Novell Identity Manager

3.0

www.novell.com

管理指南

2006 年 4 月 28 日

Novell®

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改本出版品及其內容的權利，且在進行此類修正或更動時，不需另行通知任何人士或公司。

此外，Novell, Inc. 不對任何軟體作任何陳述或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或隱喻的保證。此外，Novell, Inc. 保留隨時修改任何或全部 Novell 軟體的權利，且在進行此類更動時，不需通知任何人士或公司。

這份授權書中所提及的任何產品或技術資訊皆受到美國出口管制法 (U.S. Export Control) 及其他國家的交易法約束。您同意遵守所有出口管制法規，並取得出口、再出口或進口交付物品所需之任何必要的授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列公司，或者至美國出口法所指定之禁運或恐怖份子的國家。您同意不將交付產品用在禁止的核子武器、飛彈或化學生物武器等用途上。如需更詳細的 Novell 軟體出口資訊，請參閱 www.novell.com/info/exports/。Novell 無須承擔您無法取得任何必要的出口核准之責任。

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

線上文件：若要存取本產品及其他 Novell 產品的線上文件，或取得更新，請參閱 www.novell.com/documentation。

Novell 商標

eDirectory 是 Novell, Inc. 的商標。
exteNd 是 Novell, Inc. 的商標。
exteNd Director 是 Novell, Inc. 的商標。
GroupWise 是 Novell, Inc. 在美國與其他國家的註冊商標。
NDS 是 Novell, Inc. 在美國與其他國家的註冊商標。
NetWare 是 Novell, Inc. 在美國與其他國家的註冊商標。
NMAS 是 Novell, Inc. 的商標。
Novell 是 Novell, Inc. 在美國與其他國家的註冊商標。
Novell Certificate Server 是 Novell, Inc. 的商標。
Novell Client 是 Novell, Inc. 的商標。
SUSE 是 Novell, Inc. 在美國與其他國家的註冊商標。

協力廠商資料

所有的協力廠商商標均爲其個別擁有廠商的財產。

目錄

關於本指南

Novell® Identity Manager 3 (先前稱爲 DirXML®) 是一種資料共享和同步服務，它可讓應用程式、目錄和資料庫共享資訊。它會連結散佈的資訊，並讓您建立規則，用於在身份發生變更時管理對指定系統的自動更新。Identity Manager 提供了下列項目的基礎：帳戶提供、安全性、使用者自助服務、驗證、授權、自動工作流程和 Web 服務。它可讓您整合、管理和控制您的分散式身份資訊，以便安全地將正確的資源傳送給正確的人員。

本指南提供 Identity Manager 技術的綜覽，同時描述管理和組態設定功能。

意見反應

我們想知道您對於本手冊與其他本產品隨附之文件的意見與建議。請使用線上文件中每頁底下的「使用者意見」功能，或請造訪 http://www.novell.com/documentation/feedback.html，然後寫下您的意見。

文件更新

如需本文件的最新版本，請參閱 Identity Manager 文件網站 (http://www.novell.com/documentation)。

其他文件

如需安裝和升級 Identity Manager 的相關文件，請參閱《*Identity Manager 3.0* 安裝指南》。

如需 Identity Manager 規則和過濾器的相關文件，請參閱《規則產生器和驅動程式自訂指南》。

如需設計和部署做法的相關文件，請參閱《*Designer for Identity Manager 3*：管理指南 (http://www.novell.com/documentation/designer)》。

如需密碼規則、密碼自助服務和管理密碼的相關文件，請參閱《密碼管理管理指南 (http://www.novell.com/documentation)》。

如需使用 Identity Manager 驅動程式的相關文件，請參閱 Identity Manager 驅動程式文件網站 (http://www.novell.com/documentation/idmdrivers/index.html)。

文件慣例

在本文件中，大於符號 (>) 是用以分隔步驟中的各個動作，以及前後參照路徑中的數個項目。

商標符號 (®、™ 等) 代表 Novell 的商標。星號 (*) 代表協力廠商的商標。

Identity Manager 3.0 結構綜覽

1

Identity Manager 有三個主要元件。

- 「Identity Manager」，第 10 頁
- 「使用者應用程式」，第 17 頁
- 「Designer」，第 17 頁

1.1 舊版術語的變更

如果您未曾使用 DirXML® 1.1a 或 Identity Manager 2.0，則無需檢視本節。

在 DirXML 1.1a 中，根據上下文不同，使用詞彙「規則 (Rule)」來描述規則集、規則集中的個別規則，以及個別規則中的條件和動作。當上下文不明確時，此重疊會造成混淆。

在 Identity Manager 2 中，現在使用詞彙「規則 (Policy)」取代詞彙「規則 (Rule)」來描述所發生的高層級轉換。您現在可以定義規則 (Policy) 集，其中每個規則 (Policy) 都包含一或多個規則 (Rule)。而詞彙「規則 (Rule)」現在只用來描述個別的條件和動作集。

下表顯示從 DirXML 1.1a 到 Identity Manager 2.x 的術語變更。

表格 ***1-1*** 從 *DirXML 1.1a* 到 *Identity Manager 2.x* 的術語變更

描述的項目	DirXML 1.1a 術語	Identity Manager 2.x 術語
轉換集	規則 (Rule)	規則 (Policy) 集
轉換集中的個別轉換	規則 (Rule)	「規則 (Policy)」
個別轉換中的條件和動作	規則 (Rule)	規則 (Rule)

下表顯示從 Identity Manager 2.x 到 Identity Manager 3.0 的術語變更。

表格 ***1-2*** 從 *Identity Manager 2.x* 到 *Identity Manager 3.0* 的術語變更

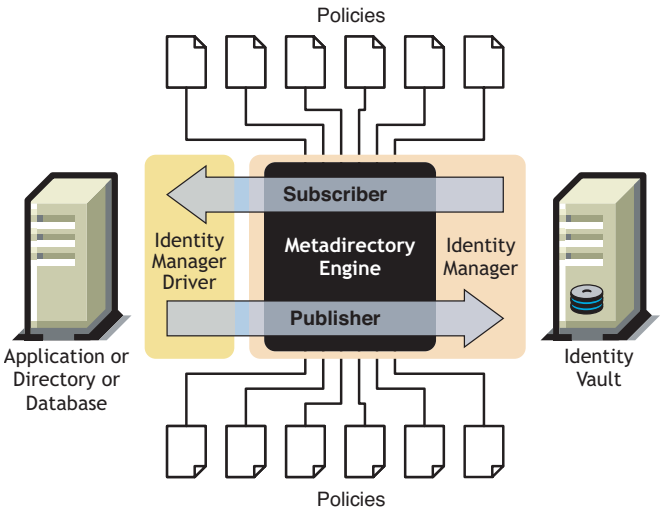
描述的項目	Identity Manager 2.x 術語	Identity Manager 3 術語
產品	DirXML	Identity Manager
已安裝產品的伺服器	DirXML 伺服器	Metadirectory 伺服器
應用程式或資料庫中進行資料同步化的伺服器	DirXML 已連接系統伺服器	已連接系統伺服器
儲存物件的位置	eDirectory™	Identity Vault
處理用元件	DirXML 引擎	Metadirectory 引擎

1.2 Identity Manager

Identity Manager 會提供 Identity Vault 與已連接系統之間的資料同步化。已連接系統由應用程式、目錄、資料庫或檔案組成。

Identity Manager 包含數個元件。下列圖例顯示基本元件及其關係：

特性 ***1-1*** *Identity Manager* 元件



Metadirectory 引擎是 Identity Manager 結構中的關鍵模組。它會提供允許 Identity Manager 驅動程式與 Identity Vault 同步化資訊的介面，甚至允許不同的資料系統連接和共享資料。

Metadirectory 引擎使用 XML 格式處理 Identity Vault 資料和 Identity Vault 事件。Metadirectory 引擎利用規則處理器和資料轉換引擎來處理兩個系統之間流動的資料。

1. 讀取所有 Identity Manager 驅動程式的過濾器。
2. 註冊適當 Identity Vault 事件的驅動程式。
3. 根據每個驅動程式的規格過濾資料。
4. 對傳遞到每個驅動程式的 Identity Vault 事件設定快取。

Identity Vault 啓始化時會執行下列動作：

- 快取事件之後，擁有快取的驅動程式會讀取事件。
- 驅動程式接收採用 eDirectory 原始格式的 Identity Vault 資料、將其轉換爲 XDS 格式 (這是 Identity Manager 所使用的 XML 詞彙，可由規則加以轉換)，並將事件傳送至 Metadirectory 引擎。該引擎會讀取已連接系統驅動程式中的所有規則，並根據那些規則建立 XML 格式的資料，然後將資料傳送至連接系統驅動程式。之後，它會將資料傳送至已連接系統。如需規則的相關資訊，請參閱《規則產生器和驅動程式自訂指南》中的「規則簡介」。
- 驅動程式中的「發行者」部份會蒐集已連接系統中的更新並將其傳送至 Identity Vault。當通知連接系統驅動程式關於兩個系統共享之資訊的變更時，已連接系統驅動程式會蒐集該資訊，確保已將其過濾至正確的資料集、將資料轉換爲 XDS 格式並傳送至引擎。

1.2.1 Metadirectory 引擎

Metadirectory 引擎可以分成兩個元件：eDirectory 介面和同步化引擎。

eDirectory 介面

內建於 Metadirectory 引擎的 eDirectory 介面用於偵測 eDirectory 中發生的事件。此介面會使用事件快取，確保事件傳送至 Identity Manager。eDirectory 介面支援多重驅動程式載入，這表示針對該 eDirectory 伺服器僅會執行一個 Identity Manager 例項，但該例項可與多個已連接系統通訊。此介面中會內建迴路偵測，以防止 Identity Vault 與已連接系統之間發生事件迴路。雖然該介面包含迴路保護，但開發人員最好也將迴路偵測內建到個別的已連接系統驅動程式。

同步化引擎

同步化引擎會將 Identity Manager 規則套用至呈現給它的每個事件。該規則是使用「DirXML 程序檔」在「規則產生器」中建立的。「規則產生器」可讓您透過 GUI 介面 (而不是使用以 XSLT 撰寫的 XML 文件或樣式表) 建立規則。您仍然可以使用樣式表，但「規則產生器」會更便於使用。如需「規則產生器」或「DirXML 程序檔」的相關資訊，請參閱《規則產生器和驅動程式自訂指南》。

同步化引擎會將每種類型的規則都套用至來源文件。完成這些轉換的能力是 Identity Manager 的其中一個最強大的功能。當資料在 Identity Vault 與已連接系統之間共享時，會即時轉換該資料。

1.2.2 驅動程式組態檔案

驅動程式組態是 Identity Manager 隨附的預先設定 XML 檔案。您可透過 iManager 和 Designer 中的精靈輸入這些組態檔案。

這些驅動程式組態包含範例規則。該範例規則不是要用於生產環境中，而是要做爲您可以修改的範本。

1.2.3 Identity Manager 事件快取

透過 eDirectory 產生的所有事件在成功處理完成之前，都儲存在事件快取中。這可保證不會由於連接不良、系統資源遺失、驅動程式無法使用或任何其他網路失敗而遺失資料。

1.2.4 驅動程式 Shim

驅動程式 Shim 的功能是做爲已連接系統與 Identity Vault 之間的資訊管道。Shim 是使用 Java、C 或 C++ 撰寫的。

Metadirectory 引擎與驅動程式 Shim 之間的通訊以 XML 文件的形式進行，該文件會描述事件、查詢和結果。驅動程式 Shim 通常是指驅動程式。它是 Identity Vault 與已連接系統之間傳送資訊的管道。

Shim 支援下列物件事件：

- 新增 (建立)
- 修改

- 刪除
- 重新命名
- 移動
- 查詢

此外，Shim 必須支援已定義的查詢功能，這樣 Identity Manager 才可以查詢已連接系統。

當 Identity Vault 中發生某事件，導致已連接系統中產生動作時，Identity Manager 會建立描述該 Identity Vault 事件的 XML 文件，並透過「訂閱者」通道將其提交至驅動程式 Shim。

已連接系統中發生事件時，驅動程式 Shim 會產生 XML 文件，描述已連接系統事件。然後驅動程式 Shim 會透過「發行者」通道將該 XML 文件提交至 Identity Manager。透過任何「發行者」規則處理事件之後，Identity Manager 會讓 Identity Vault 採取適當的動作。

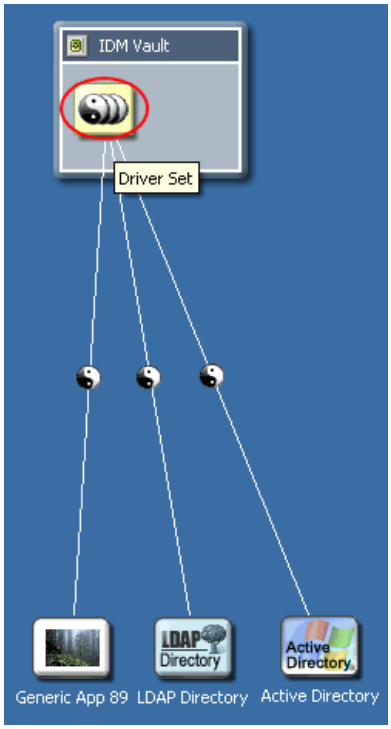
1.2.5 驅動程式集

驅動程式集是存放 Identity Manager 驅動程式的容器物件。驅動程式集一次可與一個伺服器相關聯。因此，所有執行中的驅動程式都必須分組到相同的驅動程式集中。

驅動程式集物件必須存在於使用該物件之任何伺服器上的完整讀 / 寫複製本中，因此建議您分割驅動程式集。建議您這樣做，當使用者的複製本移動到其他伺服器時，才不會移動驅動程式物件。

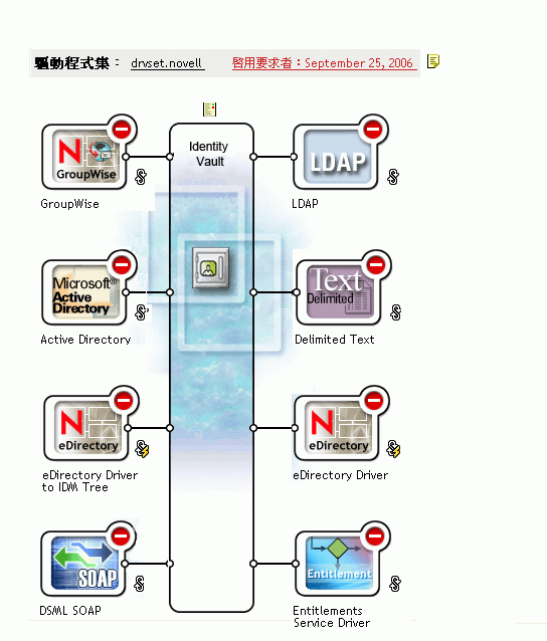
下圖顯示驅動程式集在 Designer 中的顯示方式。

特性 ***1-2*** *Designer* 中的驅動程式集



下圖顯示驅動程式集在 iManager 中的顯示方式。

特性 ***1-3*** *iManager* 中的驅動程式集



從 Designer 中的「模擬器」(在上面的特性 1-2 頁上 12 中顯示) 或 iManager 中的「綜覽」頁面 (在上面的特性 1-3 頁上 13 中顯示)，您可以：

- 檢視和修改驅動程式集及其內容
- 檢視驅動程式集中的驅動程式
- 變更驅動程式狀態
- 將驅動程式集與伺服器相關聯
- 新增或移除驅動程式
- 檢視驅動程式集的啓用資訊
- 檢視驅動程式集的狀態記錄

1.2.6 驅動程式物件

「驅動程式」物件代表連接至與 Identity Vault 整合之已連接系統的驅動程式。下列元件構成驅動程式物件及其組態參數：

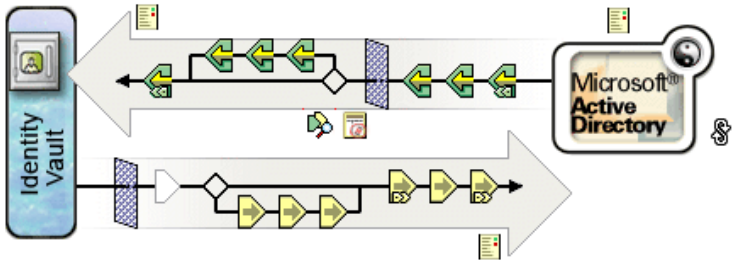
- 驅動程式集物件中包含之 eDirectory 網路樹中的「驅動程式」物件。
- 「驅動程式」物件中包含的「訂閱者」通道物件。
- 「驅動程式」物件中包含的「發行者」物件。
- 「驅動程式」、「訂閱者」和「發行者」物件所參照的數個規則物件。
- 「驅動程式」物件所參照的可執行驅動程式 Shim。
- 管理員已設定組態的 Shim 特定參數。
- 「驅動程式」物件的 eDirectory 密碼。Shim 可使用密碼來驗證 Shim 的遠端部份。

- 用於連接並驗證已連接系統的驗證參數。
- 授權 (雖然授權並不屬於每個驅動程式)。在建立驅動程式期間可啓用授權，也可稍後新增授權。
- 驅動程式的啓動選項，包含下列內容：
  - 停用：驅動程式不執行。
  - 手動：必須透過 iManager 手動啓動驅動程式。
  - 自動啓動：驅動程式在 Identity Vault 啓動時自動啓動。
- 「綱要映射」規則的參照。
- 已連接系統之綱要的 XML 表示。這通常會透過 Shim 從已連接系統自動取得。

在 iManager 中，您可以存取「Identity Manager 驅動程式概觀」，並修改現有驅動程式的參數、規則、樣式表和授權。「Identity Manager 驅動程式概觀」顯示如下。

特性 ***1-4*** *Identity Manager* 驅動程式概觀

驅動程式：Active Directory.DriverSet.South.Novell



此外，還會使用「驅動程式」物件進行 eDirectory 權限檢查。必須授予「驅動程式」物件對其所讀取或寫入之任何物件的足夠 eDirectory 權限。若要執行此動作，您可讓「驅動程式」物件成爲驅動程式同步化之 eDirectory 物件的「託管者」，或者將「安全性等值」授予「驅動程式」物件。

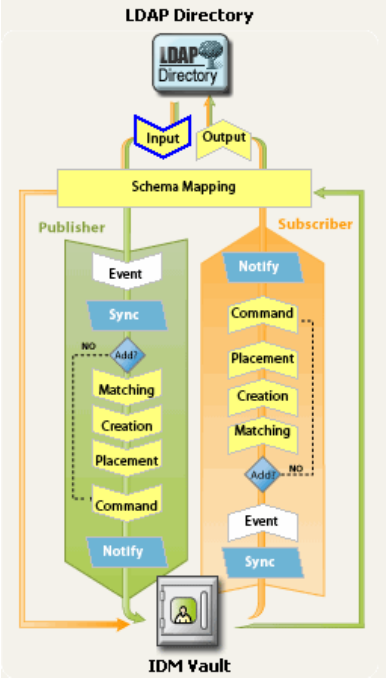
如需權限指定的相關資訊，請參閱《*Novell eDirectory 8.8* 管理指南》中的「eDirectory 權限 (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html)」。

1.2.7 發行者和訂閱者通道

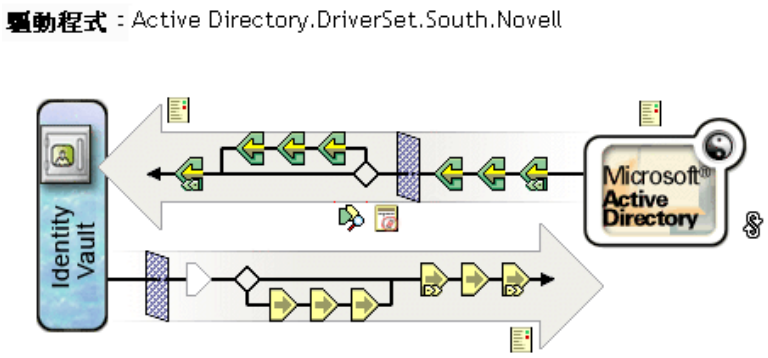
Identity Manager 驅動程式包含兩個用於處理資料的通道：「發行者」通道和「訂閱者」通道。「發行者」通道會將事件從已連接系統傳送至 Identity Vault。「訂閱者」通道會將事

件從 Identity Vault 傳送至已連接系統。每個通道都包含其本身的規則，該規則會定義如何處理和轉換資料。

特性 ***1-5*** *Designer* 中的發行者和訂閱者通道



特性 ***1-6*** *iManager* 中的發行者和訂閱者通道



1.2.8 事件和指令

Identity Manager 中事件與指令之間的差異非常重要。如果事件傳送至驅動程式，則該事件是指令。如果事件傳送至 Identity Manager，則該事件就是通知。當驅動程式將事件通知傳送至 Identity Manager 時，驅動程式會通知 Identity Manager 關於已連接系統中發生的變更。然後，Metadirectory 引擎會根據可設定組態的規則，判定必須要傳送至 Identity Vault 的指令 (如果有的話)。

當 Identity Manager 將指令傳送至驅動程式時，Identity Manager 已使用 Identity Vault 事件做爲輸入、套用適當的規則，並判定已連接系統中指令所代表的變更是必要的。

1.2.9 規則和過濾器

規則和過濾器可讓您控制資料從一個系統串流至另一個系統的方式。您是使用規則 (Policy) 中的規則 (Rule) 來定義轉換管理 Identity Vault 類別、屬性和事件如何用於已連接系統 (反之亦然)。如需規則和過濾器的詳細資訊，請參閱 《規則產生器和驅動程式自訂指南》。

1.2.10 關聯

大部份的其他身份管理產品都需要已連接系統儲存某種識別碼，以將物件從已連接系統映射至目錄。使用 Identity Manager 時，已連接系統無需任何變更。Identity Vault 中的每個物件都包含一個關聯表格，其映射在已連接系統中具有唯一識別碼的 Identity Vault 物件。該表格已反向編列索引，以便已連接系統在更新 Identity Vault 時，無需提供 Identity Vault 識別碼 (如可辨識名稱) 給驅動程式。

當尚未與 Identity Vault 中其他物件相關聯的物件發生事件時，會在兩個物件之間建立關聯。若要建立關聯，每個物件之間可定義的最小準則集必須相符。例如，您可以建立規則，指出如果四個屬性中的任何兩個相符率超過 90% (全名、電話號碼、員工 ID 和電子郵件地址)，則物件將會相關聯。

相符規則會定義判定兩個物件是否相同的準則。如果找不到變更物件的相符項目，可建立新物件。但必須符合所有的最低建立準則，才會發生此狀況。這些準則由「建立」規則定義。最後，「佈置」規則會定義在命名階層中建立新物件的位置。

可使用下面任意一種方式建立關聯：

- 做爲物件間的相符項目
- 做爲特定位置中新建立的物件

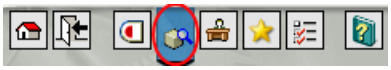
物件間的關聯建立之後，此關聯會一直有效，直到管理員刪除物件或刪除關聯爲止。

關聯表格

在 Identity Manager 中，關聯是指 eDirectory 中的物件與已連接系統中常駐的物件相符。起始安裝 Identity Manager 時，會延伸 eDirectory 綱要。此延伸的一部份是一個新屬性，連結至所有 eDirectory 物件的基礎類別。此屬性是關聯表格。關聯表格會持續追蹤 eDirectory 物件連結的所有已連接系統物件。系統會自動建立和維護此表格，因此幾乎不需要手動編輯此資訊，不過檢視該資訊經常會很有幫助。

您可以在 iManager 中檢視物件的關聯屬性。

1. 在 iManager 中，選取工具列上的 「檢視物件」圖示。



2. 瀏覽並選取物件，然後選取 「修改物件」。
3. 選取 Identity Manager 索引標籤。

Identity Manager 索引標籤上會顯示關聯屬性。

1.3 使用者應用程式

「使用者應用程式」是提供解決方案。它是 Identity Manager 3 的附加產品。「使用者應用程式」將強大的核准工作流程與 Identity Manager 相整合。這可讓組織除了根據無需手動介入的自動規則外，還可根據人員的輸入來制定提供決策。如需相關資訊，請參閱使用者應用程式文件 (http://www.novell.com/documentation/idm)。

1.4 Designer

Designer 是獨立的用戶端應用程式。其包括 「模擬器」空間、「調色盤」、檢視窗、「規則產生器」、文件產生器和其他功能，以便您可以在高生產力的環境中設計、測試、記載和部署 Identity Manager 解決方案。如需 Designer 的相關資訊，請參閱 《*Designer for Identity Manager 3*：管理指南 *(http://www.novell.com/documentation/designer)*》。

管理 Identity Manager 驅動程式 2

本節包含協助您建立和管理 Identity Manager 驅動程式的資訊。主題包含：

2.1 建立並設定驅動程式

您應針對每個規劃要使用的 Identity Manager 驅動程式，建立驅動程式物件並輸入驅動程式組態。驅動程式物件包含該驅動程式的組態參數和規則。在建立驅動程式物件的過程中，您會輸入驅動程式特定的組態檔案。驅動程式組態包含預設規則集。這些規則是爲了要在實作資料共享模型時，讓您有一個好的起頭。大部份時候，您可以使用隨附的預設組態設定驅動程式，然後根據環境要求修改驅動程式組態。

您可以使用兩種方法建立驅動程式物件。

- 「建立驅動程式」任務可讓您建立單一驅動程式並輸入其驅動程式組態。如需相關資訊，請參閱 「建立驅動程式物件」，第 19 頁。
- 「輸入驅動程式」任務可讓您同時建立多個驅動程式並輸入其組態。如需相關資訊，請參閱 「建立多個驅動程式」，第 20 頁。

2.1.1 建立驅動程式物件

驅動程式組態 (XML) 檔案會建立驅動程式正常運作所需的物件並設定其組態。它還包含可以針對您的實作加以修改的範例規則。

1. 在 iManager 中，選取「*Identity Manager* 公用程式 > 新增驅動程式」。
2. 選取您要建立驅動程式的「驅動程式集」，然後按「下一步」。

   如果您將此驅動程式置於新的「驅動程式集」中，則必須指定「驅動程式集」名稱、網路位置和相關聯的伺服器。
3. 標記「從伺服器 *(.XML* 檔案 *)* 輸入驅動程式組態」，並選取 .xml 檔案，然後按「下一步」。

   當您設定 iManager 時，驅動程式組態檔就會安裝在 Web 伺服器上。

4 遵循提示，完成驅動程式組態的輸入。

必要的 Identity Manager 物件就會建立。如果您沒有在輸入期間定義安全性等值或排除管理使用者，則可以藉由修改驅動程式物件的內容完成這些任務。

附註：如果您不在輸入程序期間啓用「授權」，則不會建立「授權」規則。如果以後想要使用「授權」，則必須建立啓用「授權」的新驅動程式。

2.1.2 建立多個驅動程式

Identity Manager 提供一次建立數個驅動程式的功能。該程序其實與建立單一驅動程式類似，因爲驅動程式組態 (XML) 檔案仍然會建立驅動程式正常運作所需的物件並設定其組態。

若要同時輸入數個驅動程式，請執行下列動作：

1 在 iManager 中，選取「*Identity Manager* 公用程式 > 輸入驅動程式」。

2 選取您要建立新驅動程式的「驅動程式集」，然後按「下一步」。

如果您將這些驅動程式置於新的「驅動程式集」中，則必須指定「驅動程式集」名稱、網路位置和相關聯的伺服器。

3 選取要新增至「驅動程式集」的應用程式組態，然後按「下一步」。

4 遵循提示並指定所要求的資料，然後按「下一步」。

當您一次選取多個要輸入的組態時，一次會呈現給您一個應用程式組態頁。

每個驅動程式的必要 Identity Manager 物件就會建立。如果您沒有在輸入期間定義安全性等值或排除管理使用者，則可以藉由修改驅動程式物件的內容完成這些任務。

2.2 在 Identity Manager 環境中管理 DirXML 1.1a 驅動程式

針對 DirXML 1.1a 建立的現有驅動程式會繼續與 Identity Manager 一起執行。

Identity Manager 3.0 隨附的 Metadirectory 引擎與舊版的驅動程式反向相容 (只要已使用所有最新的更新程式和修補程式更新舊版驅動程式 Shim 和組態)。因爲引擎是反向相容的，所以只要您願意，就可以在 Identity Manager 伺服器上執行 DirXML 1.1a 驅動程式，而不必對其進行任何變更。

不過，iManager 外掛程式的反向相容性很有限。您可以在「驅動程式集」的「綜覽」中檢視舊版驅動程式，但如果不轉換驅動程式，則無法檢視或編輯驅動程式組態。當您在「驅動程式集概觀」中按一下 DirXML 1.1a 驅動程式時，Identity Manager 外掛程式會探查驅動程式是否爲 DirXML 1.1a 格式，並提示您使用精靈將驅動程式轉換爲 3.0 格式。

如果您不想對現有驅動程式進行任何變更，可以取消精靈。

若要編輯採用 1.1a 格式的 1.1a 驅動程式，必須使用 DirXML 1.1a 外掛程式。若要執行此動作，必須使用另一個已安裝 1.1a 外掛程式的 iManager Web 伺服器。如果不將驅動程式轉換爲 Identity Manager 3.0 格式，則您無法使用 Identity Manager 隨附的 Identity Manager 外掛程式編輯驅動程式組態。

2.3 將驅動程式組態從 DirXML 1.1a 升級至 Identity Manager 格式

從 DirXML 1.1a 升級的支援方式是安裝 Identity Manager 3。Identity Manager 3 安裝會安裝新的驅動程式 Shim，但不會變更現有的驅動程式物件或驅動程式組態。

針對 DirXML 1.1a 建立的現有驅動程式組態會繼續與 Identity Manager 一起執行。不過，Identity Manager 外掛程式可讓您僅編輯 Identity Manager 格式的驅動程式。

重要：不支援將 Identity Manager 驅動程式 Shim 或驅動程式組態與 DirXML 1.1a 引擎一起執行。

我們提供了精靈協助您將 DirXML 1.1a 驅動程式轉換爲 Identity Manager 格式。

若要啓動精靈，請執行下列動作：

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。
2. 選取包含您要轉換之驅動程式的「驅動程式集」，然後按一下「搜尋」。
3. 按一下您要轉換之驅動程式的圖示。

   會提示您將驅動程式轉換爲新的格式。
4. 遵循精靈中的步驟完成轉換。

2.4 啓動、停止或重新啓動驅動程式

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。
2. 瀏覽驅動程式所在的「驅動程式集」，然後按一下「搜尋」。
3. 按一下要變更狀態之驅動程式圖示的右上角，然後按一下「啓動驅動程式」(如果驅動程式已停止)，或按一下「停止驅動程式」(如果驅動程式正在執行)。

2.5 驅動程式參數

每個驅動程式的內容上都有驅動程式參數。這些參數會儲存驅動程式特定的資訊。參數儲存的資訊包括輪詢間隔、驗證方法、使用保全插槽層 (Secure Socket Layer，SSL) 或設定驅動程式的活動訊號等等。

2.6 使用全域組態值

全域組態值 (Global Configuration Values，GCV) 是與驅動程式參數類似的設定。您可以針對「驅動程式集」和個別驅動程式指定全域組態值。如果驅動程式沒有全域組態值 (GCV)，則會從「驅動程式集」承襲該 GCV。

全域組態值 (GCV) 可讓您指定 Identity Manager 功能的設定，例如密碼同步化和驅動程式活動訊號，以及個別驅動程式組態功能特定的設定。驅動程式會提供全域組態值 (GCV)，但您還可以新增自己的 GCV。您可以參考規則中的這些值，以協助您自定驅動程式組態。

重要：雖然密碼同步化設定是全域組態值 (GCV)，但您最好在驅動程式之「伺服器變數」頁 (而不是 GCV 頁) 上提供的圖形化介面中編輯這些設定。與其他驅動程式參數類似，可以如同存取索引標籤一般存取顯示「密碼同步化」設定的「伺服器變數」頁，或者也可以

按一下「密碼管理 > 密碼同步化」、搜尋驅動程式，然後按一下驅動程式名稱，來存取該頁。該頁包含每個「密碼同步化」設定的線上說明。

若要新增、移除或編輯與「Identity Manager 密碼同步化」無關的全域組態值 (GCV)，請執行下列動作：

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。
2. 瀏覽並按一下「驅動程式集」或驅動程式物件，然後按一下「搜尋」。
3. 按一下驅動程式的右上角，然後按一下「編輯內容」。
4. 選取「全域組態值」。
5. 變更驅動程式建立期間設定的預設值。
6. 如果您要新增其他資訊，按一下「編輯 *XML*」。
7. 按一下「啓用 *XML* 編輯」。
8. 新增、移除或編輯 XML，然後按一下「確定」以套用變更。

