows 版 Traffic Analysis Agent には、デフォルトのパラメータがロードされます。デフォルトのパラメータを変更し、エージェントのアプリケーションを最適化することができます。

次の表は、Memory Manager モジュールのパラメータについて説明しています。

パラメータ	デフォルト値	[Range]	説明
Memory Bound	4MB	1MB ～ 10MB	Windows 版 Traffic Analysis Agent に動的に割り当てることができる利用可能メモリ領域の上限を設定します。
Memory Age	168 時間	1 時間～ 720 時間	Windows 版 Traffic Analysis Agent がメモリにデータを格納する期間を制御します。 この時間が経過すると、既存のデータがメモリから削除されます。

Memory Bound パラメータを変更するには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Parameters] の順にクリックします。

2 [Memory Manager] タブをクリックします。

3 [Memory Bound] スライダを、Memory Bound の値として設定する位置に移動します。

Memory Age パラメータを変更するには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Parameters] の順にクリックします。

2 [Memory Manager] タブをクリックします。

3 [Memory Age] スライダを、Memory Age の値として設定する位置に移動します。

重要： 変更されたパラメータ値が反映されるように Windows 版 Traffic Analysis Agent を再起動します。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「Management and Monitoring Services のインストール」を参照してください。

次の表は、Station Monitor モジュールのパラメータについて説明しています。

パラメータ	デフォルト値	[Range]	説明
TopN Station	4 つのレポート	2 ～ 10 個のレポート	エージェントが生成できる TopN レポートの数を制御します。
Generate Duplicate IP Address Alarms	有効	-	重複する IP アドレスアラームの生成を制御します。

エージェントが生成する TopN レポートの数を指定するには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Parameters] の順にクリックします。

2 [Station Monitor] タブをクリックします。

3 TopN レポートの数を選択します。

重複する IP アドレスアラームが生成されないようにするには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Parameters] の順にクリックします。

2 [Station Monitor] タブをクリックします。

3 [Generate Duplicate IP Address Alarms] チェックボックスを選択解除します。

次の表は、Network Trend パラメータについて説明しています。

パラメータ	デフォルトのパス	説明
Trend Files Location	*system root*¥GTREND	トレンドファイル (*.GT) が作成および更新されるディレクトリのパスと場所を指定します。

重要： *.GT ファイルを削除すると、以前のすべてのトレンド情報が削除されます。

トレンドデータを保管する場所のパスを指定するには

1 LANZCON のメインメニューから、[Configure] > [Traffic Analysis Agent Parameters] の順にクリックします。

2 [Network Trends] タブをクリックします。

3 Windows 版 Traffic Analysis Agent でトレンドデータを保管する場所のディレクトリパスを入力するか、または参照して選択します。

SNMP サービスによってエージェントが自動的にロードされる

Traffic Analysis Agent は、Windows 上の Microsoft* SNMP サービスに依存します。SNMP が起動すると、アドレススペース内のエージェント DLL がロードされます。デフォルトでは、インストールされたエージェントは、SNMP サービスの起動時に常にロードされます。

SNMP によるエージェント DLL のロードを有効または無効にするには、[Novell Traffic Analysis Agent Loading with SNMP] ダイアログボックスで、必要なオプションのチェックボックスをオンまたはオフにします。エージェントを無効にすると、SNMP サービスは正常に起動しますが、Traffic Analysis Agent は動作しません。NIC カードを無差別モードに設定しても、Traffic Analysis Agent はパケットをキャプチャせず、SNMP 要求にも応答しません。

LANZCON の使用

この節では、LANZCON ユーティリティを使用して Windows 版 Traffic Analysis Agent を設定および診断する方法について説明します。

Windows 版 LANZCON は、Windows 版 Traffic Analysis Agent によって提供されたグラフィカルユーザインタフェースです。エージェントモジュールおよびパラメータを設定し、エージェントを診断するために使用します。LANZCON を使用すると、エージェントによって監視されているネットワークセグメントに関する情報を取得し、トラブルシューティングに役立てることができます。

LANZCON ユーティリティを開くには、次のいずれかの操作を行います。

- Windows の［プログラム］メニューから、［Traffic Analysis Agent for Windows］>［LANZCON］の順にクリックします。
- デスクトップ上の LANZCON アイコン  をダブルクリックします。

LANZCON ユーティリティで異なる SNMP コミュニティ文字列を使用するには、次の手順に従います。

1 lanzcon ディレクトリに移動します。

2 コマンドプロンプトで次のコマンドを入力します。

LANZCON <*community name*>

重要： コマンドライン引数を指定せずに LANZCON を起動する場合、デフォルトのコミュニティ文字列は PUBLIC です。

LANZCON では、次のタスクを実行できます。

- 1070 ページの「ネットワークアダプタの表示」
- 1071 ページの「ネットワークアダプタの監視を有効または無効にする」
- 1071 ページの「エージェントのログの表示」
- 1071 ページの「エージェントステータスの表示」
- 1072 ページの「RMON テーブルの表示」
- 1072 ページの「SNMP トラップの表示」

ネットワークアダプタの表示

LANZCON のロード時に、［Network Adapters］ウィンドウが表示されます。［Network Adapters］ウィンドウの 2 つのペインには、監視対象アダプタに関する情報が表示されます。

次の表は、［Network Adapters］ウィンドウの 2 つのペインについて説明しています。

ペイン	表示内容	説明
左側のペイン	［Adapter Tree］ビュー	Windows 版 Traffic Analysis Agent が検出したネットワークアダプタのリストが表示されます。 デフォルトのビューには展開されたツリーが表示されます。ツリーの各ネットワークアダプタを展開し、選択したアダプタの RMON テーブルのリストを表示することができます。

ペイン	表示内容	説明
右側のペイン	[Table] ビュー	左側のペインで選択したオブジェクトに関する詳細が表示されます。 左側のペインでアダプタを選択すると、選択したアダプタのメディアタイプ、MAC アドレス、説明などの、インタフェーステーブル (RFC 1213 (http://www.isi.edu/in-notes/rfc1213.txt)) の詳細が右側のペインに表示されます。 左側のペインで RMON テーブルを選択すると、テーブルデータが右側のペインに表示されます。

ネットワークアダプタの監視を有効または無効にする

Windows 版 Traffic Analysis Agent は、監視対象アダプタに関する情報を収集し、その情報を [Network Adapters] ウィンドウの右側のペインに表示します。

デフォルトでは、アダプタ監視は有効になっています。LANZCON を使用すると、アダプタ監視を無効にすることができます。アダプタ監視を無効にすると、Windows 版 Traffic Analysis Agent はアダプタに関するデータの収集を中止し、アダプタの RMON テーブルが削除されます。

重要： LANZCON で FDDI アダプタの監視を無効にすることはできません。

アダプタ監視を有効にするには

1 [Network Adapters] ウィンドウの左側のペインでアダプタを選択します。

2 [View] > [NetWork Adapters] > [Enable] の順にクリックします。

アダプタ監視を無効にするには

1 [Network Adapters] ウィンドウの左側のペインでアダプタを選択します。

2 [View] > [NetWork Adapters] > [Disable] の順にクリックします。

エージェントのログの表示

Windows 版 Traffic Analysis Agent は、セッションの実行中に発生した重大なイベントやエラーメッセージをログに記録します。

エージェントのログを表示するには

1 LANZCON のメインメニューで、[View] > [Agent Log] の順にクリックします。

エージェントステータスの表示

[Traffic Analysis Agent Status] ウィンドウでエージェントのステータスを表示できます。このウィンドウには、エージェントモジュールがロードされているか、またはロードされていないかが示されます。

エージェントのステータスを表示するには

1 LANZCON のメインメニューで、[View] > [Agent Status] の順にクリックします。

RMON テーブルの表示

各ネットワークアダプタの下に RMON テーブルが表示されます。RMON テーブルを表示するには、[Network Adapters] ウィンドウの左側のペインでテーブルを選択します。RMON テーブルデータが左側のペインに表示されます。

[Network Adapter] ツリーには次の RMON テーブルが表示されます。

- Statistics(統計情報)
- History Control
- History Data
- Host Control
- Host Entry
- Host TopN Control
- Host TopN Entry
- Matrix Control
- Matrix SD Entry
- Filter、Channel、および Buffer

[Alarm Information] ツリーには次の RMON テーブルが表示されます。

- Alarm
- イベント
- Log

SNMP トラップの表示

Windows 版 Traffic Analysis Agent は、ネットワークセグメントを監視し、トラップを管理サーバに送信します。Novell ConsoleOne は、管理サーバからトラップを受信したときにアラームを表示します。

トラップ情報は、[SNMP Traps] ウィンドウに表示されます。テーブルは、各トラップに対し取得できるトラップデータを表示します。

統計	説明
Receive Time	トラップが発生した時刻を表示します。
Trap Summary	トラップの説明を表示します。

重要： LANZCON は、Windows SNMP がループバックトラップ宛先アドレスにトラップを送信するように設定されている場合にトラップ通知を受信します。詳細については、1064 ページの「Windows 版 Traffic Analysis Agent のインストール計画」を参照してください。

LANZCON のメインメニューから SNMP トラップを表示するには、[View] > [SNMP Traps] の順にクリックします。

29 エージェントの環境設定のカスタマイズ

Novell® ZENworks® Server Management のサーバ管理 SNMP エージェントは、ネットワーク内の Novell NetWare® サーバおよび Windows* サーバで実行されます。このエージェントは、Novell ConsoleOne® からの要求に応じて履歴データおよび動的データを収集しながら、サーバを監視します。管理者は、Novell ZENworks Server Management Novell ConsoleOne で、サーバで検出されたデバイス、オペレーティングシステム、またはサービスを表すアイコンをクリックするだけでデータを要求できます。

NetWare 版 Management Agent および Windows 版 Management Agent をネットワークの NetWare サーバや Windows サーバにインストールすると、デフォルトの設定ですぐに使用することができます。多くの場合はこの設定で十分ですが、エージェントの設定をカスタマイズして、管理機能を向上させることができます。

この章は、次に示す節で構成されています。

- 1073 ページの「エージェントのファイル」
- 1076 ページの「NetWare 版 Management Agent のカスタマイズ」
- 1078 ページの「Windows サーバ版 Management Agent のカスタマイズ」
- 1080 ページの「サードパーティのエージェントの設定」
- 1081 ページの「Advanced Trending Agent」

エージェントのファイル

次の節では、各管理対象サーバにインストールされるエージェントのファイルについて説明します。

- 1073 ページの「NetWare 版 Management Agent のファイル」
- 1075 ページの「Windows サーバ版 Management Agent のファイル」

NetWare 版 Management Agent のファイル

次の表では、NetWare サーバにインストールされる NetWare 版 Management Agent の NLM™ ファイルについて説明します。

NetWare 版 Management Agent の NLM ファイル	説明
servinst.nlm	NetWare サーバ MIB (nwserver.mib) を実装します。
hostmib.nlm	標準的なホストリソース MIB [RFC 1514] およびこの MIB (nwhostx.mib) に対する Novell® の拡張機能を実装します。

NetWare 版 Management Agent の NLM ファイル	説明
ntrend.nlm	Threshold and Trend MIB (nwtrend.mib) を実装します。ntrend.nlm は、ロードされると、サーバの環境設定に従って監視する各属性のトレンドとしきい値を設定します。ntrend.ini ファイルには、ntrend.nlm の環境設定パラメータが含まれています。
nwtrap.nlm	NetWare Server Trap MIB (nwalarm.mib) を実装します。nwtrap.cfg ファイルには、nwtrap.nlm の環境設定パラメータが含まれています。
findnms.nlm	NetWare 版 Management Agent を実行している NetWare サーバによって使用されます。findnms.nlm を利用して、SAP (Service Advertising Protocol) 番号 0x026a を使って自分自身をアドバタイズする SNMP Management コンソールをリッスンします。次に、findnms.nlm は、検出された Novell ConsoleOne の IPX™ (Internetwork Packet Exchange™) アドレスを、トラップを受信するステーションのリストに追加します。
ndstrap.nlm	ndstrap.mib を実装して、Novell eDirectory のイベントをキャプチャし、SNMP Management コンソールに転送します。
mondata.nlm	NetWare サーバの監視を可能にします。

次の表で、NetWare 版 Management Agent に関連するエンタープライズ MIB について簡単に説明します。

MIB 名	説明
ndstrap.mib	Novell eDirectory のイベントをキャプチャし、SNMP トラップとして SNMP Management コンソールに転送するための Novell 独自の MIB。現在この MIB には 130 を超えるトラップが存在し、新しいトラップが識別されるたびに追加されます。
nwalarm.mib	NetWare Core OS のすべてのアラートを処理し、SNMP トラップとして転送する Novell 独自の MIB。現在、375 を超えるトラップをサポートしており、新しいトラップが識別されるたびに追加されます。
nwhostx.mib	RFC1514 (ホストリソース MIB) に対する Novell の拡張機能。RFC1514 には直接含まれていない、NetWare に固有のデバイスおよびコンポーネントを追加します。
nwserver.mib	NetWare Core OS 管理の基礎になる Novell 独自の MIB。この MIB では、300 を超えるオブジェクトが識別されています。GET と SET の両方について、コンソールから設定できるパラメータへのアクセスが定義されています。この MIB には、ユーザ、ファイルシステム、ボリューム、キュー、ODI™ (Open Data-Link Interface™)、設定パラメータなどについての複数のグループやテーブルが含まれています。
nwtmsync.mib	timesync.nlm の SNMP 管理を実現する Novell 独自の MIB。タイムソースおよびタイムクライアントのリストへのアクセスを提供します。この MIB を通じてクロック構造にもアクセスできます。
nwtrend.mib	一定の期間トラッキングした場合に最も有効であるオブジェクトのトラッキングを実行する Novell 独自の MIB。たとえば、CPU の使用率や受信パケット数は静的な数値としての価値は限られていますが、ある期間、定期的に監視すると、サーバで何が起こっているかがよくわかります。この MIB によって、管理対象オブジェクトについてユーザ定義のしきい値を設定することもでき、しきい値を超えたときには SNMP トラップが送信されます。

MIB 名	説明
rfc1514.mib	インターネット標準のホストリソース MIB。この MIB は、ディスク、メモリ、CPU、プリンタ、アダプタカードなどのシステムの物理コンポーネントを含む、ホストコンピュータに関する一般的なカテゴリを定義します。

Windows サーバ版 Management Agent のファイル

次の表は、テキストエディタで手動で設定して、Windows 版 Management Agent のデフォルトの動作を変更できるファイルのリストです。

Windows サーバ版 Management Agent の .INI ファイル	説明
n_nttren.ini	Windows 版 Management Agent によってサポートされているトレンドとしきい値の初期値を指定します。
nttrap.ini	Windows 版 Management Agent を実行する Windows サーバのトラブルシューティングを行うための設定および Windows のイベントを SNMP トラップとして管理システムに送信できるようにするための設定を指定します。
nthost.ini	Windows 版 Management Agent によってサポートされる SNMP 設定を指定します。
n_ntfmw.ini	無視され、SNMP トラップを受信しない IPX アドレスを指定できます。

次の表で、Windows 版 Management Agent に関連するエンタープライズ MIB について簡単に説明します。Windows 版 Management Agent は、すべての Windows システム、セキュリティ、およびアプリケーションイベントを SNMP トラップに変換します。

MIB 名	説明
ntserver.mib	サーバ名、OS、メジャーバージョンとマイナーバージョン、タイムゾーン、リモートボリュームとローカルボリュームの数など、最小限の Windows システム情報を提供します。
rfc1514.mib	インターネット標準のホストリソース MIB。この MIB は、ディスク、メモリ、CPU、プリンタ、アダプタカードなどのシステムの物理コンポーネントを含む、ホストコンピュータに関する一般的なカテゴリを定義します。
nttrap.mib	RFC1514 に基づく汎用 MIB。トラップに変換された Windows イベントは、Novell ZENworks Server Management ネットワーク管理システムに転送されます。
nttrend.mib	一定の期間トラッキングした場合に最も有効であるオブジェクトのトラッキングを実行する Novell 独自の MIB。たとえば、CPU の使用率や受信パケット数は静的な数値としての価値は限られていますが、ある期間、定期的に監視すると、サーバで何が起こっているかがよくわかります。この MIB によって、管理対象オブジェクトについてユーザ定義のしきい値を設定することもでき、しきい値を超えたときには SNMP トラップが送信されます。