2.7 使用 DirXML 命令列公用程式

「DirXML 命令列公用程式」提供對 Identity Manager 特定 eDirectory 動詞的存取權。此公用程式不是要取代 iManager 或 Designer。它的主要用途是用於指令碼。如需「DirXML 命令列公用程式」的詳細資訊，請參閱附錄 A 「DirXML 命令列公用程式」，第 225 頁。如果是日常任務，請使用 iManager 或 Designer。

2.8 檢視版本設定資訊

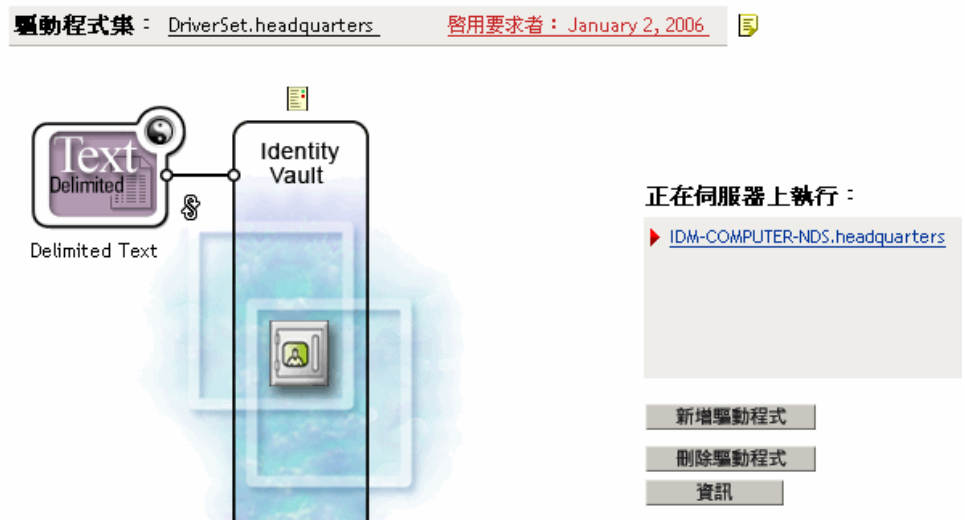
「版本設定探查工具」可讓您進行下列幾項操作：

- 「檢視版本設定資訊的階層式顯示」，第 22 頁
- 「檢視文字檔形式的版本設定資訊」，第 24 頁
- 「儲存版本設定資訊」，第 26 頁

2.8.1 檢視版本設定資訊的階層式顯示

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」，然後按一下「搜尋」以尋找「驅動程式集」。

2 在「Identity Manager 概觀」螢幕中，按一下「資訊」。



您也可以選取「*Identity Manager* 公用程式 > 版本探查」，然後瀏覽並選取「驅動程式集」，再按一下「確定」。

3 檢視版本設定資訊的頂層或未展開顯示的項目。

未展開的階層式檢視窗會顯示下列內容：

- 您已通過驗證的 eDirectory 網路樹
- 您選取的「驅動程式集」
- 與「驅動程式集」相關聯的伺服器

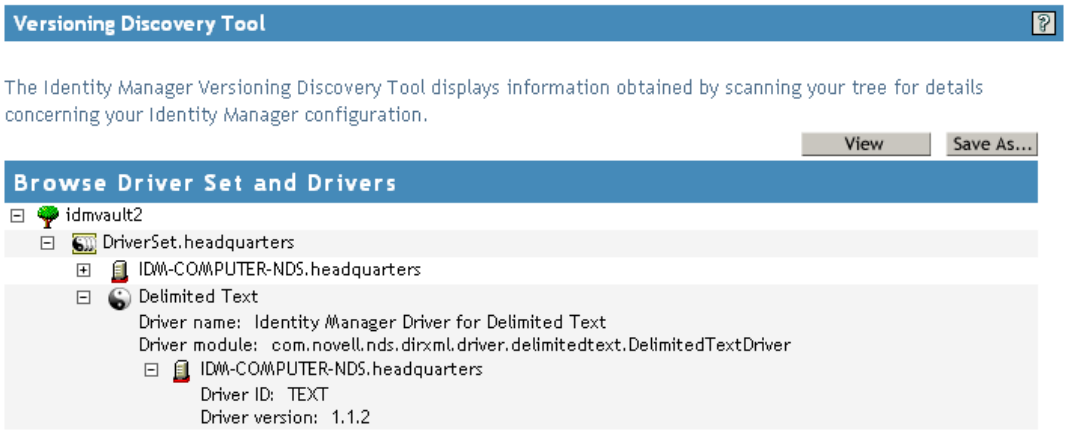
  如果「驅動程式集」與兩個或多個伺服器相關聯，則您可以檢視每個伺服器上的 Identity Manager 資訊。
- 驅動程式

4 展開伺服器圖示，可以檢視與伺服器相關的版本設定資訊。

頂層伺服器圖示的展開檢視窗會顯示下列內容：

- 上次記錄時間
- 伺服器上正在執行的 Identity Manager 版本

5 展開驅動程式圖示，可以檢視與驅動程式相關的版本設定資訊。



頂層驅動程式圖示的展開檢視窗會顯示下列內容：

- 驅動程式名稱
- 驅動程式模組 (例如 com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver)

驅動程式圖示下方伺服器的展開檢視窗會顯示下列內容：

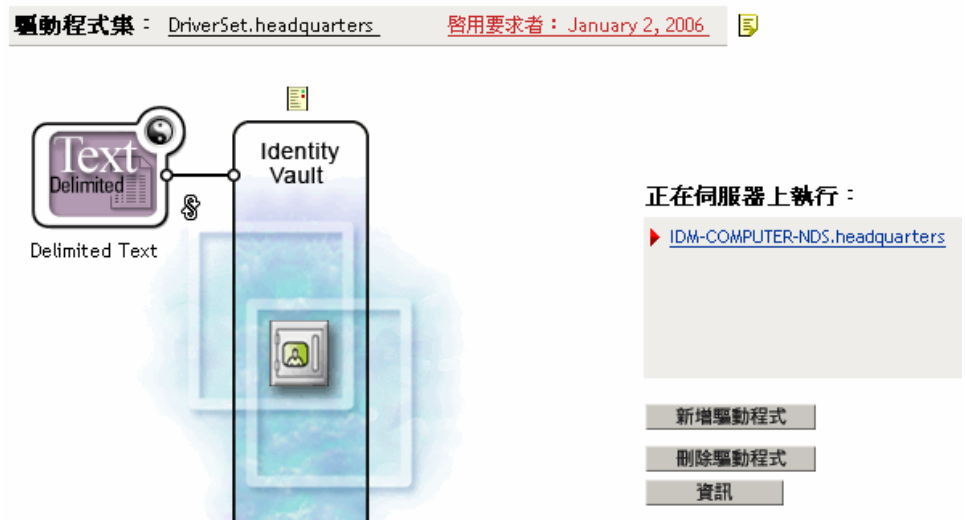
- 驅動程式 ID
- 該伺服器上正在執行之驅動程式例項的版本

2.8.2 檢視文字檔形式的版本設定資訊

Identity Manager 會將版本設定資訊發行至檔案。您可以使用文字格式檢視此資訊。文字表示與階層式檢視窗中包含的資訊是相同的。

1 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」，然後按一下「搜尋」以尋找「驅動程式集」。

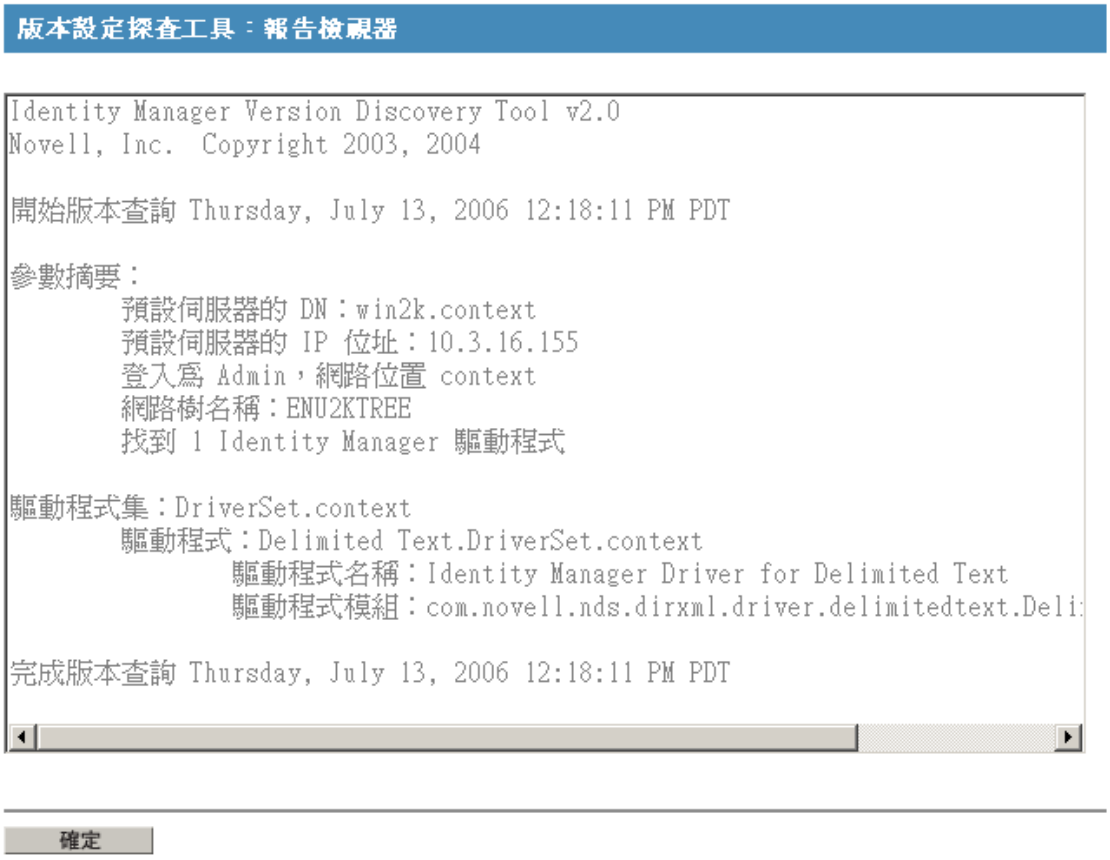
2 在「Identity Manager 概觀」螢幕中，按一下「資訊」。



您也可以選取「*Identity Manager* 公用程式 > 版本設定探查」，然後瀏覽並選取「驅動程式集」，再按一下「資訊」。

3 在「版本設定探查工具」對話方塊中，按一下「檢視」。

在「報告檢視器」視窗中，資訊會以文字檔形式顯示。

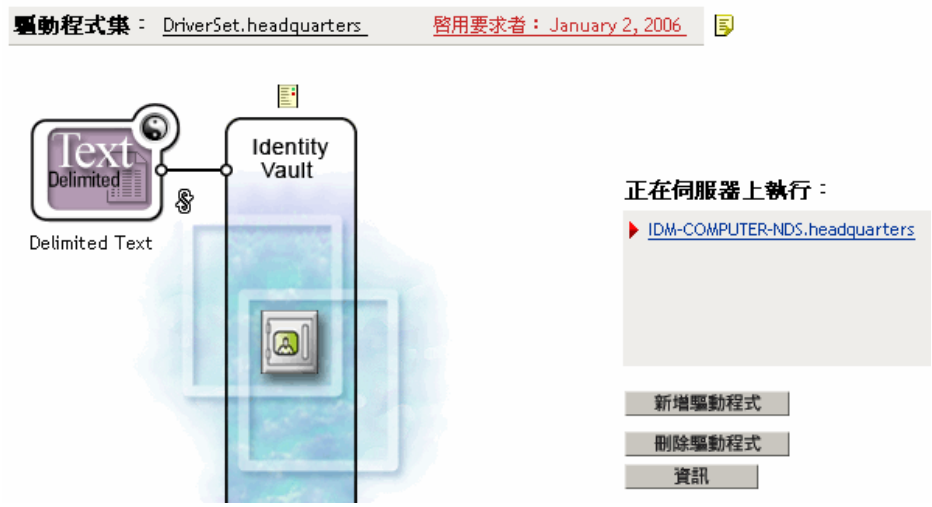


2.8.3 儲存版本設定資訊

您可以將版本設定資訊儲存至本地或網路磁碟機上的文字檔。

1 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」，然後按一下「搜尋」以尋找「驅動程式集」。

2 在「Identity Manager 概觀」螢幕中，按一下「資訊」。



您也可以選取「*Identity Manager* 公用程式 > 版本設定探查」，然後瀏覽並選取「驅動程式集」，再按一下「資訊」。

3 在「版本設定探查工具」對話方塊中，按一下「另存新檔」。

4 在「檔案下載」對話方塊中，按一下「儲存」。

5 導覽至所需的目錄、輸入檔名，然後按一下「儲存」。

Identity Manager 會將資料儲存至文字檔。

2.9 使用具名密碼

Identity Manager 可讓您安全地儲存特定驅動程式的多個密碼。此功能稱爲「具名密碼」。每個不同的密碼都是透過金鑰或名稱來存取。

您也可以使用「具名密碼」功能來安全地儲存其他資訊，例如使用者名稱。

若要在驅動程式規則中使用具名密碼，請依密碼名稱來參考密碼，而不是使用實際的密碼，Metadirectory 引擎會將密碼傳送至驅動程式。本節中所述之用於儲存和取回「具名密碼」的方法，可用於任何驅動程式，而不需要變更驅動程式 Shim。

附註：提供給 Identity Manager Driver for Lotus Notes 的範例組態包含以這種方式使用「具名密碼」的範例。此外，已自定 Notes 驅動程式 Shim，以支援「具名密碼」的其他使用方法，而且那些方法的範例也包含在內。如需相關資訊，請參閱《*Identity Manager Driver for Lotus Notes*：實作指南》中有關「具名密碼」的章節。

本節內容：

2.9.1 使用 Designer 設定具名密碼的組態

1. 選取「驅動程式」物件，然後按一下滑鼠右鍵並選取「內容」。
2. 選取「具名密碼」，然後按一下「新增」。

3. 指定「具名密碼」的「名稱」。
4. 指定「具名密碼」的「顯示名稱」。
5. 指定「具名密碼」，然後重新輸入密碼。
6. 按兩次「確定」。

2.9.2 使用 iManager 設定具名密碼的組態

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。

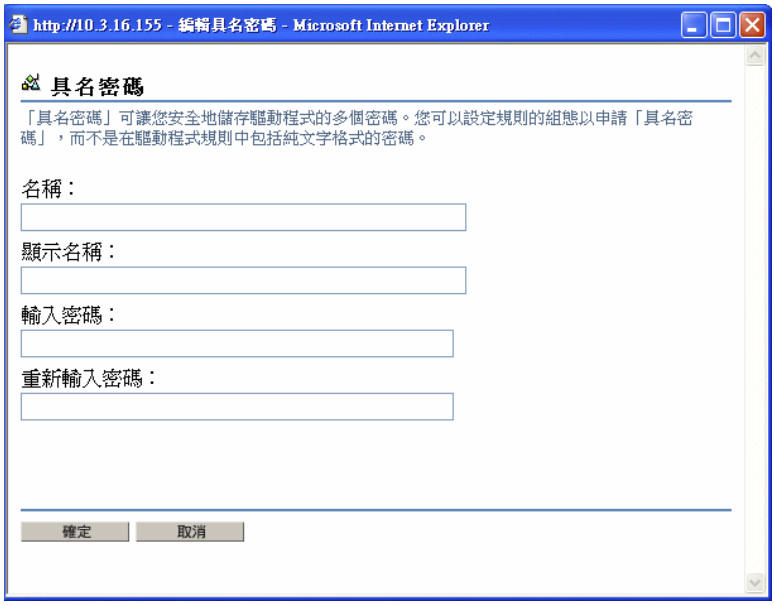
2 搜尋「驅動程式集」，或瀏覽並選取存放「驅動程式集」的容器。會顯示「驅動程式集」的圖形化表示。

3 在「Identity Manager 概觀」螢幕中，按一下驅動程式圖示的右上角，然後按一下「編輯內容」。

4 在「修改物件」頁中的 Identity Manager 索引標籤上，按一下「具名密碼」。

會顯示「具名密碼」頁，並列出此驅動程式目前的「具名密碼」。如果您尚未設定任何「具名密碼」，則該清單是空的。

5 若要新增 「具名密碼」，請按一下 「新增」、完成欄位，然後按一下 「確定」。



6 指定名稱、顯示名稱和密碼，然後按兩次 「確定」。

請記住，您可以使用此功能來安全地儲存其他類型的資訊，例如使用者名稱。

7 會顯示一則訊息：要重新啓動驅動程式以使變更生效？ (確定 = 是，取消 = 否) 按一下 「確定」。

8 若要移除 「具名密碼」，請按一下 「移除」。即會移除密碼，而不會提示您確認該動作。

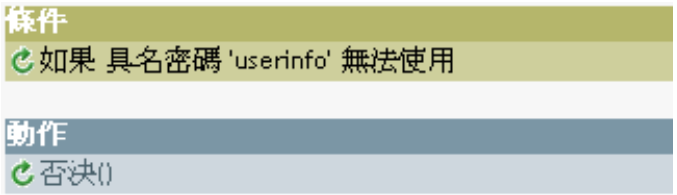
2.9.3 在驅動程式規則中使用具名密碼

- 「使用規則產生器」，第 30 頁
- 「使用 XSLT」，第 30 頁

使用規則產生器

「規則產生器」可讓您呼叫具名密碼。建立新規則並選取具名密碼做爲條件。視具名密碼是否可用而定，您可以設定動作。下列範例顯示如果具名密碼使用者資訊無法使用，則否決該事件。

特性 ***2-1*** 使用具名密碼的規則



使用 XSLT

下列範例顯示如何使用 XSLT 在 「訂閱者」通道上的驅動程式規則中參考具名密碼：

```
<xsl:value-of
select=”query:getNamedPassword($srcQueryProcessor,'mynamedpassword')”
xmlns:query=”http://www.novell.com/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.9.4 使用 DirXML 命令列公用程式設定具名密碼的組態

- 「在 DirXML 命令列公用程式中建立具名密碼」，第 31 頁
- 「在 DirXML 命令列公用程式中移除具名密碼」，第 32 頁

在 **DirXML** 命令列公用程式中建立具名密碼

1. 執行「DirXML 命令列公用程式」。

   如需相關資訊，請參閱附錄 A 「DirXML 命令列公用程式」，第 225 頁。
2. 輸入您的使用者名稱與密碼。

   下列選項清單即會出現。

   ```
   DirXML commands


    1: Start driver 2: Stop driver 3: Driver operations... 4: Driver
   set operations... 5: Log events operations... 6: Get DirXML version
   99: Quit


   Enter choice:
   ```

3. 輸入 3 以進行驅動程式相關操作。

   編號的驅動程式清單即會出現。
4. 輸入您要將「具名密碼」新增到的驅動程式號碼。

   下列選項清單即會出現。

   ```
   Select a driver operation for: driver_name


    1: Start driver 2: Stop driver 3: Get driver state 4: Get driver
   start option 5: Set driver start option 6: Resync driver 7: Migrate
   from application into DirXML 8: Submit XDS command document to
   driver 9: Check object password 10: Initialize new driver object
   11: Passwords operations 12: Cache operations 99: Exit


   Enter choice:
   ```

5. 輸入 11 以進行密碼相關密碼操作。

下列選項清單即會出現。

```
Select a password operation


 1: Set shim password 2: Reset shim password 3: Set named password
4: Clear named password(s) 5: List named passwords 99: Exit


Enter choice:
```

6 輸入 3 以設定新的「具名密碼」。

下列提示即會出現：

```
Enter password name:
```

7 輸入您要用於參考「具名密碼」的名稱。

8 在出現的下列提示中，輸入您要保護的實際密碼：

```
Enter password:
```

您輸入的密碼字元不會顯示。

9 在出現的下列提示中，重新輸入密碼進行確認：

```
Confirm password:
```

10 輸入並確認密碼之後，您將回到密碼操作功能表。

完成此程序之後，您可以使用兩次 99 選項，以結束功能表並離開「DirXML 命令列公用程式」。

在 **DirXML** 命令列公用程式中移除具名密碼

當您不再需要先前建立的「具名密碼」時，此選項很有用。

1 執行 DirXML 命令列公用程式。

如需相關資訊，請參閱附錄 A 「DirXML 命令列公用程式」，第 225 頁。

2 輸入您的使用者名稱與密碼。

下列選項清單即會出現。

```
DirXML commands


 1: Start driver 2: Stop driver 3: Driver operations... 4: Driver
set operations... 5: Log events operations... 6: Get DirXML version
99: Quit
```

```
Enter choice:
```

3 輸入 3 以進行驅動程式相關操作。

編號的驅動程式清單即會出現。

4 輸入您要移除其「具名密碼」的驅動程式號碼。

下列選項清單即會出現。

```
Select a driver operation for: driver_name


 1: Start driver 2: Stop driver 3: Get driver state 4: Get driver
start option 5: Set driver start option 6: Resync driver 7: Migrate
from application into DirXML 8: Submit XDS command document to
driver 9: Check object password 10: Initialize new driver object
11: Passwords operations 12: Cache operations 99: Exit


Enter choice:
```

5 輸入 11 以進行密碼相關密碼操作。

下列選項清單即會出現。

```
Select a password operation


 1: Set shim password 2: Reset shim password 3: Set named password
4: Clear named password(s) 5: List named passwords 99: Exit


Enter choice:
```

6 (選擇性) 輸入 5 以查看現有「具名密碼」清單。

現有「具名密碼」清單即會顯示。

此步驟有助於確保移除正確的密碼。

7 輸入 4 以移除一個或多個「具名密碼」。

8 在出現的下列提示中，輸入 No 以移除單一「具名密碼」：

```
Do you want to clear all named passwords? (yes/no):
```

9 在出現的下列提示中，輸入您要移除之「具名密碼」的名稱：

```
Enter password name:
```

在輸入要移除之「具名密碼」的名稱之後，您將回到密碼操作功能表：

```
Select a password operation


 1: Set shim password 2: Reset shim password 3: Set named password
4: Clear named password(s) 5: List named passwords 99: Exit


Enter choice:
```

10 (選擇性) 輸入 5 以查看現有「具名密碼」的清單。

現有「具名密碼」的清單即會顯示。

此步驟可讓您驗證已移除正確的密碼。

在完成此程序之後，您可以使用兩次 99 選項，以離開功能表並結束「DirXML 命令列公用程式」。

2.10 重新關聯驅動程式物件與伺服器

驅動程式物件與伺服器相關聯。

如果關聯由於某種原因而失效，則會以下列其中一種方式表示：

- 在 Identity Manager 伺服器上升級 eDirectory 時，您會看到錯誤「UniqueSPIException 錯誤：783」。
- 在「Identity Manager 概觀」螢幕中的驅動程式旁邊未列出任何伺服器。
- 在「Identity Manager 概觀」螢幕中的驅動程式旁邊列出伺服器，但其名稱是亂碼。

若要解決此問題，您必須取消驅動程式物件與伺服器的關聯，然後重新關聯兩者。

登入 iManager 並移至「Identity Manager 概觀」螢幕中的「驅動程式」物件。使用圖示來移除並新增伺服器至驅動程式圖示旁邊的伺服器名稱清單。移除並新增操作會重新關聯伺服器與「驅動程式」物件。

2.11 新增驅動程式活動訊號

驅動程式活動訊號是 Identity Manager 2 和更新版本隨附之 Identity Manager 驅動程式的一個功能。您可以選擇使用該功能。藉由以指定的時間間隔來使用驅動程式參數，可以設定驅動程式活動訊號的組態。如果活動訊號參數存在並具有非 0 的間隔值，則當在指定時間間隔「發行者」通道上沒有通訊時，驅動程式會將活動訊號文件傳送至 Metadirectory 引擎。

驅動程式活動訊號的目的是，如果驅動程式在「發行者」通道上通訊的頻率與您想要該動作發生的頻率不符時，它可讓您透過觸發作業來定期啓始動作。如果您要利用活動訊號，必須自定驅動程式組態或其他工具。Metadirectory 引擎會接受活動訊號文件，但不會因此採取任何動作。

對於大部份驅動程式而言，範例組態中並沒有使用活動訊號的驅動程式參數，但您可以新增它。

如果驅動程式開發人員已撰寫驅動程式以提供支援，則 Identity Manager 未提供的自定驅動程式也可以提供活動訊號文件。

若要設定活動訊號的組態，請執行下列動作：

1. 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」。
2. 瀏覽並選取「驅動程式集」，然後按一下「搜尋」。
3. 在「Identity Manager 概觀」螢幕中，按一下驅動程式圖示的右上角，然後按一下「編輯內容」。
4. 在 Identity Manager 索引標籤中，按一下「驅動程式組態」、向下捲動至「驅動程式參數」，並尋找「活動訊號」或類似的顯示名稱。

   如果已存在活動訊號的驅動程式參數，您可以變更間隔並儲存變更，即可完成組態設定。

   間隔值不可以小於 1。若值爲 0，則表示已關閉該功能。

   時間單位通常爲分鐘；不過，部份驅動程式可能有不同的選擇，例如使用秒。
5. 如果不存在活動訊號的驅動程式參數，請按一下「編輯 XML」。
6. 新增驅動程式參數項目 (如下列範例所示) 做爲 <publisher-options> 的子代 (若爲 AD 驅動程式，請將其設爲 <driver-options> 的子代)。

   ```
   <pub-heartbeat-interval display-name="Heart Beat">10</pub-
   heartbeat-interval>
   ```

   提示：如果驅動程式在重新啓動後沒有產生活動訊號文件，請檢查 XML 中驅動程式參數的位置。

   ---
7. 儲存變更，並確定已停止和重新啓動驅動程式。

新增驅動程式參數之後，您可以使用圖形化檢視窗來編輯時間間隔。您也可以針對時間間隔建立全域組態值 (GCV) 的參考。與其他全域組態值類似，驅動程式活動訊號可以在「驅動程式集」層級 (而不是在每個個別驅動程式物件上) 設定。如果驅動程式沒有特定全域組態值，而「驅動程式集」有該值，則前者會從後者承襲該值。

下列是 Notes 驅動程式傳送的範例活動訊號狀態文件：