NetWare 版 Management Agent のカスタマイズ

NetWare 版 Management Agent のインストールプロセスによって、nma2.ncf ファイル（Novell NetWare 3.*x* および 4.*x* サーバの場合）または nma5.ncf ファイル（Novell NetWare 5.*x* サーバの場合）が、sys:¥zfs_agnt¥nma ディレクトリに作成されます。NetWare サーバを起動すると、このファイルによって、NetWare 版 Management Agent をデフォルトの設定状態で使用するために必要なすべての NLM ファイルが自動的にロードされます。ただし、このエージェントで使用される各 NLM ファイルについて、いくつかの LOAD パラメータを設定できます。

サーバ上の nma2.ncf または nma5.ncf ファイルを編集することによって、これらのオプションを使用するようにサーバを設定できます。サーバがすでに実行中である場合は、これらの NLM ファイルをアンロードし、NetWare サーバコンソールで設定パラメータを指定してロードすることもできます。これらのパラメータは、NetWare サーバコンソールで設定するか、または NetWare リモートコンソールユーティリティ RCONSOLEJ を使用して設定できます。

次の節では、NetWare 版 Management Agent について設定できる各コマンドラインパラメータについて説明します。

- 1076 ページの「servinst.nlm のロードパラメータ」
- 1077 ページの「hostmib.nlm のロードパラメータ」
- 1077 ページの「ntrend.nlm のロードパラメータ」

servinst.nlm のロードパラメータ

servinst.nlm は NetWare Server MIB である nwserver.mib を実装します。コマンドラインで、次のいずれかまたはすべてのパラメータを指定して servinst.nlm をロードできます。

LOAD SERVINST D, U=n, V, B=n H

パラメータ	説明
D	DisableSets: このパラメータを指定した場合、servinst.nlm は nwserver.mib 内のオブジェクトについて SNMP SET コマンドを許可しません。 デフォルト :SETS は有効です（SNMP セキュリティを前提とします）。
U=*n*	UpdateInterval=*n*: リストの更新間隔を *n* に設定します。*n* は秒単位の値です。これによって、servinst.nlm によって保持されている特定の内部リスト（ボリュームやキューなど）を更新する頻度が決まります。このパラメータの値を大きくすると、servinst.nlm によって使用される CPU サイクル数が最小化されます。値を小さくすると、リストに影響するサーバステータスの変化がすぐにレポートされます。 デフォルト :300 秒。
V	Verbose: 情報メッセージを表示します。 デフォルト：オフ。
B=*n*	BuildUserListHour=*n*: 毎日、servinst.nlm ソフトウェアがサーバへのアクセス権を持つユーザのリストを作成する時刻を 24 時間表記 (0 ～ 23) のローカルタイムで指定します。 デフォルト :2（午前 2 時）。

パラメータ	説明
H	Help: コマンドラインパラメータのヘルプを表示します。H パラメータを使用する場合、servinst.nlm はヘルプメッセージを表示して終了します。コマンドラインで他のパラメータが入力されている場合でも、ロードされたままにはなりません。 デフォルト：オフ。

hostmib.nlm のロードパラメータ

hostmib.nlm は、標準的なホストリソース MIB (RFC 1514) と、このホストリソース MIB に対する Novell の拡張機能 (nwhostx.mib) の両方を実装します。コマンドラインで、次のいずれかまたはすべてのパラメータを指定して hostmib.nlm をロードできます。

LOAD HOSTMIB.NLM D, U=n, V, H

パラメータ	説明
D	DisableSets: このパラメータを指定した場合、hostmib.nlm は RFC1514.MIB または nwhostx.mib 内のオブジェクトについて SNMP SET コマンドを許可しません。 デフォルト :SETS は有効です (SNMP セキュリティを前提とします)。
U=*n*	UpdateInterval=*n*: リストの更新間隔を *n* に設定します。*n* は秒単位の値です。これによって、HOSTMIB.NLM によって保持されている特定の内部リストを更新する頻度が決まります。このパラメータの値を大きくすると、HOSTMIB.NLM によって使用される CPU サイクル数が最小化されます。値を小さくすると、リストに影響するサーバステータスの変化がすぐにレポートされます。 デフォルト :60 秒。
V	Verbose: 情報メッセージを表示します。 デフォルト：オフ。
H	Help: コマンドラインパラメータのヘルプを表示します。H パラメータを使用する場合、HOSTMIB.NLM はヘルプメッセージを表示して終了します。コマンドラインで他のパラメータが入力されている場合でも、ロードされたままにはなりません。 デフォルト：オフ。

ntrend.nlm のロードパラメータ

ntrend.nlm は Threshold and Trend MIB (nwtrend.mib) を実装します。

ntrend.nlm は、最初にロードされたときに、ntrend.ini ファイル (sys:¥etc ディレクトリにある) に格納されている値から、サーバの設定に従って監視対象の各属性のトレンドとしきい値を自動的に設定します。このファイルの編集方法については、913 ページの「デフォルトのトレンドとしきい値の設定」を参照してください。

その後、時間の経過と共に設定が変更された場合、ntrend.nlm は、物理的なネットワークインタフェース、キュー、ボリューム、およびディスクの数および種類の変更を調整します。デフォルトのしきい値は、重要なパラメータについてのみ設定されています。後で SNMP SET コマンドを使用して、読み込まれたファイルや受信パケットなどのパラメータのしきい値を設定できます。

トレンドファイルは、そのオブジェクトのトレンド分析が無効になっている場合でも、監視対象属性の各インスタンスについて作成されます。ファイルヘッダには nwtControlTableEntry のすべての情報が格納され、ファイルの残りの部分にはサンプル履歴（存在する場合）が格納されます。作成されたトレンドファイルは、監視対象オブジェクト（キューなど）が存在しなくなっても、オペレータによって明示的に削除されるまで存在しています。監視対象オブジェクトが存在しなくなった場合、関連付けられた nwtControlStatus は無効として記録されます。

コマンドラインで、次のいずれかまたはすべてのパラメータを指定して ntrend.nlm をロードできます。

LOAD NTREND D=dir, R, V, H

パラメータ	説明
D=*dir*	Directory=*dir*:ntrend.nlm が履歴データファイルを格納するボリュームおよびディレクトリを指定できます。例：トレンド分析ファイルのディレクトリとして vol1:¥test を使用するには、次のコマンドを入力します。 **load ntrend D=vol1:\test** デフォルト：sys:¥ntrend。
R	Reset:ntrend.nlm で、古いトレンド分析の履歴データをすべて破棄し、サンプリングを再開します。
V	Verbose: 情報メッセージを表示します。 デフォルト：オフ。
H	Help: コマンドラインパラメータのヘルプを表示します。 デフォルト：オフ。

Windows サーバ版 Management Agent のカスタマイズ

次のファイルを手動で編集して、管理対象 Windows サーバ上の Windows 版 Management Agent のデフォルトの設定を変更できます。

Windows サーバ版 Management Agent の .INI ファイル	説明
n_ntfmw.ini	無視され、SNMP トラップを受信しない IPX アドレスを指定できます。
nttrap.ini	管理対象 Windows サーバのトラブルシューティングを行うための設定、および管理システムに SNMP トラップとして送信する Windows イベントの種類を指定するトラップフィルタを構成するための設定を指定します。 トラップフィルタの設定およびトラップ生成の詳細については、917 ページの「アラーム生成の管理」を参照してください。 Server Management Agent は、1079 ページの「カスタムイベントログタイプからのイベント収集」および 1080 ページの「Nttrap.ini ファイルにおける否定のフィルタ条件の指定」によって強化されています。

Windows サーバ版 Management Agent の .INI ファイル	説明
n_nttren.ini	Windows 版 Management Agent によってサポートされているトレンドとしきい値の初期値を指定します。 デフォルトのトレンドおよびしきい値の変更の詳細については、913 ページの「デフォルトのトレンドとしきい値の設定」を参照してください。

Windows サーバ版 Management Agent の設定

デフォルトでは、Windows 版 Management Agent は、SAP (Service Advertising Protocol) ID 0x026 をブロードキャストして、IPX ネットワーク上の SNMP Management コンソールにトラップを送信します。n_ntfmw.ini ファイルを編集して、トラップのターゲットとして含めない SNMP Management コンソールの IPX アドレスを追加できます。

トラップの自動受信の対象から除外するために SNMP Management コンソールの IPX アドレスを追加するには

1 テキストエディタで n_ntfmw.ini ファイルを開きます。

2 次の構文を使用して、除外する SNMP Management コンソールの IPX アドレスを追加します。

xxxxxxxx.yyyyyyyyyyyy

ここで、*xxxxxxxx* はネットアドレス、*yyyyyyyyyyyy* はノードアドレスであり、01014044.00001B4DDAFD のように指定します。

3 ファイルを保存し、Windows 版 Management Agent を再起動します。

カスタムイベントログタイプからのイベント収集

Server Management Agent for Windows は、Windows イベントログからイベントを収集し、こうしたイベントをトラップに変換します。変換されたトラップはサイトサーバに転送されます。

Windows 版 Server Management Agent では、nttrap.ini を使用してカスタムイベントログタイプを指定し、DNS サーバ、ディレクトリサービスログ、ファイルレプリケーションサービスログなどからトラップを収集できます。

1 *installation_path*¥zfs_agnt¥ntagent¥ini ディレクトリから nttrap.ini ファイルを開きます。

2 ファイル内の指示に従って、[Monitor Settings] セクションでカスタムログタイプのイベントを有効にします。

3 nttrap.ini ファイルを保存します。

Nttrap.ini ファイルにおける否定のフィルタ条件の指定

Server Management Agent for Windows を使って、否定の条件を指定できるようになりました。

nttrap.ini ファイルで否定のフィルタ条件を指定するには

1 *installation_path*¥zfs_agnt¥ntagent¥ini ディレクトリから nttrap.ini ファイルを開きます。

2 [Available Filters] セクションで、否定のフィルタ条件を指定します。たとえば、ID が 500 以外のイベントを収集するように指定します。

3 [Actual Filters] セクションで、これらのフィルタを有効にします。

4 nttrap.ini ファイルを保存します。

サードパーティのエージェントの設定

サードパーティの SNMP エージェントでトラップを受信するには、次の作業を完了しておく必要があります。

- 1080 ページの「トラップを受信できることの確認」
- 1080 ページの「ベンダ固有の SNMP トラップの統合」

トラップを受信できることの確認

ネットワークデバイス上の SNMP エージェントや SNMP Remote Network Monitoring (RMON) エージェントを設定するときに、エージェントのトラップの送信先リスト (トラップターゲットリスト) に、Novell ZENworks Server Management 管理サーバステーションの IP アドレスまたはサーバ名を含めます。この設定方法については、エージェントのマニュアルを参照してください。Novell ConsoleOne には、アラームを管理サーバに転送するすべてのデバイスのアラームが表示されます。

ネットワークデバイスで NetWare 版 Management Agent、Windows サーバ版 Management Agent、NetWare 版 Traffic Analysis ® Agent™、または Windows 版 Traffic Analysis Agent を使用している場合、エージェントのトラップの送信先リストは自動的に設定されます。トラップの送信先リストの設定に関して、設定情報については 862 ページの「検出のセットアップ」を、RMOM エージェントの設定については 28 章 981 ページの「トラフィック分析の理解」を参照してください。

ベンダ固有の SNMP トラップの統合

アラーム管理システムでアラームを処理する前に、サードパーティの SNMP エージェント用のベンダ固有の MIB を、管理サーバの MIB プールに含める必要があります。ベンダの MIB でトラップの定義に注釈を付けることによって、サードパーティの SNMP エージェントをさらに統合することができます。

アラーム管理システムでは、ASN.1 の注釈を MIB のトラップ定義として解釈して、アラームに割り当てられる重要度のレベルとデバイスのステータスを設定します。Novell ZENworks Server Management に含まれている MIB には、すでに適切な注釈が含まれています。注釈によって、重要度のレベルやデバイスのステータスについての詳細がアラーム管理システムに伝えられます。

管理サーバの MIB プールに MIB を追加したり、サードパーティの MIB に注釈を付ける方法については、26 章 951 ページの「MIB ツールの使用」を参照してください。

Advanced Trending Agent

この節では、次のトピックについて説明します。

- 1081 ページの「Advanced Trending Agent について」
- 1081 ページの「トレンド変数の設定」
- 1082 ページの「Linux 上での Advanced Trending Agent の設定」
- 1083 ページの「すべてのプラットフォーム上でのAdvanced Trending Agentの設定」
- 1084 ページの「クイックリファレンステーブル」
- 1085 ページの「設定の更新」
- 1086 ページの「Advanced Trending Agent のインストール」

Advanced Trending Agent について

Advanced Trending Agent は、SNMP エージェントによって計測されるパラメータが MIB 変数により定義されており、単なる設定済み MIB 変数ではない場合に、そのパラメータのトレンドデータ（履歴データ）を収集および格納するアプリケーションです。

Advanced Trending Agent の機能は、NetWare、Windows、および Linux プラットフォームで利用できます。

Advanced Trending Agent は、設定済みの MIB 変数のサンプルを定期的に収集して格納します。収集されたデータは SNMP インタフェースを通じて表示されます。このデータを使用して、パラメータの長期的なトレンドグラフを表示できます。

設定ファイルまたは SNMP インタフェースを使用して Advanced Trending Agent を設定できます。Advanced Trending Agent には、更新のために設定ファイルを読み込むコマンドラインユーティリティが含まれています。このユーティリティは収集されたデータをリセットし、新しいデータの収集を開始します。Advanced Trending Agent でパラメータのしきい値を設定し、値がしきい値を超えた場合にトラップを生成することもできます。

トレンド変数の設定

Advanced Trending Agent は、設定ファイルで指定されている MIB 変数に関するトレンド分析を開始します。

- **NetWare の場合：** *installation_path*/advtrend/advtrend.ini ファイル
- **Windows の場合：** *installation_path*/advtrend/ini/advtrend.ini ファイル
- **Linux の場合：** /etc/opt/novell/Novell ZENworks/zfs-mms-advtrend.conf ファイル

内容を変更して、トレンド分析する新しいパラメータを追加したり、既存のパラメータを変更したりできます。設定ファイルは標準的な INI 形式に従います。

セクション名には任意の値を使用できますが、通常は設定するパラメータについてのわかりやすい名前です。特定のファイル内のすべてのセクション名は区別できる必要があります。

重要： セクションの名前は変更できません。セクション名を変更すると、そのパラメータのデータは失われ、新しいデータが収集されます。

キーの名前は変更できません。各キーは、そのパラメータのトレンド分析アクティビティを定義する特定の設定を表します。任意のセクションについて定義する必要がある必須キーがあります。このようなキーが存在しない場合、Advanced Trending Agent ではセクション全体が無視されます。

設定キーのセットで、一部のキーは必須キーとして処理されます。必須設定キーのデータが指定されている場合や、特定の設定エントリが破棄された場合、その設定エントリは読み込み専用になります。

標準的なセクションは次のようになります。

```
[Interface In-Octets]
MIBVariable=1.3.6.1.2.1.2.2.1.10.1
MIBVariable Type=1
MIBVariableTrendingStatus=1
MIBVariableDisplayName=Interfaces
SampleInterval=5
SampleType=1
Buckets=80
ThresholdRising=100
ThresholdFalling=60
AlarmType=1
AlarmSeverity=4
ThresholdAlarmGenerationStatus=1
IdentifierOID={1.3.6.1.2.1.2.2.1.10.3}
Filters=2
F1={I1=MS TCP Loopback interface}
F2={I1=3COM 3C920 Integrated Fast Ethernet Controller 3C905C-TX Compatible) -
Packet Scheduler Miniport}
FilterType=1
```

次の必須キーを指定する必要があります。

```
MIBVariable (key 1)
SampleInterval (key 5)
ThresholdRising (key 8, only if ThersholdAlarmGenerationStatus=1)
ThresholdFalling (key 9, only if ThersholdAlarmGenerationStatus=1)
AlarmType1 (key 10, only if ThersholdAlarmGenerationStatus=1)
```