```
<nds dtdversion="2.0" ndsversion="8.x"> <source> <product
build="20031112_1037" instance="blackcap" version="2.0">DirXML Driver
for Lotus Notes</product> <contact>Novell, Inc.</contact> </source>
<input> <status level="success" type="heartbeat"/> </input> </nds>
```

2.12 檢視 Identity Manager 程序

若要檢視 Identity Manage 處理事件，請使用 DSTRACE。僅在測試和疑難排解 Identity Manager 時才會使用它。在驅動程式用於生產時執行 DSTRACE，會提高 Identity Manager 伺服器的使用率，且會導致事件處理非常緩慢。

爲了在 DSTRACE 中看到 Identity Manager 程序，會將值新增至「驅動程式集」和「驅動程式」物件。您可以在 Designer 和 iManager 中這樣做。

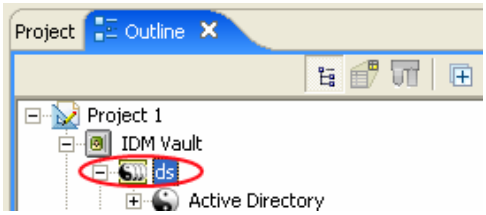
- 「在 Designer 中新增追蹤層級」，第 36 頁
- 「在 iManager 中新增追蹤層級」，第 37 頁
- 「擷取 Identity Manager 程序至檔案」，第 38 頁

2.12.1 在 Designer 中新增追蹤層級

您可以將追蹤層級新增至 「驅動程式集」物件或每個 「驅動程式」物件。

驅動程式集

1 在 Designer 中開啓的專案內，選取 「大綱」檢視窗中的 「驅動程式集」物件。



2 按一下滑鼠右鍵並選取 「內容」，然後按一下 「*5.* 追蹤」。

3 設定用於追蹤的參數，然後按一下 「確定」。如需 「驅動程式集」追蹤參數的相關資訊，請參閱表格 2-1 頁上 36。

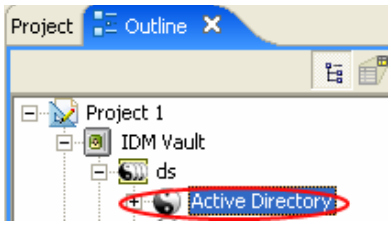
如果在 「驅動程式集」物件上設定追蹤層級，則所有驅動程式都會顯示在 DSTRACE 記錄中。

表格 ***2-1*** 驅動程式集追蹤參數

參數	描述
驅動程式追蹤層級	隨著 「驅動程式」物件追蹤層級的增加，DSTRACE 中顯示的資訊量也會增加。 追蹤層級一顯示錯誤，但不會顯示錯誤原因。如果您要查看密碼同步化資訊，請將追蹤層級設爲五。
XSL 追蹤層級	DSTRACE 會顯示 XSL 事件。僅在疑難排解 XSL 樣式表時才設定此追蹤層級。如果您不想要查看 XSL 資訊，請將層級設爲零。
Java 除錯埠	允許開發人員連接 Java 除錯程式。
Java 追蹤檔案	在此欄位中設定值時，「驅動程式集」物件的所有 Java 資訊都會寫入檔案。此欄位中的值是該檔案的修補。 只要指定該檔案，Java 資訊就會寫入此檔案。如果您不需要除錯 Java，請將此欄位保留空白。
追蹤檔案大小限制	允許您設定 Java 追蹤檔案的限制。如果您將檔案大小設爲沒有限制，則檔案大小會一直增加，直到沒有剩餘的磁碟空間爲止。

驅動程式

1 在 Designer 中開啓的專案內，選取「大綱」檢視窗中的「驅動程式」物件。



2 按一下滑鼠右鍵並選取「內容」，然後按一下「*8.* 追蹤」。

3 設定用於追蹤的參數，然後按一下「確定」。如需這些參數的相關資訊，請參閱表格 2-2 頁上 37。

如果僅在「驅動程式」物件上設定參數，則 DSTRACE 記錄中僅會顯示該驅動程式的資訊。

表格 **2-2** 驅動程式追蹤參數

參數	描述
追蹤層級	隨著「驅動程式」物件追蹤層級的增加，DSTRACE 中顯示的資訊量也會增加。 追蹤層級一顯示錯誤，但不會顯示錯誤原因。如果您想要查看密碼同步化資訊，請將追蹤層級設爲五。 如果選取「*使用驅動程式集的設定*」，則會從「驅動程式集」物件取得該值。
追蹤檔案	爲選定的驅動程式指定要寫入 Identity Manager 資訊的檔名和位置。 如果選取「*使用驅動程式集的設定*」，則會從「驅動程式集」物件取得該值。
追蹤檔案大小限制	允許您設定 Java 追蹤檔案的限制。如果您將檔案大小設爲沒有限制，則檔案大小會一直增加，直到沒有剩餘的磁碟空間爲止。 如果選取「*使用驅動程式集的設定*」，則會從「驅動程式集」物件取得該值。
追蹤名稱	輸入的值 (而不是驅動程式名稱) 會預加在驅動程式追蹤訊息中。請在驅動程式名稱過長時使用。

2.12.2 在 iManager 中新增追蹤層級

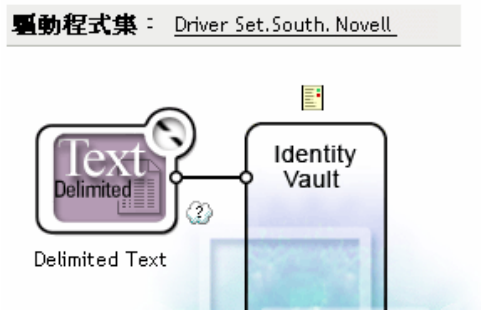
您可以新增追蹤層級至「驅動程式集」物件或每個「驅動程式」物件。

驅動程式集

1 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」。

2 瀏覽至 「驅動程式集」物件，然後按一下 「搜尋」。

3 按一下 「驅動程式集」名稱。



4 選取 「驅動程式集」物件的 「其他」索引標籤。

5 設定用於追蹤的參數，然後按一下 「確定」。如需這些參數的相關資訊，請參閱表格 2-1 頁上 36。

驅動程式

1 在 iManager 中，選取 「*Identity Manager* > *Identity Manager* 概觀」。

2 瀏覽至 「驅動程式」物件所在的 「驅動程式集」物件，然後按一下 「搜尋」。

3 按一下 「驅動程式」物件的右上角，然後按一下 「編輯內容」。

4 選取 「驅動程式」物件的 「其他」索引標籤。

5 設定用於追蹤的參數，然後按一下 「確定」。如需相關資訊，請參閱表格 2-2 頁上 37。

附註：選項 「使用驅動程式集的設定」不存在於 iManager 中。

2.12.3 擷取 Identity Manager 程序至檔案

爲了將 Identity Manager 程序儲存至檔案中，會透過 「驅動程式」物件上的參數或透過 DSTRACE 來進行儲存。 「驅動程式」物件上的參數是 「追蹤檔案」參數。

下列方法可協助您透過不同 OS 平台上的 DSTRACE 擷取並儲存 Identity Manager 程序。

NetWare

使用 DSTRACE.NLM，將追蹤訊息顯示在系統主控台上，或將追蹤訊息擷取到檔案 (SYS:\SYSTEM\DSTRACE.LOG)。DSTRACE.NLM 將追蹤訊息顯示到標示爲 「DSTRACE 主控台」的螢幕中。

1 在伺服器主控台中輸入 DSTRACE.NLM。

即會將 DSTRACE.NLM 載入至記憶體中。

2 在伺服器主控台上輸入 DSTRACE SCREEN ON。

允許追蹤訊息出現在 「DSTRACE 主控台」螢幕上。

3 在伺服器主控台中輸入 DSTRACE FILE ON。

將傳送至 「DSTRACE 主控台」的追蹤訊息擷取至 DSTRACE.LOG 中。

4 在伺服器主控台中輸入 DSTRACE -ALL。

關閉所有追蹤旗標。

5 在伺服器主控台中輸入 DSTRACE +DXML DSTRACE +DVRS。
顯示 Identity Manager 事件。

6 在伺服器主控台中輸入 DSTRACE +TAGS DSTRACE +TIME。
顯示訊息標籤和時戳。

7 切換至「DSTRACE 主控台」螢幕，並監視要傳遞的事件。

8 切換回伺服器主控台。

9 在伺服器主控台中輸入 DSTRACE FILE OFF。
停止將追蹤訊息擷取到記錄檔案。同時會停止將資訊記錄到檔案中。

10 在文字編輯器中開啓 DSTRACE.LOG，並搜尋已修改的物件或事件。

Windows

1 開啓「控制台」>「NDS 服務」>「dstrace.dlm」，然後按一下「啓動」。
即會開啓名爲「NDS 伺服器追蹤公用程式」的視窗。

2 選取「編輯」>「選項」，然後按一下「全部清除」。
即會清除所有預設旗標。

3 選取「*DirXML*」和「*DirXML* 驅動程式」。

4 按一下「確定」。

5 選取「檔案 > 新增」。

6 指定要儲存 DSTRACE 資訊的檔名和位置，然後按一下「開啓」。

7 等待事件發生。

8 選取「檔案 > 關閉」。
即會停止將資訊寫入記錄檔案中。

9 在文字編輯器中開啓該檔案，並搜尋已修改的物件或事件。

UNIX

1 輸入 ndstrace 以啓動 ndstrace 公用程式。

2 輸入 set ndstrace=nodebug
關閉目前設定的所有追蹤旗標。

3 輸入 set ndstrace on
將追蹤訊息顯示到主控台。

4 輸入 set ndstrace file on
將追蹤訊息擷取至 eDirectory 安裝目錄的 ndstrace.log 檔案中。預設爲 /var/nds。

5 輸入 set ndstrace=+dxml
顯示 Identity Manager 事件。

6 輸入 set ndstrace=+dvrs
顯示 Identity Manager 驅動程式事件。

7 等待事件發生。

8 輸入 set ndstrace file off

即會停止將資訊記錄到檔案中。

9 輸入 exit 以結束 ndstrace 公用程式。

10 在文字編輯器中開啓該檔案。搜尋已修改的物件或事件。

iMonitor

iMonitor 可讓您從網頁瀏覽器取得 DSTRACE 資訊。Identity Manager 的執行位置並不重要。執行 iMonitor 的檔案如下所示：

- NDSIMON.NLM，在 NetWare 上執行。
- NDSIMON.DLM，在 Windows 上執行。
- ndsimonitor，在 UNIX 上執行。

1 從 http://*server_ip*:8008/nds 存取 iMonitor。

預設連接埠是連接埠 8008。

2 輸入具有管理權限的使用者名稱和密碼，然後按一下 「登入」。

3 選取左邊的 「追蹤組態」。

4 按一下 「全部清除」。

5 選取 「DirXML」和 「DirXML 驅動程式」。

6 按一下 「開啓追蹤」。

7 選取左邊的 「追蹤歷程」。

8 按一下具有 「目前修改時間」的文件，以查看即時追蹤。

9 如果要更常查看資訊，請變更 「重新整理間隔」。

10 選取左邊的 「追蹤組態」，然後按一下 「關閉追蹤」，以關閉追蹤。

11 您可以選取 「追蹤歷程」來檢視追蹤的歷程。您可以依時戳來區分這些檔案。

如果需要 HTML 檔案的副本，則預設位置爲：

- NetWare：SYS:\SYSTEM\ndsimon\DSTRACE*.htm
- Windows：*Drive_letter*:\Novell\NDS\ndsimon\dstrace*.htm
- UNIX：/var/nds/dstrace/*.htm

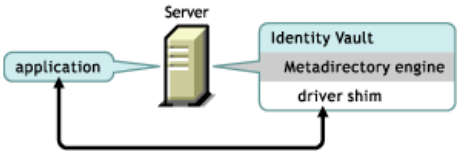
設定已連接系統。 3

本節提供下列資訊：

3.1 綜覽

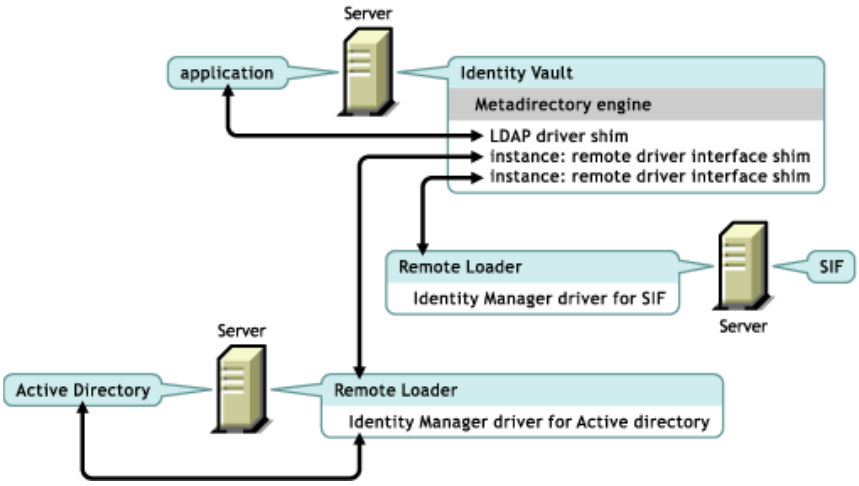
如下圖所示，Metadirectory 引擎在伺服器上做爲 eDirectory 的一部份執行。Identity Manager 驅動程式 Shim 及其已設定組態的驅動程式會與應用程式進行通訊，並且會與 Metadirectory 引擎進行通訊。

特性 ***3-1*** 在 *eDirectory* 下執行的 *Metadirectory* 引擎



如下圖所示，已連接系統會在應用程式中擴充 Identity Manager 功能：

特性 ***3-2*** 已連接系統，包含遠端載入器



已連接系統需要 「遠端載入器」。此服務可讓 Metadirectory 引擎與做爲不同程序並在不同位置執行的 Identity Manager 驅動程式交換資料，包含下列情況：

- 做爲執行 Metadirectory 引擎所在伺服器的單獨程序

Metadirectory 引擎做爲 eDirectory 程序的一部份執行。Identity Manager 驅動程式可以在執行 Metadirectory 引擎所在的伺服器上執行。實際上，它們可以與 Metadirectory 引擎做爲部份相同的程序執行。

不過，基於策略性原因，您可能想要讓 Identity Manager 驅動程式做爲單獨程序在伺服器上執行。然而，Identity Manager 驅動程式通常會在單獨的伺服器上執行。

如果驅動程式是做爲單獨的程序執行，則「遠端載入器」會在 Metadirectory 引擎與驅動程式之間提供通訊通道。

- 在執行 Metadirectory 引擎所在伺服器之外的伺服器上

  部份 Identity Manager 驅動程式無法在執行 Metadirectory 引擎所在的伺服器上執行。「遠端載入器」可讓您在一個環境中執行 Metadirectory 引擎，而在另一個環境中的伺服器上執行 Identity Manager 驅動程式。例如，您無法在 NetWare 伺服器上執行 Active Directory 驅動程式。Metadirectory 引擎可以在 NetWare 伺服器上執行，而「遠端載入器」會在 Active Directory 伺服器上執行。

  案例：單獨的伺服器。Metadirectory 引擎在 NetWare 伺服器上執行。您需要執行 Identity Manager Driver for Active Directory。因爲此驅動程式必須在 Active Directory 環境中執行，所以它無法在 NetWare 伺服器上執行。您可以在 Windows Server 2003 上安裝和執行「遠端載入器」。「遠端載入器」會在 Active Directory 驅動程式與 Metadirectory 引擎之間提供通訊通道。

  案例：非主機。Metadirectory 引擎在 Solaris 伺服器上執行。您需要與要供應使用者帳戶的網路資訊服務 (Network Information Services，NIS) 系統進行通訊。該系統通常不代管 Metadirectory 引擎。您可以在網路資訊服務 (NIS) 系統上安裝「遠端載入器」和 Identity Manager Driver for NIS。NIS 系統上的「遠端載入器」會執行 NIS 驅動程式，並可讓 Metadirectory 引擎和 NIS 驅動程式交換資料。

Identity Manager 3 透過 dirxml_remote、rdxml 或 dirxml_jremote 提供「遠端載入器」功能。.

Dirxml_remote

Dirxml_remote 是執行檔，可讓 Metadirectory 引擎與在 Windows 上執行的 Identity Manager 驅動程式進行通訊。

「遠端載入器主控台」使用 dirxml_remote.exe。如果您不使用任何參數而從指令行指定 dirxml_remote.exe，則會啓動「遠端載入器應用程式精靈」。如果輸入 dirxml_remote.exe，然後傳入參數，則會啓動「遠端載入器」。

Rdxml

Rdxml 是執行檔，可讓 Metadirectory 引擎與在 Solaris、Linux 或 AIX 環境中執行的 Identity Manager 驅動程式進行通訊。

Rdxml 可支援原生和 Java 驅動程式。

Dirxml_jremote

Dirxml_jremote 是純「Java 遠端載入器」。它用來在一個伺服器上執行的 Metadirectory 引擎與在其他位置 (未執行 rdxml 或 Dirxml_jremote) 執行的 Identity Manager 驅動程式之間交換資料。它應該可以在具有相容 JRE (最低 1.4.0、1.4.2 或以上版本 (建議)) 和 Java Sockets 的任何系統上執行，但只在下列系統上受到正式支援：

- HP-UX
- AS/400

- OS/390
- z/OS

綜覽：主要任務

使用「遠端載入器」涉及下列任務：

- 如果您規劃使用保全插槽層 (SSL)，請提供證書以進行安全的資料傳送。
- 安裝、設定和執行「遠端載入器」。
- 輸入、設定和啓動 Identity Manager 驅動程式。

部份管理員希望在設定「遠端載入器」之前，輸入並設定 Identity Manager 驅動程式的組態。例如，驅動程式可能已在執行中，但您想要讓其遠端執行。

另一方面，如果「遠端載入器」正在執行中，則您可以輸入、設定和啓動驅動程式，然後立即檢查在 Metadirectory 引擎、「遠端載入器」與 Identity Manager 驅動程式之間是否在進行適當的通訊。

3.2 提供安全資料傳送

如果您規劃使用保全插槽層 (SSL)，以便可以提供安全資料傳送，請完成下列任務：

1. 建立伺服器證書。

   如果您不熟悉證書，請建立一個新的證書。

   不過，如果保全插槽層 (SSL) 伺服器證書已存在，且您熟悉 SSL 證書，則可以使用現有的證書，而不是建立並使用新的證書。

   當伺服器加入網路樹時，eDirectory 會建立下列預設證書：
   - SSL CertificateIP
   - SSL CertificateDNS
2. 輸出自行簽署的證書。

3.2.1 建立伺服器證書

1 在 Novell iManager 中，按一下「*Novell Certificate Server* > 建立伺服器證書」。

2 選取將擁有證書的伺服器，並爲證書提供綽號 (例如，remotecert)。

重要：建議您在證書綽號中不要使用空格。例如，請使用 remotecert 而非 remote cert。

同時，請記下證書綽號。您會將此綽號用於驅動程式之遠端連接參數的金鑰材料物件 (Key Material Object，KMO) 名稱。

3 保持「建立」方法設爲「標準」不變，然後按「下一步」。

4 檢視「摘要」、按一下「完成」，然後按一下「關閉」。

您已建立伺服器證書。繼續執行「輸出自行簽署的證書」，第 44 頁。

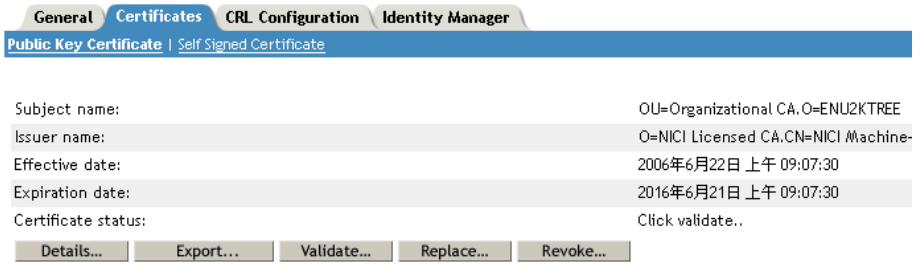
3.2.2 輸出自行簽署的證書

1 在 iManager 中，按一下「*eDirectory* 管理 > 修改物件」。

2 瀏覽並選取「安全性」容器中的「證書權限」，然後按一下「確定」。

證書權限 (Certificate Authority，CA) 是以網路樹名稱 (Treename-CA.Security) 命名的。

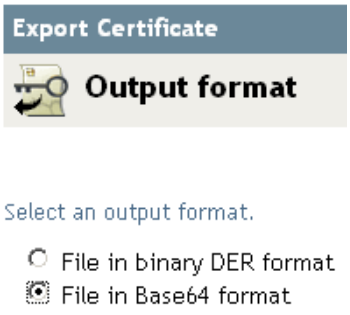
3 按一下「證書」索引標籤，按一下「自行簽署的證書」，然後按一下「輸出」。



4 在「輸出證書精靈」中，選取「否」，然後按「下一步」。

您不應將證書與私密金鑰一起輸出。

5 選取「*Base64* 格式的檔案」(例如，akranes-tree CA.b64)，然後按「下一步」。



6 按一下「將輸出證書儲存至檔案」連結、指定檔名、指定位置，然後按一下「儲存」。

根部檔案名稱需要 .pem 做爲副檔名。

7 在「另存新檔」對話方塊中，將此檔案複製到本地目錄。

8 按一下「關閉」。

3.3 設定遠端載入器

本節提供下列資訊：

- 「安裝遠端載入器」，第 45 頁
- 「設定遠端載入器的組態」，第 48 頁
- 「在 Solaris、Linux 或 AIX 上設定環境變數」，第 58 頁
- 「啓動遠端載入器」，第 58 頁「停止遠端載入器」，第 61 頁
- 「停止遠端載入器」，第 61 頁

3.3.1 安裝遠端載入器

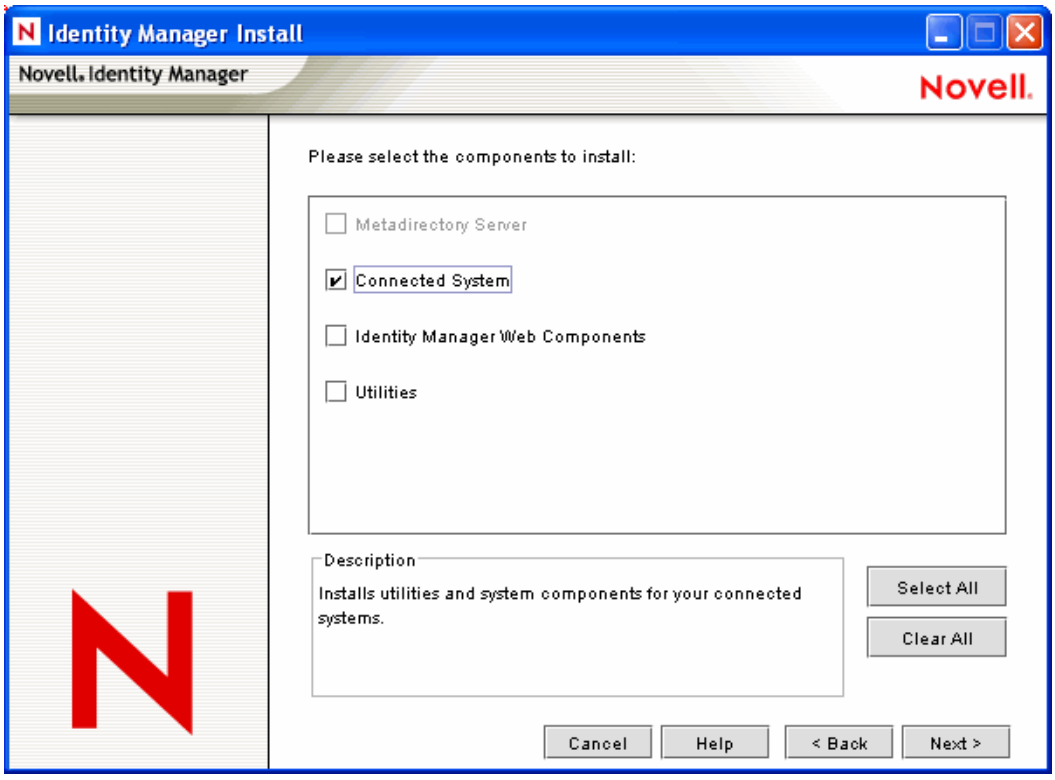
本節提供下列資訊：

- 「在 Windows 伺服器上安裝遠端載入器」，第 46 頁
- 「在 Solaris、Linux 或 AIX 上安裝遠端載入器」，第 47 頁

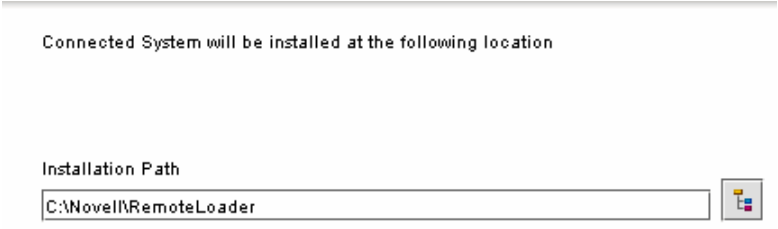
- 「在 HP-UX、AS/400、OS/390 或 z/OS 上安裝遠端載入器」，第 48 頁

在 **Windows** 伺服器上安裝遠端載入器

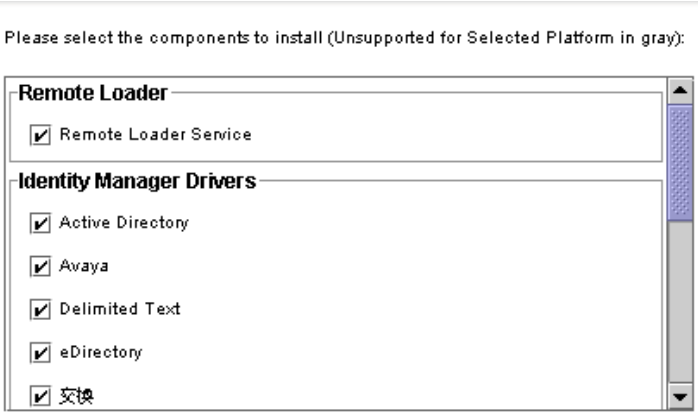
1. 執行 Identity Manager 3 安裝程式 (例如，\nt\install.exe)。
2. 檢視「歡迎」頁面、接受授權合約，並檢視兩個「綜覽」頁面。
3. 在「Identity Manager 安裝」對話方塊中，取消選取除了「已連接系統」之外的所有元件，然後按「下一步」。



4. 選取已連接系統 (「遠端載入器」和遠端驅動程式 Shim) 的位置，然後按「下一步」。



5 選取 「遠端載入器服務」和遠端驅動程式 Shim (驅動程式)，然後按 「下一步」。



6 確認啓用要求、檢視要安裝的產品，然後按一下 「完成」。

7 選取是否在桌面放置 「遠端載入器主控台」圖示。

在 Solaris、Linux 或 AIX 上安裝遠端載入器

本節假設您已下載並展開 Identity Manager 3。如果您需要下載 Identity Manager，請造訪 Novell 下載網站 (http://download.novell.com)。

展開您從 Novell 網站下載的 Identity Manager 3 檔案之後，完成下列步驟：

1 根據您的平台而定，執行下列其中一個安裝檔案：

- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 接受授權合約之後，按 Enter 以進入 「選擇安裝集」頁面：

```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   :
```

3 輸入 2 以選取已連接系統伺服器，然後按 Enter。

4 在「預先安裝摘要」螢幕上，檢視您已選取要安裝的元件，然後按 Enter。

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Install Set
    Connected System Server

Product Components:
    LDAP Driver,
    SAP Driver,
    JDBC Driver,
    Delimited Text Driver,
    Notes Driver,
    Remote Loader,
    Groupwise Driver,
    AVAYA Driver,
    SOAP Driver,
    REMEDY Driver


PRESS <ENTER> TO CONTINUE:
```

在 HP-UX、AS/400、OS/390 或 z/OS 上安裝遠端載入器

HP-UX、AS/400、OS/390 和 z/OS 平台需要「Java 遠端載入器」。

1 在您要執行「Java 遠端載入器」的目標系統上建立目錄。

2 從 Identity Manager 3 CD 或下載影像檔，將 /java_remoteloader 目錄中的適當檔案複製到在步驟 1 中建立的目錄：

平台	檔案
HP-UX AS/400 z/OS OS/390	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar dirxml_jremote_mvs.tar

3 若爲 HP-UX、AS/400 或 z/OS，解除壓縮 dirxml_jremote 檔案。

4 還原您剛才複製的檔案。

「Java 遠端載入器」準備進行組態設定。因爲 tar 檔案不包含驅動程式，所以您必須手動將驅動程式複製到 lib 目錄中。lib 目錄位於進行還原項目所在的目錄之下。

如需 MVS 的相關資訊，請還原 dirxml_jremote_mvs.tar 檔案。然後請參閱 usage.html 文件。

3.3.2 設定遠端載入器的組態

「遠端載入器」可以代管包含在 .dll、.so 或 .jar 檔案中的 Identity Manager 應用程式 Shim。「Java 遠端載入器」只代管 Java 驅動程式 Shim。而不會載入或代管原生 (C++) 驅動程式 Shim。

- 「在 Windows 上設定遠端載入器的組態」，第 49 頁
- 「使用指令行選項設定遠端載入器的組態」，第 53 頁
- 「啓動遠端載入器」，第 58 頁
- 「停止遠端載入器」，第 61 頁

在 **Windows** 上設定遠端載入器的組態

- 「使用遠端載入器主控台公用程式」，第 49 頁
- 「新增遠端載入器例項」，第 50 頁
- 「編輯遠端載入器例項」，第 53 頁

使用遠端載入器主控台公用程式

「遠端載入器主控台」只在 Windows 上執行。「主控台」可讓您管理在該電腦之「遠端載入器」下執行的所有 Identity Manager 驅動程式：

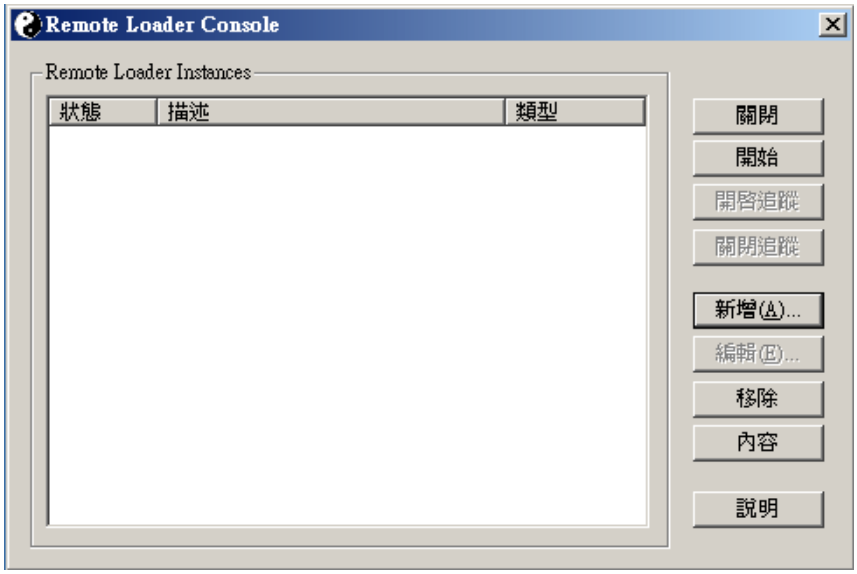
如果您升級至 Identity Manager 3，則「主控台」會偵測和輸入「遠端載入器」的現有例項 (若要自動輸入，驅動程式組態必須儲存在遠端載入器目錄中，通常爲 c:\novell\remoteloader)。然後您可以使用「主控台」管理遠端驅動程式。

若要啓動「遠端載入器主控台」，請按一下桌面上的「遠端載入器主控台」圖示。

特性 ***3-3*** 遠端載入器主控台圖示

「遠端載入器主控台」可讓您啓動、停止、新增、移除和編輯「遠端載入器服務」的每個例項。

特性 ***3-4*** 遠端載入器主控台



如果您從指令行輸入 dirxml_remote.exe，而不帶有任何參數，則會啓動「遠端載入器應用程式精靈」。

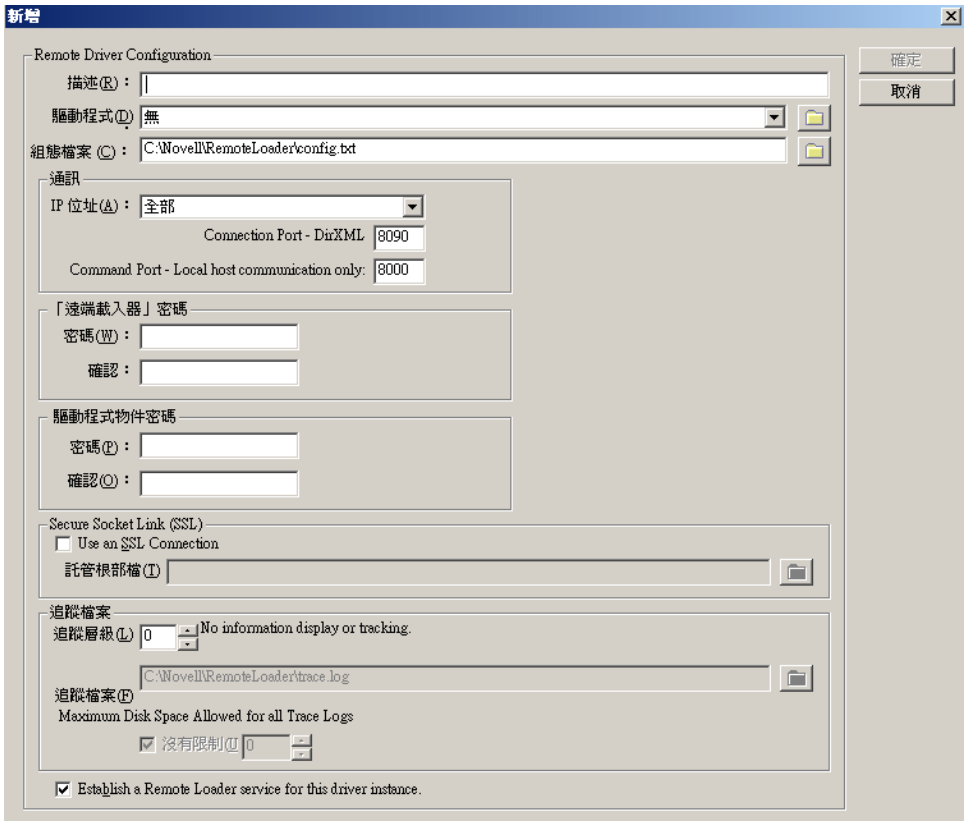
附註：同時使用該精靈與「主控台」可能會導致未預期的行爲。因此，建議您一直使用「遠端載入器主控台」，並將現有組態升級至「主控台」。

新增遠端載入器例項

若要新增「遠端載入器」例項，請按一下「新增」，然後提供下列資訊：

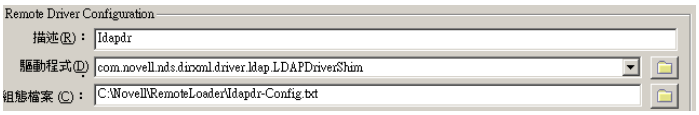
- 「遠端驅動程式組態」，第 51 頁
- 「通訊參數」，第 51 頁
- 「遠端載入器密碼」，第 51 頁
- 「驅動程式物件密碼」，第 52 頁
- 「保全插槽連結 (保全插槽層)」，第 52 頁
- 「追蹤檔案」，第 52 頁
- 「建立此驅動程式例項的遠端載入器服務」，第 53 頁

特性 ***3-5*** 遠端載入器組態參數



遠端驅動程式組態

特性 ***3-6*** 遠端驅動程式組態

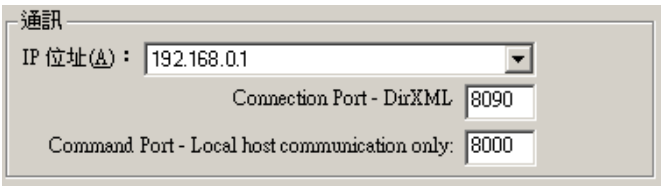


- 描述：指定識別 「遠端載入器」例項的描述。
- 驅動程式：瀏覽並選取驅動程式的適當 Shim。
- 組態檔案：指定組態檔案的名稱。

  「遠端載入器主控台」將組態參數置於此文字檔中，並在執行時使用那些參數。

通訊參數

特性 ***3-7*** 通訊參數



- IP 位址：指定 「遠端載入器」監聽來從 Metadirectory 伺服器連接的 IP 位址。
- 連接埠 - Metadirectory 伺服器。指定 「遠端載入器」監聽來自 Metadirectory 伺服器連接的傳輸控制通訊協定 (Transmission Control Protocol，TCP) 連接埠。

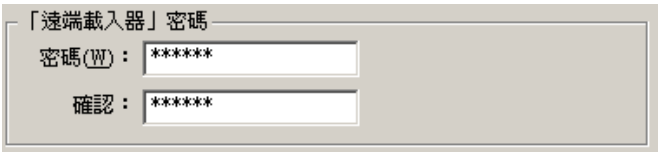
  此連接的預設傳輸控制通訊協定 / 網際網路通訊協定 (Transmission Control Protocol/Internetwork Protocol，TCP/IP) 連接埠是 8090。每建立一個新例項，預設連接埠號碼都會自動加一。
- 指令連接埠 - 僅限本地主機通訊：指定 「遠端載入器」監聽指令 (例如 「停止和變更追蹤層級」) 的 TCP 連接埠號碼。

  在特定電腦上執行的每個 「遠端載入器」例項都必須具有不同的指令連接埠號碼。預設指令連接埠是 8000。每建立一個新例項，預設連接埠號碼都會自動加一。

  附註：藉由指定不同的連接埠和指令連接埠，您可以在代管不同驅動程式例項的同一伺服器上執行 「遠端載入器」的多個例項。

遠端載入器密碼

特性 ***3-8*** 遠端載入器密碼



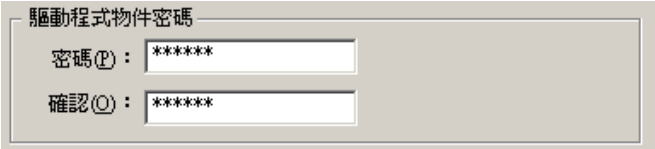
- 密碼：此密碼用於控制對驅動程式之 「遠端載入器」例項的存取。

密碼必須與您在設定驅動程式組態時，在「Identity Manager 組態」頁之「驗證」區段「輸入遠端載入器密碼」編輯方塊中輸入的密碼相同，且區分大小寫。

- 確認：重新輸入密碼。

驅動程式物件密碼

特性 ***3-9*** 驅動程式物件密碼

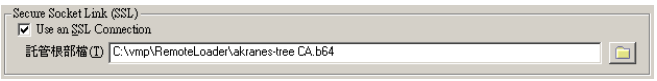


- 密碼：「遠端載入器」使用此密碼來對 Metadirectory 伺服器進行自我驗證。

  此密碼必須與您在設定驅動程式組態時，在「驅動程式組態」頁「驅動程式物件密碼」編輯方塊中輸入的密碼相同。
- 確認：重新輸入密碼。

保全插槽連結 (保全插槽層)