詳細については、1084 ページの「クイックリファレンステーブル」を参照してください。

Linux 上での Advanced Trending Agent の設定

Linux 上で Advanced Trending Agent を起動する前に、次の作業を完了していることを確認してください。

- 1083 ページの「ローカルホストの SNMPv1/SNMPv2c アクセスの有効化」
- 1083 ページの「SNMP v1 トラップをサイトサーバに送信するためのトラップシンクの設定」
- 1083 ページの「Advanced Trending Agent によって使用されるデフォルトのコミュニティ文字列の変更」

ローカルホストの SNMPv1/SNMPv2c アクセスの有効化

snmpd マスタエージェントが Advanced Trending Agent に対して SNMPv1/v2c 読み込み専用アクセスを許可するように、snmpd マスタエージェントを設定する必要があります。

1 snmpd マスタエージェントによって使用される snmpd.conf ファイルを編集します。

2 アクセス制御の設定により、OID ツリー全体（.1 から始まる）でのローカルホストへの SNMPv1/SNMPv2c アクセスが許可されていることを確認します。

詳細については、SNMP Frequently Asked Question (http://www.net-snmp.org/FAQ.html) の「How do I configure access control?」を参照してください。

SNMP v1 トラップをサイトサーバに送信するためのトラップシンクの設定

Advanced Trending Agent によって生成されたトラップがサイトサーバに送信されるように、snmpd マスタエージェントを設定する必要があります。

1 snmpd.conf ファイルを編集します。

2 サイトサーバを指すトラップシンクを設定する行を追加します。

トラップシンクを設定するための特定の構文については、man snmpd.conf (5) マニュアルページを参照してください。

Advanced Trending Agent によって使用されるデフォルトのコミュニティ文字列の変更

ローカルホストの SNMPv1/SNMPv2c アクセスの有効化でアクセスを許可するために使用したコミュニティ文字列と同じ文字列を使用するように Advanced Trending Agent を設定する必要があります。

1 /etc/opt/novell/Novell ZENworks/zfs-mms-advtrend.conf 設定ファイルを編集します。

2 Agent Config セクションで、*ReadCommunity* キーの値を、SNMPv1/SNMPv2c アクセスを許可した適切なコミュニティ文字列に設定します。

すべてのプラットフォーム上での Advanced Trending Agent の設定

Advanced Trending Agent を設定するには、デフォルトのパージ間隔を変更する必要があります。

Advanced Trending Agent は、利用できる特定の MIB 変数または一部の SNMP テーブルのインスタンスについて自動的にトレンド分析を行います。これらのインスタンスが利用できなくなった場合、そのトレンド分析に関連付けられたリソースをクリーンアップすることができます。Advanced Trending Agent でこのようなクリーンアップを行うまでのパージ間隔を設定する必要があります。

1 設定ファイルを編集します。

- **NetWare の場合：** *installation_path*/advtrend/advtrend.ini ファイル
- **Windows の場合：** *installation_path*/advtrend/ini/advtrend.ini ファイル
- **Linux の場合：** /etc/opt/novell/Novell ZENworks/zfs-mms-advtrend.conf ファイル

2 Agent Config セクションで、PurgeInterval キーの値を秒単位の値に設定します。

クイックリファレンステーブル

次の表は、キーの値とその意味のクイックリファレンスです。

キー名	説明	許容値	必須	デフォルト値
MIBVariable	トレンド分析する変数	SNMP OID 値の任意の整数	Yes	なし
MIBVariableType	変数がスカラであるか、SNMP テーブルの列であるか	1（スカラ）、2（列）	No	1
MIBVariableTrendingStatus	トレンド分析が有効であるか、無効であるか	1（有効）、2（無効）	No	2
MIBVariableDisplayName	[Console] ビューからこの変数を参照するための名前	任意の文字列	No	オブジェクト
SampleInterval	サンプルを取得する時期を示す秒単位の時間間隔	正の整数	Yes	なし
SampleType	格納されたサンプルが絶対値であるか、デルタであるか	1（絶対値）、2（デルタ）	-	-
Buckets	変数を格納するサンプルの数	正の整数	No	50
ThresholdAlarmGenerationStatus	トラップを送信するかどうか	1（有効）、2（無効）	No	2
ThresholdRising	サンプル値が初めてしきい値を上回り、AlarmType 値が上昇に設定されている場合に、トラップを送信する	整数	ThresholdAlarmGenerationStatus が有効の場合、はい	なし
ThresholdFalling	サンプル値が初めてしきい値を下回り、AlarmType 値が降下に設定されている場合に、トラップを送信する	整数	ThresholdAlarmGenerationStatus が有効の場合、はい	なし
AlarmType	ThresholdRising または ThresholdFalling 値を超過した場合にトラップを生成するかどうか	1（上昇）、2（降下）	ThresholdAlarmGenerationStatus が有効の場合、はい	なし
AlarmSeverity	送信されるトラップの重大度	1 重大 2 メジャー 3 マイナー 4 情報 5 不明	No	3

キー名	説明	許容値	必須	デフォルト値
IdentifierOID	MIBVariableType 2 の OID の場合に、テーブル内の行を一意に識別する	書式設定された文字列	No	なし
Filters	指定するフィルタ条件の数	1 ～ 5 の整数	No	なし
FilterType	フィルタに一致する SNMP 行をトレンド分析するか、無視するか	1 包含（含める）、2 除外（無視する）	No	1

設定の更新

Advanced Trending Agent では、1 つまたは複数の MIB 変数のトレンド分析アクティビティのパラメータを動的に変更できます。設定ファイルで、トレンド分析の対象になる新しいエントリを追加したり、既存のエントリを削除したりできます。

変更を行った後、advtrend コマンドを実行して、Advanced Trending Agent で最新情報を取得する必要があります。advtrend コマンドは、次の場所で利用できます。

- **Windows の場合：** *install_directory*/zfs_agnt
- **Linux の場合：** /opt/novell/Novell ZENworks/bin

advtrend コマンドを使って、次の操作を実行します。

- 1085 ページの「情報のリセット」
- 1085 ページの「トレンド分析のための新しいパラメータの追加」
- 1086 ページの「既存のトレンド分析対象パラメータの削除」
- 1086 ページの「既存のパラメータのキー値の変更」

情報のリセット

パラメータのトレンド分析を再開するには

1. 設定ファイルを変更して設定セクションを追加、変更、または削除します。
2. サーバプロンプトで、「**advtrend reset**」と入力します。

設定に従って、新しいエントリによって既存のエントリが置換されます。トレンド分析は最初から開始されます。

警告： 情報をリセットすると、古いデータは失われます。

トレンド分析のための新しいパラメータの追加

1. 設定ファイルを編集して、パラメータの新しいセクションを追加します。
2. 新しいセクションで必要なキーを定義します。
3. NetWare のサーバプロンプトで、「**advtrend reread**」と入力します。Windows または Linux の場合は、「**advtrend read_cfg**」と入力します。

トレンド分析の対象になる新しいエントリが追加されます。

既存のトレンド分析対象パラメータの削除

1. 設定ファイルを編集して、トレンド分析しているパラメータを表すセクションを削除します。
2. NetWare のサーバプロンプトで、「**advtrend reread**」と入力します。Windows または Linux の場合は、「**advtrend read_cfg**」と入力します。

この設定セクションのトレンド分析されるエントリが削除されます。

既存のパラメータのキー値の変更

トレンド分析する MIB 変数のキーの値を変更する場合は、次の操作を行います。

1 設定ファイルを編集して、キーの値を変更します。

2 NetWare のサーバプロンプトで、「**advtrend reread**」と入力します。Windows または Linux の場合は、「**advtrend read_cfg**」と入力します。

Advanced Trending Agent で新しいパラメータが使用されます。

次のパラメータを変更する場合は、以前のデータは削除されます。

MIBVariable
MIBVariableType
SampleInterval
SampleType
IdentifierOID

Advanced Trending Agent のインストール

詳細については、『*Novell ZENworks Server Management インストールガイド*』を参照してください。

Management and Monitoring Services for Linux

Novell ZENworks Server Management for Linux の Management and Monitoring Services コンポーネントは、ネットワーク上の Linux サーバを一元管理する機能を提供します。

すべてのリアルタイム統計情報および履歴情報を Novell ConsoleOne® からビューとして表示できます。重要なイベントについて生成されたトラップを管理したり、Linux サーバに関する履歴情報を取得して Novell ConsoleOne からビューとしてすべての情報を表示したり、Linux サーバの全体的な稼動状況に関するレポートを生成したりできます。

Management and Monitoring Services の Linux Management Agent を使用することによって、Linux サーバに関するすべての情報を管理および監視できます。

リアルタイム統計情報の提供

Linux Management Agent は、サーバの重要なリソースに関するリアルタイム統計情報を収集して提供する SNMP エージェントです。

Linux Management Agent は、次の統計情報を提供します。

- プロセッサの統計情報

- システムレベルのメモリの使用状況
- ディスクの使用状況および統計情報
- パーティションの使用状況の統計情報
- 開始されたサービスの統計情報
- プロセス情報
- ユーザログインの統計情報
- カーネルキャッシュ情報
- ディスクパーティションの統計情報
- システムのページングおよびスワッピング
- さまざまなプロセッサの割り込みの統計情報

設定ファイルのカスタマイズ

zfs-mms-servinst.conf ファイルを使用して、リアルタイム統計情報を監視するように Linux Management Agent をカスタマイズできます。zfs-mms-servinst.conf ファイルで自動的に監視されるサービスのリストを変更できます。

1 /etc/opt/novell/Novell ZENworks/ ディレクトリにある zfs-mms-servinst.conf ファイルを開きます。

2 Monitored Services セクションで、サービスのリストにサービス名を追加またはリストから削除します。

3 zfs-mms-servinst.conf ファイルを保存します。

4 snmpd を再起動します。

システムイベントのトラップの生成

Linux Management Agent は、実行中のサーバプロセスに関する重要で重大なイベントを収集します。イベントの重大度に基づいて、トラップが生成され、サイトサーバに転送されます。Linux Management Agent には、これらのイベントについてさまざまなカテゴリのシステムログを監視する novell-trapd サービスが含まれています。システムログから収集されるイベントのカテゴリには、次のようなものがあります。

- ユーザログイン
- ルートログインの失敗
- サービスの開始 / 停止 / 再開
- ログに記録された重要なカーネルイベント

設定ファイルのカスタマイズ

zfs-mms-log2trap.conf ファイルを使用して、トラップが生成されるイベントを監視するように Linux Management Agent をカスタマイズできます。

次のような方法があります。

トラップが転送されるホストのリストの変更

1 /etc/opt/novell/Novell ZENworks/ ディレクトリにある zfs-mms-log2trap.conf ファイルを開きます。

2 TrapTargets セクションで、トラップを送信するホストの IP アドレスを追加します。同じ行に、トラップを送信するために使用する SNMP コミュニティ文字列を追加します。

3 zfs-mms-log2trap.conf ファイルを保存します。

4 novell-trapd サービスを再起動します。

特定のシステムログメッセージに対するトラップ生成の防止

zfs-mms-log2trap.conf ファイルを使用して、特定のシステムログメッセージについてトラップが生成されるのを防止できます。設定ファイルにセクションを作成し、次のキーを追加します。

キー名	説明	指定できる値
Severity	無視するログメッセージの重大度。	◆ CRITICAL ◆ MAJOR ◆ MINOR ◆ INFORMATIONAL ◆ MISCELLANEOUS ◆ ALL
Constraints	ログメッセージでサブ文字列を検索する方法を定義します。サブ文字列が指定された条件を満たす場合、このログメッセージは無視されます。	指定できる値は、オプションの CASE_COMPARE と、CONTAINS、ENDS_WITH、または BEGINS_WITH のいずれかです。 オプションの CASE_COMPARE は、大文字と小文字を区別して文字列を検索する必要があるかどうかを指定します。その他の値は、それぞれ、文字列がログ内、ログの最後、ログの先頭に含まれている必要があるかどうかを指定します。
string *number*	検索対象の文字列を定義します。*number* の値をインクリメントすることによって、このようなキーを必要な数だけ定義できます。これらの値のいずれかに一致するメッセージは無視されます。	任意の文字列。

例文字列 telnet を含むすべてのログメッセージの除外

1 /etc/opt/novell/Novell ZENworks/ ディレクトリにある zfs-mms-log2trap.conf ファイルを開きます。

2 設定ファイルにセクションを作成します。たとえば、[Telnet Reject] を作成します。

3 次のキーと値を追加します。

```
severity = ALL
constraints = CASE_COMPARE
string1 = telnet
```

4 _Reject Setting Names_ セクションを検索し、作成したセクション名を追加します。たとえば、Telnet Reject を追加します。

5 設定ファイルを保存します。

6 novell-trapd サービスを再起動します。

例重大度の値が Info で、文字列 127.0.0.1 または localhost を含むすべてのメッセージを除外

1 /etc/opt/novell/Novell ZENworks/ ディレクトリにある zfs-mms-log2trap.conf ファイルを開きます。

2 設定ファイルにセクションを作成します。たとえば、[Localhost] を作成します。

3 次のキーと値を追加します。

```
severity = INFO
constraints = CASE_COMPARE
string1 = 127.0.0.1
string2 = localhost
```

4 _Reject Setting Names_ セクションを検索し、作成したセクション名を追加します。たとえば、Localhost を追加します。

5 設定ファイルを保存します。

6 novell-trapd サービスを再起動します。

履歴収集情報の提供

Linux Management Agent は、Linux オペレーティングシステムについて追加情報を提供する SNMP 機能を実装しています。SNMP インタフェースの情報を使用して、Linux オペレーティングシステムの次の属性を取得できます。

- CPU 使用率
- 使用メモリおよび使用スワップサイズ
- ディスクの空き容量
- ネットワークインタフェースの統計情報（受信および送信パケット数）
- ディスクの読み書き
- ログインユーザ数

Advanced Trending Agent を使用して、これらのパラメータに関する定期的な統計情報のサンプリングを設定および制御できます。Advanced Trending Agent を使用して、これらの属性についてトラップを生成するしきい値を設定することもできます。

Advanced Trending Agent の詳細については、1081 ページの「Advanced Trending Agent」を参照してください。

[Linux Management] ビュー

Unified View for Devices を使用して、ネットワーク上のすべての Linux デバイスを一覧表示できます。

Linux では次のビューが作成され、Linux サーバに関する詳細情報にアクセスできます。

- Node Summary
- Processor Statistics and Trend
- Storage Devices Summary and Trend
- Running Software
- Interrupt Summary Node
- Memory Statistics and Trend
- Network Interface Statistics and Trend
- Currently Logged-in Users and Trend
- Services Started by the Node

[Linux Management] ビューは、NetWare サーバおよび Windows サーバに関するビューと似ています。

Linux Server Health Report

Linux Server Profile という新しいプロファイルがプロファイルのリストに追加され、レポートを生成できるようになります。このレポートによって、Linux サーバの全体的な稼動状況に関する情報を取得できます。Linux Server Health Report を使用すると、日ごと、週ごと、月ごとにレポートを生成できます。

30 Novell ZENworks Server Management でサポートされるプロトコルデコードスイート

Novell ZENworks® Server Management には、ネットワークアクティビティを分析し、ネットワークの問題の原因を特定するためのパケットキャプチャツールやデコードツールが用意されています。パケットのキャプチャおよびデコードによって、セグメントアクティビティに関する詳細情報を取得し、ネットワークの問題を解決することができます。詳細については、1017 ページの「パケットのキャプチャ」および 1021 ページの「キャプチャされたパケットの表示」を参照してください。

この章では、Novell ZENworks Server Management でサポートされる次のプロトコルスイートのデコードについて説明します。

- 1091 ページの「Novell NetWare プロトコルスイート」
- 1093 ページの「Network File System プロトコルスイート」
- 1094 ページの「Systems Network Architecture プロトコルスイート」
- 1094 ページの「AppleTalk プロトコルスイート」
- 1096 ページの「TCP/IP プロトコルスイート」

Novell NetWare プロトコルスイート

Novell NetWare® には、Novell NetWare ネットワークでさまざまな機能を実行するプロトコルのグループが含まれています。Novell NetWare プロトコルスイートの各プロトコルは、IPX™ プロトコルと共に機能します。Novell ZENworks Server Management では、Novell NetWare プロトコルスイートの次のプロトコルをサポートしています。