特性 ***3-10*** 保全插槽連結 (保全插槽層)

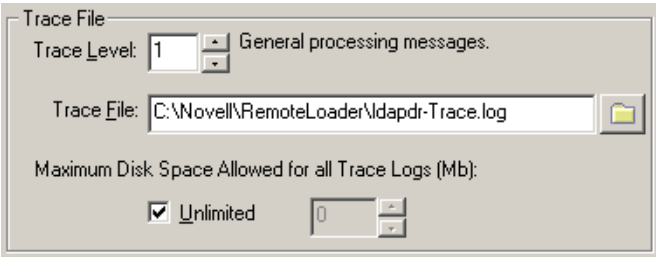


- 使用 SSL 連接：若要指定保全插槽層 (SSL) 連接，請選取此選項。
- 託管根部檔：瀏覽並選取託管根部檔。

  此檔案是來自 eDirectory 網路樹之「組織證書權限」的輸出自行簽署證書。請參閱「輸出自行簽署的證書」，第 44 頁。

追蹤檔案

特性 ***3-11*** 追蹤檔案



- 追蹤層級：針對要顯示追蹤視窗 (其中包含來自「遠端載入器」和驅動程式的資訊訊息) 的「遠端載入器」例項，將追蹤層級設定爲大於零。最常見的設定爲追蹤層級 3。

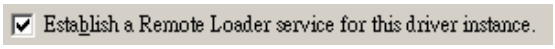
  如果追蹤層級設爲 0，則追蹤視窗不會出現或顯示訊息。
- 追蹤檔案：指定寫入追蹤訊息的追蹤檔名。

在特定機器上執行的每個 「遠端載入器」例項都必須使用不同的追蹤檔案。僅當追蹤層級大於零時，追蹤訊息才會寫入追蹤檔案。

- 所有追蹤記錄允許的最大磁碟空間 (MB)：指定此例項的追蹤檔案資料可以在磁碟上佔用的大約最大大小。

建立此驅動程式例項的遠端載入器服務

特性 ***3-12*** 建立此驅動程式例項的遠端載入器服務



- 若要設定 「遠端載入器」例項的組態做爲服務，請選取此選項。若啓用該選項，在啓動電腦時，作業系統會自動啓動 「遠端載入器」。

編輯遠端載入器例項

1. 從 「描述」欄中選取 「遠端載入器」例項。
2. 按一下 「停止」、輸入 「遠端載入器」密碼，然後按一下 「確定」。
3. 按一下 「編輯」，然後修改組態資訊。這些欄位與您新增 「遠端載入器」例項時使用的欄位相同。

使用指令行選項設定遠端載入器的組態

若要執行 「遠端載入器」，所有平台都會使用組態檔案 (例如，LDAPShim.txt)。您可以使用指令行選項來建立或編輯組態檔案。下列步驟提供組態檔案基本參數的相關資訊。如需其他參數的相關資訊，請參閱附錄 B 「設定遠端載入器組態的選項」，第 235 頁 。

1. 開啓文字編輯器。
2. (選擇性) 使用 胨 escription 選項來指定描述。

選項	次要名稱	參數	描述
-description	-desc	簡短描述	指定要用於追蹤視窗標題和 「Nsure 稽核」記錄的簡短描述字串 (例如，SAP)。 範例： -description SAP -desc SAP 「遠端載入器主控台」在組態檔案中使用完整格式。您可以使用完整格式 (例如，-description) 或簡短格式 (例如，-desc)。

3. 透過 胎 ommandport 選項，指定 「遠端載入器」例項將使用的 TCP/IP 連接埠。

選項	次要名稱	參數	描述
-commandport	-cp	連接埠號碼	指定「遠端載入器」例項用於控制的 TCP/IP 連接埠。如果「遠端載入器」例項正在代管應用程式 Shim，則指令連接埠是另一個「遠端載入器」例項與代管 Shim 之例項進行通訊的連接埠。如果「遠端載入器」例項正在將指令傳送至正在代管應用程式 Shim 的例項，則指令連接埠是代管例項正在監聽的連接埠。如果未指定，則預設指令連接埠爲 8000。藉由指定不同的連接埠和指令連接埠，「遠端載入器」的多個例項可以在代管不同驅動程式例項的同一伺服器上執行。 範例： -commandport 8001 -cp 8001

4 藉由使用 -connection 選項，指定執行 Identity Manager 遠端介面 Shim 之 Metadirectory 伺服器的連接參數。

輸入 -connection "*parameter* [parameter] [parameter]"。

例如，輸入下列其中一項：

```
-connection "port=8091 rootfile=server1.pem" -conn "port=8091
rootfile=server1.pem"
```

所有參數都必須包含在引號中。參數包含下列項目：

選項	次要名稱	參數	描述
-connection	-conn	連接組態字串	指定用於連接執行 Identity Manager 遠端介面 Shim 之 Metadirectory 伺服器的連接參數。「遠端載入器」的預設連接方法是使用保全插槽層 (SSL) 的 TCP/IP。此連接的預設 TCP/IP 連接埠是 8090。多個「遠端載入器」例項可以在相同的伺服器上執行。每個「遠端載入器」例項會代管個別 Identity Manager 應用程式 Shim 例項。藉由針對每個「遠端載入器」例項指定不同的連接埠和指令連接埠，區分「遠端載入器」的多個例項。 範例： -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
port		十進位連接埠號碼	必要的參數。它會指定 TCP/IP 連接埠，「遠端載入器」會在其上監聽遠端介面 Shim 的連接。 範例： port=8090

選項	次要名稱	參數	描述
address		IP 位址	選擇性參數。指定「遠端載入器」會在特定的本地 IP 位址上監聽。如果代管「遠端載入器」的伺服器具有多個 IP 位址，並且「遠端載入器」必須僅監聽一個位址，則這會很有用。 您有三個選項：address=*address number* address= 捻 ocalhost' 請勿使用此參數。 如果您不使用 -address，則「遠端載入器」會監聽所有本地 IP 位址。 範例：address=137.65.134.83
rootfile			條件參數。如果您正在執行保全插槽層 (SSL)，並且需要「遠端載入器」與原生驅動程式通訊，請輸入 rootfile='*trusted certname*'
keystore			條件參數。僅用於 .jar 檔案中包含的 Identity Manager 應用程式 Shim。 指定 Java KeyStore 的檔名，該 Java KeyStore 包含遠端介面 Shim 使用之證書發證者的託管根部證書。這一般是代管遠端介面 Shim 之 eDirectory 網路樹的「證書權限」。 如果您正在執行保全插槽層 (SSL)，並且需要「遠端載入器」與 Java 驅動程式通訊，請輸入鍵值配對： keystore='*keystorename*' storepass='*password*'
-storepass		storepass	僅用於 .jar 檔案中包含的 Identity Manager 應用程式 Shim。指定由 KeyStore 參數所指定的 Java KeyStore 密碼。 範例： storepass=mypassword 此選項僅適用於「Java 遠端載入器」。

5 (選擇性) 使用 -trace 選項來指定追蹤參數。

選項	次要名稱	參數	描述
-trace	-t	整數	指定追蹤層級。這僅在代管應用程式 Shim 時使用。追蹤層級對應 Metadirectory 伺服器上使用的追蹤層級。 範例： -trace 3 -t 3

6 (選擇性) 使用 -tracefile 選項來指定追蹤檔案。

選項	次要名稱	參數	描述
-tracefile	-tf	檔名	指定要寫入追蹤訊息的檔案。如果追蹤層級大於零，則追蹤訊息會寫入該檔案。即使追蹤視窗沒有開啓，追蹤訊息也會寫入該檔案。 範例： -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt

7 (選擇性) 使用 -tracefilemax 選項來限制追蹤檔案的大小。

例如，輸入下列其中一項：

```
-tracefilemax 1000M -tfm 1000M
```

在此範例中，追蹤檔案僅可以是 1 GB。

選項	次要名稱	參數	描述
-tracefilemax	-tfm	大小	指定追蹤檔案資料可以在磁碟上佔用的大約大小上限。如果您指定此選項，則會有使用追蹤檔案選項指定名稱的追蹤檔案，並且會有 9 個額外的「延展」檔案。延展檔案是以使用主追蹤檔名加上 "*_n*" 爲其命名基礎，其中 n 是 1 至 9 的數字。 大小參數是位元組的數目。藉由針對 KB、MB 或 GB 使用字首 K、M 或 G，以指定大小。 「遠端載入器」啓動時，如果追蹤檔案資料大於指定的最大值，則在所有 10 個檔案都完成延展之前，追蹤檔案資料會保持大於指定的最大值。 範例： -tracefilemax 1000M -tfm 1000M 在此範例中，追蹤檔案僅可以是 1 GB。

8 使用 -class 選項指定類別，或者使用 -module 選項指定模組。

選項	次要名稱	參數	描述
-class	-cl	Java 類別名稱	指定要代管之 Identity Manager 應用程式 Shim 的 Java 類別名稱。 例如，針對 Java 驅動程式，輸入下列其中一個： -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java 會使用 KeyStore 來讀取證書。-class 選項和 -module 選項互斥。 若要查看 Java 類別名稱的清單，請參閱附錄 B「設定遠端載入器組態的選項」，第 235 頁 中的表格 B-2 頁上 240。
-module	-m	modulename	指定包含要代管之 Identity Manager 應用程式 Shim 的模組。 例如，針對原生驅動程式，輸入下列其中一項： -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" 或 -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module 選項使用根部檔案證書。-module 選項和 -class 選項互斥。

9 命名並儲存檔案。

您可以在執行「遠端載入器」時變更部份設定。如需這些設定的相關資訊，請參閱附錄 B「設定遠端載入器組態的選項」，第 235 頁 。

參數	描述
-commandport	指定「遠端載入器」的例項。
-config	指定組態檔案。
-javadebugport	指定「遠端載入器」例項要在指定的連接埠上啓用 Java 除錯。
-password	指定用於驗證的密碼。
-service	將例項安裝爲服務。僅限 Windows。
-tracechange	變更追蹤層級。
-tracefilechange	變更正在寫入的追蹤檔案名稱。
-unload	卸載「遠端載入器」例項。

參數	描述
-window	在「遠端載入器」例項中開啓或關閉追蹤視窗。僅限 Windows。

在 Solaris、Linux 或 AIX 上設定環境變數

在安裝「遠端載入器」之後，您可以設定環境變數 RDXML_PATH，這會變更 rdxml 的目前目錄。然後，後續建立的檔案會採用此目錄作爲基礎路徑。若要設定 RDXML_PATH 變數的值，請輸入下列指令：

- set RDXML_PATH=*path*
- export RDXML_PATH

啓動遠端載入器

- 「在 Windows 上啓動「遠端載入器」」，第 58 頁
- 「從指令行啓動遠端載入器」，第 59 頁

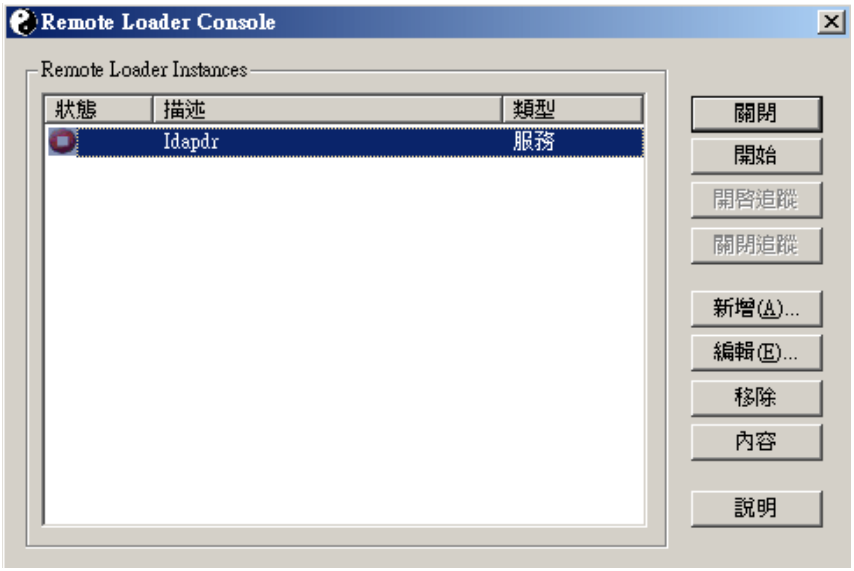
在 Windows 上啓動「遠端載入器」

若要在 Windows 上執行「遠端載入器」，請執行下列動作：

特性 ***3-13*** 遠端載入器主控台圖示

1 按一下桌面上的 「遠端載入器主控台」圖示。

特性 ***3-14*** 遠端載入器主控台



2 選取驅動程式例項，然後按一下 「啓動」。

從指令行啓動遠端載入器

在 Solaris、Linux 或 AIX 上，二進位元件 rdxml 會提供 「遠端載入器」功能。此元件位於 /usr/bin/ 目錄中。在 Windows 上，預設目錄是 c:\novell\RemoteLoader。

若要執行 「遠端載入器」，請執行下列動作：

1 設定密碼。

平台	指令
Windows	dirxml_remote -config *path_to_config_file* -sp *password password*
Solaris Linux AIX	rdxml -config *path_to_config_file* -sp *password password*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -sp *password password*

選項	次要名稱	參數	描述
-password	-p	密碼	指定用於指令驗證的密碼。此密碼必須與使用 **setpasswords** 指定的第一個受指令載入器例項密碼相同。如果已指定指令選項 (例如，unload 或 tracechange)，並且沒有指定 **password** 選項，則會提示使用者輸入指令目標的載入器密碼。 範例： -password novell4 -p novell4

選項	次要名稱	參數	描述
-setpasswords	-sp	密碼 密碼	指定「遠端載入器」例項的密碼，以及與「遠端載入器」通訊之遠端介面 Shim 的「Identity Manager 驅動程式」物件密碼。引數中的第一個密碼是「遠端載入器」的密碼。選擇性引數中的第二個密碼是「Identity Manager 驅動程式」物件的密碼，該物件與 Metadirectory 伺服器上的遠端介面 Shim 相關聯。您可以不指定密碼；如果指定密碼，必須同時指定兩個密碼。如果沒有指定任何密碼，則「遠端載入器」會提示指定密碼。這是組態選項。使用此選項會設定「遠端載入器」例項的組態，且會指定密碼，但不會載入 Identity Manager 應用程式 Shim，或與另一個載入器例項通訊。 範例： -setpasswords novell4 staccato3 -sp novell4 staccato3

2 啓動「遠端載入器」。

平台	指令
Windows	dirxml_remote -config *path_to_config_file*
Solaris Linux AIX	rdxml -config *path_to_config_file*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file*

3 使用 iManager，啓動驅動程式。

4 確認「遠端載入器」運作正常。

「遠端載入器」僅在與 Metadirectory 伺服器上的遠端介面 Shim 通訊時，才會載入 Identity Manager 應用程式 Shim。例如，這可能表示如果「遠端載入器」失去與 Metadirectory 伺服器的通訊，則應用程式 Shim 會關閉。

若爲 Linux、Solaris 或 AIX，使用 ps 指令或追蹤檔案，以查看指令和連接埠是否在監聽。

若爲 HP-UX 和類似的平台，在追蹤檔案上使用 tail 指令監控「Java 遠端載入器」：

```
tail -f trace filename
```

如果記錄的最後一行顯示下列內容，則表示載入器正在順利地執行並等待從 Identity Manager 遠端介面 Shim 的連接：

```
TRACE: Remote Loader: Entering listener accept()
```

若要設定「遠端載入器 (rdxml)」的組態，以在 UNIX 上自動啓動，請參閱 TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm)。

停止遠端載入器

平台	指令
Windows	使用 「遠端載入器主控台」以停止驅動程式例項。
Solaris Linux AIX	rdxml -config *path_to_config_file* -u
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -u

如果多個 「遠端載入器」例項在電腦上執行，則傳送 -cp *command port* 選項，以便 「遠端載入器」可以停止適當的例項。

在停止 「遠端載入器」時，您必須具有足夠的權限，或輸入 「遠端載入器」密碼。

案例：足夠的權限。「遠端載入器」在做爲 Windows 服務執行。您具有足夠的權限停止它。您輸入密碼，但意識到它是錯誤的。 「遠端載入器」仍會停止。

「遠端載入器」不會 「接受」該密碼。而是會忽略該密碼，因爲在此案例中該密碼是多餘的。如果做爲應用程式而非服務執行 「遠端載入器」，則會使用該密碼。

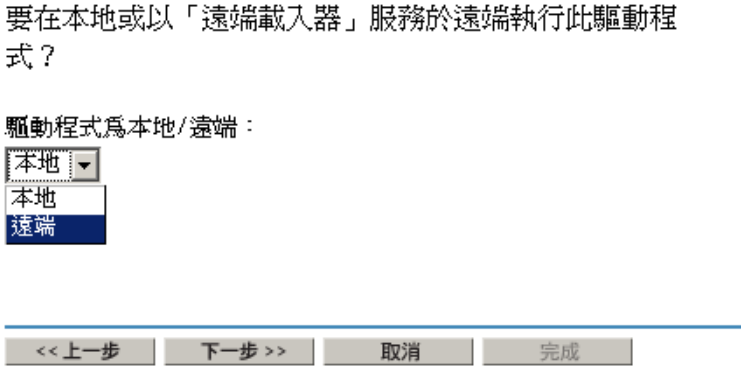
3.4 設定 Identity Manager 驅動程式的組態，以與遠端載入器搭配使用

您可以設定新驅動程式的組態，或者啓用現有的驅動程式，以與 「遠端載入器」通訊。本節會提供設定驅動程式組態，以使它們與 「遠端載入器」通訊的一般資訊。如需其他驅動程式特定的資訊，請參閱相關的驅動程式實作指南。

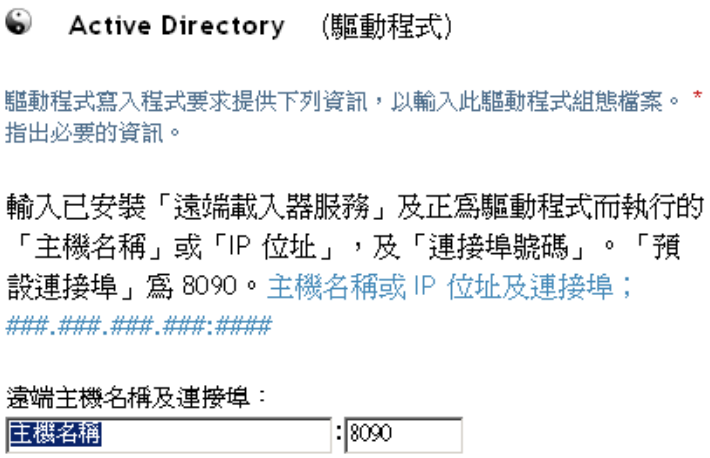
- 「輸入並設定新驅動程式」，第 61 頁
- 「設定現有驅動程式的組態」，第 62 頁
- 「建立 KeyStore」，第 64 頁

3.4.1 輸入並設定新驅動程式

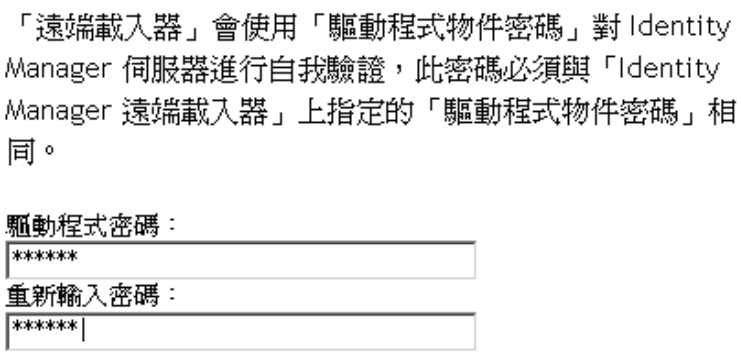
1. 在 Novell iManager 中，輸入或建立並設定新驅動程式的組態。
2. 捲動到組態選項的底端，從下拉式清單選取 「遠端」，然後按一下 「下一步」。



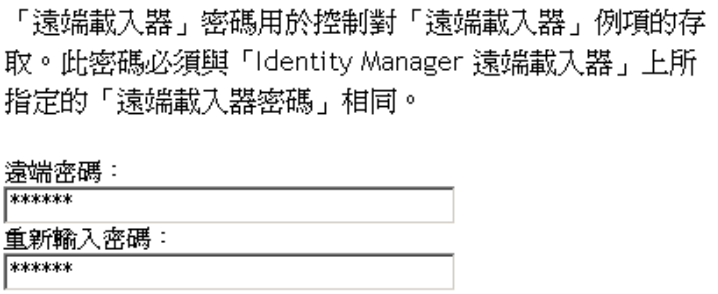
3 輸入遠端主機名稱和連接埠。



4 輸入並重新輸入 「驅動程式」物件的密碼。



5 輸入並重新輸入 「遠端載入器」密碼，然後按一下 「下一步」。



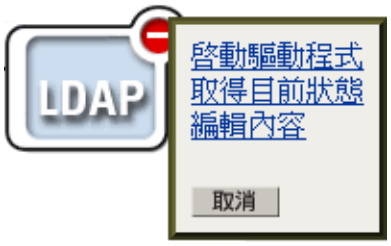
6 定義安全性等值使用者，按一下 「下一步」，然後按一下 「完成」。

3.4.2 設定現有驅動程式的組態

在 「驅動程式」物件上指定參數，以連接至 「遠端載入器」。

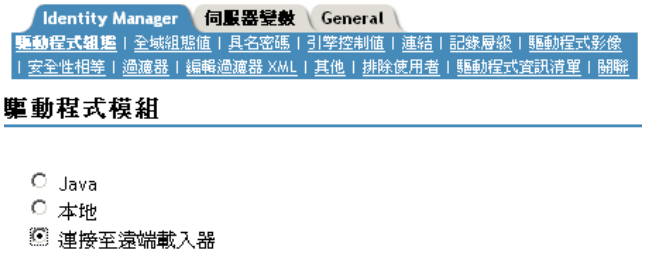
1 在 Novell iManager 中，按一下 「*Identity Manager* > *Identity Manager* 概觀」。

2 瀏覽並選取您想要修改的驅動程式。



3 按一下驅動程式狀態圖示，然後按一下「編輯內容」。

4 在「驅動程式模組」區段中，選取「連接至遠端載入器」。



5 在「驗證」區段中，輸入「遠端載入器」的參數。

- 遠端載入器連接參數

  您先前已輸出自行簽署的證書 (請參閱 「輸出自行簽署的證書」，第 44 頁)。針對保全插槽層 (SSL)，您需要自行簽署之證書的綽號。

  在「遠端載入器連接參數」編輯方塊中，輸入鍵值配對參數。例如，輸入

  ```
  hostname=192.168.0.1 port=8090 kmo=remotecert
  ```

```
hostname=192.168.0.1 port=8090 kmo='remote cert'
```

- hostname

  主機名稱或 IP 位址 (例如，190.162.0.1)。指定執行「遠端載入器」之電腦的位址或名稱。如果沒有指定 IP 位址或伺服器名稱，則此值預設爲本地主機。

- port

  「遠端載入器」會在這裡接受遠端介面 Shim 的連接。如果沒有指定此通訊參數，則此值預設爲 8090。

- kmo

  指定包含保全插槽層 (SSL) 所用金鑰和證書之金鑰材料物件 (KMO) 的「金鑰名稱」(例如，kmo=remotecert)。

  如果已在證書名稱中使用空格，則需要將金鑰材料物件 (KMO) 物件綽號包含在單引號中。

  提示：金鑰材料物件 (KMO) 物件名稱是您在 「建立伺服器證書」，第 44 頁 步驟 2 中指定的綽號值。

- 輸入應用程式密碼

  指定應用程式使用者 ID 的密碼。通常，驅動程式 Shim 需要此密碼，以便驅動程式可以連接至應用程式。

- 輸入遠端載入器密碼

  指定遠端載入器的密碼。遠端介面 Shim 會使用此密碼來對「遠端載入器」進行自我驗證。

  附註：同時設定或重新設定應用程式密碼和「遠端載入器」密碼。

  ---

6 按一下「確定」。

3.4.3 建立 KeyStore

KeyStore 是包含加密金鑰和證書 (選擇性) 的 Java 檔案。如果您想要在「遠端載入器」和 Metadirectory 引擎之間使用保全插槽層 (SSL)，且使用 Java Shim，則需要建立 KeyStore 檔案。

- 「Windows 上的 KeyStore」，第 64 頁
- 「Solaris、Linux 或 AIX 上的 KeyStore」，第 64 頁
- 「所有平台上的 KeyStore」，第 65 頁

Windows 上的 KeyStore

在 Windows 上，執行 Keytool 公用程式，它一般位於 c:\novell\remoteloader\jre\bin 目錄。

Solaris、Linux 或 AIX 上的 KeyStore

在 Solaris、Linux 或 AIX 環境上，使用 create_keystore 檔案。create_keystore 會與 rdxml 一起安裝，而且也包含在 dirxml_jremote.tar.gz 檔案中，其位於 \dirxml\java_remoteloader 目錄中。create_keystore 檔案是呼叫 Keytool 公用程式的 shell 程序檔。

在 UNIX 上，使用自行簽署的證書建立 KeyStore 時，證書可以使用 Base64 或二進位 .der 格式輸出。

在指令行輸入下列指令：

create_keystore *self-signed_certificate_name keystorename*

例如，輸入下列其中一項

```
create_keystore tree-root.b64 mystore create_keystore tree-root.der
mystore
```

create_keystore 程序檔會針對 KeyStore 密碼指定硬式編碼密碼 "dirxml"。因爲只有公用證書和公用金鑰儲存在 KeyStore 中，所以這不是安全性風險。

所有平台上的 KeyStore

若要在平台上建立 KeyStore，可以在指令行輸入下列指令：

keytool -import -alias trustedroot -file *self-signed_certificate_name* -keystore *filename* -storepass

Filename 可以是任何名稱 (例如，rdev_keystore)。

建立規則

4

規則可讓您針對特定環境，自定 Identity Vault 的資訊流入和流出。

例如，一個公司可能會使用 inetorgperson 做爲主要使用者類別，而另一個公司可能會使用 User。爲了處理這種情況，會建立規則以告知 Metadirectory 引擎每個系統中使用者的名稱。每次影響使用者的操作在已連接系統之間傳遞時，Identity Manager 都會套用進行此變更的規則。

規則還會建立新的物件、更新屬性值、進行綱要轉換、定義相符準則、維護 Identity Manager 關聯和執行許多其他作業。

「規則」的詳細指南包含在《規則產生器和驅動程式自訂指南》中。本指南包含：

- 每個可用規則的詳細描述
- 深入的「規則產生器」使用者指南和參考，包含每個條件、動作、名詞和動詞的範例和語法。
- 使用 XSLT 樣式表建立規則的相關討論。

請參閱《規則產生器和驅動程式自訂指南》，以取得規則的相關資訊。

已連接系統間的密碼同步化

5

5.1 綜覽

藉由利用「通用密碼」和已連接系統對發行密碼或訂閱密碼的支援，Identity Manager 會提供雙向密碼同步化。

與使用者帳戶的其他屬性一樣，您可以選擇授權資料來源。

5.1.1 密碼綜覽

Novell 目錄服務 (Novell Directory Services，NDS®) 密碼、簡易密碼、配送密碼和通用密碼用於不同目的。在 eDirectory™ 和 Identity Manager 的先前版本中，已連接系統僅能以單向同步來更新 NDS 密碼。

Identity Manager 會使用「通用密碼」，它是一種可以與其他 Identity Vault 密碼同步化的可回復密碼。「通用密碼」在 eDirectory 8.7.1 中引入，並且由三層加密進行保護。

Novell 模組化驗證服務 (Novell Modular Authentication Service，NMAS™) 控制「通用密碼」與其他 Identity Vault 密碼之間的關係。例如，NMAS 會控制是否保持「通用密碼」與「NDS 密碼」、「簡易密碼」或「配送密碼」之間的同步化。NMAS 會攔截要變更密碼的內送申請，並根據 NMAS 密碼規則中的設定處理它們。

Identity Manager 會控制 Identity Vault 密碼與已連接系統密碼之間的關係。Identity Manager 會使用「配送密碼」進行這項控制，該密碼位於 Identity Vault 中，且可以提供給已連接系統。與「通用密碼」類似，「配送密碼」由三層加密保護，並且可以回復。

在 NMAS 密碼規則中，您可以指定「配送密碼」是否應該與「通用密碼」相同 (設定是「設定「通用密碼」時同步化配送密碼」)。如果「配送密碼」與「通用密碼」相同，並且您選擇使用與已連接系統的雙向「密碼同步化」，請記住使用 Identity Manager 從 eDirectory 擷取「通用密碼」，並將其傳送至其他已連接系統。您需要確保密碼輸送和儲存密碼之已連接系統的安全 (請參閱 第 7 章 「安全性：最佳作法」, 第 183 頁)。

如果「配送密碼」與「通用密碼」不同 (由於您停用 NMAS 密碼規則中的設定)，您可以「通道封裝」使用「配送密碼」之已連接系統間的密碼，而無需使用或影響「通用密碼」或「NDS 密碼」。請記住，通道封裝僅同步化已連接系統之間的密碼。如果已啓用，則通道封裝不會設定 Identity Vault/ 通用密碼。

如需各種 eDirectory 密碼的相關資訊，請參閱《*Novell* 模組化驗證服務 *(NMAS) 2.3* 管理指南 (http://www.novell.com/documentation/nmas23/index.html)》。如需使用與 Identity Manager 密碼同步化的不同方法範例，請參閱 「實作密碼同步化」，第 100 頁。

5.1.2 雙向密碼同步化是什麼？

雙向密碼同步化是 Identity Manager 從指定的已連接系統接受密碼，以及將密碼配送至指定的已連接系統兩方面的結合。

是否能夠與特定已連接系統進行雙向密碼同步化，是根據已連接系統所支援的功能而定。

部份已連接系統可以從 Identity Manager 接受新的和修改的密碼，並且還可以將使用者的實際密碼提供給 Identity Manager。下列已連接系統就是支援與 Identity Manager 的雙向密碼同步化：

- Active Directory
- Novell® eDirectory
- 網路資訊服務 (NIS)
- NT Domain

若爲這些已連接系統，使用者可以變更一個系統中的密碼，並且透過 Identity Manager 使該密碼與其他系統同步化。然而，如果您使用 NMAS 密碼規則中的「進階密碼規則」，則最好讓使用者在 iManager 自助服務主控台中進行密碼變更。因爲它會列出使用者密碼必須符合的所有規則，所以這是密碼變更的最佳位置。

因爲其他已連接系統無法提供使用者的實際密碼，所以它們無法支援完整雙向密碼同步。然而，藉由在驅動程式組態中定義規則，已連接系統可提供能夠用於建立密碼的資料，並傳送至 Identity Manager。

數個其他系統可以從 Identity Manager 接受密碼，包括設定新使用者的啓始密碼、修改密碼，或同時執行這兩個動作。請參閱「已連接系統支援密碼同步化」，第 78 頁。

5.1.3 比較密碼同步化 1.0 與 Identity Manager 密碼同步化

表格 ***5-1*** 比較：密碼同步化 *1.0* 與 *Identity Manager* 密碼同步化

	密碼同步化 1.0	Identity Manager 2 和 3 提供的密碼同步化
產品交付方式	與 Identity Manager 分開的單獨產品。	隨附於 Identity Manager，不單獨出售。
平台	◆ Active Directory ◆ NT Domain ◆ eDirectory	在下列平台上支援完全雙向密碼同步： ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT Domain 這些已連接系統支援將使用者密碼發行至 Identity Manager。因爲「通用密碼」與「配送密碼」是可回復的，所以 Identity Manager 可以將密碼配送至已連接的系統。 所有支援「訂閱者」密碼元素的已連接系統都可以從 Identity Manager 訂閱密碼。 請參閱 「已連接系統支援密碼同步化」，第 78 頁。
Identity Vault 中使用的密碼	NDS 密碼 (不可回復)	通用密碼 (可回復)，或配送密碼 (也可回復)。如果願意，NDS 密碼還可以保持同步化。如需範例案例，請參閱 「實作密碼同步化」，第 100 頁。
Windows 已連接系統的主要功能	將密碼傳送至 Identity Manager，以便 Identity Vault 密碼與 Windows 密碼保持同步。因爲 NDS 密碼是不可回復的，所以這些密碼將不會傳送回 NT 或 AD。	提供雙向密碼同步化。因爲「通用密碼」和「配送密碼」是可回復的，所以在兩個方向密碼都可以同步化。
輕量目錄存取協定 (Lightweight Directory Access Protocol，LDAP) 變更	不支援。	支援
Novell® Client™	必要。	非必要。
nadLoginName 屬性	用於保持密碼不斷更新。	未使用。
包含密碼同步化功能的元件	包含更新 nadLoginName 功能的 Identity Manager 驅動程式。	驅動程式組態中的 Identity Manager 規則提供密碼同步化功能。驅動程式只執行由 Metadirectory 引擎提供的任務，這些任務來自規則中的邏輯。驅動程式資訊清單、全域組態值和驅動程式過濾器設定也必須支援密碼同步化。它們包含在範例驅動程式組態中，也可新增至現有的驅動程式。請參閱 「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁。