Novell NetWare プロトコル	説明
BCAST	Novell NetWare Broadcast Message Notification。Novell NetWare サーバが、アイドルワークステーションに、メッセージが保留になっていることを通知するために使用するプロトコル。このメッセージは、DOS ステーションのモニタの先頭または最後の行に表示されます。
DIAG	Diagnostic Responder。接続状態のテストおよび情報の収集に使用されるプロトコル。デフォルトでは、Novell NetWare クライアントは、Diagnostic Responder を使用して診断要求に応答します。

Novell NetWare プロトコル	説明
IPX	Internetwork Packet Exchange™。ネットワーク上で送信データパケットをルーティングするプロトコル。各 Novell NetWare ネットワークには、サーバを設定したときに、一意のアドレスが割り当てられます。IPX ルータは、このアドレスを使用して、インターネットワークを通じてパケットをルーティングします。 IPX では、RIP (Routing Information Protocol) によって集計された情報に基づいてルーティングを決定します。
LSP	Novell NetWare Lite™ Sideband Protocol。Novell NetWare Lite Transport Protocol (NLTP) 接続のサイドバンドとして機能する接続レス (データグラム) 指向プロトコル。
NBIOS	NetBIOS。IBM* NetBIOS 呼び出しをサポートするアプリケーションをワークステーションで実行できるようにするエミュレータ。NetBIOS は、トークンリングネットワーク上でピアツーピア通信を実行するように開発されたアプリケーション用の IBM 標準プロトコルです。
NCP™	Novell NetWare Core Protocol™。ワークステーションの要求を受け付けて応答するためにファイルサーバのオペレーティングシステムが従うプロシージャのセット。 NCP は、ワークステーションがファイルサーバに要求するすべてのサービスについて存在します。NCP プロトコルによって処理される一般的な要求には、ファイルの作成や削除、ディレクトリやファイルの操作、ディレクトリの一覧表示、バインダリ (ドライブマッピングやセキュリティ) の変更、および印刷があります。
NDS®	NDS プロトコルは、NDAP (Novell Directory Access Protocol) と呼ばれ、Novell eDirectory がクライアントの要求にサービスを提供し、クライアントの要求を他の Novell eDirectory サーバに送信できるようにするワイヤプロトコルです。NDAP は NCP に基づいて構築されています。
NLP	Novell NetWare Lite Protocol。Novell NetWare Lite の中心になるプロトコルであり、Novell IPX プロトコル上で動作します。NLP は、ファイルシステムおよび印刷の機能を実行するアプリケーション層およびサービス層のプロトコルです。NLP は、NCP で使用される転送プロトコルと類似した機能の NLTP も使用します。
NLSP™	Novell NetWare Link Services Protocol™。IPX インターネットワーク用に設計されたリンクステートルーティングプロトコル。
RIP	Routing Information Protocol。ルーティングテーブルの更新処理を自動化するプロトコル。ルーティングは、独立したネットワーク間でネットワークパケットを移動する処理です。RIP を使用することによって、あるルータがそのルートの変更を認識したときに、隣接するルータにこの情報をブロードキャストし、隣接するルータがルーティングテーブルを更新できるようにします。これによって、ネットワークコンポーネント (ルータや電話回線) に障害が発生した場合、他のネットワークコンポーネントは相互に代替ルートを通知できます。障害の発生したコンポーネントが修復されると、ネットワークは元の状態に戻ります。
SAP	Service Advertising Protocol。Novell NetWare サーバが名前と種類によってサービスをアドバタイズできるようにするプロトコル。ワークステーションは要求をブロードキャストして、利用できるすべてのサービスを検索したり、クライアントに最も近い特定のサービスを検索したりできます。

Novell NetWare プロトコル	説明
SER	Novell Serialization (Copy Protection) Packets。各サーバが一意のシリアル番号を持っていることを確認するために Novell NetWare サーバが他の Novell NetWare サーバに送信するパケット。
SNMP	Simple Network Management Protocol。ネットワークデバイス間で管理情報の交換を容易にするために設計されたアプリケーション層のプロトコル。SNMP を使用して管理情報データ (1 秒あたりのパケット数やネットワークエラー率など) にアクセスすることによって、ネットワーク管理者は容易にネットワークのパフォーマンスを管理し、ネットワークの問題を検出して解決できます。
SPX™	Sequenced Packet Exchange™。ネットワーク伝送を監視して、正常なパケットの配信を保証する接続指向の転送プロトコル。SPX は、ネットワークで送信されるデータを監視することによって IPX プロトコルを強化します。SPX では、一連の個別パケットで構成されるデータ伝送をトラッキングできます。 SPX では通信相手に確認を要求し、通信相手に確認を返すことによって、正常なデータ配信を保証します。指定した時間内に確認要求に対して応答がない場合、SPX は要求を再送信します。再送信を何度か行っても肯定応答が得られない場合、SPX は接続に障害が発生していると見なし、エラーをレポートします。 Novell NetWare プリントサーバは SPX を使用します。
WDOG	Watchdog。Novell NetWare で提供される保守プロトコル。Watchdog は、Novell NetWare サーバにログインしているステーションを監視します。Watchdog は、Novell NetWare シェルがまだ動作しているかどうかを判断し、動作していない場合は、接続を解放します。

Network File System プロトコルスイート

次の表では、Network File System (NFS) プロトコルスイートについて説明します。

Network File System プロトコル	説明
MOUNT	MOUNT プロトコルは、NFS と組み合わせて使用され、NFS クライアントがリモートディレクトリツリーをローカルファイルシステム内のポイントに接続できるようにするオペレーティングシステム固有の機能を実行します。
NFS	Network File System。このプロトコルは、ネットワークを介して共有ファイルシステムへの透過的なリモートアクセスを提供します。NFS は RPC (Remote Procedure Call) を使用し、コンピュータ、オペレーティングシステム、ネットワークアーキテクチャ、および転送プロトコルに依存しません。
PORTMAP	PORTMAP プロトコルは、RPC プログラム番号を TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ポート番号に変換します。クライアントが特定のプログラム番号に対して RPC 呼び出しを行う場合、クライアントは、まずリモートコンピュータ上の PORTMAP に問い合わせて、RPC パケットを送信するポート番号を特定します。

Network File System プロトコル	説明
RPC	Remote Procedure Call。このプロトコルは、あるコンピュータ上のプログラムがリモートコンピュータ上のサブルーチンを呼び出すことができるようにします。各サブルーチンやリモートプロシージャは、一意のプログラム番号によって識別されます。

Systems Network Architecture プロトコルスイート

次の表では、Systems Network Architecture (SNA) プロトコルスイートについて説明します。

Systems Network Architecture プロトコル	説明
RH	Request/Response Header。このプロトコルは、SNA Request/Response Unit をペイロードとして伝送します。
RU	Request/Response Unit。SNA クライアントは、このプロトコルを使用して SNA サーバと通信します。
TH	Transmission Header。このプロトコルはデータリンク層で実行され、SNA Path Information Unit の伝送層として機能します。
XID	Exchange Station Identification。SNA ノードはこのプロトコルを使用して、ピア SNA ノードで通信の準備ができているかどうかをチェックし、ピア SNA ノードとステーションの詳細情報を交換します。

AppleTalk プロトコルスイート

次の表では、AppleTalk* および AppleTalk 関連のプロトコルスイートについて説明します。

AppleTalk プロトコル	説明
AARP	Address Resolution Protocol。データリンクプロトコルとプロトコルファミリの他のプロトコルとの間で、アドレス指定の違いを調停する AppleTalk プロトコル。たとえば、イーサネットのアドレス指定方式と AppleTalk のアドレス指定方式の違いを解決することによって、AARP は高速 EtherTalk* 接続での DDP (Datagram Delivery Protocol) パケットの転送を容易にします。
ADSP	AppleTalk Data Stream Protocol。AppleTalk インターネットワーク内の 2 つのソケット間で、信頼性の高い、全二重、バイトストリームサービスを提供する接続指向プロトコル。ADSP は、その接続上で、連続的で、重複のないデータ配信を保証します。
AEP	AppleTalk Echo Protocol。AppleTalk インターネットワーク内のあるノードが他のノードにパケットを送信し、エコーされたそのパケットのコピーを受信できるようにする単純なプロトコル。
AFP	AppleTalk Filing Protocol。ファイルサーバなどの AppleTalk 共有リソース内に存在するデータファイルやアプリケーションをユーザが共有できるようにするプレゼンテーション層のプロトコル。

AppleTalk プロトコル	説明
ASP	AppleTalk Session Protocol。ATP (AppleTalk Transaction Protocol) のサービスを使用して、要求の順序付けと共に、セッションの確立、維持、およびティアダウンを提供する汎用プロトコル。
ATP	AppleTalk Transaction Protocol。ソケット間で損失のないトランザクションサービスを提供する転送プロトコル。このサービスによって、2 つのソケットクライアント間での交換が可能になり、あるクライアントが別のクライアントに特定のタスクの実行や結果のレポートを要求できるようになります。ATP は要求と応答をバインドして、信頼性の高い要求と応答の交換を保証します。
E-DDP	Extended Datagram Delivery Protocol。拡張ヘッダを使用するデータグラム配信プロトコル。拡張ヘッダは、AppleTalk インターネット内のあるネットワークから別のネットワークに送信されるパケットで必要です。
ELAP	EtherTalk Link Access Protocol。EtherTalk ネットワークで使用されるリンクアクセスプロトコル。標準的なイーサネットデータリンク層の上に構築されます。
NBP	Name Binding Protocol。文字列名を対応するソケットクライアントのインターネットワークアドレスに変換するトランスポート層のプロトコル。NBP は、このような名前と対応するソケットアドレスをマップする変換テーブルを提供および管理することによって、AppleTalk プロトコルでユーザ定義のゾーンやデバイス名が認識されるようにします。
PAP	Printer Access Protocol。このプロトコルは、ワークステーションとプリントサーバとのやり取りを管理します。このプロトコルは、接続の設定、維持、および終了を処理します。データ転送も処理できます。
RTMP	Routing Table Maintenance Protocol。この AppleTalk プロトコルは、インターネットワークルータがインターネットワーク内の送信元ソケットから送信先ソケットにデータグラムをルーティングするために必要とするルーティング情報を確立および維持します。RTMP を使用することによって、インターネットワークルータは動的にルーティングテーブルを管理し、インターネットワークトポロジの変化に対応することができます。
S-DDP	Short Datagram Delivery Protocol。ショートヘッダを使用する DDP。ショートヘッダは、通常、送信元ソケットと送信先ソケットが単一の AppleTalk ネットワークの境界内にあるパケットで使用されます。
ZIP	Zone Information Protocol。インターネットワーク内の最新のルーティング情報を管理するプロトコル。

TCP/IP プロトコルスイート

次の表では、TCP/IP プロトコルスイートについて説明します。

TCP/IP プロトコル	説明
ARP	Address Resolution Protocol。ホストが別のホストのハードウェアアドレスを調べるために使用するプロトコル。TCP/IP システムには、IP アドレスをインターネットワーク上のホストとルータのハードウェアアドレスにマップするテーブルが含まれています。このテーブルは、IP アドレスをイーサネットアドレスに変換するホストテーブルと同じように機能します。ただし、ホストテーブルとは異なり、通常、ユーザやネットワーク管理者は ARP テーブルを管理しません。ARP プロトコルは、必要に応じて、このテーブルにエントリを作成します。 送信先のハードウェアアドレスがステーションの ARP テーブル内に見つからない場合、ネットワーク上の各ホストにこのアドレスを要求するブロードキャストが送信されます。そのホストが稼動しており、ARP プロトコルをサポートしている場合、ステーションからブロードキャストを受信したホストは、ステーションにハードウェアアドレスを送信することによって応答します。このアドレスが、ステーションの ARP テーブルに追加されます。
IMAP	IMAP は Internet Message Access Protocol を意味します。このプロトコルは、メールサーバ (共有されている場合もある) に保存されている電子メールまたは電子掲示板のメッセージにアクセスするための方法です。このプロトコルによって、電子メールの「クライアント」プログラムは、ローカルの場合と同様にリモートメッセージストアにアクセスできます。
BOOTP	BootStrap Protocol。このプロトコルによって、ディスクレスワークステーションでは、RARP (Reverse Address Resolution Protocol) を使用せずに、IP アドレスおよびその他の情報を設定できます。
DHCP	Dynamic Host Configuration Protocol。このプロトコルは、ホストに設定パラメータを提供し、動的に割り当てられた IP アドレスをリースし、BOOTP の拡張として機能します。
DNS	Domain Name System。インターネット上で使用される分散ネーミングサービス。コンピュータのドメイン名が存在する場合、DNS はコンピュータの IP アドレスを提供します。
FTP	File Transfer Protocol。ファイル転送をサポートする TCP/IP のアプリケーション層のプロトコル。
HTTP	Hypertext Transfer Protocol。Web ブラウザと Web サーバが互いに通信するために使用するアプリケーション層のプロトコル。
ICMP	Internet Control Message Protocol。IP と連携して、ルーティングの効率性やエラーの情報を提供するプロトコル。ICMP は TCP/IP プロトコルスイートの一部です。IP は接続レスであるため、インターネットワークの異常な状態を検出できません。ICMP は IP と連携し、TCP や他の上位層のプロトコルにこの情報を提供します。
IGMP	Internet Group Management Protocol。IP ホストがマルチキャストグループメンバーシップをルータにレポートするために使用するプロトコル。このプロトコルは、メンバーシップをルータに照会する場合や、グループメンバーシップに関するレポートを生成する場合にも使用されます。グループメンバーシップが終了した場合は、このプロトコルを使用して迅速にレポートすることができます。

TCP/IP プロトコル	説明
IP	Internet Protocol。インターネットワークでトランスポート層のパケット（トランスポートプロトコルデータユニットまたは TPDU とも呼ばれる）の接続レス、非保証の配信を行うプロトコル。IP は TCP/IP プロトコルスイートの一部です。 IP は、必要に応じて、TPDU をさらに小さい単位に分割し、中間ステーション（通常はルータ）または送信先ホストで再構築します。 各 TPDU または分割されたデータには IP ヘッダが付けられ、下位層のプロトコルによってパケットとして送信されます。IP は、一度に 1 ホップずつ、インターネットワークを通じてデータグラムを移動します。TPDU の断片が順序に関係なく送信先に到着した場合は、送信先では IP によって断片が正しい順序で再構築されます。
LDAP	Lightweight Directory Access Protocol。このプロトコルは、DAP (Directory Access Protocol) のリソースの要件を満たしていない場合でも、x.500 ディレクトリへのアクセスを提供します。LDAP は、特に、x.500 ディレクトリに対する読み書き操作のアクセスを実現する単純な管理アプリケーションやブラウザアプリケーションを対象としており、DAP 自体を補完することを目的としています。
NFS	NFS (Network File System) プロトコルは、ネットワーク上の共有ファイルへの透過的なリモートアクセスを実現します。NFS プロトコルは、異なるコンピュータ、オペレーティングシステム、ネットワークアーキテクチャ、および転送プロトコル間で移植できるように設計されています。この移植性は、XDR (eXternal Data Representation) 上で構築された RPC (Remote Procedure Call) プリミティブを使用することによって実現されています。
NTP	Network Time Protocol。分散タイムサーバとクライアントのセット間で、時間の計測を同期するために使用されるプロトコル。このプロトコルは、サーバからクライアントに階層化された方法で時間の情報を伝えるために使用されます。クロックを相互に確認したり、機器や伝達の障害によるエラーを制御するためにも使用されます。
NWIP	Novell NetWare/IP。Novell NetWare ネットワークで、IPX トランスポートサブシステムを全面的または部分的に、業界標準の TCP/IP サブシステムに置き換えることができるようにします。このテクノロジの中心的なコンポーネントは次のとおりです。 ◆ Novell NetWare/IP サーバと DSS (Domain SAP/RIP Service) 間の通信。これにより次のことが実現されます。 - 設定パラメータの取得 - SAP および RIP 情報の登録 - SAP/RIP データベースの同期 ◆ Novell NetWare/IP サーバと DSS データベースとの SAP/RIP 情報に関する同期。 ◆ 2台のサーバ間でSAP/RIPデータベースを同期するためのセカンダリ DSS とプライマリ DSS 間の通信。
OSPF	Open Shortest Path First。内部ゲートウェイプロトコルアルゴリズムであり、インターネットの標準として提案されている、TCP/IP プロトコルスイート内のプロトコル。OSPF には、最小コストルーティング、マルチパスルーティング、負荷分散、および効率的な帯域幅の使用が組み込まれています。

TCP/IP プロトコル	説明
POP3	Post Office Protocol 3。中央メールボックスサーバを操作するために使用されるプロトコル。このプロトコルは、電子メールを受信するために使用されるクライアント / サーバプロトコルです。このプロトコルでは、電子メールメッセージをインターネットサーバに保持します。定期的に、このサーバからメッセージをダウンロードできます。
RARP	Reverse Address Resolution Protocol。ハードウェアアドレスに基づいてソフトウェアアドレスを特定するために使用される、TCP/IP プロトコルスイートのプロトコル。このプロトコルは、通常、ディスクレスワークステーションの起動時に使用されます。
RIP	Routing Information Protocol。ルーティングテーブルの更新処理を自動化する、Novell NetWare プロトコルスイートのプロトコル。ルーティングは、独立したネットワーク間でネットワークパケットを移動する処理です。RIP を使用することによって、あるルータがそのルートの変更を認識したときに、隣接するルータにこの情報をブロードキャストし、隣接するルータがルーティングテーブルを更新できるようにします。RIP によって、ネットワークコンポーネント (ルータや電話回線) に障害が発生した場合、他のネットワークコンポーネントは相互に代替ルートを通知できます。障害の発生したコンポーネントが修復されると、ネットワークは元の状態に戻ります。
SSL	SSL はオープンで一般的なプロトコルです。SSL は、インターネット上の World Wide Web ブラウザおよびサーバの標準的なセキュリティのアプローチとしての検討事項として、W3 Consortium (W3C) のワーキンググループに提出されました。
SLP	Service Location Protocol。このプロトコルは、ネットワークサービスの発見と選択についてスケーラブルなフレームワークを提供します。このプロトコルを使用することによって、インターネットを利用するコンピュータで、ネットワークベースのアプリケーションと同じ数のネットワークサービスの静的な設定を保持する必要がなくなります。
SMTP	Simple Mail Transfer Protocol。電子メールクライアントとサーバが電子メールメッセージを相互に交換するために使用するアプリケーション層のプロトコル。
SNMP	Simple Network Management Protocol。SNMP Manager と呼ばれる単一のネットワーク管理ステーションからネットワークを監視できるようにする、TCP/IP プロトコルスイートのプロトコル。SNMP Manager から、SNMP Agent と呼ばれる別のネットワークデバイスに照会することができます。SNMP Agent は、TCP/IP ホスト、ルータ、ターミナルサーバ、または別の SNMP Manager である場合があります。 SNMP Agent に要求できる情報は、その TCP/IP ホストの MIB に格納されています。RFC 1066 (http://www.isi.edu/in-notes/rfc1066.txt) (インターネット標準 MIB) で、SNMP Agent MIB に格納できるオブジェクトの種類が定義されています。このようなオブジェクトには、ネットワークやハードウェアのアドレス、カウンタ、統計情報、およびルーティングテーブルや Address Resolution Protocol テーブルが含まれます。ベンダによって、MIB ですべてのデータタイプをサポートしていない場合や、RFC で定義されていないその他の情報を含めている場合があります。
TCP	Transmission Control Protocol。このプライマリインターネットトランスポートプロトコルは、上位層のプロトコルから任意の長さのメッセージを受け取り、全二重、確認応答あり、接続指向、フロー制御ありの転送を提供します。

TCP/IP プロトコル	説明
TELNET	文字指向のターミナルトラフィックを制御する TCP/IP スイートのプロトコル。
TFTP	Trivial File Transfer Protocol。ソフトウェアのダウンロードで一般的に使用される TCP/IP プロトコル。
UDP	User Datagram Protocol。接続レス、非保証のトランスポートサービスを提供する、TCP に類似したプロトコル。UDP は、上位層のプロトコルからデータグラムを受け取って転送します。接続の確立および削除、データフローの制御、およびその他の TCP 機能の負荷がないので、通常、UDP は TCP よりも高速なデータ経路を提供します。このような理由と、実装が容易であることから、上位層の多くのプロトコルで転送方法として使用されます。

31 Novell ZENworks Management and Monitoring Services データベース

Novell ZENworks® Server Management では、Management and Monitoring Services 管理サーバ上に一元化された CIM (Common Information Model) 準拠の Sybase* データベースが用意されています。このデータベースはサーバおよびネットワークのデータのリポジトリとして機能し、ネットワークの管理に必要な情報を適切に提供するために、データをさまざまな方法で表示または書式設定できます。

次の節では、Novell ZENworks データベースの概要と使用方法について説明します。

- 1101 ページの「Novell ZENworks Server Management データベースの理解」
- 1102 ページの「データベースのバックアップ」
- 1102 ページの「データベースパスワードの変更」

Novell ZENworks Server Management データベースの理解

Novell ZENworks Server Management データベースは、管理サーバ上の ¥Novell ZENworks¥MMS¥DB ディレクトリにあるファイルで構成されます。Novell ZENworks Server Management のデータは、次の論理データベースに格納されます。

- 次のファイルに関連するトポロジ、アラーム、およびマップ情報を格納するトポロジ / アラームデータベース。
  - MW.DB
  - MW1.DB
  - MW2.DB
  - MW3.DB

  ¥Novell ZENworks¥MMS¥DB サブディレクトリにある MW.LOG ファイルには、データベースファイルに関するトランザクション情報が保存されます。

データベースの実行

このデータベースは、サーバボリュームの ¥system ディレクトリにある mgmtdbs.ncf ファイルを使用して実行されます。mgmtdbs.ncf ファイルは autoexec.ncf から実行されます。

重要： Novell ZENworks Server Management サービスの実行中は、データベースを実行しておいてください。

データベースのキャッシュ

データベースのキャッシュを大きくすると、データベースのパフォーマンスが向上します。デフォルトでは、データベースのキャッシュサイズは 48MB です。サーバのメモリ容量に応じて、キャッシュサイズを最適なレベルまで大きくすることができます。キャッシュサイズを大きくするには、sys:¥system¥mgmtdbs.ncf で **-c** オプションを変更します。たとえば、**-c 64M** はキャッシュサイズを 64 MB に設定します。キャッシュサイズを変更した後、データベースを再ロードします。

データベースのバックアップ

Novell ZENworks Server Management データベースは、定期的なバックアップを計画する必要があります。

- 1102 ページの「トポロジ / アラームデータベースのバックアップ」

トポロジ / アラームデータベースのバックアップ

トポロジ / アラームデータベースをバックアップするには、Novell ConsoleOne で次の手順に従ってください。

1. サイトサーバオブジェクトを右クリックし、[Properties] を選択します。
2. [Database Administration] タブをクリックします。
3. バックアップするディレクトリのパスを入力します。

   データベースファイルは、管理サーバ上の任意のボリュームにバックアップできます。
4. [Apply] をクリックします。

   Novell ZENworks Server Management によって、ファイルを保存するリモート SQL コマンドが送信されます。4 つの MW*.DB ファイルと mw.log ファイルが、バックアップディレクトリにコピーされます。

データベースパスワードの変更

Novell ZENworks Server Management では、Administrator アカウント、Updater アカウント、および Reader アカウントの 3 つの異なるレベルで、トポロジ / アラームデータベースにアクセスできます。3 種類のユーザアカウントのそれぞれについてパスワードを設定できます。

データベースパスワードを変更するには、Novell ConsoleOne で次の手順に従ってください。

1. サイトサーバオブジェクトを右クリックし、[Properties] を選択します。
2. [Change Database Passwords] タブをクリックします。
3. 新しいパスワードを入力し、確認します。
4. [Apply] をクリックします。

   Novell ZENworks Server Management によって、データベース内の適切なユーザオブジェクトのパスワードを変更するためのリモート SQL コマンドが送信されます。このパスワードは、Novell eDirectory にも保存されます。

データベースを空にする

Novell ZENworks Server Management では、使用中の現在のデータベースを空にして、空のデータベースを使用できます。現在使用しているデータベースファイルは Novell ZENworks¥mms¥db ディレクトリにあります。データベースを空にするには、次の手順に従ってください。

1. Novell ZENworks¥mms¥emptydb ディレクトリ内のすべてのファイルを選択します。
2. Novell ZENworks¥mms¥emptydb ディレクトリのすべてのファイルを Novell ZENworks¥mms¥db ディレクトリにコピーします。

32 Management and Monitoring Servicesでのレポートの使用

Novell ZENworks® Server Management and Monitoring Services には、次のような定義済みのレポートが用意されています。

- トポロジレポート
- アラームレポート
- ヘルスレポート

次の節では、利用できるレポートについて説明し、レポートのカスタマイズおよび生成の手順を示します。

- 1105 ページの「Management and Monitoring Services のレポートの理解」
- 1111 ページの「レポートの管理」

Management and Monitoring Services のレポートの理解

次の節では、Management and Monitoring Services で利用できる定義済みの各レポートについて説明します。

- 1105 ページの「トポロジレポートについて」
- 1108 ページの「アラームレポートについて」
- 1109 ページの「ヘルスレポートについて」

トポロジレポートについて

トポロジレポートは、選択した Novell ZENworks Server Management Site、セグメント、またはカスタムアトラスコンテナのトポロジに関する情報を提供します。サイトレベルのレポートには、Novell ZENworks Server Management サイトの各セグメントで発見されたデバイスに関する詳細が示されます。セグメントレベルのレポートには、選択したネットワークセグメントで発見されたデバイスに関する情報が示されます。カスタムアトラスコンテナレポートには、選択したコンテナ内のコンピュータシステムに関する情報が示されます。

レポートを生成する前に、いくつかの作業を行う必要があります。詳細については、1106 ページの「レポートを生成するための前提条件」を参照してください。

定義済みのトポロジレポートは 5 つあります。

- 1106 ページの「Computer Systems by Segment レポート」
- 1107 ページの「NCP Servers レポート」
- 1107 ページの「Router レポート」

- 1107 ページの「Segment レポート」
- 1108 ページの「Segment Topology レポート」

注： NCP Servers レポートは、サイトレベルでのみ使用できます。

カスタムアトラスレポートには、レポーティングが起動された現在のコンテナにあるノードの情報が表示され、サブレベルのコンテナにあるノードの情報は表示されません。

レポートを生成するための前提条件

Crystal Reports はシステム上の DLL によって呼び出されるので、Sybase ODBC ドライバをインストールする必要があります。ドライバがインストールされているかどうかを確認するには、次の手順に従ってください。

1 デスクトップの［スタート］メニューから、［設定］>［コントロールパネル］>［ODBC データソース］の順にクリックします。

1a ［System Data Source Name (DSN)］ペインで、［Add］をクリックします。

1b Adaptive Server Anywhere ドライバを選択します。システムに Adaptive Server Anywhere が存在しない場合は、Adaptive Server Anywhere をインストールする必要があります。companioncd¥odbc¥sybase¥*.* にある SYBASE.ZIP ファイルからインストールできます。

2 古いバージョンの Novell ZENworks Server Management が存在している場合は、レポートを実行する前に古いバージョンをアンインストールして、最新バージョンの Novell ZENworks Server Management をインストールする必要があります。

以前のバージョンをアンインストールするには

2a デスクトップの［スタート］メニューから、［設定］>［コントロールパネル］>［プログラムの追加と削除］の順にクリックします。

2b リストから［Novell ConsoleOne］を選択し、削除します。

すでに最新バージョンをインストールしている場合は、Novell ConsoleOne¥LIB¥ZEN から zenSnapins.jar ファイルを削除します。

3 Crystal Reports を実行するには、特に Windows コンピュータ上で実行する場合は、MDAC 2.6 SP1 (Microsoft Data Access Component) 以降が必要です。ご自分のコンピュータにインストールされている MDAC のバージョンを確認します。［コントロール パネル］>［ODBC データ ソース］の順に選択し、［バージョン情報］タブペインを選択します。最低限必要なバージョンは 3.520.7326.0 です。使用しているバージョンが最低要件を満たしていない場合、ODBC のコアコンポーネントを Microsoft サイト (http://microsoft.com/data/download.htm) からダウンロードしてアップグレードする必要があります。

Computer Systems by Segment レポート

このレポートには、選択したセグメント上のコンピュータシステムの数が一覧表示されます。このレポートをサイトレベルで生成した場合、レポートには各セグメント上のシステム数が一覧表示されます。各セグメントについて、このレポートには、接続されている各コンピュータシステムに関する次の情報が示されます。

- セグメント名
- セグメントタイプ
- セグメント上の合計ノード数
- ノード名

- ノードアドレス
- サービス
- MIB

NCP Servers レポート

このレポートには、選択した Novell ZENworks Server Management サイトの各サーバについて次の情報が一覧表示されます。

- サーバ名
- サイトの NCP サーバの合計数
- サーバラベル
- サーバアドレス
- ラベル（サーバを識別するためのその他の名前）
- MIB

Router レポート

このレポートには、選択した Novell ZENworks Server Management のセグメントまたはサイトの各ルータについて次の情報が一覧表示されます。

- セグメントまたはサイトのルータの合計数
- IPX アドレス
- 境界セグメント
- サービス
- MIB
- IP Address
- MAC Address

Segment レポート

このレポートには、選択したセグメント上のコンピュータシステムの数（セグメントレベルの場合）、または Novell ZENworks Server Management サイトのすべてのセグメント上のコンピュータシステムの数（サイトレベルの場合）が一覧表示されます。各セグメントについて、このレポートには、セグメントに接続されているシステムに関する次の情報が示されます。

- セグメント名
- セグメントタイプ
- サイトの合計セグメント数
- IP 設定
- IPX 設定
- セグメント上の合計ノード数

Segment Topology レポート

このレポートには、選択した Novell ZENworks Server Management のセグメントまたはサイトのルータまたはブリッジに関する情報が一覧表示されます。

各ルータについて、このレポートには次の情報が示されます。

- ルータ名
- IP Address
- IPX アドレス
- MAC Address
- 境界セグメント

このレポートには、各ブリッジに関する次の情報が示されます。

- ブリッジ名
- ブリッジタイプ
- ポート数
- ポート :MAC アドレスおよび境界セグメント

アラームレポートについて

アラームレポートには、Novell ZENworks Server Management サーバが受信したアラームに関する情報が示されます。生成できるアラームレポートには、詳細レポートと概要レポートの 2 つの種類があります。

ここでは、次の内容について説明します。

- 1108 ページの「レポートを生成するための前提条件」
- 1108 ページの「Alarms Details レポート」
- 1109 ページの「Alarms Summary レポート」
- 1109 ページの「サイトに関する Available Trap Information レポート」

注 : カスタムアトラスでは、レポーティングが起動された現在のコンテナにあるノードからのアラーム情報のみがレポートされ、サブレベルのコンテナにあるノードからのアラーム情報は表示されません。

レポートを生成するための前提条件

Crystal Reports はシステム上の DLL によって呼び出されるため、Sybase ODBC ドライバがインストールされていることを確認してください。詳細については、『*Novell ZENworks 6.5 Server Management インストールガイド*』の「&ODBC ドライバのインストール」を参照してください。

Alarms Details レポート

このレポートには、サイトに関するアラームの情報が一覧表示されます。このレポートは、カスタマイズした設定に基づいて生成されます。このレポートには、接続されている各コンピュータシステムに関する次の情報が示されます。

- アラームの重要度
- 影響を受けるオブジェクトの名前
- ソースアドレス

- アラームの状態
- アラームのカテゴリ
- アラームの生成者
- アラームの時刻
- アラームの所有者
- アラームタイプ
- アラームの概要

Alarms Summary レポート

このレポートには、サイトに関するアラームの概要が示されます。このレポートでは、選択した日数について、アラームの分布が視覚的に表示されます。このレポートには、接続されている各コンピュータシステムに関する次の情報が示されます。

- アラームの重要度
- アラームのカテゴリ
- アラームの所有者
- アラームの状態
- 上位のアラームタイプ
- 上位の影響を受けるオブジェクト
- 上位のソースアドレス