	密碼同步化 1.0	Identity Manager 2 和 3 提供的密碼同步化
代辦	單獨的軟體。	未安裝任何代辦；現在該功能是驅動程式的一部份。

5.1.4 Identity Manager 密碼同步化功能

「Identity Manager 密碼同步化」是雙向的。您可以從已連接系統傳送密碼，並由 Identity Manager 接受密碼，也可由 Identity Manager 配送密碼，並由已連接系統來接受。

從已連接系統接受密碼

與在前一版 DirXML® 和 Identity Manager 中一樣，任何已連接系統都可以將密碼發行至 Identity Vault。

您可以指定 Identity Manager 從中接受密碼的已連接系統應用程式。您甚至可以選擇 Identity Manager 是否在與執行 Identity Manager 的相同 Identity Vault 中更新使用者密碼，或者 Identity Manager 是否只做爲已連接系統之間同步化密碼的管道或「通道」。這表示可以保持讓 Identity Vault 密碼有別於 Identity Manager 配送至已連接系統的密碼 (如果有需要的話)。

部份已連接系統 (AD、其他 Identity Vault、NT 和 NIS) 可以提供使用者的實際密碼，這表示當使用者在某個已連接系統上變更密碼時，該變更可以同步化至 Identity Manager，並置換其他已連接系統中的密碼。

其他已連接系統不支援提供使用者的實際密碼，但是您可以設定這些已連接系統的組態，以提供給 Identity Manager 一個在樣式表中建立的密碼，如基於姓氏或員工 ID 的啓始密碼。

配送密碼至已連接系統

「Identity Manager 密碼同步化」可以將公用密碼配送至已連接系統。

在前一版 Identity Manager 中，驅動程式可以將密碼從已連接系統上的使用者帳戶傳送至 Identity Manager，且該密碼可用於更新 eDirectory 中對應的使用者。但是因爲 eDirectory 中的 NDS 密碼是不可回復的，所以您無法將密碼從集中式 Identity Manager Identity Vault 置入多個已連接系統。您只能在將密碼儲存在 eDirectory 中之前，透過擷取密碼來取得 eDirectory 密碼，如透過 Novell Client。

eDirectory 8.7.3 所提供的「通用密碼」是可回復的。且可以進行配送。

Identity Manager 可以從已連接系統接受密碼。因爲「通用密碼」是可回復的，所以 Identity Manager 可以將密碼從 Identity Vault 配送至已連接系統 (這些系統支援設定新帳戶的啓始密碼及修改密碼)。

無論密碼來自哪裡，Identity Manager 都會使用 「配送密碼」做爲儲存機制，Identity Manager 可以從該儲存機制將密碼配送至已連接系統。與 「通用密碼」一樣，「配送密碼」可讓您強制執行密碼規則。

如需同步化密碼時，使用 「通用密碼」和 「配送密碼」的相關資訊，請參閱 「實作密碼同步化」，第 100 頁。

與其他使用者屬性一樣，您可以決定哪個系統做爲密碼的授權來源。Identity Manager 會將密碼從授權來源配送至其他已連接系統。

您可以在支援雙向密碼同步化的已連接系統之間設定該同步化。

在資料儲存和已連接系統上強制執行密碼規則

透過呼叫 NMAS，Identity Manager 可以對收到的密碼強制執行密碼規則。如果從已連接系統發行至 Identity Manager 的密碼不一致，則您可以指定讓該 Identity Manager 不接受將密碼置入 Identity Vault。這還表示與規則不一致的密碼不會配送至其他已連接系統。

此外，Identity Manager 可以在已連接系統上強制執行密碼規則。如果發行至 Identity Manager 的密碼與規則 (Policy) 中的規則 (Rule) 不一致，則您可以指定讓 Identity Manager 不僅不接受配送的密碼，而且還要藉由使用 Identity Vault 中的目前 「配送密碼」，在已連接系統上實際重設不相容的密碼。

例如，您需要至少包含一個數值字元的密碼。然而，已連接系統本身沒有能力強制執行這樣的規則 (Policy)。您指定讓 Identity Manager 重設源自已連接系統、但是與規則 (Policy) 中的規則 (Rule) 不一致的密碼。

如果您正在使用 「進階密碼規則 (Rule)」和 「Identity Manager 密碼同步化」，則建議您研究所有已連接系統的密碼規則 (Policy)，以確定 eDirectory 密碼規則中的 「進階密碼規則 (Rule)」是相容的。此研究可協助您確保順利同步化密碼。

請記住，您必須確定被指定 NMAS 密碼規則的使用者與您要參與已連接系統之 「密碼同步化」的使用者相符。

NMAS 密碼規則是使用網路樹中心的方式指定的。相對地，「密碼同步化」是依每個驅動程式設定的。同時，驅動程式會在每個伺服器上安裝，且僅可以管理主複製本或讀 / 寫複製本中的那些使用者。若要取得預期的 「密碼同步化」結果，請確定執行 「密碼同步化」驅動程式之伺服器上主複製本或讀 / 寫複製本中的容器，與您指定密碼規則且啓用 「通用密碼」的容器相符。將密碼規則指定給分割區根容器，可確保將密碼規則指定給該容器和次容器中的所有使用者。

如需如何將 NMAS 密碼規則指定給使用者的相關資訊，請參閱 《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的 「將密碼規則指定給使用者」。

同步化密碼案例

Identity Manager 可讓您指定應做爲密碼之授權來源的系統。同時，您還可決定使用的密碼流程。

「Identity Manager 密碼同步化」的許多功能都依賴 「通用密碼」 (由 Identity Vault 提供的可回復密碼功能)。然而，部份案例不需要部署 「通用密碼」。

「Identity Manager 密碼同步化」還依賴 「配送密碼」。與 「通用密碼」一樣，也可以對 「配送密碼」強制執行規則。

如需可用來實作密碼同步化的基本方式，請參閱 「實作密碼同步化」，第 100 頁。您可以結合這些案例，以滿足環境需要。

在沒有 **Novell Client** 的 **Windows** 上同步化密碼

Active Directory 與 NT Domain 的密碼同步化不再需要 Novell Client。

通知使用者密碼同步化失敗

在資料儲存和已連接系統上強制執行密碼規則一節說明 Identity Manager 可以藉由不接受 (來自已連接系統) 不一致的密碼，來強制執行密碼規則。

您可以使用電子郵件通知功能，指定當使用者未順利變更密碼時，Identity Manager 會通知使用者。

案例。您已將 Identity Manager 設爲從 NT Domain 收到的密碼與您的密碼規則不一致時，不接受該密碼。您已啓用電子郵件通知。NMAS 密碼規則 (Policy) 中的一個規則 (Rule) 指定公司名稱無法用做密碼。使用者在 NT Domain 已連接系統上將密碼變更爲公司名稱。NMAS 不接受該密碼，Identity Manager 會傳送給使用者一則電子郵件訊息，說明未同步化密碼變更。

在您可以使用此功能之前，必須先設定電子郵件伺服器和範本。您可自定下列內容：

- Identity Manager 傳送的訊息文字
- 將副本傳送至管理員的通知

如需相關資訊，請參閱 「設定電子郵件通知的組態」，第 132 頁。

檢查使用者的密碼同步化狀態

Identity Manager 可讓您查詢已連接系統，以檢查使用者的密碼同步化狀態。如果已連接系統支援檢查密碼功能，則您可瞭解是否順利同步化密碼。

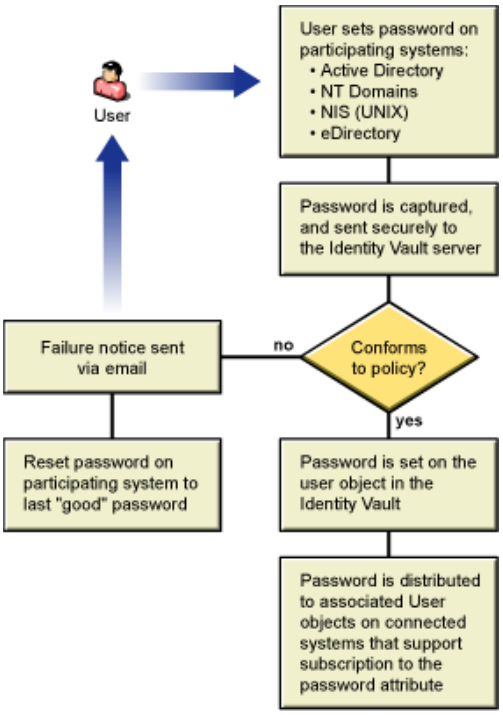
如需如何檢查密碼的相關資訊，請參閱 「檢查使用者的密碼同步化狀態」，第 131 頁。

如需支援檢查密碼的系統清單，請參閱 「已連接系統支援密碼同步化」，第 78 頁。

5.1.5 密碼同步化流程綜覽說明

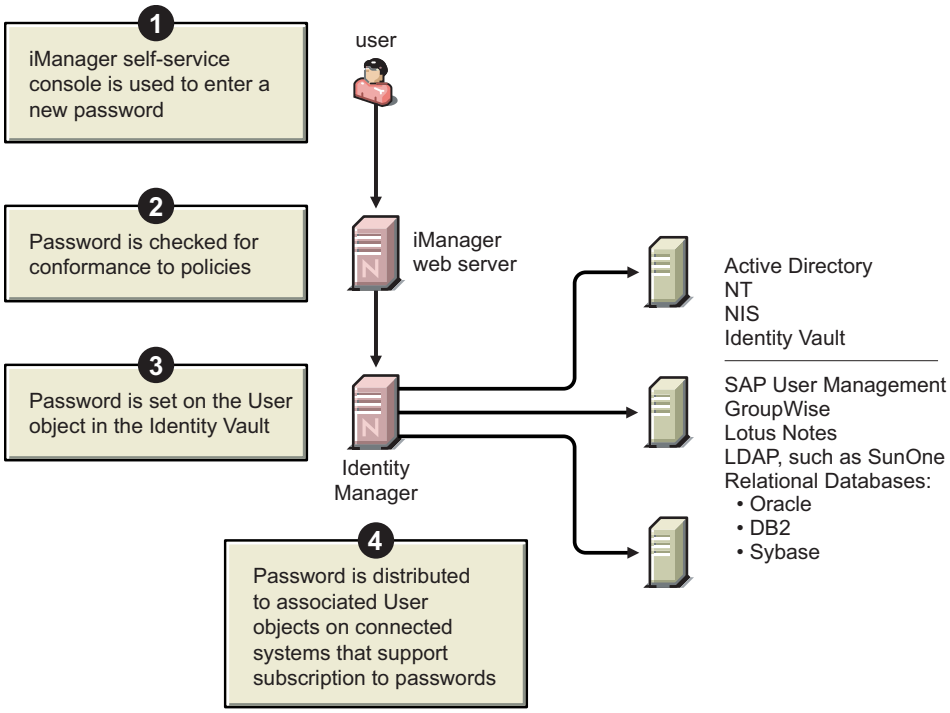
下圖描述已連接系統如何將密碼發行至 Identity Manager。

特性 ***5-1*** 已連接系統如何將密碼發行至 *Identity Manager*。



下圖描述 Identity Manager 如何將密碼配送至已連接系統。

特性 ***5-2*** *Identity Manager* 如何將密碼配送至已連接系統

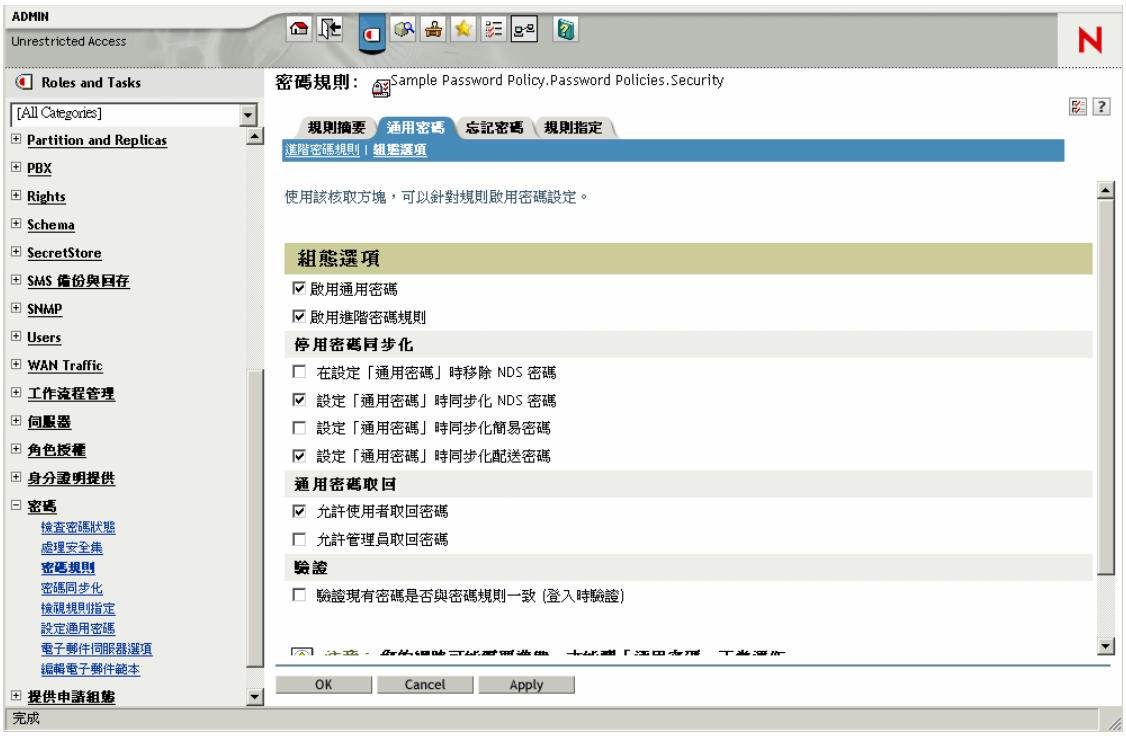


5.1.6 圖表的顯示方式

本文件經常在程序中使用圖表，以說明 iManager 中的選項。選項在桌面上的實際顯示方式視您的瀏覽器而定。

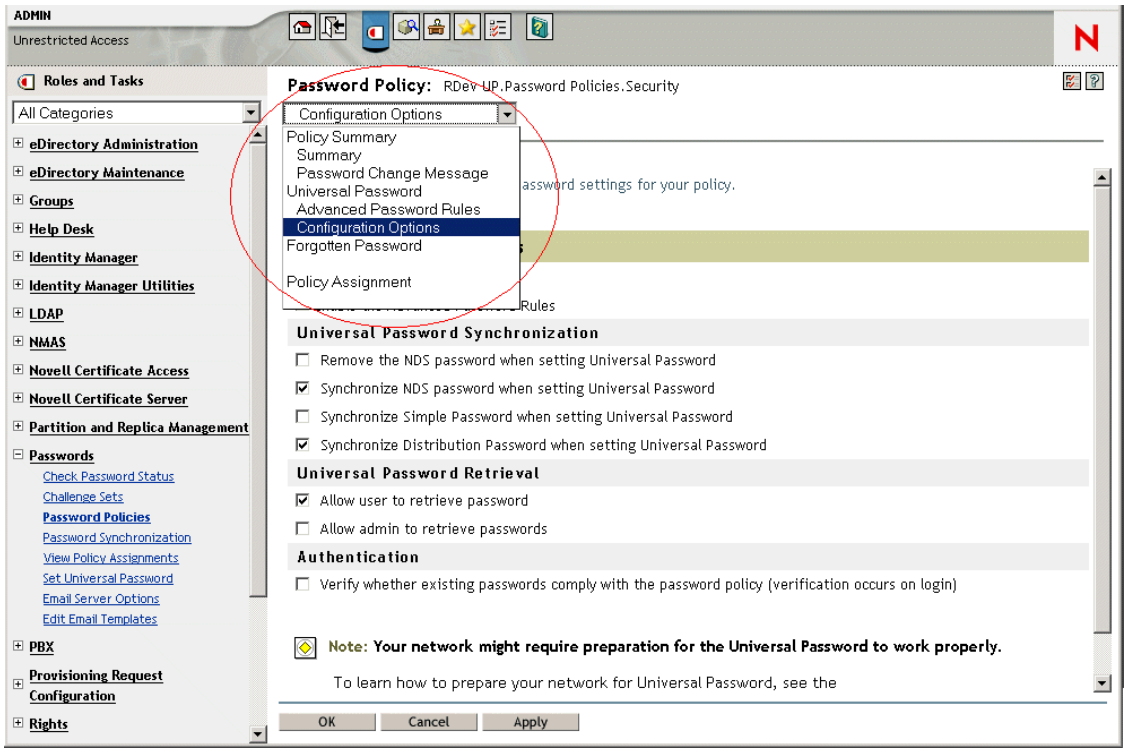
例如，Internet Explorer 使用索引標籤顯示 iManager 選項。

特性 ***5-3*** *iManager* 中的索引標籤



然而，Firefox 瀏覽器使用下拉式清單顯示 iManager 選項。

特性 ***5-4*** *iManager* 中的下拉式清單



在本文件中，圖表的顯示方式與它們在 Firefox 瀏覽器中顯示的方式相同。

5.2 已連接系統支援密碼同步化

建立「使用者」物件時，Identity Manager 一直可以接受來自已連接系統的密碼，即使已連接系統不支援提供該系統的使用者實際密碼也是如此。

AD、NT、eDirectory 和 NIS 可以接受來自 Identity Manager 的密碼，還支援將使用者的實際密碼傳送至 Identity Manager。這表示它們提供對雙向密碼同步化的完全支援。

當您在「發行者」通道的驅動程式組態內定義規則時，其他系統可以提供可用於建立密碼的資料。大部份驅動程式的範例驅動程式組態都包括依據「姓」提供預設密碼的範例規則。

已連接系統具有從 Identity Manager 接受密碼的各種能力。部份已連接系統支援針對新帳戶設定啓始密碼集，但不支援設定「密碼修改」事件。

範例驅動程式組態的功能記載在驅動程式資訊清單中。下列表格提供不在驅動程式資訊清單中的其他資訊。表格指出應用程式是否接受新帳戶的啓始密碼集，以及是否可以接受對現有密碼的修改。資訊清單指出只有已連接系統才可以接受密碼，但不顯示此區別。

驅動程式以群組爲單位，因此您可以查看具有類似功能的範例驅動程式組態。

5.2.1 支援雙向密碼同步化的系統

下列已連接系統支援雙向密碼同步化。它們可以在已連接系統上提供使用者實際密碼，並接受來自 Identity Manager 的密碼。

表格 **5-2** 支援雙向密碼同步化的系統

已連接系統驅動程式	訂閱者通道 應用程式可以接受啓始密碼的設定	訂閱者通道 應用程式可以接受密碼的修改	訂閱者通道 應用程式支援檢查密碼	發行者通道 應用程式可以提供 (同步化) 密碼
Active Directory	是	是	是	是
eDirectory[1]	是	是	是	是
NT Domain	是	是	否	是
NIS	是	是	是	是
SIF	是	是	否	是

[1] 在 Identity Vault 網路樹之間，您可以對使用者啓用雙向密碼同步化，即使未對那些使用者啓用「通用密碼」也是如此。請參閱「案例 1：使用 NDS 密碼將兩個 Identity Vault 同步化」，第 101 頁。

5.2.2 接受來自 Identity Manager 之密碼的系統

下列已連接系統在一定程度上可接受來自 Identity Manager 的密碼。它們無法在已連接系統上爲 Identity Manager 提供使用者實際密碼。

雖然它們無法提供使用者實際密碼，但是可依據已連接系統中的其他使用者資料，將它們設定爲使用「發行者」通道上的規則建立密碼 (範例驅動程式組態依據姓顯示預設密碼)。

表格 **5-3** 接受來自 *Identity Manager* 之密碼的系統

已連接系統驅動程式	訂閱者通道 應用程式可以接受啓始密碼的設定	訂閱者通道 應用程式可以接受密碼的修改	訂閱者通道 應用程式支援檢查密碼	發行者通道 應用程式可以提供 (同步化) 密碼
Groupwise®	是	是	否	否[2]
JDBC	是[3]	否[4]	否	否[5]
LDAP	是[6]	是[6]	是	否
Notes	是	是[7]	是[7]	否
SAP 使用者管理	是	是	否	否

[2]GroupWise 支援兩種驗證方法：

- GroupWise 會提供其自己的驗證，並維護使用者密碼。
- GroupWise 使用 LDAP 驗證 eDirectory，但不維護密碼。

  當您使用此選項時，GroupWise 會忽略驅動程式同步化密碼。

[3] 在 OS 使用者帳戶與資料庫使用者帳戶不同的所有資料庫上 (如 Oracle*、MS SQL、MySQL* 和 Sybase*)，都具有設定啓始密碼的能力。

[4]Identity Manager Driver for JDBC 可用於修改已連接系統上的密碼，但是該功能未在範例驅動程式組態中展示。

[5] 當將密碼儲存在表格中時，可將其做爲資料來同步化。

[6] 如果 LDAP 伺服器允許設定使用者密碼屬性。

[7]Notes 驅動程式可以接受密碼修改，且只檢查 Lotus Notes 中 HTTPPassword 欄位的密碼。

5.2.3 不接受或提供密碼的系統

下列已連接系統無法使用範例驅動程式組態，在已連接系統上接受密碼或提供使用者密碼。

雖然它們無法將使用者密碼提供給 Identity Manager，但是可依據已連接系統中的其他使用者資料，將它們設定爲使用「發行者」通道上的規則建立密碼 (範例驅動程式組態依據姓顯示預設密碼)。

表格 ***5-4*** 不接受或提供密碼的系統

已連接系統驅動程式	訂閱者通道	訂閱者通道	訂閱者通道	發行者通道
	應用程式可以接受啓始密碼的設定	應用程式可以接受密碼的修改	應用程式支援檢查密碼	應用程式可以提供 (同步化) 密碼
分隔文字	否[8]	否[8]	否[8]	否[8]
Exchange 5.5	否	否	否	否
PeopleSoft 3.6	否	否	否	否
PeopleSoft 4.0	否	否	否	否
SAP HR	否	否	否	否

[8]Identity Manager Driver for Delimited Text 不具有在驅動程式 Shim 中直接支援「密碼同步化」的功能。然而，視您正與其進行同步化之已連接系統的不同，可將驅動程式設定爲處理密碼。

5.2.4 不支援密碼同步化的系統

下列已連接系統不支援使用密碼同步化功能。

表格 ***5-5*** 不支援密碼同步化的系統

已連接系統驅動程式	訂閱者通道	訂閱者通道	訂閱者通道	發行者通道
	應用程式可以接受啓始密碼的設定	應用程式可以接受密碼的修改	應用程式支援檢查密碼	應用程式可以提供 (同步化) 密碼
Avaya* PBX	否	否	否	否
授權服務驅動程式	否	否	否	否
迴路服務驅動程式	否	否	否	否

已連接系統驅動程式	訂閱者通道	訂閱者通道	訂閱者通道	發行者通道
	應用程式可以接受啓始密碼的設定	應用程式可以接受密碼的修改	應用程式支援檢查密碼	應用程式可以提供 (同步化) 密碼
手動任務服務驅動程式	否	否	否	否

5.3 密碼同步化的先決條件

「密碼同步化」取決於已備妥的下列元素：

- 「支援通用密碼」，第 81 頁
- 「在驅動程式資訊清單中宣告的密碼同步化功能」，第 81 頁
- 「使用全域組態值控制密碼同步化」，第 82 頁
- 「驅動程式組態中所需的規則」，第 84 頁
- 「安裝在已連接系統上以擷取密碼的過濾器」，第 87 頁
- 「針對使用者建立的 NMAS 密碼規則」，第 87 頁
- 「NMAS 登入方法」，第 87 頁

5.3.1 支援通用密碼

若要在已連接系統中進行密碼同步化，Identity Manager 需要 「通用密碼」。請參閱下列內容：

- 《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的 「部署通用密碼」
- 「準備使用通用密碼」，第 88 頁

5.3.2 在驅動程式資訊清單中宣告的密碼同步化功能

驅動程式資訊清單宣告已連接系統是否支援下列密碼同步化功能：

- 將使用者實際密碼發行至 Identity Manager
- 接受來自 Identity Manager 的密碼

  資訊清單不會區分是接受啓始密碼的建立還是接受密碼的修改。
- 允許 Identity Manager 檢查已連接系統上的密碼，以決定使用者的密碼同步化狀態。

附註：驅動程式資訊清單由驅動程式開發人員或建立驅動程式組態的 Identity Manager 專家撰寫。它不該由網路管理員進行編輯。驅動程式資訊清單代表驅動程式 Shim 和組態的真正功能。只變更資訊清單不會變更功能。若要新增功能，則需要增強驅動程式 Shim、已連接系統或驅動程式組態。

與 Identity Manager 一併提供的範例驅動程式組態包含驅動程式資訊清單項目。若要將這些項目新增至現有驅動程式，請參閱 「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁。

5.3.3 使用全域組態值控制密碼同步化

全域組態值可讓您設定可在規則中參考的常數值。全域組態值有時稱爲伺服器變數，因爲它們保留在每個複製本的屬性中。

針對「密碼同步化」，全域組態值可讓您建立在 Identity Manager 中流入和流出的密碼設定。因爲驅動程式組態中的 Identity Manager 密碼同步化規則經過撰寫，會隨全域組態值中的設定進行不同的行爲，所以無需編輯規則即可輕鬆變更密碼流程。

使用全域組態值，您可以分別控制每個已連接系統的下列設定。

表格 ***5-6*** 已連接系統的設定

設定	描述
Identity Manager 是否接受來自已連接系統的密碼	此設定適用於由已連接系統提供的密碼，以及「發行者」通道上驅動程式組態中 Identity Manager 規則建立的密碼。如果您停用此設定，則會將這兩種密碼排除在外，以便它們不會到達 Identity Manager。
Identity Manager 使用的同步化方法：直接更新「通用密碼」，或直接更新「配送密碼」	Identity Manager 控制進入點 (Identity Manager 所更新的密碼)。NMAS 會根據您在 NMAS 密碼規則中的設定，控制每個不同種類密碼之間的密碼流程。若要檢視 NMAS 密碼規則，請執行下列動作： 1. 在 iManager 中，選取「*密碼*」>「*密碼規則*」。 2. 選取「*密碼規則清單*」中的規則。 3. 按一下「*編輯*」。 4. 從下拉式清單或索引標籤選取選項 (視您所使用的 iManager 版本而定)。 如需使用這些方法的案例，請參閱 5.8 節 「實作密碼同步化」。
是否針對從已連接系統進入 Identity Manager 的密碼強制執行 NMAS 密碼規則	如果強制執行這些規則，則正在進入的不相容密碼不會寫入 Identity Manager 資料儲存。
Identity Manager 是否藉由重設與規則不一致的密碼，在已連接系統上使用 Identity Manager 密碼來強制執行 NMAS 密碼規則。	如果已連接系統不支援此選項 (如在驅動程式資訊清單中宣告的一樣)，則該選項在 NMAS 介面中會變成灰色。只有密碼操作在「發行者」通道上失敗之後，才會重設密碼。
已連接系統是否接受密碼	此設定適用於由 Identity Manager 配送的密碼，以及「訂閱者」通道上驅動程式組態中 Identity Manager 規則建立的密碼。如果您停用此設定，則會將這兩種密碼排除在外，以便它們不會到達已連接系統。 如果已連接系統不支援此選項 (如在驅動程式資訊清單中宣告的一樣)，則該選項在介面中會變成灰色。
當密碼未同步化時，是否會以電子郵件通知使用者	自動將電子郵件傳送至受影響的使用者。

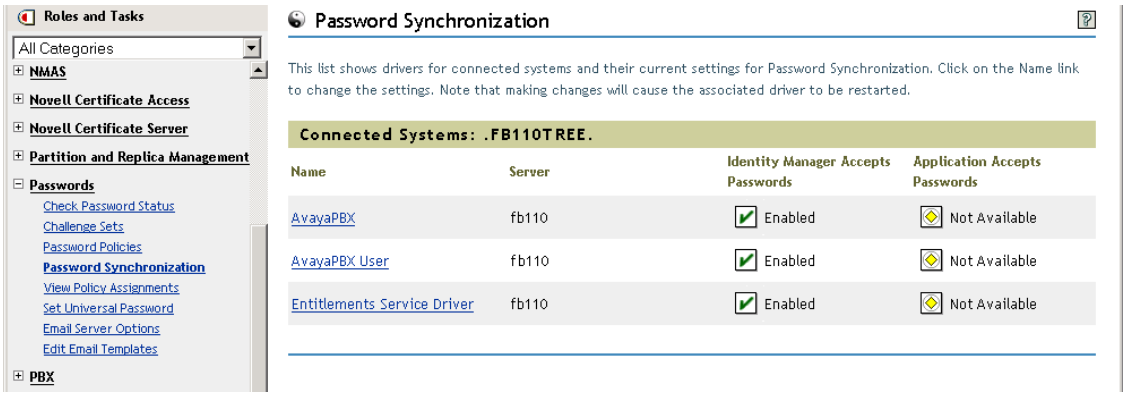
與 Identity Manager 一併提供的驅動程式組態包含驅動程式資訊清單項目。若要將這些項目新增至現有驅動程式，請參閱「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁。

若要編輯全域組態值，請執行下列動作：

1 在 iManager 中，選取「密碼」>「密碼同步化」。

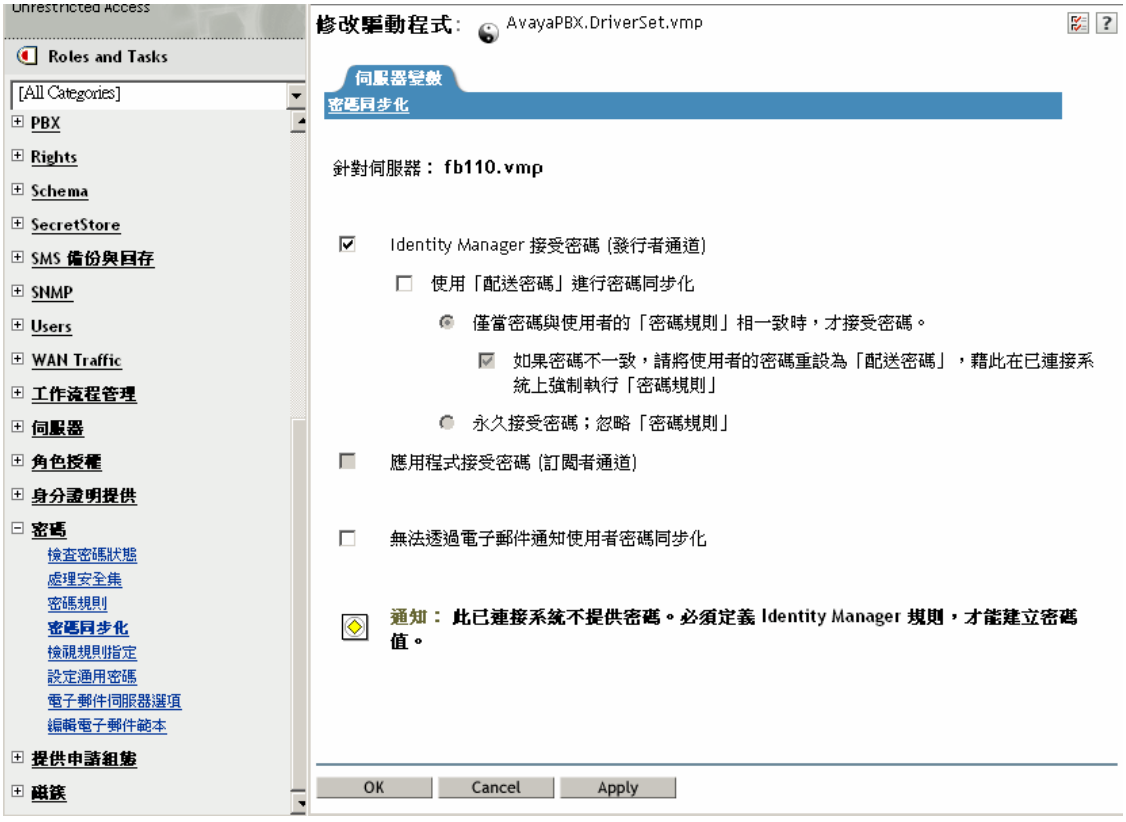
2 搜尋驅動程式。

在您指定要搜尋已連接系統驅動程式的位置之後，iManager 會顯示它找到的所有已連接系統驅動程式密碼流程設定之綜覽。



3 若要檢視設定，請按一下驅動程式名稱。

「修改驅動程式」頁面會顯示「密碼同步化」的全域組態值。



如果此頁面上有選項變成灰色，則驅動程式資訊清單顯示已連接系統不支援該選項。

4 進行變更，然後按一下「確定」。

附註：您可以分別在每個驅動程式上設定全域組態值。驅動程式上的全域組態值會置換驅動程式集上的那些全域組態值。在特定驅動程式上設定值可爲您提供更加具體的控制。此頁面只顯示在個別驅動程式上呈現的全域組態值。