サイトに関する Available Trap Information レポート

Available Trap Information レポートには、サイトサーバで現在使用できる SNMP トラップの情報が一覧表示されます。このレポートはサイトサーバに関してコンパイルされた MIB に基づいて生成され、次の情報が示されます。

- 合計トラップ数
- アラームのカテゴリ
- アラームの重要度
- アラームタイプ
- トラップの OID
- トラップの説明

ヘルスレポートについて

ヘルスレポートには、指定した Novell ZENworks Server Management サイトまたはネットワークセグメントの全体的なヘルスに関する情報が表示されます。各ヘルスレポートは、定義済みのヘルスプロファイルに基づいています。ヘルスプロファイルは、セグメント野菜との全体的なヘルスを計算するために使用されるトレンドパラメータを定義します。定義済みのヘルスプロファイルは 5 つあります。

- 1110 ページの「Novell NetWare サーバプロファイル」
- 1110 ページの「Microsoft Windows プロファイル」
- 1110 ページの「イーサネットネットワークプロファイル」

- 1111 ページの「トークンリングネットワークプロファイル」
- 1111 ページの「FDDI ネットワークプロファイル」

既存のプロファイルを編集したり、独自のヘルスレポートプロファイルを作成することもできます。1112 ページの「ヘルスプロファイルのカスタマイズ」または 1113 ページの「新しいヘルスプロファイルの追加」を参照してください。

Novell NetWare サーバプロファイル

このプロファイルを使用して生成されたレポートでは、次のトレンドパラメータのグラフが表示され、これらのパラメータを使用して、選択したアトラス、セグメント、またはページ内の Novell NetWare サーバの全体的なヘルスが計算されます。

- キャッシュバッファ
- キャッシュヒット数
- CPU 使用率
- ボリュームの空き容量

Microsoft Windows プロファイル

このプロファイルを使用して生成されたレポートでは、次のトレンドパラメータを使用してヘルスが計算されます。

- キャッシュヒット数
- CPU 使用率
- ディスクの空き容量
- 使用可能なメモリ

このプロファイルを使用して生成されたレポートには、次のパラメータのトレンドグラフも示されます。

- ログインしているユーザ数

イーサネットネットワークプロファイル

このプロファイルを使用して生成されたレポートでは、次のトレンドパラメータを使用して全体的なヘルスが計算されます。

- 合計エラー数
- ネットワーク使用率

このプロファイルを使用して生成されたレポートには、次のパラメータのトレンドグラフも示されます。

- CRC エラーパケット
- サイズの小さすぎるパケット
- サイズの大きすぎるパケット
- 断片化されたパケット
- 超過送信

トークンリングネットワークプロファイル

このプロファイルを使用して生成されたレポートでは、次のトレンドパラメータを使用して全体的なヘルスが計算されます。このプロファイルを使用して生成されたレポートには、次のパラメータのトレンドグラフも示されます。

- ネットワーク使用率
- 合計エラー数

FDDI ネットワークプロファイル

このプロファイルを使用して生成されたレポートでは、次のトレンドパラメータを使用して全体的なヘルスが計算されます。

- 合計エラー数
- ネットワーク使用率

このプロファイルを使用して生成されたレポートには、次のパラメータのトレンドグラフも示されます。

- CRC エラーパケット
- サイズの小さすぎるパケット
- サイズの大きすぎるパケット
- 損失フレームエラー

レポートの管理

次の節では、Novell ZENworks Server Management レポートのカスタマイズ、生成、印刷、およびエクスポートの手順を説明します。

- 1111 ページの「トポロジレポートの管理」
- 1112 ページの「Server Management のヘルスレポートの管理」

トポロジレポートの管理

トポロジレポートでは、サイトレベルのレポートとセグメントレベルのレポートの 2 つの種類を生成できます。サイトレベルのレポートには、Novell ZENworks Server Management サイトの各セグメントで発見されたデバイスに関する詳細が示されます。セグメントレベルのレポートには、選択したネットワークセグメントの管理対象デバイスに関する情報が示されます。NCP Servers レポートは、サイトレベルでのみ使用できます。

次の節では、トポロジレポートの生成、印刷、およびエクスポートの方法について説明します。

トポロジレポートの生成

トポロジレポートを生成するには

1 Novell ZENworks Server Management サイトオブジェクト、ネットワークセグメントオブジェクト、またはカスタムアトラスコンテナオブジェクトを選択します。

2 [Tools] > [Reports] の順にクリックします。

3 生成するレポートを選択し、[Run Selected Report] をクリックします。

4 レポートを印刷するには、  をクリックします。

5 レポートをエクスポートするには、  をクリックします。

Server Management のヘルスレポートの管理

サーバ管理コンポーネントには、ヘルスレポートの生成に使用できる 5 つの標準的なプロファイルが用意されています。これらの標準的なプロファイルに基づいてレポートを設定することも、これらのプロファイルをカスタマイズしたり、レポートの基になる独自のプロファイルを作成することもできます。標準的なヘルスプロファイルについては、1109 ページの「ヘルスレポートについて」を参照してください。

この節では、次のタスクについて説明します。

- 1112 ページの「ヘルスプロファイルのカスタマイズ」
- 1113 ページの「新しいヘルスプロファイルの追加」
- 1114 ページの「ヘルスレポートの作成とスケジュール」
- 1115 ページの「ヘルスレポートの表示と印刷」
- 1116 ページの「ヘルスレポートの実行」
- 1116 ページの「全体的なヘルスの計算」

ヘルスプロファイルのカスタマイズ

ヘルスプロファイルをカスタマイズするには

1 Novell ZENworks Server Management サイトオブジェクトを右クリックし、[Properties] をクリックします。

2 [Health Profiles] タブをクリックします。

3 カスタマイズするヘルスプロファイルを選択し、[Edit] をクリックします。

[Edit Profile] ダイアログボックスが表示されます。このダイアログボックスには、プロファイルを適用するデバイスやセグメントの全体的なヘルスを計算するために使用できるパラメータのリストが表示されます。

4 [Publish Directory] フィールドに値を入力して、このプロファイルを使用して生成するレポートの発行先のディレクトリ位置を指定します。

ディレクトリを参照するには、参照ボタン (...) をクリックします。

5 ヘルスを計算するために使用するパラメータを変更するには、各パラメータの横にある [In Health Calculation] チェックボックスをオンまたはオフにします。ヘルスの計算に使用されるパラメータの詳細については、1109 ページの「ヘルスレポートについて」を参照してください。

6 ヘルスの計算で各トレンドパラメータの重要性をランク付けするには、ヘルスの計算に含めることを選択した各パラメータの［Weight］フィールドに数値を入力します。

［Weight］フィールドには任意の整数を入力できます。システムは、この重みを使用して、全体的なヘルスの計算におけるパラメータの重要性を決定します。数値が大きくなるほど、ヘルスの計算でのパラメータの重みは大きくなります。

7 ヘルスレポートでグラフ表示するパラメータを変更するには、各パラメータの横にある［Show Trend on Report］チェックボックスをオンまたはオフにします。

8 変更を保存するには、［OK］をクリックします。

新しいヘルスプロファイルの追加

新しいヘルスプロファイルを追加するには

1 Novell ZENworks Server Management サイトオブジェクトを右クリックし、［Properties］をクリックします。

2 ［Health Profiles］タブをクリックします。

3 ［New］をクリックします。

［New Profile］ダイアログボックスが表示されます。

4 ［Name］フィールドに新しいプロファイルの名前を入力します。

5 ［Type］ドロップダウンリストから、プロファイルを適用するデバイスまたはセグメントのタイプを選択し、［OK］をクリックします。

［Edit Profile］ダイアログボックスが表示されます。

6 ［Publish Directory］フィールドに値を入力して、このプロファイルを使用して生成するレポートの発行先のディレクトリ位置を指定します。

ディレクトリを参照するには、参照ボタン（...）をクリックします。

7 このプロファイルを使用して生成されるレポート用にヘルスを計算するために使用するパラメータを選択するには、該当するパラメータの横にある［In Health Calculation］チェックボックスをクリックします。ヘルスの計算に使用されるパラメータの詳細については、1109 ページの「ヘルスレポートについて」を参照してください。

8 ヘルスの計算に含めることを選択した各パラメータについて、全体的なヘルスの計算におけるパラメータの重要性を指定するには、［Weight］列に値を入力します。

［Weight］フィールドには任意の整数を入力できます。システムは、この重みを使用して、全体的なヘルスの計算におけるパラメータの重要性を決定します。数値が大きくなるほど、ヘルスの計算でのパラメータの重みは大きくなります。

9 関連付けられたヘルスレポートでグラフ表示する各パラメータについて、［Show Trend on Report］チェックボックスをクリックします。

10 ［OK］をクリックします。

ヘルスレポートの作成とスケジュール

ヘルスレポートを作成およびスケジュールするには

1 コンテナオブジェクトを右クリックし、[Properties] をクリックします。

2 [Health Reports] タブをクリックします。

3 [New] をクリックします。

[Edit Report] ダイアログボックスが表示されます。

4 [Name] フィールドにレポートの名前を入力します。

5 [Profile] ドロップダウンリストから値を選択して、レポートを生成するときに使用するプロファイルを選択します。

6 [Period] ドロップダウンリストから値を選択して、レポートを生成する頻度を指定します。

日ごと、週ごと、または月ごとにレポートを生成することを選択できます。

7 [Start Time]、[Day of the Week]、および [Day of the Month] フィールドで適切な値を選択または入力して、レポートを生成する日時を設定します。

使用できるフィールドは、選択した期間によって異なります。

8 [OK] をクリックします。

入力した日時にレポートが生成され、関連付けられたレポートプロファイルで指定されたディレクトリに保存されます。レポートの表示については、1115 ページの「ヘルスレポートの表示と印刷」を参照してください。

ヘルスレポートの編集、スケジュール、および削除

ヘルスレポートを編集およびスケジュールするには

1 アトラス、ページ、またはセグメントを右クリックし、[Properties] をクリックします。

2 [Health Reports] タブをクリックします。

3 [Edit] をクリックします。

[Edit Report] ダイアログボックスが表示されます。必要な情報を変更します。

4 [OK] をクリックします。

重要： レポートのスケジュールを編集する場合は、レポートを新規作成して新しいスケジュールを設定し、元のレポートを削除することをお勧めします。

ヘルスレポートを削除するには

1 アトラス、セグメント、またはページを右クリックし、[Properties] をクリックします。

2 [Health Reports] タブをクリックします。

3 [Delete] をクリックします。

4 [OK] をクリックします。

ヘルスレポートの表示と印刷

ヘルスレポートを作成すると、レポートは指定した日時に自動的に生成されます。レポートを表示するには、関連付けられたレポートプロファイルで発行ディレクトリとして指定したディレクトリにある INDEX.HTM ファイルを Web ブラウザで開きます。

重要： ヘルスレポートを表示するには、Java* プラグイン 1.3.1_01 をインストールしておく必要があります。このプラグインは、Sun Microsystems, Inc. から入手できます。

ヘルスレポートを表示するには

1 関連付けられたプロファイルでヘルスレポートが保存されるディレクトリを参照します。

2 ブラウザを使用して index.htm ファイルを開きます。

index.htm ファイルは、このディレクトリに保存されているすべてのレポートを含む Java ファイルです。index.htm ファイルの左側の列にはレポート階層が一覧表示されます。

3 表示するレポートに関連付けられているプロファイルの横にあるプラス記号をクリックします。

プロファイルオブジェクトが展開され、コンテナオブジェクトが一覧表示されます。

4 表示するレポートに関連付けられているコンテナオブジェクトの横にあるプラス記号をクリックします。

オブジェクトが展開され、オブジェクトに関連付けられているレポート名が一覧表示されます。

5 表示するレポートの横にあるプラス記号をクリックします。

オブジェクトが展開され、個々のレポートインスタンスが一覧表示されます。たとえば、毎日実行するようにスケジュールされているレポートの場合、毎日のレポートインスタンスが存在します。レポートには、日付と時刻の名前が付けられます。たとえば、2000.09.09_11.15.10_PDT は、2000 年 9 月 9 日、11 時 15 分 10 秒（太平洋標準時、夏時間）に生成されたレポートに付けられた名前です。

6 レポート名の横にあるプラス記号をクリックして、個々のレポートページを一覧表示します。

個々のレポートページの数は、選択したレポートプロファイルおよびレポートを生成するオブジェクトによって異なります。たとえば、Ethernet Network プロファイルを使用して、セグメントレベルでレポートを生成する場合、そのセグメントについてレポートページは 1 つだけです。Ethernet Network プロファイルを使用して、サイトレベルでレポートを生成する場合、サイト内の各イーサネットセグメントについてレポートページが生成されます。Novell NetWare Server プロファイルを使用して、セグメントレベルでレポートを生成する場合、セグメントの各 Novell NetWare サーバについてレポートページが個別に生成されます。

7 個々のレポートページをクリックして、右側のフレームにヘルスレポートを表示します。

レポートの上部にはセグメントやサーバに関する統計情報が表示され、全体的なヘルスの計算が示されます。全体的なヘルスを判断するために使用されるパラメータは、関連付けられたヘルスレポートプロファイルで定義されます。プロファイルの下部には、サーバやセグメントの全体的なパフォーマンスを示すトレンドグラフが表示されます。標準的な各プロファイルでトラッキングおよびグラフ化されるパラメータの一覧については、1109 ページの「ヘルスレポートについて」を参照してください。

8 レポートを印刷するには、左側のフレームの下部にある［Print Report］ボタンをクリックします。

ヘルスレポートの実行

通常、ヘルスレポートは、日、週、月の指定された時刻に実行されるようにスケジュールされていますが、必要なときにヘルスレポートを実行することもできます。必要に応じてヘルスレポートを生成するには、次の手順に従ってください。

1 アトラス、セグメント、またはページを右クリックし、［Properties］をクリックします。

2 ［Health Reports］タブをクリックします。

3 生成するレポートを選択し、［Now］をクリックします。

レポートプロファイルで指定されたディレクトリにレポートが保存されます。1115 ページの「ヘルスレポートの表示と印刷」を参照してください。

全体的なヘルスの計算

全体的なヘルスは次のパラメータを使用して計算されます。

- ヘルスの計算用に選択した属性。
- 各属性に割り当てられた重み。

  関連付けることができるのは、ヘルスの計算で使用される重みだけです。
- 各属性の値。

  Yellow threshold (YT)、Red threshold (RT)、および最大値 (maxValue)。
- グローバルしきい値。

  Global Green threshold (GG) は 100、Global Yellow threshold (GY) は 66、Global Red threshold (GR) は 33 です。

ヘルスの計算

全体的なヘルスの計算で使用される各属性について、レポートの生成時に指定したスケジュールに基づいてサンプル値が収集されます。これらのサンプル値は、グローバルしきい値と属性のしきい値を使用して正規化されます。ここで、Global Green は 100、Global Yellow は 66、および Global Red は 33 です。global Green range = global Green - global Yellow、global Yellow range = global Yellow - global Red、および global Red range = global Red です。

正規化の式

Normalized Value = Global Threshold - ((value - attribute Threshold))/ (attribute Threshold Range) * (Global Range)

if (value > attribute's RED threshold)

global Threshold = global Red

attribute threshold = attribute Red threshold

attribute threshold range = attribute maxValue - attribute Red threshold

global Range = global Red range

if (value > attribute's Yellow threshold)

global threshold = global Yellow

attribute threshold = attribute Yellow threshold

attribute threshold range = attribute Red - attribute Yellow

global range = global Yellow range

if (value > 0)

global threshold - ((value)) / (attribute threshold range) * (global range)

global threshold = global Green

attribute threshold Range = attribute Yellow threshold

global range = global Green range

これらの各属性には、それぞれのプロファイルで設定された重みが割り当てられている場合がありますこれらの各属性サンプルには、次の式を使用して対応する重みが乗算されます。

value = value * attributeWeight / TotalWeight;

ここで、value は正規化後の特定のサンプル、attributeWeight は属性に関連付けられた重み、TotalWeight はヘルスの計算で使用されるすべての属性の重みの合計です。

ヘルスレポートに表示されるその他の値は、次のように計算されます。

- Minimum Value = 特定のサンプルのすべての値の最小値
- Maximum Value = 特定のサンプルのすべての値の最大値
- Average Value = すべての値の合計 / サンプル数
- Trend は Slope に基づいて計算されます。