如果您在「驅動程式集」物件上設定全域組態值，則當驅動程式自身沒有值時，在該驅動程式集中的驅動程式會繼承那些值。如果驅動程式沒有其自身的設定，而是繼承驅動程式集的全域組態值，則 iManager 不會顯示它們。雖然 iManager 不顯示繼承的全域組態值，但是它們仍然受密碼同步化規則的限制。

5.3.4 驅動程式組態中所需的規則

每個驅動程式之「發行者」和「訂閱者」通道上的 Identity Manager 規則都會根據上面所述之全域組態變數中的設定，來控制密碼流程。這些規則包含於 Identity Manager 的驅動程式組態中。

如果您要升級現有的驅動程式組態，而不是取代它，則必須將某些規則新增至該組態 (請參閱 「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁)。若要讓密碼同步化運作，這些規則必須位於驅動程式組態中的正確位置。

- 「發行者指令轉換集中所需的規則」，第 84 頁
- 「發行者輸入轉換規則集中所需的規則」，第 85 頁
- 「訂閱者指令轉換規則集中所需的規則」，第 86 頁
- 「訂閱者輸出轉換規則集中所需的規則」，第 86 頁

發行者指令轉換集中所需的規則

「密碼同步化規則名稱」欄中列出的規則必須以列出的順序呈現。同時，它們必須是「發行者指令轉換」規則集中的最終規則。

表格 ***5-7*** 發行者指令轉換集中所需的規則

驅動程式組態中的位置	密碼同步化規則名稱	規則執行的動作
發行者指令轉換	密碼 (發行者)：預設密碼規則	如果「新增」物件尚未包含密碼，則將預設密碼新增至該「新增」物件。 此規則和「密碼 (發行者)：預設密碼規則」是您可以修改或移除的僅有規則。若要讓密碼同步化功能正常運作，使用其他規則時，不應有任何變更。
	密碼 (發行者)：檢查密碼 GCV	檢查全域組態值 (GCV) 以判定您是否已指定 Identity Manager 接受來自此已連接系統的密碼。如果尚未指定，則會將所有的密碼元素排除在外。 全域組態值 (GCV) 的名稱是 enable-password-publish，顯示名稱是「*Identity Manager 接受來自應用程式的密碼*」。
	密碼 (發行者)：發行配送密碼	將 <password> 元素轉換爲允許更新「通用密碼」的格式。 此規則參考下列全域組態值 (GCV)： ◆ publish-password-to-dp ◆ enforce-password-policy
	密碼 (發行者)：發行 NDS 密碼	如果您已指定應更新 NDS 密碼，則接受 <password> 元素。如果未指定，則會將 <password> 元素排除在外。 此規則會參考名爲 publish-password-to-nds 的全域組態值 (GCV)。
	密碼 (發行者)：新增密碼封包內容	放入封包內容資料中，該資料在引擎中傳遞以進行電子郵件通知。
	密碼 (訂閱者)：新增密碼封包內容	放入封包內容資料中，該資料在引擎中傳遞以進行電子郵件通知。

發行者輸入轉換規則集中所需的規則

如果「輸入轉換」中有多個規則，建議您將「密碼 (發行者)：訂閱電子郵件通知」規則列在最後。

表格 ***5-8*** 發行者輸入轉換規則集中所需的規則

驅動程式組態中的位置	密碼同步化規則名稱	規則執行的動作
發行者輸入轉換	密碼 (發行者)：訂閱電子郵件通知	如果接收到密碼封包內容資訊，且狀態顯示有問題，則會向使用者傳送電子郵件。它會將郵件傳送至 eDirectory 之 Internet EMail Address 屬性中指出的使用者電子郵件地址。 此規則參考名爲 notify-user-on-password-dist-failure 的全域組態值 (GCV)，以判定是否要傳送通知電子郵件。

訂閱者指令轉換規則集中所需的規則

「密碼同步化規則名稱」欄中列出的規則必須以列示的順序呈現。同時，它們必須是 「訂閱者指令轉換」規則集中的最終規則。

表格 ***5-9*** 訂閱者指令轉換規則集中所需的規則

驅動程式組態中的位置	密碼同步化規則名稱	規則執行的動作
訂閱者指令轉換	密碼 (訂閱者)：轉換配送密碼	將 「通用密碼」轉換爲 <password> 元素。
	密碼 (訂閱者)：預設密碼規則	如果 「新增」物件尚未包含密碼，則將預設密碼新增至該 「新增」物件。 此規則和 「密碼 (發行者)：預設密碼規則」是您可以修改或移除的僅有規則。若要讓密碼同步化功能正常運作，使用其他規則時，不應有任何變更。
	密碼 (訂閱者)：檢查密碼 GCV	檢查全域組態值 (GCV) 以判定您是否已指定已連接的系統接受密碼。如果尚未指定，則會將所有的密碼元素排除在外。 全域組態值 (GCV) 的名稱是 enable-password-subscribe，顯示名稱是 「*應用程式接受來自 Identity Manager 資料儲存的密碼*」。
	密碼 (訂閱者)：新增密碼封包內容	放入密碼封包內容資料中，該資料在引擎中傳遞以進行電子郵件通知。

訂閱者輸出轉換規則集中所需的規則

如果在 「輸出轉換」中有多個規則，建議您將 「密碼 (訂閱者)：發行者電子郵件通知」規則列在最後。

表格 *5-10* 訂閱者輸出轉換規則集中所需的規則

驅動程式組態中的位置	密碼同步化規則名稱	規則執行的動作
訂閱者輸出轉換	密碼 (訂閱者)：發行者電子郵件通知	如果接收到密碼封包內容資訊，且狀態顯示有問題，則會向使用者傳送電子郵件。 此規則參考名爲 notify-user-on-password-dist-failure 的全域組態值 (GCV)，以判定是否要傳送通知電子郵件。

5.3.5 安裝在已連接系統上以擷取密碼的過濾器

針對 AD、NT Domain 和 NIS，必須安裝過濾器來擷取使用者的密碼。

請參閱 「設定密碼過濾器」，第 128 頁。

5.3.6 針對使用者建立的 NMAS 密碼規則

雖然您可以在不具有「通用密碼」的情況下使用「密碼同步化」的部份功能，但是必須使用 NMAS 密碼規則爲使用者啓用「通用密碼」。密碼規則 (Policy) 也可讓您指定「進階密碼規則 (Rule)」，並指定是否檢查使用者現有密碼與規則 (Rule) 的相符性。

若要使用「Identity Manager 密碼同步化」，您必須瞭解密碼規則。您可以在《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》的「使用密碼規則管理密碼」中瞭解密碼規則。

5.3.7 NMAS 登入方法

在某些情況下，您必須具有可用的「NMAS 簡易密碼登入方法」，才能執行密碼功能。例如，LDAP 就需要它。

如需登入方法的相關資訊，請參閱《*Novell* 模組化驗證服務 *(NMAS) 3.0* 管理指南 (http://www.novell.com/documentation/nmas30/index.html)》。

5.4 準備使用 Identity Manager 密碼同步化和通用密碼

5.4.1 將使用者從 NDS 密碼切換到通用密碼

當您使用密碼規則針對使用者群組開啓「通用密碼」時，使用者需要填入該「通用密碼」。

如果您先前已使用「密碼同步化」來更新 NDS 密碼，則需要規劃使用者密碼的轉換。若要切換爲使用「通用密碼」，您可以執行下列其中一個動作，以讓使用者建立「通用密碼」：

- 如果您使用 Novell Client，請展示支援「通用密碼」的 Novell Client。

  「Identity Manager 密碼同步化」不需要 Novell Client。

  您推行 Novell Client 之後，下一次使用者使用 Novell Client 登入時，會在雜湊 NDS 密碼之前先擷取該密碼，並使用它來填入「通用密碼」(請參閱「密碼管理」指南中的「爲使用者規劃登入和變更密碼的方法」)。
- 如果您不是在使用 Novell Client，請讓使用者登入 iManager 自助服務主控台。該登入方法會填入「通用密碼」。若要存取 iManager 自助服務主控台，請前往 iManager 伺服器上的 /nps。例如，https://www.myiManager.com/nps。
- 使用啓用「通用密碼」的 LDAP 伺服器，讓使用者使用任何驗證的服務登入。例如，透過公司入口網站登入。

5.4.2 協助使用者變更密碼

當使用者在 iManager、iManager 自助服務主控台或 Novell Client 中變更密碼時，會顯示 NMAS 密碼規則 (Policy) 中的「進階密碼規則 (Rule)」。檢視規則可讓使用者建立相容的密碼，而無需猜測規則。

依據您密碼流程的設定方式，使用者可以在已連接的系統上變更密碼，且會將該密碼同步化至 Identity Manager 和其他已連接系統。然而，當使用者變更密碼時，已連接系統不會顯示「進階密碼規則」。

如果您要強制執行「進階密碼規則」，並避免不相容的密碼，則最好是要求使用者僅在 iManager 自助服務主控台或 Novell Client 中變更密碼，或至少確定使用者已非常瞭解「進階密碼規則」。

在已連接系統上，允許使用者在不檢視密碼規則的情況下變更密碼。因此，使用者可能不會正確地記住規則。當使用者首次進行變更時，僅強制執行已連接系統自身的規則。當在已連接系統上建立不相容的密碼時，使用者可能遇到下列問題，視 Identity Manager 的設定而定：

- 如果您已啓用對從已連接系統進入 Identity Manager 的密碼強制執行規則的設定，則使用者的新密碼不會同步化至 Identity Vault。如果您已設定 Identity Manager 來通知使用者有關失敗的情況，則他們會透過電子郵件瞭解到其密碼未同步化。
- 如果您還設定 Identity Manager 來取代已連接系統上不相容的密碼，則使用者無法使用其選擇的新密碼來登入至已連接系統。

  Identity Manager 會在已連接系統上將密碼重設爲「配送密碼」，其可能爲使用者建立的最終相容密碼。

5.4.3 準備使用通用密碼

若要準備使用「通用密碼」，請參閱《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「部署通用密碼」。您可以在該章內找到需要的大部份資訊。

此外，請記住下列內容：

- 需要 eDirectory 8.7.1 或更新版本，才能使用「通用密碼」。無需 NetWare® 6.5。

- 「Identity Manager 密碼同步化」依賴「通用密碼」和「配送密碼」兩者。「配送密碼」是一種儲存機制，Identity Manager 可以從該儲存機制將密碼配送至已連接系統。與「通用密碼」一樣，也可以對「配送密碼」強制執行 NMAS 規則。
- Identity Manager 隨附的 Identity Manager iManager 外掛程式，包括「密碼管理」外掛程式。這些外掛程式可讓您建立密碼規則，並判定您要將「通用密碼」與「NDS 密碼」、「簡易密碼」和「配送密碼」同步化的方式。

  這些外掛程式會取代 NetWare 6.5 隨附的「通用密碼」外掛程式。您可以在《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》的「使用密碼規則管理密碼」中瞭解這些外掛程式。
- 無法將 eDirectory 8.6.2 用於 Identity Manager 所使用的網路樹。然而，eDirectory 8.6.2 支援密碼同步化功能的子集。因此，如果您尚未準備升級整個環境，則可以將 eDirectory 8.6.2 用於其他網路樹。
- 升級軟體以部署「通用密碼」時可降低影響的一種方法是，針對 Identity Manager 建立個別的網路樹做爲 Identity Vault。許多環境已將 Identity Vault 用於 Identity Manager 和驅動程式。
- 「通用密碼」會爲您提供先前密碼管理工具不支援的功能，例如強制執行密碼規則和使用特殊字元的能力。
- 務必更新 Novell Client 和其他公用程式，以避免「NDS 密碼」與「通用密碼」不同步化 (有時稱爲「密碼漂移」)。請參閱《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「爲使用者規劃登入和變更密碼的方法」。
- 最新版本的 Novell Client 支援「通用密碼」，可以在您首次爲該使用者啓用「通用密碼」時，填入使用者的「通用密碼」，並可以在使用者變更密碼時，顯示並強制執行 NMAS 密碼規則。
- 已連接系統不會顯示您在密碼規則 (Policy) 中建立的「進階密碼規則 (Rule)」。此時，雖然 Novell Client 會強制執行這些規則，但也不會進行顯示。

  最好是要求使用者僅在 iManager 自助服務主控台中變更密碼。

  如果您允許使用者在已連接系統上，或藉由使用最新版本的 Novell Client 來變更其密碼，請確定使用者已非常瞭解密碼規則，以協助使用者順利建立相容的密碼。
- 請確定管理員和 Help Desk 瞭解只有在 NetWare® 6.5 伺服器或更新版本上，或在具有最新 Novell Client 的機器上使用 ConsoleOne® 時，它才會支援「通用密碼」。
- 請確定管理員和 Help Desk 使用者瞭解使用僅支援「NDS 密碼」之公用程式的含意。這些公用程式可用於登入，但是不應將它們用於變更密碼。此方法會避免密碼漂移。

  《*Novell 模組化驗證服務 (NMAS) 3.0* 管理指南 (http://www.novell.com/documentation/nmas30/index.html)》會參考列出公用程式及其對「通用密碼」之支援的技術資訊文件 (Technical Information Document，TID)。

5.4.4 相符容器

NMAS 密碼規則是使用網路樹中心的方式指定的。相對地，「密碼同步化」是依每個驅動程式設定的。驅動程式會在每個伺服器上安裝，且僅可以管理主複製本或讀 / 寫複製本中的那些使用者。

若要取得預期的「密碼同步化」結果，請確定執行「密碼同步化」驅動程式之伺服器上主複製本或讀 / 寫複製本中的容器，與您指定密碼規則且已啓用「通用密碼」的容器相符。將密碼規則指定給分割區根容器，可確保將密碼規則指定給該容器和次容器中的所有使用者。

5.4.5 設定電子郵件通知

若要使用電子郵件通知功能，您必須執行下列動作：

- 使用 iManager 中的「通知組態」任務，來設定電子郵件伺服器。
- 使用 iManager 中的「通知組態」任務，自定電子郵件範本 (如果需要的話)。
- 確定 Identity Vault 使用者已填入 Internet EMail Address 屬性。

遵循「設定電子郵件通知的組態」，第 132 頁中的指示。

5.5 設定並同步化新的驅動程式

如果您的環境中尚未使用「密碼同步化 1.0」，而且您正在建立驅動程式，或以新的 Identity Manager 組態取代現有的組態，請設定「Identity Manager 密碼同步化」功能。

1. 確定您的環境已可以使用「通用密碼」。

   請參閱「準備使用 Identity Manager 密碼同步化和通用密碼」，第 87 頁。

2. 建立驅動程式，或以 Identity Manager 3 組態取代現有驅動程式的組態。

   Identity Manager 組態包含 Identity Manager 規則和「Identity Manager 密碼同步化」所需的其他項目。如需匯入新範例驅動程式組態的相關資訊，請參閱其各自的《Identity Manager 驅動程式指南 (http://www.novell.com/documentation/beta/dirxmldrivers)》。

3. 藉由建立已啓用「通用密碼」的 NMAS 密碼規則，開啓使用者的「通用密碼」。

   請參閱《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「建立密碼規則」。如果您先前將「通用密碼」與 NetWare 6.5 搭配使用，則可以在《密碼管理管理指南》的「(僅限 NetWare 6.5) 重新建立通用密碼指定」中找到部份額外的步驟。

   建議您將密碼規則儘量指定爲網路樹中的高層級。

「組態選項」頁面可讓您選取如何讓 NMAS 將不同密碼同步化的方式。

如需使用 「密碼同步化」的案例以及如何套用 Identity Manager 密碼規則的相關資訊，請參閱 「實作密碼同步化」，第 100 頁。另請參閱線上說明。

4 (僅限 Active Directory、NIS 或 NT Domain) 如果您要讓已連接系統提供使用者密碼給 Identity Manager，請安裝新的 「密碼同步化」過濾器並設定其組態。

如需指示，請參閱每個驅動程式的驅動程式實作指南，其位於 Identity Manager 驅動程式 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

5 針對每個已連接系統，確定依您要的方式設定密碼流程。

5a 在 iManager 中，按一下 「密碼」 > 「密碼同步化」，然後搜尋您要管理之已連接系統的驅動程式。

5b 檢視密碼流程的目前設定。

這是全域組態值 (GCV) 的圖形化介面。按一下驅動程式的名稱，以進行編輯。您可以編輯下列設定：

- Identity Manager 是否接受此系統的密碼。
- Identity Manager 要更新的密碼：直接更新 「通用密碼」，或直接更新 「配送密碼」。

  Identity Manager 控制進入點，表示 Identity Manager 所更新的密碼。NMAS 會根據 「組態選項」中的密碼規則設定，控制每一種不同密碼之間的密碼流程。請參閱步驟 3, 第 90 頁中的圖表。
- 是否對進入 Identity Manager 的密碼變更強制執行使用者的密碼規則。
- 是否藉由重設不一致的密碼，在已連接系統上強制執行使用者的密碼規則。
- 此已連接系統是否接受密碼。
- 密碼同步化失敗時，是否傳送電子郵件通知。

6 測試密碼同步化。

- 確認將 Identity Manager 密碼配送至指定的系統。
- 確認指定的已連接系統即將密碼發行至 Identity Manager。

如需疑難排解祕訣，請參閱 「實作密碼同步化」，第 100 頁。

5.6 升級密碼同步化 1.0

此任務僅適用於與 「密碼同步化 1.0」搭配使用之現有 Active Directory 和 NT Domain 的 「Identity Manager 驅動程式」。

在從 「密碼同步化 1.0」升級時，請務必遵循正確的程序。

如需指示，請參閱 Active Directory 和 NT Domain 之 「Identity Manager 驅動程式」的驅動程式實作指南，其位於 Identity Manager 驅動程式 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

5.7 升級現有的驅動程式組態以支援密碼同步化

本節說明如何將 「Identity Manager 密碼同步化」的支援新增至現有的驅動程式組態，而不是以 Identity Manager 範例組態取代現有的驅動程式組態。

針對要參與密碼同步化的每個驅動程式新增支援。執行此動作的方式爲，匯入 「重疊」組態檔案，以一次新增規則、驅動程式資訊清單和全域組態值 (GCV)。

新增規則、驅動程式資訊清單和全域組態值 (GCV) 之後，還必須將 nspmDistributionPassword 屬性新增至驅動程式過濾器。

重要：如果您要升級 AD 或 NT Domain 的 「Identity Manager 驅動程式」，且該驅動程式與 「密碼同步化 1.0」搭配使用，請遵循 Active Directory 和 NT Domain 之 「Identity Manager 驅動程式」的驅動程式實作指南，其位於 Identity Manager 驅動程式 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

此程序中新增的規則適用於支援 「通用密碼」和 「配送密碼」，方法是使用 「密碼同步化」功能。如果使用 Identity Manager 驅動程式時只同步化 「NDS 密碼」，則不應使用 Identity Manager 驅動程式組態的規則。同步化 「NDS 密碼」的方式是使用 「公用金鑰」和 「私密金鑰」屬性，而不是這些規則，如 「案例 1：使用 NDS 密碼將兩個 Identity Vault 同步化」，第 101 頁中所述。

- 「步驟 1：將驅動程式轉換爲 Identity Manager 3 格式」，第 93 頁
- 「步驟 2：新增至驅動程式組態」，第 95 頁
- 「步驟 3：變更過濾器設定」，第 97 頁
- 「步驟 4：設定密碼同步化流程」，第 99 頁

先決條件

- ❑ 使用 「輸出驅動程式精靈」，建立現有驅動程式的備份。
- ❑ 確定您已安裝新的驅動程式 Shim。

  有些密碼同步化功能 (例如，「檢查密碼狀態」) 沒有新的 Identity Manager 驅動程式 Shim 就不會運作。

重要：如果您在升級 AD 或 NT Domain 的「Identity Manager 驅動程式」，而該驅動程式正與「密碼同步化 1.0」搭配使用中，則請先檢閱升級指示，再安裝驅動程式 Shim。請遵循 Active Directory 和 NT Domain 之「Identity Manager 驅動程式」驅動程式實作指南中的升級指示，其位於 Identity Manager 驅動程式 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

5.7.1 步驟 1：將驅動程式轉換爲 Identity Manager 3 格式

1 確定您的環境已可以使用「通用密碼」。

請參閱「準備使用 Identity Manager 密碼同步化和通用密碼」，第 87 頁。

如果您在使用 DirXML® 1.1a，請參閱「將驅動程式組態從 DirXML 1.1a 升級至 Identity Manager 格式」，第 21 頁。

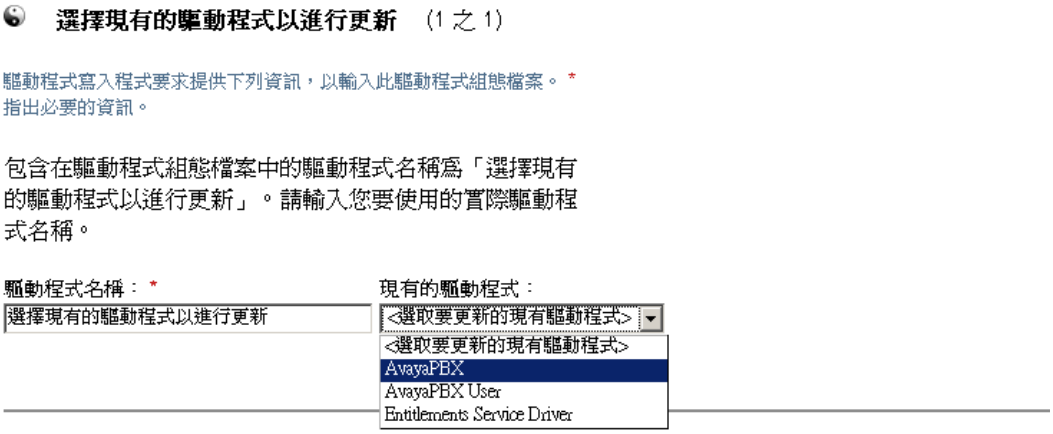
2 在 iManager 中，按一下「*Identity Manager* 公用程式」>「輸入驅動程式」。

3 選取現有驅動程式所在的驅動程式集，然後按「下一步」。

4 在出現的驅動程式組態清單中，捲動至「其他規則」，然後只選取「密碼同步化 *2.0* 規則」。

5 按「下一步」。

6 在「現有的驅動程式」下拉式清單中，選取要更新的現有驅動程式。



7 在「已連接系統」下拉式清單中，選取已連接系統類型。

如果下拉式清單中沒有該驅動程式名稱，請選取「其他系統」。

根據驅動程式類型，「輸入驅動程式精靈」會在驅動程式資訊清單中輸入項目，指出驅動程式組態和已連接系統的功能：

- 已連接系統是否可以提供密碼給 Identity Manager。

  這是指已連接系統上使用者的實際密碼，而不是指使用樣式表建立的密碼。只有 AD、eDirectory 和 NIS 可以這樣做。
- 已連接系統是否可以接受 Identity Manager 的密碼
- 已連接系統是否可以檢查密碼，查看它是否與 Identity Manager 中的密碼相符。

驅動程式資訊清單中需要正確的項目，「密碼同步化」規則才能運作。驅動程式資訊清單指出已連接系統、Identity Manager 驅動程式 Shim 和驅動程式組態規則的結合能力，其通常不該由網路管理員進行編輯。

8 按「下一步」。

9 如果您沒有要儲存的驅動程式資訊清單或全域組態值 (GCV) 值，請選取「更新驅動程式的所有項目」。

此選項會提供給您密碼同步化所需的驅動程式資訊清單、全域組態值 (GCV) 和 Identity Manager 規則。

驅動程式資訊清單和全域組態值 (GCV) 會覆寫已經存在的任何值。因爲這些是 Identity Manager 2 中的新驅動程式參數類型，所以 DirXML 1.*x* 驅動程式不應有任何要覆寫的現有值。

密碼同步化規則不會覆寫任何現有的規則物件。只是單純地新增至「驅動程式」物件。

附註：如果您有想要儲存的驅動程式資訊清單或全域組態值 (GCV) 值，請選取「僅更新驅動程式中選定的規則」，並針對所有規則選取該核取方塊。此選項會輸入密碼規則，但不會變更驅動程式資訊清單或全域組態值 (GCV)。您需要手動貼入任何其他值。

---

10 按「下一步」，然後按一下「完成」，即可完成精靈。

此時，「驅動程式」物件下已建立新的規則做爲規則物件，但還不是驅動程式組態的一部份。若要連結它們，您必須在「訂閱者」和「發行者」通道上驅動程式組態中的正確位置以手動方式將每個規則插入。

5.7.2 步驟 2：新增至驅動程式組態

如需新增的規則清單及其插入位置，請參閱「驅動程式組態中所需的規則」，第 84 頁。

將每個新規則插入現有驅動程式組態的正確位置。

如果規則集有多個規則，請確定這些 Identity Manager 密碼同步化規則列在最後。

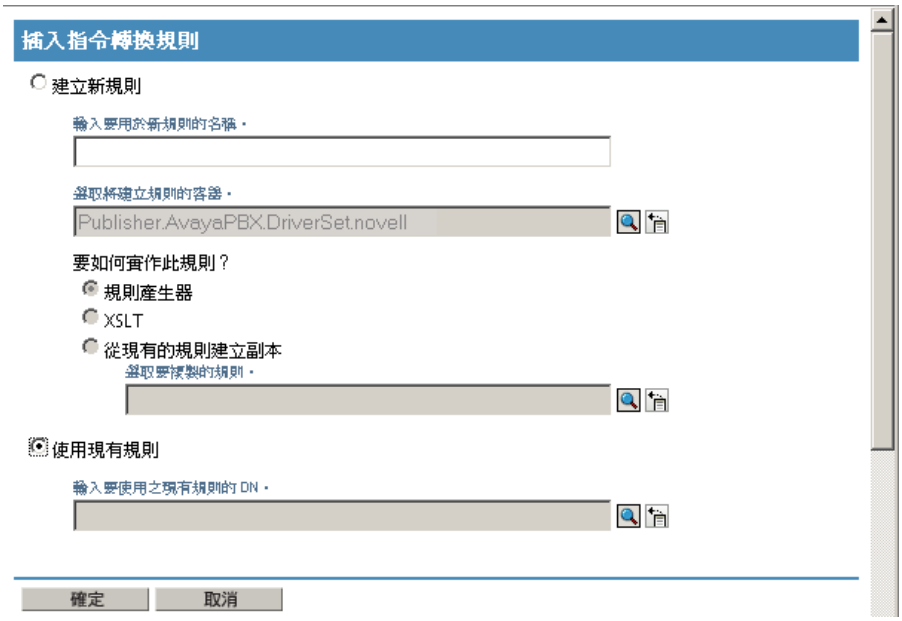
針對每個規則重複下列步驟。

1 選取「*Identity Manager*」>「*Identity Manager* 概觀」，然後搜尋包含所更新之驅動程式的驅動程式集。

2 按一下您剛剛更新的驅動程式 (例如，AvayaPBX)。

3 在需要新增其中一個新規則的位置按一下圖示 (例如，「發行者」通道上的 「指令轉換規則」)。

4 按一下 「插入」，即可新增規則。



5 按一下 「使用現有規則」，瀏覽新的規則物件，然後按一下 「確定」。

6 如果任何新規則在清單中都有一個以上的規則，請使用箭頭按鈕，將新規則移至清單中的正確位置。

請確定規則以 「驅動程式組態中所需的規則」，第 84 頁中的順序列出。

5.7.3 步驟 3：變更過濾器設定

1 針對您想要同步化密碼的物件類別 (例如，「使用者」)，確定 nspmDistributionPassword 屬性位於過濾器中，並具有下列設定：

- 若爲 「發行者」通道，將過濾器的 「*nspmDistributionPassword*」屬性設爲 「忽略」。
- 若爲 「訂閱者」通道，將過濾器的 「*nspmDistributionPassword*」屬性設爲 「通知」。

若要檢視屬性，您可能需要捲動到該類別並選取它 (例如，「使用者」)，然後在屬性中捲動。

如果 nspmDistributionPassword 未列出，請執行下列動作：

1a 確定已選取類別，然後按一下 「新增屬性」。

1b 捲動至 nspmDistributionPassword 並選取它，然後按一下 「確定」。

2 針對將 「*nspmDistributionPassword*」屬性設爲 「通知」的所有物件，將 「公用金鑰」和 「私密金鑰」屬性都設爲 「忽略」。

3 針對您要升級以參與密碼同步化的每個驅動程式，重複步驟 2, 第 93 頁 (在 「將驅動程式轉換爲 Identity Manager 3 格式」中) 一直到本節 (「變更過濾器設定」) 中的步驟 2。

此時，驅動程式具有新的驅動程式 Shim、Identity Manager 格式，以及驅動程式組態中支援密碼同步化所需的其他元素：驅動程式資訊清單、全域組態值 (GCV)、密碼同步化規則和過濾器設定。

4 檢查個別驅動程式實作指南，以取得設定 「Identity Manager 密碼同步化」的任何其他步驟或資訊。請參閱 Identity Manager 驅動程式 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

5 以啓用之 「通用密碼」建立密碼規則，開啓使用者的 「通用密碼」。

請參閱 《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的 「建立密碼規則」。如果您先前將 「通用密碼」與 NetWare 6.5 搭配使用，則可以在 《密碼管理管理指南》的 「(僅限 NetWare 6.5) 重新建立通用密碼指定」中找到部份額外的步驟。

建議您將密碼規則儘量指定爲網路樹中的高層級。

「組態選項」頁面具有如何讓 NMAS 將不同密碼同步化的選項。預設值應可運用於大部份實作。如需相關資訊，請參閱該網頁的線上說明。

如需使用 「密碼同步化」的案例以及如何套用密碼規則的相關資訊，請參閱 「實作密碼同步化」，第 100 頁。

NMAS 密碼規則是使用網路樹中心的方式指定的。相對地，「密碼同步化」是依每個驅動程式設定的。驅動程式會在每個伺服器上安裝，且僅可管理主複製本或讀 / 寫複製本中的那些使用者。

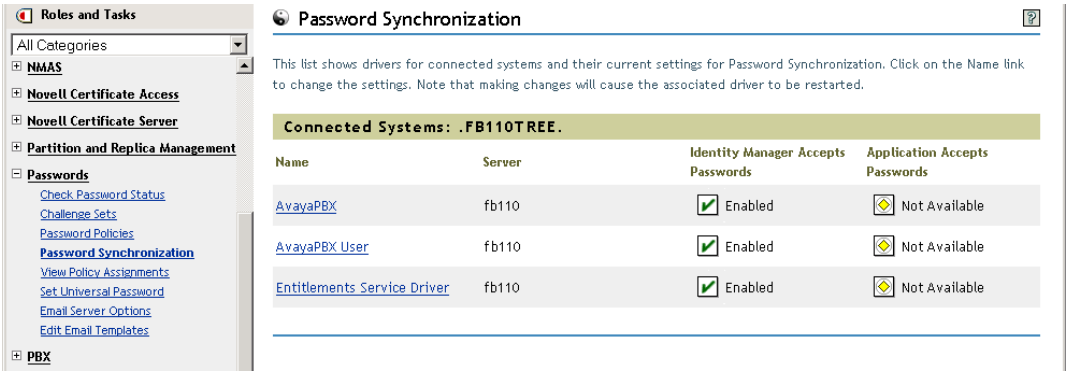
若要取得預期的 「密碼同步化」結果，請確定執行 「密碼同步化」驅動程式之伺服器上主複製本或讀 / 寫複製本中的容器，與您指定密碼規則且啓用 「通用密碼」的容器相符。將密碼規則指定給分割區根容器，可確保將密碼規則指定給該容器和次容器中的所有使用者。