  Slope = (n * Σ x *y - Σ x * Σ y) / (n * Σ x * x - Σ x * Σ x)

  ここで、

  n = サンプル数

  x = これらのサンプルをキャプチャした時刻

  y = トレンド値。

  Slope > 0 の場合、トレンドは増加です。

  Slope < 0 の場合、トレンドは減少です。

  Slope = 0 の場合、トレンドは一定です。

- Intercept = (Σ y - Slope * Σ x) / n
- Next Week Projection または Next Month Projection Value = Slope * time + Intercept

  ここで、time = Report Schedule Time（レポートがスケジュールされていた時刻）+ 7 * 24 * 60 * 60 * 1000（Weekly Projection の場合）
- Report Schedule Time（レポートがスケジュールされていた時刻）+ 30 * 24 * 60 * 60 * 1000（Monthly Projection の場合）

警告： データを CSV（カンマ区切り）、文字区切り、および TSV（タブ区切り）形式でエクスポートする場合、完全なデータがエクスポートされません。回避策として、まずデータを MS Excel 形式でエクスポートし、次に必要な形式で保存する必要があります。

生成されたレポートを HTML または DHTML 以外の形式でエクスポートする場合、正しいページ番号が表示されません。すべてのページで、ページ番号が Page -1 of 1 と表示されます。

33 SNMP コミュニティ文字列の使用

この章は、他の章から参照されます。この章では、SNMP、SNMP コミュニティ文字列、および SNMP コミュニティ文字列の設定方法について説明します。

この節では、次のトピックについて説明します。

- 1119 ページの「SNMP コミュニティ文字列について」
- 1120 ページの「SNMP コミュニティ文字列の設定」

SNMP コミュニティ文字列について

SNMP は、インターネットプロトコルスイートで、ネットワーク管理サービスを提供するプロトコルです。

SNMP では軽量のセキュリティメカニズムが使用され、これによって各プロトコルデータユニット (PDU) にはコミュニティ文字列が含まれます。SNMP Control 操作では SET コミュニティ文字列が使用され、SNMP Monitor 操作では GET コミュニティ文字列が使用されます。

SNMP コミュニティ文字列は、各 SNMP 要求の中でクリアテキストで送信されるので、提供されるセキュリティの形態は基本的なものです。したがって、コミュニティ文字列は、IP または IPX™ (Internetwork Packet Exchange™) ネットワークを監視できるステーションで表示することができます。

NetWare 版 Management Agent と Windows 版 Management Agent は、SNMP に基づいているため、ネットワーク Novell ConsoleOne からサーバに指示されるすべてのアクションには、マネージャからエージェントへの SNMP SET 要求および GET 要求が含まれます。Novell ConsoleOne® は、SNMP GET 要求を発行することによって、管理対象サーバにデータを要求します。SNMP SET コマンドは、サーバのアラームしきい値や設定パラメータを設定するために必要です。多くの場合、Novell ConsoleOne で要求を実行するために必要な下位の SNMP コマンドは、MIB Browser を使用して SNMP 対応デバイスで要求を発行する場合を除いて、ユーザに意識されることはありません。

SNMP のセキュリティ

Novell ConsoleOne から管理操作を実行する場合、セキュリティの保証の問題が発生します。特に、許可されていないユーザがサーバのパラメータを設定すると、パフォーマンスの問題が発生したり、ネットワーク操作を実行できなくなる場合もあります。

このような理由から、デフォルトのコミュニティ文字列 PUBLIC を、管理システムと SNMP エージェントとの通信で使用される独自のコミュニティ文字列に変更する方法を確立する必要があります。

生成されるトラップで使用されるコミュニティ文字列を定義するには、コミュニティキーワードを使用します。コミュニティ文字列の長さは 32 バイトに制限されており、空白（引用符で囲まれている場合を除く）、タブ、角括弧、等号、コロン、セミコロン、番号記号 (#) は使用できません。コミュニティ文字列には、Unicode* または各国文字を使用できます。

Monitor 操作のデフォルトのコミュニティ文字列は PUBLIC であり、Control 操作の場合は null です。

SNMP コミュニティ文字列の設定

この節では、次のトピックについて説明します。

- 1120 ページの「SNMP コミュニティ文字列の設定 :Novell NetWare サーバ」
- 1122 ページの「SNMP コミュニティ文字列の設定 :Novell ConsoleOne 」
- 1123 ページの「個々のノードのコミュニティ文字列の設定」
- 1123 ページの「SNMP コミュニティ文字列の設定 :Windows: 」

SNMP コミュニティ文字列の設定 :Novell NetWare サーバ

SNMP 通信のセキュリティアクセスを設定するには、SNMP LOAD コマンドラインパラメータ (Novell NetWare 3.*x*/4.*x*/5.*x*/6 サーバ) または INETCFG (Novell NetWare 4.*x*/5.*x*/6 サーバ、または Novell NetWare MultiProtocol Router™ ソフトウェアがインストールされたサーバ) のいずれかを使用します。

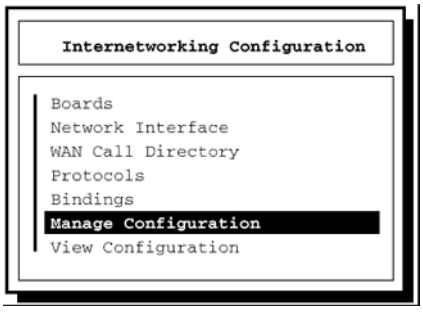
次の節では、Novell NetWare サーバの設定に役立つ追加情報を示します。

- 1121 ページの「INETCFG を使用したコミュニティ文字列オプションの設定」
- 1122 ページの「SNMP LOAD コマンドを使用したコミュニティ文字列オプションの設定」

INETCFG を使用したコミュニティ文字列オプションの設定

INETCFG を使用してコミュニティ文字列オプションを設定するには

1 サーバプロンプトで、「**LOAD INETCFG**」と入力します。



2 [Internetworking Configuration] メニューから、[Manage Configuration] > [Configure SNMP Parameters] > [Monitor State] の順にクリックします。

3 次のオプションのいずれかを選択します。

これらのオプションによって、このサーバの外部からの SNMP 読み込み操作を SNMP でどのように処理するかを指定できます。

オプション	説明
Any Community May Read	受信した読み込み要求に含まれているコミュニティ文字列に関係なく、すべての GET（読み込み）コマンドを許可します。
Leave as Default Setting	Monitor コミュニティ文字列をデフォルト値（通常は PUBLIC）から変更しません。デフォルトの Monitor Community は、SNMP コマンドラインオプションを使って手動で変更できます。詳細については、1122 ページの「SNMP LOAD コマンドを使用したコミュニティ文字列オプションの設定」を参照してください。
No Community May Read	SUPERVISOR または OPERATOR 特権を使ってサーバにログインしている Novell ConsoleOne からの要求に対してのみ、GET（読み込み）コマンドを許可します。受信した読み込み要求に含まれるすべてのコミュニティ文字列は無視されます。
Specified Community May Read	[Monitor Community] フィールドで指定された名前を含む要求に対してのみ、GET（読み込み）コマンドを許可します。このオプションを選択した場合、[Monitor Community] フィールドに名前を入力し、(Enter) キーを押します。管理情報の読み込みを許可するコミュニティの名前を入力します。このコミュニティに属する SNMP 管理ステーションは、ネットワーク管理データベースを読み込むことができます。

4 (Enter) キーを押します。

Control コミュニティオプションを変更するには、手順 1 から手順 4 までを繰り返して、コミュニティ文字列の適切なオプションを選択します。

5 設定が終了したら、(Esc) キーを押します。メッセージが表示されたら、[Yes] をクリックして SNMP パラメータに対する変更を保存し、(Enter) キーを押します。

6 [Internetworking Configuration] メニューに戻るには、(Esc) キーを押します。

7 INETCFG を終了するには、(Esc) キーを押します。

8 システムを再初期化します。

再初期化するには、サーバプロンプトで、「**reinitialize system**」と入力します。

SNMP LOAD コマンドを使用したコミュニティ文字列オプションの設定

LOAD コマンドでは、次の SNMP オプションパラメータを使用できます。

- **MonitorCommunity:** 読み込み専用 (GET) アクセスのコミュニティ文字列を設定します。デフォルト値は PUBLIC です。構文は次のとおりです。

  LOAD SNMP MonitorCommunity=*community_name*

- **ControlCommunity:** 読み書き(GETおよびSET)アクセスのコミュニティ文字列を設定します。デフォルトでは、このコミュニティ文字列は無効になっています。

  構文は次のとおりです。

  LOAD SNMP ControlCommunity=*community_name*

  これらのオプションは、指定されたコミュニティのコミュニティ文字列を設定します。次の表では、使用できる設定の例を示します。

  重要: コミュニティ文字列では、大文字と小文字が区別されます。

要求元に許可するアクセス	読み込み専用	読み書き
コミュニティ名 :"secret"	Load SNMP MonitorCommunity=*secret* または LOAD SNMP ControlCommunity=*secret*	LOAD SNMP ControlCommunity=*secret*
コミュニティ名 : "str1" または "str2"	Load SNMP MonitorCommunity=*str1* および LOAD SNMP ControlCommunity=*str2*	
任意のコミュニティ名	Load SNMP MonitorCommunity= "" または LOAD SNMP ControlCommunity=""	LOAD SNMP ControlCommunity=""

SNMP コミュニティ文字列の設定 :Novell ConsoleOne

グローバルコミュニティおよびトラップターゲット情報を設定するには、サイトレベルのオブジェクトに関連付けられた SNMP プロパティページを使用します。デバイス自体の SNMP プロパティページを使用して、特定のデバイスの設定をカスタマイズすることもできます。

個々のノードのコミュニティ文字列の設定

この節では、個々のノードで SNMP SET および GET 操作のコミュニティ文字列を設定する手順について説明します。

一般的に、コミュニティ文字列はネットワーク内のすべてのノード、または少なくともネットワークの一部で同じになるように設定されます。デフォルト値は、SET および GET のいずれの場合も public です。コミュニティ文字列では、大文字と小文字が区別されます。

デフォルトの場合、Novell ZENworks Server Management は、SNMP GET および SET 操作でコミュニティ文字列 public を使用します。ノードごとに public 以外のコミュニティ文字列を設定したり、すべての SNMP 管理対象ノードに対してグローバルなコミュニティ文字列を設定したりできます。Novell ZENworks Server Management が使用するコミュニティ文字列は、管理対象ノード内の SNMP エージェントで想定されている文字列と一致している必要があります。コミュニティ文字列が一致しない場合、操作は失敗します。

個々のノードの SET および GET 操作のコミュニティ文字列を設定するには

1 Novell ConsoleOne で、ターゲットの SNMP 管理対象ノードをクリックします。

2 ノードを右クリックし、[SNMP Settings] をクリックします。

3 コミュニティ文字列を入力します。

Novell ZENworks Server Management では、このデバイスと通信するときに、SET および GET 操作でこのコミュニティ文字列を使用します。

4 [OK] をクリックします。

SNMP コミュニティ文字列の設定 :Windows:

Windows サーバで SNMP 通信のセキュリティアクセスを設定するには、Windows のコントロールパネルにある［ネットワーク］アプレットを使用します。詳細については、Windows のマニュアルまたはオンラインヘルプを参照してください。

Windows サーバに Microsoft* SNMP Service をロードする必要があります。SNMP コミュニティ文字列の設定は、Novell ConsoleOne での SNMP コミュニティ文字列の設定と同じでなければなりません。

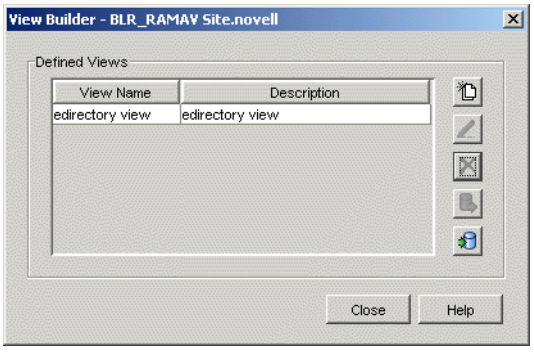
34 View Builder の理解

View Builder は、SNMP MIB を計測したエージェントからの情報およびエージェントによって Management Site Server に送信されたトラップを表示するビューを作成できるメカニズムを提供します。View Builder を使用して、Novell ConsoleOne で使用できるビュー以外のビューを作成できます。これらのビューは、テキスト、表、およびグラフとして表示できます。

ビューを特定のノードに関連付けて、管理することができます。

[View Builder] ダイアログボックスを表示するには

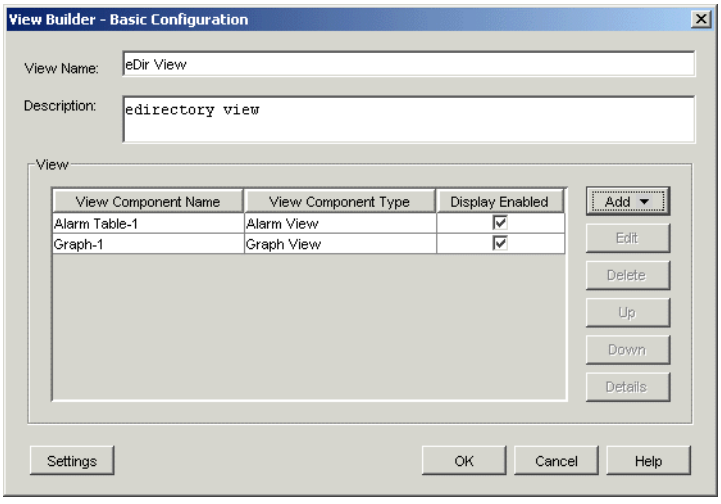
1 Novell ConsoleOne で、[Tools] > [View Builder] の順に選択します。



- **[Defined Views]**： 作成されたビューを一覧表示します。
- **[View Name]**： ビューの名前。
- **説明**： ビューの説明。
- **[Add]**： をクリックします。[Basic Configuration] ダイアログボックスが表示されます。このダイアログボックスでビューコンポーネントを作成できます。
- **[Edit]**： ビューの詳細を編集するには、をクリックします。
- **[Delete]**： ビューを削除するには、をクリックします。
- **[Export]**： ビューをファイルにエクスポートするには、をクリックします。
- **[Import]**： ファイルからビューをインポートするには、をクリックします。

2 [View Builder] ダイアログボックスで、をクリックします。

[View Builder - Basic Configuration] ダイアログボックスが表示されます。



ビューには、ビューコンポーネントまたはビューコンポーネントの組み合わせを含めることができます。作成できるビューコンポーネントには、Name-Value Pairs View、Alarm View、Table View、および Graph View があります。

3 次のいずれかの操作を行います。

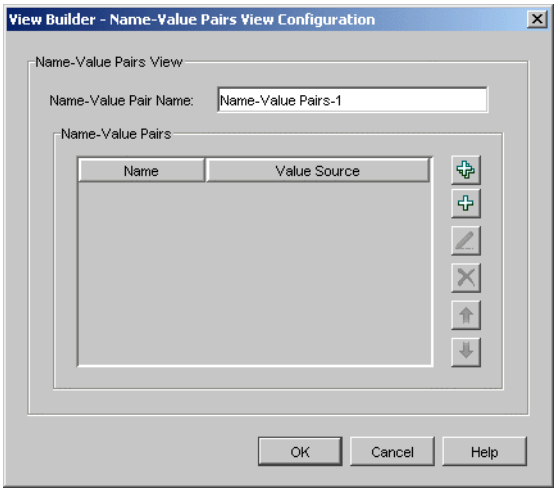
- 1127 ページの「Name-Value Pairs View コンポーネントの作成」
- 1129 ページの「Alarm View コンポーネントの作成」
- 1130 ページの「Table View コンポーネントの作成」
- 1132 ページの「Graph View コンポーネントの作成」
- 1133 ページの「ビューを表示する条件の設定」

4 [OK] をクリックします。

Name-Value Pairs View コンポーネントの作成

Name-Value Pairs View コンポーネントには、複数の名前と値のペアを含めることができます。

1 [View Builder - Basic Configuration] ダイアログボックスで、[Add] > [Name-Value Pairs View] の順にクリックします。