5.7.4 步驟 4：設定密碼同步化流程

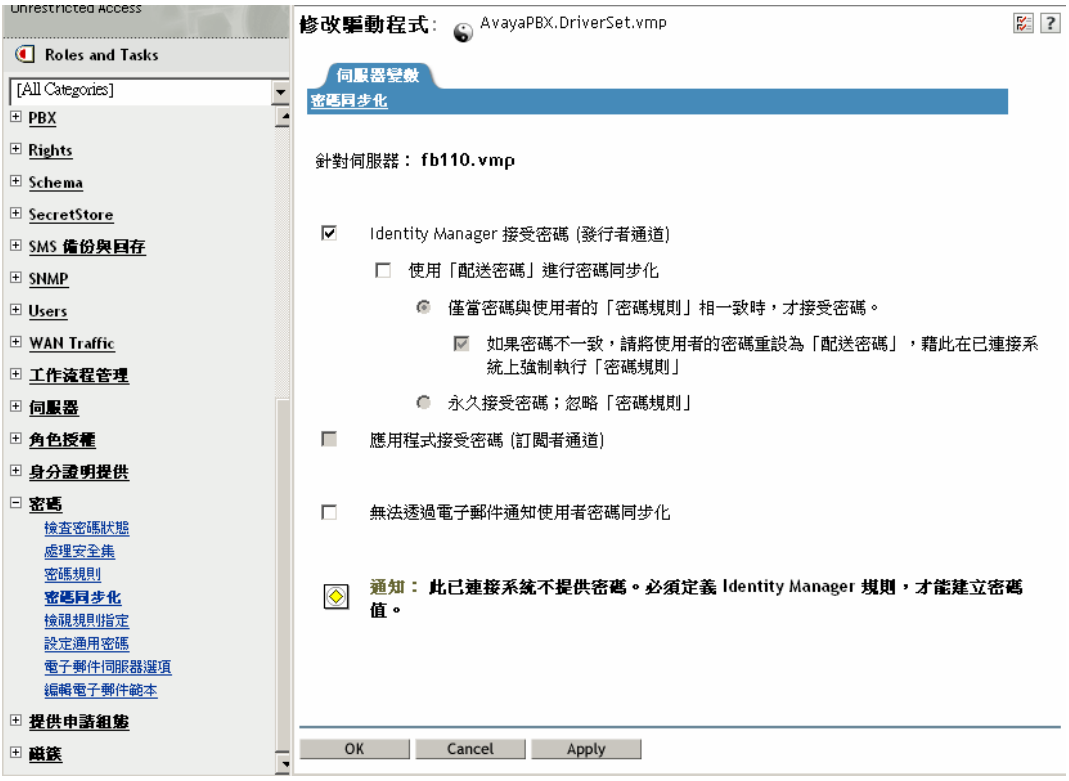
確定每個已連接系統都已按照您要的方式設定密碼流程。

1 在 iManager 中，選取「密碼」>「密碼同步化」。

2 在網路樹或容器中搜尋要管理之已連接系統的驅動程式。



3 藉由選取驅動程式檢視密碼流程的目前設定



此頁面列出全域組態值 (GCV)。您可以選取選項以進行變更。

Identity Manager 會控制進入點 (Identity Manager 所更新的密碼)。NMAS 會根據您在「組態選項」中設定的選項，控制每一種不同密碼之間的密碼流程 (步驟 3, 第 83 頁 顯示「組態選項」頁面)。如果您選取「使用 「配送密碼」進行密碼同步化」，則

Identity Manager 會直接使用 「配送密碼」。如果取消選取此選項，則 Identity Manager 會直接使用 「通用密碼」。

如需這些選項的相關資訊 (包含說明)，請參閱 「實作密碼同步化」，第 100 頁。另請參閱線上說明。

4 測試密碼同步化。

確認將 Identity Manager 密碼配送至指定的系統。

確認指定的已連接系統將密碼發行至 Identity Manager。

如需疑難排解祕訣，請參閱 「實作密碼同步化」，第 100 頁。

5.8 實作密碼同步化

Identity Manager 中提供的 「密碼同步化」功能，可讓您實作數個不同的案例。本節說明基本案例，協助您瞭解 「Identity Manager 密碼同步化」中的設定，以及 NMAS 密碼規則如何影響密碼同步化。您可以使用一或多個案例來滿足環境的需要。

5.8.1 Identity Manager 與 NMAS 之間關係的概觀

公用程式和 NMAS

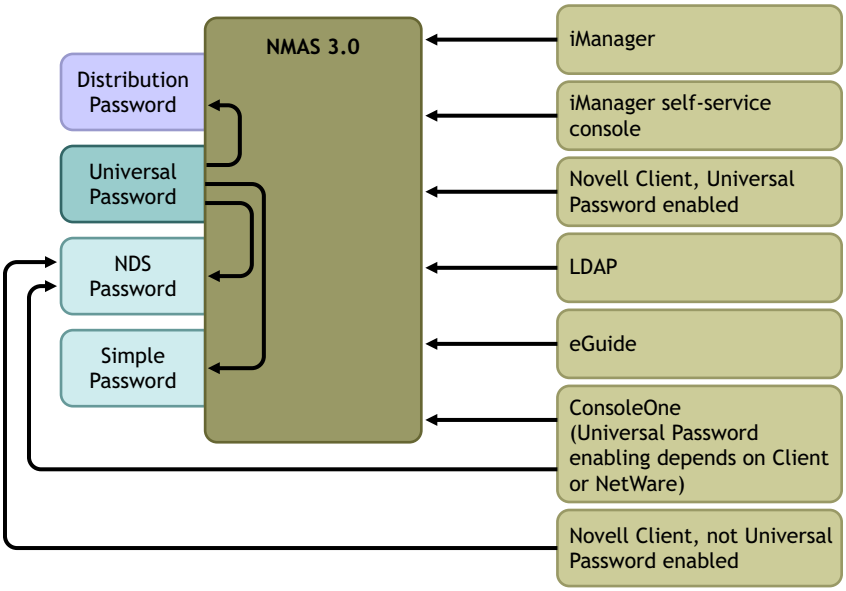
公用程式 (例如，iManager 和 Novell Client) 與 NMAS 進行通訊，而非直接更新特定的密碼。NMAS 是決定要更新之密碼的實體。

NMAS 會根據 NMAS 密碼規則中的設定，同步化 Identity Vault 中的密碼。

非啓用之 「通用密碼」的舊公用程式，會直接更新 NDS 密碼，而不是與 NMAS 進行通訊，讓 NMAS 決定所更新的密碼。請留意使用者和 Help Desk 管理員在您的環境中使用舊公用程式的方式。由於舊公用程式會直接更新 NDS 密碼，而不是透過 NMAS 進行更新，因此如果您在使用 「通用密碼」和 NMAS 2.3，則會發生密碼漂移 (「通用密碼」和 NDS 密碼不同步)。

例如，若要確保支援「通用密碼」，請確定使用者升級至 Novell Client，而且 Help Desk 使用者僅與最新的 Novell Client 或 NetWare 版次搭配使用 ConsoleOne。

特性 ***5-5*** 使用 *NMAS* 同步化密碼



Identity Manager 和 NMAS

Identity Manager 會控制「進入點」(直接更新「通用密碼」或「配送密碼」)。NMAS 控制 Identity Vault 中同步化密碼的流程。

在案例 1 中，Identity Manager Driver for eDirectory 可用於直接更新 NDS 密碼。此案例基本上與 DirXML 1.*x* 中提供的案例相同。

在 案例 2、案例 3 和案例 4 中，Identity Manager 用於更新 「通用密碼」或 「配送密碼」。Identity Manager 會透過 NMAS 執行密碼變更。如此一來，NMAS 便可以更新 NMAS 密碼規則設定所決定的其他 Identity Vault 密碼，也可以強制執行 NMAS 密碼規則的 「進階密碼規則」，讓密碼和已連接系統同步化。在這些案例中，Identity Manager 配送至已連接系統的密碼一律爲 「配送密碼」。

案例 2、案例 3 與案例 4 之間的差異在於，每個已連接系統驅動程式之 NMAS 密碼規則設定和 「Identity Manager 密碼同步化」設定的組合不同。

5.8.2 案例 1：使用 NDS 密碼將兩個 Identity Vault 同步化

如同 「密碼同步化 1.0」，您可以使用 eDirectory 驅動程式，將兩個 Identity Vault 之間的「NDS 密碼」同步化。此案例不需要實作 「通用密碼」，且可以與 eDirectory 8.6.2 或更新版本搭配使用。用於此類密碼同步化的另一個名稱，正在同步化公用 / 私密金鑰配對。

此方法只能用來將 Identity Vault 之間的密碼同步化。由於不是使用 NMAS，因此，無法用來將密碼同步化至已連接的應用程式。

- 「案例 1 的優點和缺點」，第 102 頁
- 「設定案例 1」，第 102 頁
- 「疑難排解案例 1」，第 103 頁

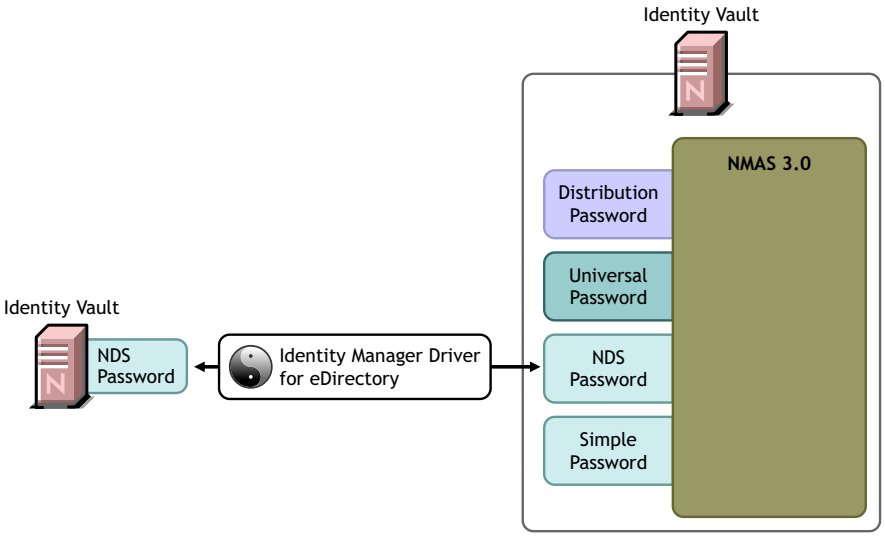
案例 1 的優點和缺點

表格 ***5-11*** 優點：使用 *NDS* 密碼在 *eDirectory* 之間進行密碼同步化

優點	缺點
簡易組態。只包含驅動程式過濾器中的正確屬性。 如果是分階段部署 Identity Manager 3 和 eDirectory 8.7.3，此方法可協助您逐步部署。 ◆ 您不需要將新密碼同步化規則新增至驅動程式組態。 ◆ 不需要在 Identity Vault 中執行「通用密碼」。 ◆ 可以與執行 eDirectory 8.6.2 或更新版本的已連接 Vault 搭配使用。 ◆ 不需要 NMAS 2.3。 強制執行您可以爲「NDS 密碼」設定的基本密碼限制。	此方法會將 Identity Vault 之間的密碼同步化。但無法將密碼同步化至其他已連接系統。 不更新「通用密碼」或「配送密碼」。 由於此方法不使用 NMAS，對於來自另一個 Identity Vault 的密碼，您無法根據密碼規則中的「進階密碼規則」來驗證密碼。 由於此方法不使用 NMAS，如果密碼與 NMAS 密碼規則不符，則無法重設已連接 Identity Vault 上的密碼。 密碼同步化失敗時，不提供電子郵件通知。 不支援 iManager 任務的「檢查密碼狀態」操作 (此功能需要「配送密碼」)。

下圖顯示可使用 Identity Manager Driver for eDirectory，將兩個 Identity Vault 之間的 NDS 密碼同步化 (如同 DirXML 1.*x*)。此案例不需要透過 NMAS。

特性 ***5-6*** 使用 *NDS* 密碼將兩個 *Identity Vault* 同步化



設定案例 1

若要設定此類密碼同步化，請設定驅動程式的組態。

通用密碼部署

不需要。

密碼規則組態

無。

密碼同步化設定

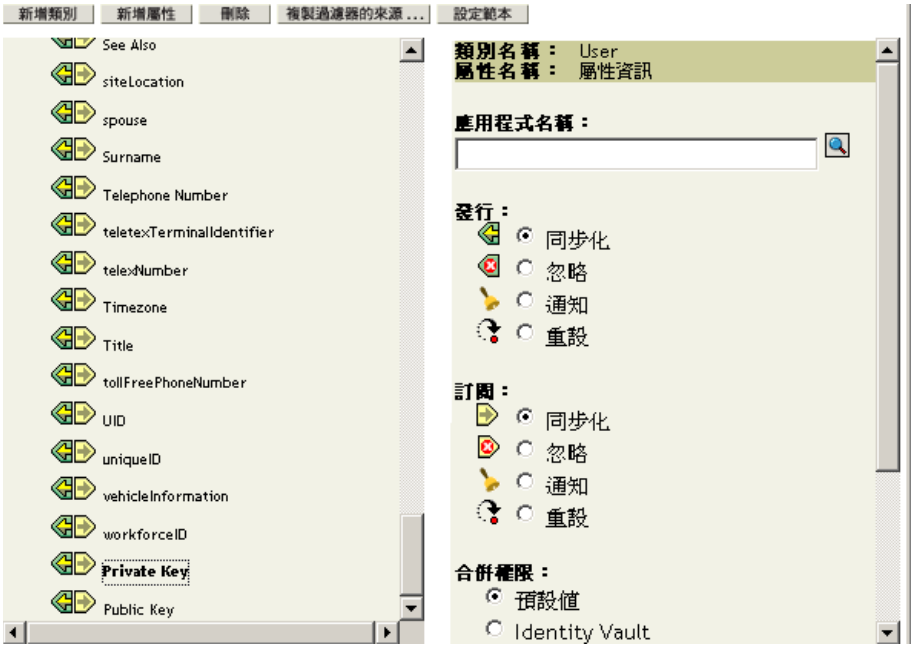
無。「密碼同步化」頁面上驅動程式的設定，對於這個同步化「NDS 密碼」的方法沒有任何影響。

驅動程式組態

移除「驅動程式組態中所需的規則」，第 84 頁中列出的「密碼同步化」規則。那些規則將支援「通用密碼」和「配送密碼」。使用「公用金鑰」及「私密金鑰」屬性 (而不是這些規則) 同步化「NDS 密碼」。

請確定兩個 Identity Vault 驅動程式的驅動程式過濾器，正在爲應同步化密碼的所有物件類別同步化「公用金鑰」和「私密金鑰」屬性。範例如下圖所示。

特性 ***5-7*** 同步化私密和公用金鑰屬性



疑難排解案例 **1**

- 開啓 DSTrace 選項。
- 檢查驅動程式「過濾器」，以確定「公用金鑰」和「私密金鑰」屬性正在同步化，而非被忽略。
- 另請參閱「疑難排解密碼同步化」，第 143 頁中的祕訣。

5.8.3 案例 2：使用通用密碼同步化

有了 Identity Manager，就可以將已連接系統密碼與 Identity Vault 中的「通用密碼」同步化。

更新「通用密碼」時，可以視您在 NMAS 密碼規則中的設定，同時更新「NDS 密碼」、「配送密碼」或「簡易密碼」。

雖然不是所有已連接系統都能提供使用者的實際密碼，但是任何已連接系統都可以將密碼發行至 Identity Manager。例如，Active Directory 可以將使用者的實際密碼發行至 Identity Manager。雖然 PeopleSoft 不會從 PeopleSoft 系統自行提供密碼，但是它可以提供驅動程式組態之規則中建立的啓始密碼，例如以使用者的員工 ID 或姓氏爲主的密碼。不是所有驅動程式都可以訂閱 Identity Manager 的密碼變更。請參閱「已連接系統支援密碼同步化」，第 78 頁。

- 「案例 2 的優點和缺點」，第 104 頁
- 「設定案例 2」，第 105 頁
- 「疑難排解案例 2」，第 109 頁

案例 2 的優點和缺點

表格 *5-12* 優點：使用通用密碼同步化

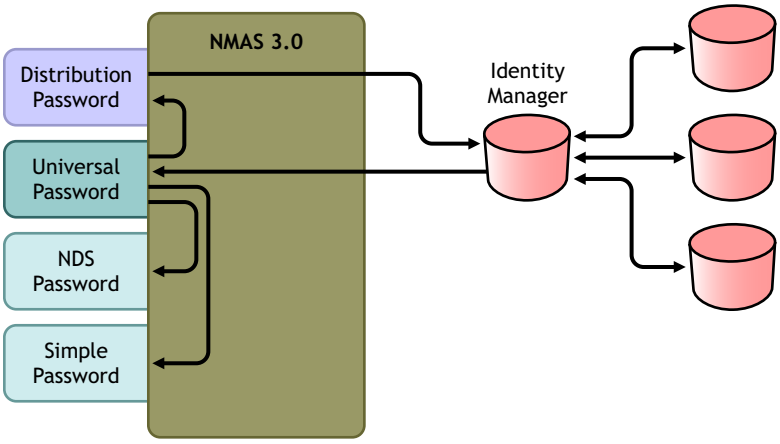
優點	缺點
允許將 Identity Vault 與已連接系統之間的密碼同步化。 允許根據 NMAS 密碼規則驗證密碼。 允許以電子郵件通知密碼操作失敗，例如已連接系統的密碼與「密碼」不一致時。 如果「通用密碼」與「配送密碼」在進行同步化，而且已連接系統支援檢查密碼，則會支援 iManager 中的「檢查密碼狀態」任務。 如果啓用規則 (Rule)，則 NMAS 會強制執行密碼規則 (Policy) 中的「進階密碼規則」。如果已連接系統的密碼不符合規則，則會產生錯誤，而您若指定該選項，便會傳送電子郵件通知。 如果不想強制執行密碼規則，則可以取消選取 NMAS 密碼規則 (Policy) 中的「啓用進階密碼規則」。	根據您在密碼規則中的設定，「配送密碼」與「通用密碼」可能會不同。因此，在設計上，此方法不支援重設已連接系統中的密碼。

本案例中的圖表說明下列流程：

1. 密碼透過 Identity Manager 引入。
2. Identity Manager 透過 NMAS 直接更新「通用密碼」。
3. NMAS 根據 NMAS 密碼規則設定，將「通用密碼」與「配送密碼」及其他密碼同步化。
4. Identity Manager 取回「配送密碼」，配送至設定爲接受密碼的已連接系統。

雖然此圖中顯示有多個已連接系統連接至 Identity Manager，但是請記住，要針對每個已連接系統驅動程式分別建立設定值。

特性 ***5-8*** 使用通用密碼同步化密碼



設定案例 **2**

若要設定此類的密碼同步化，請執行下列動作：

- 「通用密碼部署」，第 105 頁
- 「密碼規則組態」，第 105 頁
- 「密碼同步化設定」，第 107 頁
- 「驅動程式組態」，第 108 頁

通用密碼部署

確定您的環境已可以使用 「通用密碼」。請參閱 「準備使用 Identity Manager 密碼同步化和通用密碼」，第 87 頁。

密碼規則組態

確定已將 NMAS 密碼規則指定到要進行此類密碼同步化之部份的 Identity Vault。

1. 在 iManager 中，選取 「密碼」 > 「密碼規則」。
2. 選取規則，然後按一下 「編輯」。

3 瀏覽並選取要進行密碼同步化的物件。

您可以將規則指定給整個網路樹結構 (藉由瀏覽並選取 「安全性」容器中的 「登入規則」物件)、分割區根容器、容器或特定的使用者。爲了簡化管理，建議您將密碼規則儘量指定至網路樹中的高層級。

4 在密碼規則中，確定已選取下列選項：

- 啓用通用密碼

- 設定「通用密碼」時同步化 *NDS* 密碼
- 設定「通用密碼」時同步化配送密碼

  因爲 Identity Manager 會取回「配送密碼」以將密碼配送至已連接系統，所以請務必勾選此選項，以允許雙向密碼同步化。

5 視需要完成密碼規則。

如果已啓用規則 (Rule)，則 NMAS 會強制執行密碼規則 (Policy) 中的「進階密碼規則」。如果不強制執行密碼規則，則取消選取「啓用進階密碼規則」。

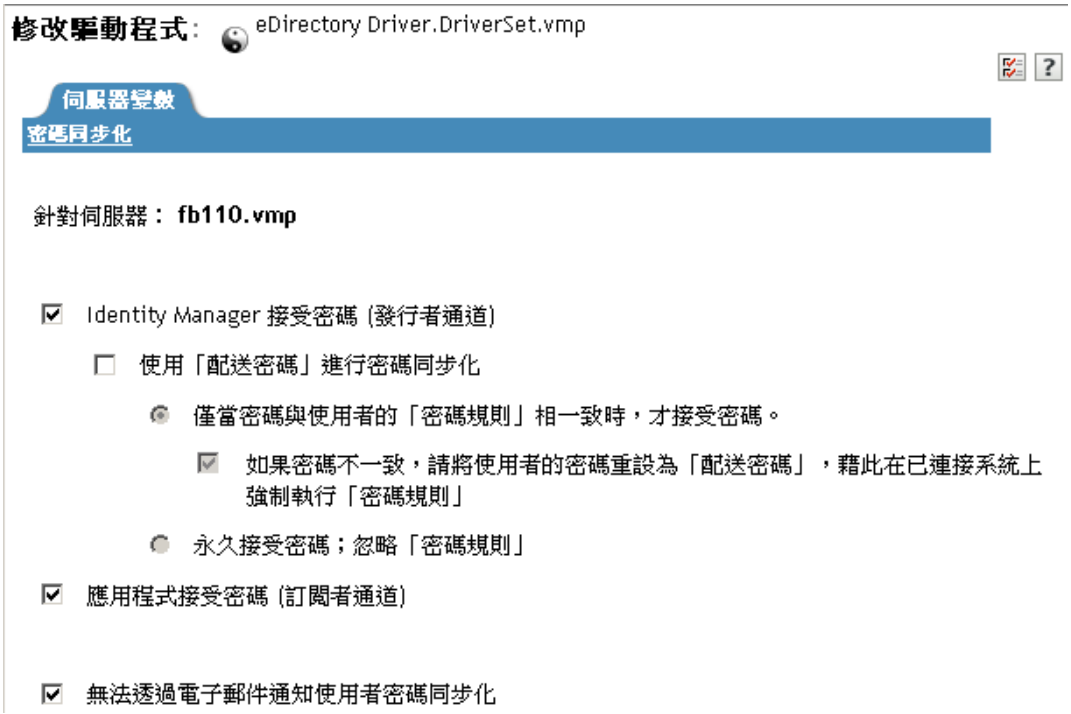
如果您正在使用「進階密碼規則」，請確定這些規則 (Rule) 不會與正在訂閱密碼之任何已連接系統上的密碼規則 (Policy) 產生衝突。

密碼同步化設定

1 在 iManager 中，選取「密碼」>「密碼同步化」。

2 搜尋已連接系統的驅動程式，然後選取驅動程式。

3 建立已連接系統驅動程式的設定。



確定已選取下列選項：

- *Identity Manager* 接受密碼 *(* 發行者通道 *)*。

  如果驅動程式資訊清單不包含「密碼發行」功能，則頁面上會顯示訊息。這是要通知使用者，密碼無法從應用程式中取回，只能藉由使用規則在驅動程式組態中建立密碼來發行密碼。

- 應用程式接受密碼 *(* 訂閱者通道 *)*

  如果已連接系統不支援接受密碼，則選項會變成灰色。

如果已連接系統提供支援，則這些設定允許雙向的密碼同步化。

您可以調整設定，以符合密碼授權來源的業務規則。例如，如果已連接系統應訂閱密碼，而非發行密碼，則僅選取「應用程式接受密碼 *(* 訂閱者通道 *)*」。

4 確定沒有選取「使用配送密碼進行密碼同步化」：

在此案例中，Identity Manager 會直接更新「通用密碼」。「配送密碼」仍然用於將密碼配送至已連接系統，但是其會由 NMAS 而非 Identity Manager 從「通用密碼」進行更新。

5 (選擇性) 如有必要，選取下列選項：

- 透過電子郵件通知使用者密碼同步化失敗

  請記住，電子郵件通知需要填入 eDirectory「使用者」物件的 Internet EMail Address 屬性。

  電子郵件通知爲非侵入式，不會影響觸發電子郵件的 XML 文件處理。如果失敗，將不再重試，除非操作本身重試。然而，電子郵件通知的除錯訊息會寫入追蹤檔案。

驅動程式組態

1 確定應該參與密碼同步化之每個驅動程式的驅動程式組態，都包含必要的 Identity Manager 程序檔密碼同步化規則。

在驅動程式組態中，規則必須在正確的位置及正確的順序。如需規則的清單，請參閱「驅動程式組態中所需的規則」，第 84 頁。

Identity Manager 範例組態已包含規則。如果您在升級現有的驅動程式，請利用「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁中的指示新增規則。

2 針對 nspmDistributionPassword 屬性正確設定過濾器：

- 若爲「發行者」通道，針對所有物件類別，將驅動程式過濾器的 nspmDistributionPassword 屬性設爲「忽略」。
- 若爲「訂閱者」通道，針對應訂閱密碼變更的所有物件類別，將驅動程式過濾器的 nspmDistributionPassword 屬性設爲「通知」。

3 針對將 nspmDistributionPassword 屬性設爲 「通知」的所有物件，請將 「公用金鑰」和 「私密金鑰」屬性同時設爲 「忽略」。

4 爲了確保密碼安全性，請確定您可以控制誰能擁有 Identity Manager 物件權限。

疑難排解案例 2

- 「案例 2 的流程圖」，第 109 頁
- 「登入 Identity Vault 時出現問題」，第 111 頁
- 「登入訂閱密碼的另一個已連接系統時出現問題」，第 111 頁
- 「密碼失敗時未產生電子郵件」，第 112 頁
- 「使用檢查物件密碼時發生錯誤」，第 112 頁
- 「實用的 DSTrace 指令」，第 112 頁

另請參閱 「疑難排解密碼同步化」，第 143 頁中的祕訣。

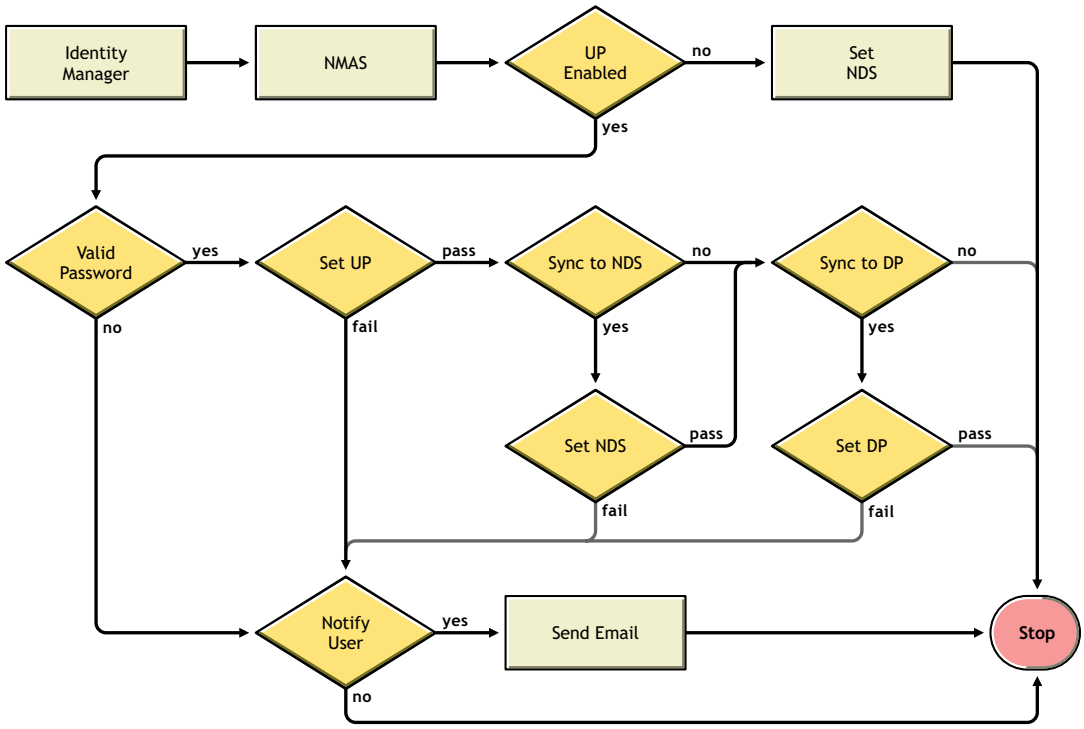
案例 2 的流程圖

下列流程圖說明 NMAS 如何處理從 Identity Manager 接收的密碼。此案例中會將密碼同步化到 「通用密碼」。NMAS 會決定如何根據下列情況處理密碼：

- NMAS 密碼規則中是否啓用 「通用密碼」。

- 內送密碼必須符合的「進階密碼規則」是否已啓用。
- 密碼規則中將「通用密碼」與其他密碼同步化的其他設定爲何。

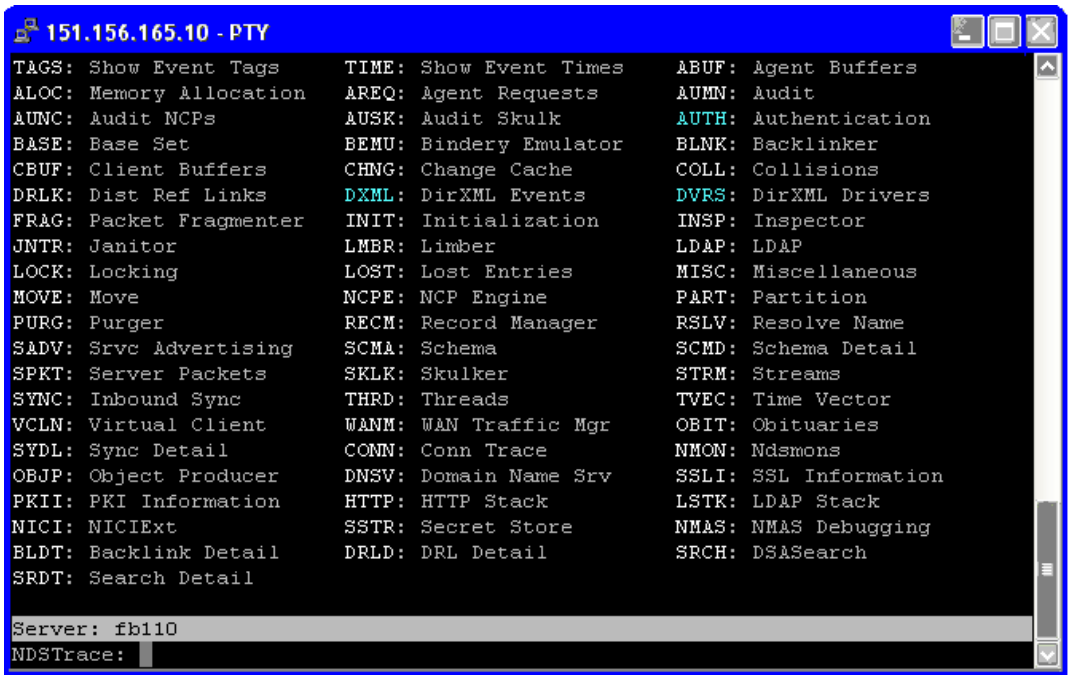
特性 **5-9** *NMAS* 如何處理從 *Identity Manager* 接收的密碼



登入 Identity Vault 時出現問題

- 開啓 DSTrace 中的 *+AUTH*、*+DXML* 和 *+DVRS* 設定。

特性 ***5-10*** *DSTrace* 指令



- 驗證 <password> 或 <modify-password> 元素是否正傳遞至 Identity Manager。若要驗證是否正在傳遞，請監視已開啓上述選項的追蹤畫面。
- 根據密碼規則驗證密碼是否有效。
- 檢查 NMAS 密碼規則組態和指定。嘗試將規則直接指定給使用者，以確定使用的是正確的規則。
- 在驅動程式的「密碼同步化」頁面上，確定已選取「*DirXML* 接受密碼」。
- 在密碼規則中，確定已選取「設定通用密碼時同步化配送密碼」。

登入訂閱密碼的另一個已連接系統時出現問題

本節內容主要用在解決已連接系統將密碼發行至 Identity Manager 的相關問題，但訂閱密碼的另一個已連接系統並未從這個系統接收到變更的情況。此關係的另一個名稱是次要已連接系統，表示它會透過 Identity Manager 從第一個已連接系統接收密碼。

- 開啓 DSTrace 中的 *+DXML* 和 *+DVRS* 設定，查看 Identity Manager 規則處理。
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。
- 確定已選取「密碼同步化」的「*Identity Manager* 接受密碼」選項。
- 檢查驅動程式過濾器，確定已依步驟 2, 第 108 頁中的說明，正確設定 nspmDistributionPassword 屬性。
- 驗證「新增」的 *<password>* 或 <modify-password> 元素是否正傳送至已連接系統。若要驗證，請監視開啓追蹤選項的 DSTrace 螢幕或檔案，如第一個項目所述。