2 [Name-Value Pairs View] の名前を指定します。

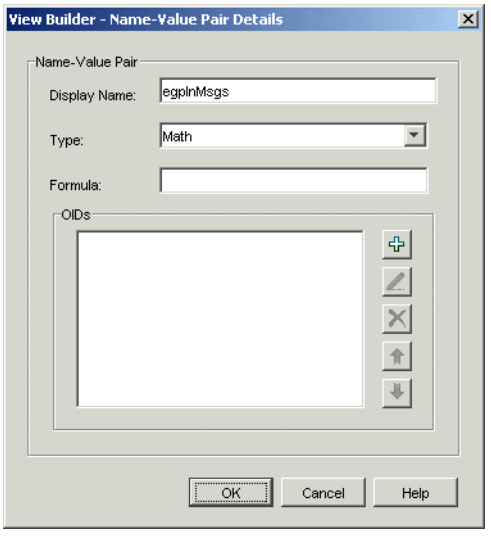
[Name-Value Pairs] ボックスには、作成したすべてのビューコンポーネントが表形式で一覧表示されます。作成したビューコンポーネントの [Name] および [Value Source] が表示されます。

3 次のいずれかの操作を行います。

- **[Add Multiple]** : 複数の名前と値のペアを追加するには、をクリックします。
- **[Add]** : 名前と値のペアを追加するには、をクリックします。
- **[Edit]** : 情報を変更するには、編集する名前と値のペアを [Name-Value Pairs] の一覧から選択し、をクリックします。
- **[Delete]** : 名前と値のペアを削除するには、[Name-Value Pairs] の一覧でペアを選択し、をクリックします。
- **[Arrange Order]** : 表示の順序を変更するには、または を使用します。

名前と値のペアの追加

1 [Name-Value Pairs View Configuration] ダイアログボックスで、✚をクリックします。



2 名前と値のペアコンポーネントの表示名を指定します。

3 ドロップダウンリストから、名前と値のペアのタイプを選択します。

Name-Value Pair のタイプとして、[Simple]、[Rate]、[Math] のいずれかを選択できます。タイプとして [Rate] を選択した場合は、GAUGE または COUNTER タイプの OID を指定する必要があります。タイプとして [Math] を選択した場合は、式を指定する必要があります。

式の指定： 表に表示される OID には、0、1、2 などの番号が付けられます。番号の前には、OID の現在の値を示すデータ識別子 v、および OID の以前の値を示す h が付けられます。式を指定する場合は、演算子 +、-、/、*、^、() を使用できます。式で定数を使用することもできます。

例 :OID snmpInPkts (1.3.6.1.2.1.11.1) および snmpOutPkts (1.3.6.1.2.1.11.2) を選択します。式は v0+v1 と指定できます。この結果は、トランスポートサービスによって処理された SNMP パケットの総数になります。

4 [OK] をクリックします。

作成した名前と値のペアが、[Name-Value Pairs Configuration] ダイアログボックスに表示されます。同じ手順で複数の名前と値のペアを追加し、[OK] をクリックします。Name-Value Pair View コンポーネントが、[Basic Configuration] ダイアログボックスに表示されます。

Name-Value Pairs View コンポーネントの編集

1 [Basic Configuration] ダイアログボックスで、変更する名前と値のペアのビューコンポーネントを選択し、[Edit] をクリックします。

2 名前と値のペアコンポーネントの詳細を変更し、[OK] をクリックします。

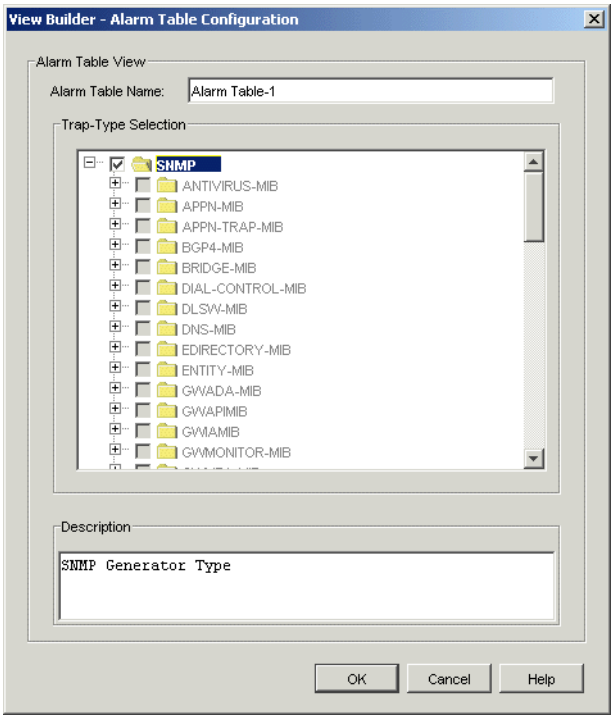
Name-Value Pairs View の削除

1 [Basic Configuration] ダイアログボックスで、削除する名前と値のペアのビューコンポーネントを選択します。

2 [Delete] をクリックします。

Alarm View コンポーネントの作成

1 [View Builder - Basic Configuration] ダイアログボックスで、[Add] > [Alarms View] の順にクリックします。



2 Alarm Table の名前を指定します。

3 トラップのタイプを選択します。

3 つの階層に基づいてトラップタイプを選択できます。ノード、特定のカテゴリ、またはカテゴリ内の特定のトラップタイプからすべてのトラップを選択できます。

4 [OK] をクリックします。

作成した Alarms View コンポーネントが、[Basic Configuration] ダイアログボックスに表示されます。

Alarms View コンポーネントの編集

1 [Basic Configuration] ダイアログボックスで、Alarms View コンポーネントを選択し、[Edit] をクリックします。

2 Alarms View コンポーネントの詳細を変更し、[OK] をクリックします。

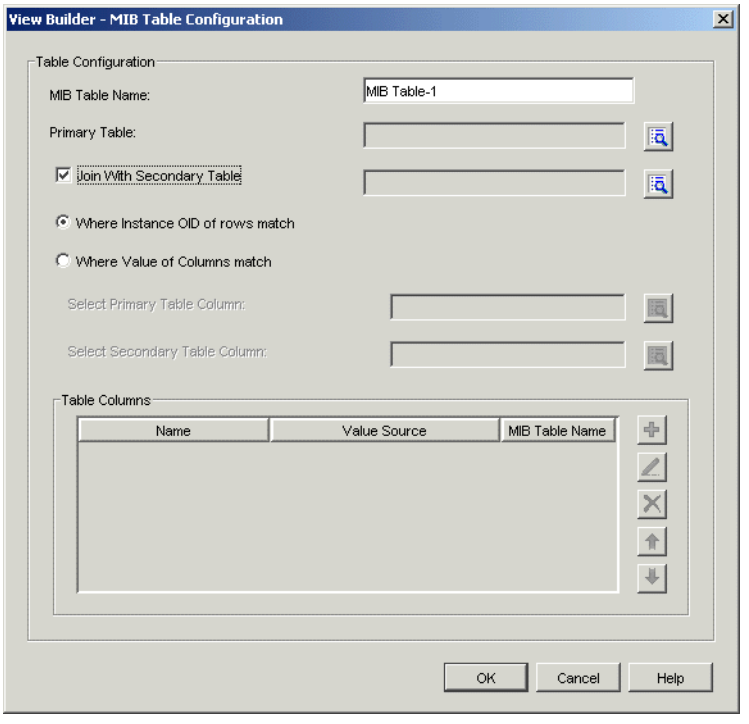
Alarm View コンポーネントの削除

1 [Basic Configuration] ダイアログボックスで、削除する Alarms View コンポーネントを選択します。

2 [Delete] をクリックします。

Table View コンポーネントの作成

1 [View Builder - Basic Configuration] ダイアログボックスで、[Add] > [Table View] の順にクリックします。



2 MIB テーブル名を指定します。

3 をクリックして、プライマリテーブルにする MIB テーブルを選択します。ステップ 7 に進みます。

4 プライマリテーブルとセカンダリテーブルを結合します。

5 プライマリテーブルとセカンダリテーブルを結合する場合は、[Join With Secondary Table] チェックボックスをオンにします。をクリックして、セカンダリテーブルを選択します。

6 プライマリテーブルとセカンダリテーブルを結合する条件を設定します。

[Where Instance OID of Rows Match]: 一致するインスタンスの OID に基づいてプライマリテーブルとセカンダリテーブルを結合します。

通常、標準テーブルの拡張テーブルが作成されます。拡張テーブルには明示的なインデックスがなく、標準テーブルのインデックスを使用します。たとえば、テーブル hrSWRunTable(1.3.6.1.2.1.25.4.2) と hrSWRunPerfTable (1.3.6.1.2.1.25.5.1) を結合できます。

[Where Values of Columns Match] : 一致する列の OID に基づいてプライマリテーブルとセカンダリテーブルを結合します。この条件を満たすには、プライマリテーブルの列とセカンダリテーブルの列を選択する必要があります。をクリックして、プライマリテーブルの列とセカンダリテーブルの列を選択します。

たとえば、プライマリテーブルの ifIndex:1.3.6.1.2.1.2.2.1.1 とセカンダリテーブルの ipAdEntIfIndex 1.3.6.1.2.1.4.20.1.2 が一致する列である場合、ifTable(1.3.6.1.2.1.2.2) と ipAddrTable(1.3.6.1.2.1.4.20) を結合できます。

7 [Table Columns] で次のいずれかの操作を行います。

- [Add] : テーブルの列を追加するには、をクリックします。
- [Edit] : テーブルの列を変更するには、をクリックします。
- [Delete] : テーブルの列を削除するには、をクリックします。
- [Arrange Order] : 表示の順序を変更するには、または を使用します。

8 [OK] をクリックします。

作成したテーブルビューコンポーネントが、[Basic Configuration View] ダイアログボックスに表示されます。

Table View の編集

1 [Basic Configuration] ダイアログボックスで、変更する Table View コンポーネントを選択し、[Edit] をクリックします。

2 Table View の詳細を変更し、[OK] をクリックします。

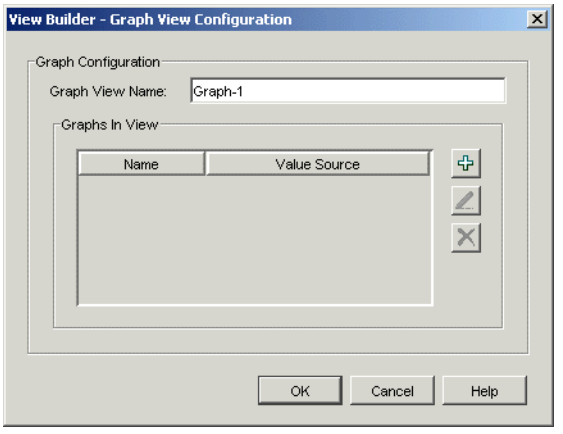
Table View の削除

1 [Basic Configuration] ダイアログボックスで、削除する Table View コンポーネントを選択し、[Delete] をクリックします。

Graph View コンポーネントの作成

Graph View に追加するグラフは、特定のノードで実行中の Advanced Trending Agent によって収集されるトレンドデータに基づいて表示されます。グラフを作成するには、次の手順に従ってください。

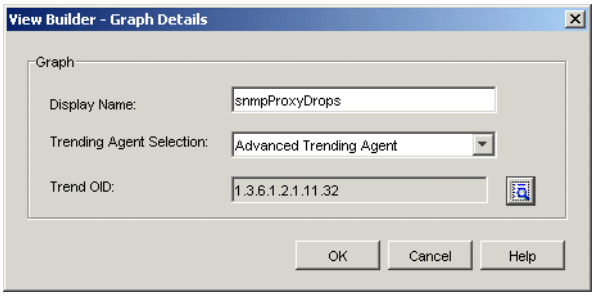
1 [View Builder - Basic Configuration] ダイアログボックスで、[Add]、[Graph View] の順にクリックします。



2 Graph View 名を指定します。

グラフの詳細の追加

1 [Graph View Configuration] ダイアログボックスで、✚をクリックします。



2 グラフの表示名を指定します。

3 グラフ表示の基になるトレンド分析エージェントであるため、[Advanced Trending Agent] が選択されています。

4 をクリックして、トレンドの OID を選択します。

重要： 選択した OID は、Advanced Trending Agent によってトレンド分析されている必要があります。

5 [OK] をクリックします。

作成したグラフが、[Graph View Configuration] ダイアログボックスに表示されます。この手順を使用して複数のグラフを追加し、[OK] をクリックします。Graph View コンポーネントが、[Basic Configuration] ダイアログボックスに表示されます。

Graph View コンポーネントの編集

1 [Basic Configuration] ダイアログボックスで、Graph View コンポーネントを選択し、[Edit] をクリックします。

2 グラフの詳細を変更し、[OK] をクリックします。

Graph View コンポーネントの削除

1 [Basic Configuration] ダイアログボックスで、削除する Graph View コンポーネントを選択します。

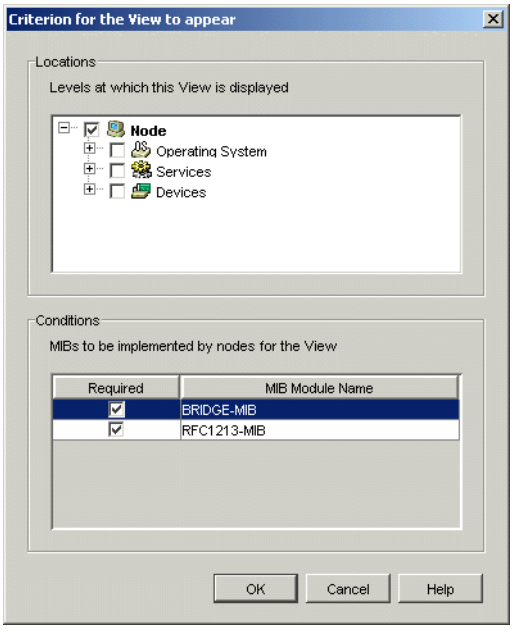
2 [Delete] をクリックします。

ビューを表示する条件の設定

選択したレベルで表示するビューの条件を設定できます。この設定には、ビューの場所とビューを表示する条件が含まれます。

ビューを表示する条件を設定するには

1 [Basic Configuration] ダイアログボックスで、[Settings] をクリックします。



2 ビューを表示する場所を指定します。

デフォルトでは、作成したビューはノードレベルで表示されます。

3 ビューを表示する条件を指定します。

ノードによって実装される MIB と、ビューを表示するノードの MIB モジュール名が、この一覧に表示されます。デフォルトでは、すべての MIB モジュールについて、ノードへの実装が選択されていません。MIB モジュールをノードに実装する必要がある場合は、MIB モジュールを選択します。この一覧に表示されている MIB は、Discovery によって自動的に発見されます。

4 [OK] をクリックします。

N ドキュメントの更新

この節では、Novell® ZENworks® 6.5 Server Management の初回リリース後に、Management and Monitoring Services の『*管理*』ガイドに加えられたマニュアル内容の変更に関する情報を提供します。お使いのドキュメントを最新の状態に更新するために、この情報を役立ててください。

この節で列挙する変更はすべてドキュメントにも反映されているものです。マニュアルは、Web 上で HTML と PDF の 2 つの形式で提供されています。HTML および PDF ドキュメントは、ここに示すドキュメントの変更に基づいて最新の状態になっています。

ドキュメントの変更が発行された日付ごとに、更新情報をグループ化しています。同じ日付のセクション内では、変更は Management and Monitoring Services の主な目次の節の名前に基づいて、アルファベット順に表示されています。

ドキュメントは次に示す日付で更新されました。

- 1135 ページの「2004 年 9 月 2 日」
- 1135 ページの「2004 年 7 月 28 日」

2004 年 9 月 2 日

ガイド全体を通して、グラフィックのフォントを変更し、新しいアイコンを使用しました。グラフィックの内容には、目立った変更はありません。

2004 年 7 月 28 日

次の節が更新されました。

場所	変更
959 ページの「注釈を追加した後のトラップ定義の例」	この節では、次の変更が行われました。 • 例から次の行を削除 ::=8 • ZENworks 6.5 Server Management には適用されないため、次の文を削除： [Alarm Report] 表でアラームを選択し、[Novell Network Expert] ボタンをクリックすると、このアラームに関するヘルプ情報が表示されます。