- 驗證驅動程式組態是否將 Identity Manager 程序檔密碼規則包含在正確的位置及正確的順序，如 「驅動程式組態中所需的規則」，第 84 頁中所述。
- 比較 Identity Vault 中的 NMAS 密碼規則與已連接系統強制執行的任何密碼規則，以確定它們是相容的。

密碼失敗時未產生電子郵件

- 開啓 DSTrace 中的 *+DXML* 設定，查看 Identity Manager 規則處理。
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。
- 驗證是否已選取產生電子郵件的規則。
- 驗證 Identity Vault 物件的 Internet EMail Address 屬性中是否包含正確的使用者電子郵件地址。
- 在「通知組態」任務中，確定已正確設定 SMTP 伺服器和電子郵件範本的組態。請參閱 「設定電子郵件通知的組態」，第 132 頁。

使用檢查物件密碼時發生錯誤

iManager 中的「檢查密碼狀態」任務，會使驅動程式檢查物件密碼動作。如果有問題，請檢視下列各項：

- 如果「檢查物件密碼」傳回 -603，則 Identity Vault 物件不包含 nspmDistributionPassword 屬性。檢查驅動程式過濾器的 nspmDistributionPassword 屬性設定是否正確。同時，確定密碼規則已選取「設定通用密碼時同步化配送密碼」。
- 如果「檢查物件密碼」傳回「未同步化」，請驗證驅動程式組態是否包含適當的「密碼同步化」規則。
- 比較 Identity Vault 中的 NMAS 密碼規則與已連接系統強制執行的任何密碼規則，以確定它們是相容的。
- 「檢查物件密碼」的操作是從「配送密碼」執行的。如果「配送密碼」不在更新中，則「檢查物件密碼」可能不會回報密碼已同步化。
- 請記住，「檢查密碼狀態」會檢查「NDS 密碼」而不是「配送密碼」，而這僅限 Identity Manager 驅動程式。

實用的 DSTrace 指令

+DXML：檢視 Identity Manager 規則處理和潛在錯誤訊息

+DVRS：檢視 Identity Manager 驅動程式訊息

+AUTH：檢視 NDS 密碼修改

5.8.4 案例 3：Identity Manager 更新配送密碼後，將 Identity Vault 與已連接系統同步化

在此案例中，Identity Manager 會直接更新「配送密碼」，且可讓 NMAS 決定如何同步化其他 Identity Vault 密碼。

雖然不是所有的已連接系統都能提供使用者的實際密碼，但是任何已連接系統都可以將密碼發行至 Identity Manager。例如，Active Directory 可以將使用者的實際密碼發行至 Identity Manager。雖然 PeopleSoft 不會從 PeopleSoft 系統自行提供密碼，但是它可以提供驅動程式組態之規則中建立的啓始密碼，例如以使用者的員工 ID 或姓氏爲主的密碼。不是所有驅動

程式都可以訂閱 Identity Manager 的密碼變更。請參閱 「已連接系統支援密碼同步化」，第 78 頁。

- 「案例 3 的優點和缺點」，第 113 頁
- 「設定案例 3」，第 114 頁
- 「疑難排解案例 3」，第 117 頁

案例 3 的優點和缺點

表格 ***5-13*** 優點：藉由更新配送密碼將 *Identity Vault* 與已連接系統同步化

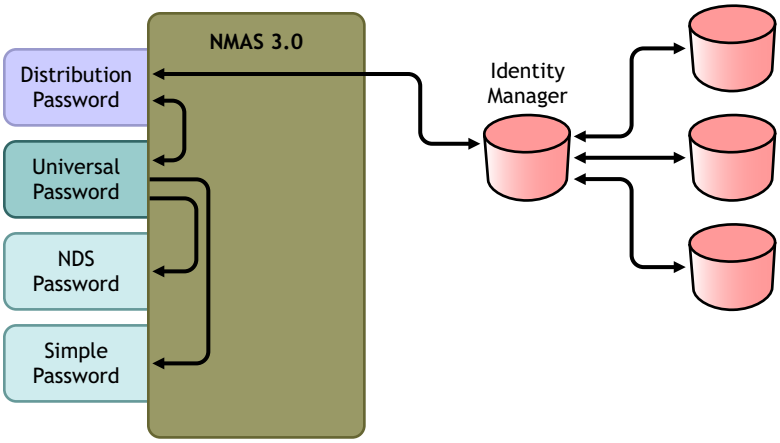
優點	缺點
允許將 Identity Manager 與已連接系統之間的密碼同步化。 讓您選擇是否要強制執行來自已連接系統之密碼的密碼規則。 如果密碼同步化失敗，您可以指定傳送通知。 如果強制執行密碼規則，當密碼不符合規則時，可以選擇將已連接系統上的密碼重設爲「配送密碼」。	

本案例中的圖表說明下列流程：

1. 密碼透過 Identity Manager 引入。
2. Identity Manager 會透過 NMAS 以直接更新「配送密碼」
3. Identity Manager 也會使用「配送密碼」，配送至您指定應該接受密碼的已連接系統
4. NMAS 會根據密碼規則設定，將「通用密碼」與「配送密碼」及其他密碼同步化。

雖然在此圖中多個已連接系統顯示爲連接至 Identity Manager，但是請務必針對每個已連接系統驅動程式個別建立設定值。

特性 ***5-11*** 藉由更新配送密碼將 *Identity Vault* 與已連接系統同步化



設定案例 **3**

設定此類密碼同步化：

- 「通用密碼部署」，第 114 頁
- 「密碼規則組態」，第 114 頁
- 「密碼同步化設定」，第 115 頁
- 「驅動程式組態」，第 116 頁

通用密碼部署

確定您的環境已可以使用 「通用密碼」。請參閱 「準備使用 Identity Manager 密碼同步化和通用密碼」，第 87 頁。

密碼規則組態

1. 在 iManager 中，選取 「密碼」 > 「密碼規則」。
2. 確定已將密碼規則指定到要進行此類密碼同步化之部份的 Identity Vault 網路樹。您可以將其指定到整個樹狀結構、分割區根容器、容器或特定使用者。爲了簡化管理，建議您將密碼規則儘量指定至網路樹中的高層級。
3. 在密碼規則中，確定已選取下列選項：

   - 啓用通用密碼
   - 設定 「通用密碼」時同步化 *NDS* 密碼
   - 設定 「通用密碼」時同步化配送密碼

     由於 Identity Manager 會取回 「配送密碼」以將密碼配送至已連接系統，所以一定要選取此選項，才能進行雙向的密碼同步化。

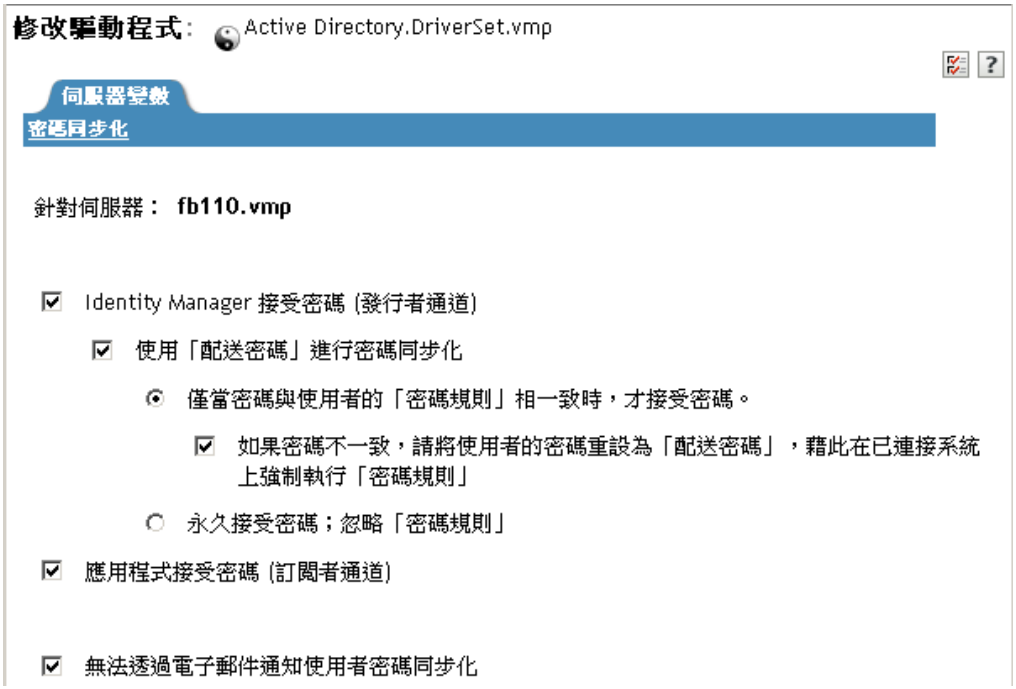
4 如果您使用「進階密碼規則」，請確定這些規則不會與正在訂閱密碼之任何已連接系統上的密碼規則產生衝突。

密碼同步化設定

1 在 iManager 中，選取「密碼」>「密碼同步化」。

2 搜尋已連接系統的驅動程式，然後選取驅動程式。

3 建立已連接系統驅動程式的設定值。



確定已選取下列選項：

- *Identity Manager* 接受密碼 *(* 發行者通道 *)*
- 使用「配送密碼」進行密碼同步化

  如果驅動程式資訊清單不包含「密碼發行」功能，則頁面上會顯示訊息。這是要通知使用者，密碼無法從應用程式中取回，只能藉由使用規則在驅動程式組態中建立密碼來發行密碼。
- 應用程式接受密碼 *(* 訂閱者通道 *)*

如果已連接系統有提供支援，則這些設定允許雙向的密碼同步化。

您可以調整設定，以符合密碼授權來源的業務規則。例如，如果已連接系統應訂閱密碼，而非發行密碼，則僅選取「應用程式接受密碼 *(* 訂閱者通道 *)*」。

4 使用「使用配送密碼進行密碼同步化」下面的選項，指定要強制執行還是忽略 NMAS 密碼規則。

5 (條件式) 如果您已指定要強制執行密碼規則，也請指定如果密碼不符合規則時，是否要讓 Identity Manager 重設已連接系統密碼。

6 (選擇性) 如有必要，請選取下列選項：

- 透過電子郵件通知使用者密碼同步化失敗

請記住，電子郵件通知需要填入 eDirectory 使用者物件的 Internet EMail Address 屬性。

電子郵件通知爲非侵入式，不會影響觸發電子郵件的 XML 文件處理。如果失敗，將不再重試，除非操作本身重試。然而，電子郵件通知的除錯訊息會寫入追蹤檔案。

驅動程式組態

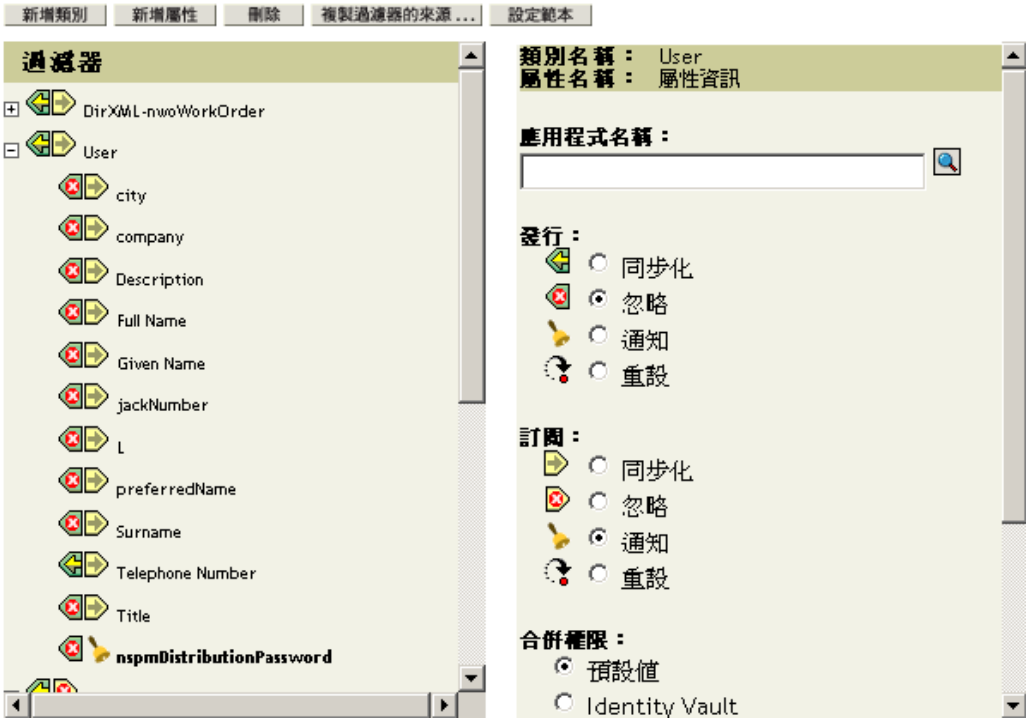
1 確定應該參與密碼同步化之每個驅動程式的驅動程式組態，都包含必要的 Identity Manager 程序檔密碼同步化規則。

在驅動程式組態中，規則必須在正確的位置及正確的順序。如需規則的清單，請參閱「驅動程式組態中所需的規則」，第 84 頁。

Identity Manager 範例組態已包含規則。如果您升級現有的驅動程式，請利用「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁的指示新增規則。

2 針對 nspmDistributionPassword 屬性正確設定過濾器：

- 若爲「發行者」通道，針對所有物件類別，將驅動程式過濾器的 nspmDistributionPassword 屬性設爲「忽略」。
- 若爲「訂閱者」通道，針對應該訂閱密碼變更的所有物件類別，將驅動程式過濾器的 nspmDistributionPassword 屬性設爲「通知」。



3 針對將 nspmDistributionPassword 屬性設爲 「通知」的所有物件，將驅動程式過濾器中的 「公用金鑰」和 「私密金鑰」屬性同時設爲 「忽略」。

4 爲了確保密碼安全性，請確定您可以控制誰能擁有 Identity Manager 物件權限。

疑難排解案例 **3**

- 「案例 3 的流程圖」，第 117 頁
- 「登入 eDirectory 時出現問題」，第 119 頁
- 「登入訂閱密碼的其他已連接系統時出現問題」，第 120 頁
- 「密碼失敗時未產生電子郵件」，第 120 頁
- 「使用檢查密碼狀態時發生錯誤」，第 120 頁
- 「實用的 DSTrace 指令」，第 121 頁

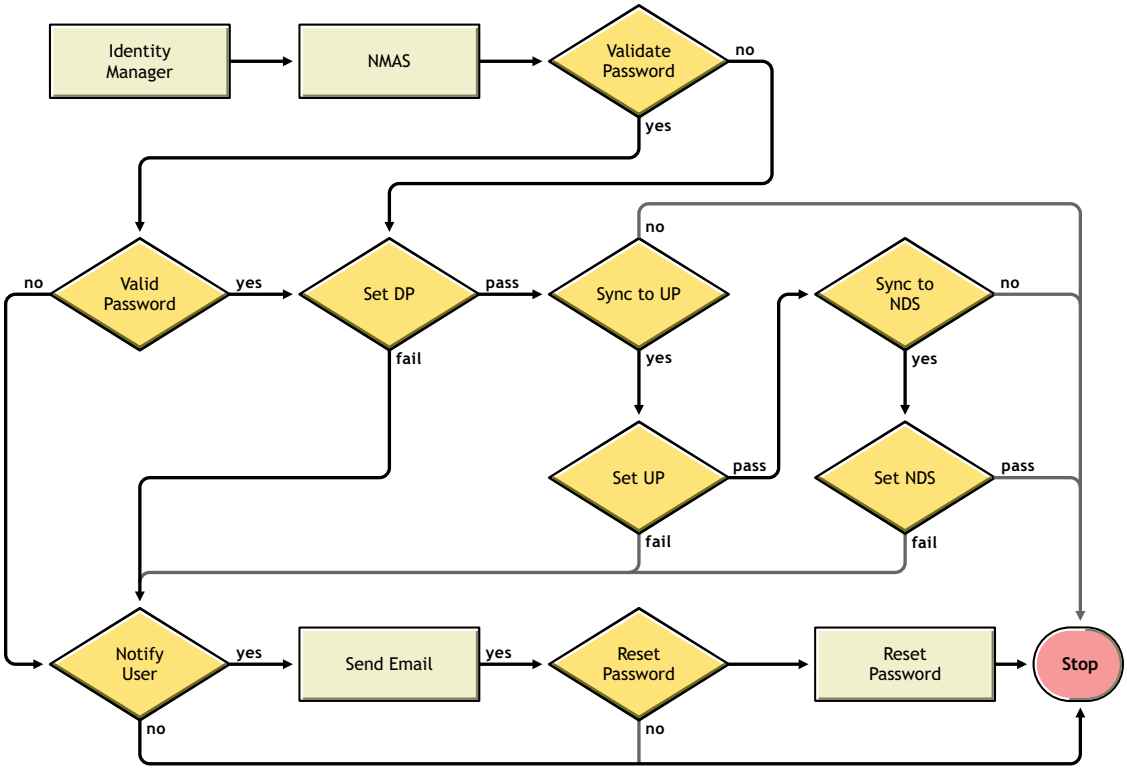
另請參閱 「疑難排解密碼同步化」，第 143 頁中的祕訣。

案例 3 的流程圖

下列流程圖說明 NMAS 如何處理從 Identity Manager 接收的密碼。在此案例中，密碼會同步化到 「通用密碼」，且 NMAS 會決定下列內容：

- 根據是否已指定應該依密碼規則驗證內送密碼，決定該如何處理密碼 (如果已啓用 「通用密碼」和 「進階密碼規則」)。
- 密碼規則中將 「通用密碼」與其他密碼同步化的其他設定爲何。

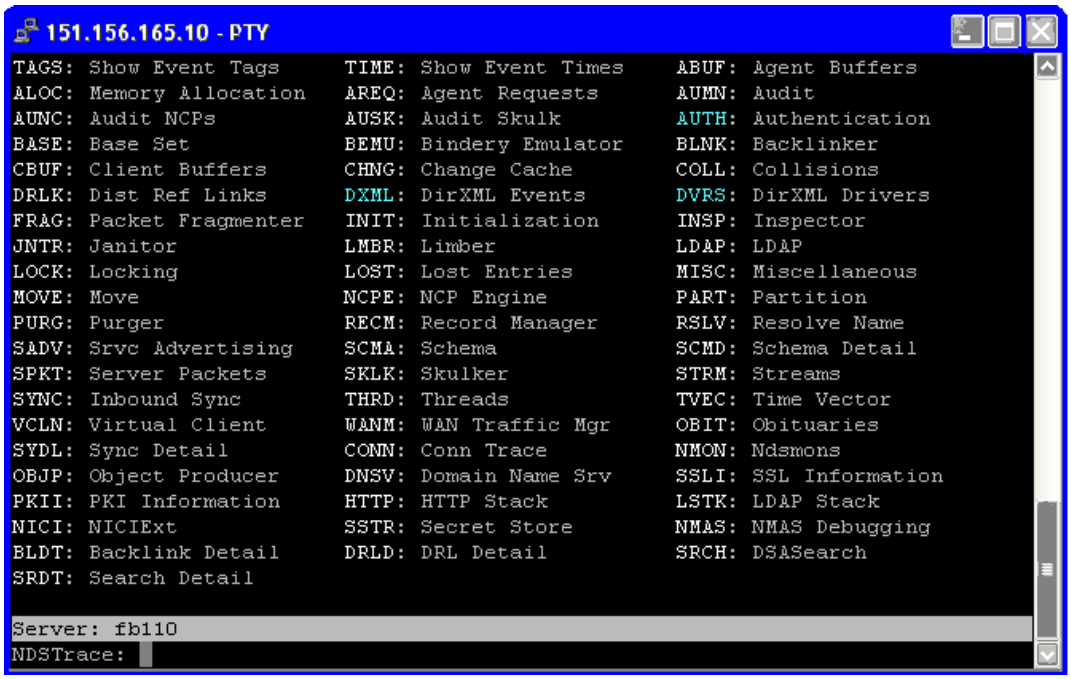
特性 ***5-12*** 將 *Identity Manager* 的密碼同步化到配送密碼



登入 eDirectory 時出現問題

- 開啓 DSTrace 中的 *+AUTH*、*+DXML* 和 *+DVRS* 設定

特性 ***5-13*** *DSTrace* 指令



- 驗證 <password> 或 <modify-password> 元素是否正傳遞至 Identity Manager。若要驗證，請監視已開啓追蹤選項的 DSTtrace 螢幕或檔案，如第一個項目所述。
- 根據 NMAS 密碼規則，驗證密碼是否有效。
- 檢查 NMAS 密碼規則組態和指定。嘗試將規則直接指定給使用者，以確定使用的是正確的規則。
- 在驅動程式的「密碼同步化」頁面上，確定已選取「*Identity Manager* 接受密碼 *(* 發行者通道 *)*」。
- 在 NMAS 密碼規則中，確定已選取「設定通用密碼時同步化配送密碼」。
- 在 NMAS 密碼規則中，確定已選取「設定通用密碼時同步化 *NDS* 密碼」(視需要而定)。
- 如果使用者透過 Novell Client 或 ConsoleOne 登入，請檢查其版本。如果未將「通用密碼」與「NDS 密碼」同步化，則舊的 Novell Client 和 ConsoleOne 可能無法登入 Identity Vault。

  現在 Novell Client 和 ConsoleOne 已有可辨識「通用密碼」的新版本。請參閱《*Novell* 模組化驗證服務 *(NMAS) 3.0* 管理指南 (http://www.novell.com/documentation/nmas30/index.html)》。
- 如果未將「通用密碼」與「NDS 密碼」同步化，則使用「NDS 密碼」進行驗證的部份舊公用程式同樣無法登入 Identity Vault。如果您不想要將「NDS 密碼」用於多數使用者，但是管理員或 Help Desk 使用者需要使用舊公用程式進行驗證時，請嘗試針對 Help Desk 使用者使用不同的密碼規則，如此便可以爲它們指定不同的「通用密碼」同步化選項。

登入訂閱密碼的其他已連接系統時出現問題

本節內容主要用在解決已連接系統將密碼發行至 Identity Manager 的相關問題，但是訂閱密碼的另一個已連接系統並未從這個系統接收到變更的情況。此關係的另一個名稱是次要已連接系統，表示它會透過 Identity Manager 從第一個已連接系統接收密碼。

- 開啓 DSTrace 中的 *+DXML* 和 *+DVRS* 設定，查看 Identity Manager 規則處理和潛在錯誤
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。
- 確定已選取「密碼同步化」頁面中的「*Identity Manager* 接受密碼 *(* 發行者通道 *)*」選項。
- 在密碼規則中，確定未選取「設定通用密碼時同步化配送密碼」。

  Identity Manager 會使用「配送密碼」，將密碼同步化到已連接系統。針對此同步化方法，「通用密碼」必須與「配送密碼」同步化。
- 檢查驅動程式過濾器的 nspmDistributionPassword 屬性。
- 驗證「新增」的 <password> 元素或 <modify-password> 元素是否已轉換成 nspmDistributionPassword 的「新增」和「修改」屬性操作。若要驗證，請監視已開啓追蹤選項的 DSTtrace 螢幕或檔案，如第一個項目所述。
- 驗證驅動程式組態是否將 Identity Manager 程序檔密碼規則包含在正確的位置及正確的順序，如「驅動程式組態中所需的規則」，第 84 頁中所述。
- 比較 Identity Vault 中的密碼規則與已連接系統強制執行的所有密碼規則，以確定它們是相容的。

密碼失敗時未產生電子郵件

- 開啓 DSTrace 中的 *+DXML* 設定，查看 Identity Manager 規則處理
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。
- 驗證是否已選取產生電子郵件的規則。
- 驗證 Identity Vault 物件的 Internet EMail Address 屬性中是否包含正確的值。
- 在「通知組態」任務中，確定已設定 SMTP 伺服器和電子郵件範本的組態。請參閱「設定電子郵件通知的組態」，第 132 頁。

電子郵件通知爲非侵入式，不會影響觸發電子郵件的 XML 文件處理。如果失敗，將不再重試，除非操作本身重試。電子郵件通知的除錯訊息會寫入追蹤檔案。

使用檢查密碼狀態時發生錯誤

iManager 中的「檢查密碼狀態」任務，會使驅動程式執行檢查物件密碼動作。

- 確定已連接系統支援檢查密碼。請參閱「已連接系統支援密碼同步化」，第 78 頁。

  如果驅動程式資訊清單未指出已連接系統支援密碼檢查功能，則無法透過 iManager 進行此操作。
- 如果「檢查物件密碼」傳回 -603，則 Identity Vault 物件不包含 nspmDistributionPassword 屬性。檢查驅動程式過濾器，以及密碼規則中的「將通用密碼同步化爲配送密碼」選項。
- 如果「檢查物件密碼」傳回「未同步化」，請驗證驅動程式組態包含適當的「Identity Manager 密碼同步化」規則。
- 比較 Identity Vault 中的密碼規則與已連接系統強制執行的任何密碼規則，以確定它們是相容的。

- 「檢查物件密碼」會檢查 「配送密碼」。如果 「配送密碼」不在更新中，則 「檢查物件密碼」可能不會回報密碼已同步化
- 請記住，對於 Identity Vault，「檢查密碼狀態」會檢查 「NDS 密碼」而不是 「通用密碼」。這表示，如果使用者的密碼規則未指定將 「NDS 密碼」與 「通用密碼」同步化，則密碼會一直被回告爲未同步化。事實上，「配送密碼」和已連接系統上的密碼可能已同步化，但 「檢查密碼狀態」不會是正確的，除非 「NDS 密碼」和 「配送密碼」都與 「通用密碼」同步化。

實用的 DSTrace 指令

+DXML：檢視 Identity Manager 規則處理和潛在錯誤訊息。

+DVRS：檢視 Identity Manager 驅動程式訊息

+AUTH：檢視 NDS 密碼修改

5.8.5 案例 4：Identity Manager 更新「配送密碼」後，會通道封裝 --- 同步化「已連接系統」，而不是 Identity Vault

Identity Manager 可讓您將已連接的系統之間的密碼同步化，同時使用不同的 Identity Vault 密碼。這就是所謂的 「通道封裝」。

在此案例中，Identity Manager 會直接更新 「配送密碼」。此案例與 「案例 3：Identity Manager 更新配送密碼後，將 Identity Vault 與已連接系統同步化」，第 112 頁幾乎是相同的。不同之處在於，要確定 「通用密碼」與 「配送密碼」之間未進行同步化。藉由不使用 NMAS 密碼規則，或使用密碼規則但停用 「設定通用密碼時同步化配送密碼」選項，即可執行此項操作。

- 「案例 4 的優點和缺點」，第 122 頁
- 「設定案例 4」，第 123 頁
- 「疑難排解案例 4」，第 124 頁

案例 4 的優點和缺點

表格 *5-14* 通道封裝的優點

優點	缺點
允許在同步化已連接系統之間的密碼時，同時使用不同的 Identity Vault 密碼。 不需要密碼規則。 如果使用密碼規則，則規則不需要啓用「通用密碼」。然而，環境必須支援「通用密碼」。 如果已連接系統提供支援，則會支援 iManager 中的「檢查密碼狀態」任務。 如果密碼同步化失敗，您可以指定傳送通知。 您可以重設與密碼規則不符的已連接系統密碼。 如果啓用「通用密碼」和「進階密碼規則」，當指定應該強制執行時，則會強制執行密碼規則，而且可以重設已連接系統的密碼。	如果未啓用「通用密碼」和「進階密碼規則」，則不會強制執行密碼規則，而且無法重設已連接系統的密碼。

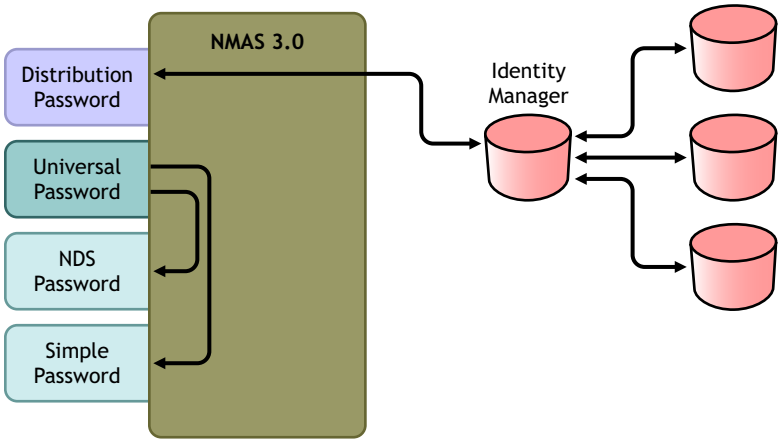
本案例中的圖表說明下列流程：

1. 密碼透過 Identity Manager 引入。
2. Identity Manager 會透過 NMAS 直接更新「配送密碼」。
3. Identity Manager 也會使用「配送密碼」，將密碼配送至您指定應該接受密碼的已連接系統。

此案例的關鍵是，在 NMAS 密碼規則中，「同步化通用密碼與配送密碼」已停用。由於「配送密碼」未與「通用密碼」同步化，所以 Identity Manager 會將已連接系統之間的密碼同步化，而不影響 Identity Vault 中的密碼。

雖然在此圖中多個已連接系統顯示爲連接至 Identity Manager，但是請務必針對每個已連接系統驅動程式個別建立設定值。

特性 *5-14* *Identity Manager* 更新配送密碼後通道封裝



設定案例 **4**

若要設定此類密碼同步化，請設定下列項目的組態：

- 「通用密碼部署」，第 123 頁
- 「密碼規則組態」，第 123 頁
- 「密碼同步化設定」，第 124 頁
- 「驅動程式組態」，第 124 頁

通用密碼部署

雖然您不需要有啓用 「通用密碼」的密碼規則，但是環境仍然必須使用支援 「通用密碼」的 eDirectory 8.7.3。請參閱 「準備使用 Identity Manager 密碼同步化和通用密碼」，第 87 頁。

密碼規則組態

針對此方法，Identity Vault 使用者不需要任何密碼規則。

然而，如果您使用密碼規則，則必須執行下列動作：

1 確定未選取下列選項：

- 設定 「通用密碼」時同步化配送密碼

  這是通道封裝密碼而不影響 Identity Vault 密碼的關鍵。不將 「通用密碼」與 「配送密碼」同步化，會使 「配送密碼」區分開來，僅讓 Identity Manager 用在已連接系統上。Identity Manager 的作用如同管道，在其他已連接系統之間配送密碼，而不會影響 Identity Vault 密碼。

2 視需要完成其他密碼規則設定。

  密碼規則中的其他密碼設定是選擇性的。

密碼同步化設定

使用與「案例 3：Identity Manager 更新配送密碼後，將 Identity Vault 與已連接系統同步化」，第 112 頁中密碼同步化設定相同的設定。

驅動程式組態

使用與「案例 3：Identity Manager 更新配送密碼後，將 Identity Vault 與已連接系統同步化」，第 112 頁中驅動程式組態相同的設定。

疑難排解案例 4

如果針對通道封裝設定密碼同步化，則「配送密碼」會與「通用密碼」和「NDS 密碼」不同。

- 「登入訂閱密碼的另一個已連接系統時出現問題」，第 124 頁
- 「密碼失敗時未產生電子郵件」，第 124 頁
- 「使用檢查密碼狀態時發生錯誤」，第 125 頁
- 「實用的 DSTrace 指令」，第 125 頁

另請參閱「疑難排解密碼同步化」，第 143 頁中的祕訣。

登入訂閱密碼的另一個已連接系統時出現問題

本節內容主要用在解決已連接系統將密碼發行至 Identity Manager 的相關問題，但是訂閱密碼的另一個已連接系統並未從這個系統接收到變更的情況。此關係的另一個名稱是次要已連接系統，表示它會透過 Identity Manager 從第一個已連接系統接收密碼。

- 開啓 DSTrace 中的 *+DXML* 和 *+DVRS* 設定，查看 Identity Manager 規則處理和潛在錯誤。
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。
- 確定已選取「密碼同步化」頁面上的「*Identity Manager* 接受密碼 *(* 發行者通道 *)*」選項。
- 在密碼規則中，確定未選取「設定通用密碼時同步化配送密碼」。

  Identity Manager 會使用「配送密碼」，將密碼同步化到已連接系統。針對此同步化方法，「通用密碼」必須與「配送密碼」同步化。
- 確定驅動程式過濾器的 nspmDistributionPassword 屬性具有正確的設定。
- 驗證「新增」的 <password> 元素和 <modify-password> 元素是否已轉換成 nspmDistributionPassword 的「新增」和「修改」屬性操作。若要驗證，請監視已開啓追蹤選項的 DSTtrace 螢幕或檔案，如第一個項目所述。
- 驗證驅動程式組態是否將 Identity Manager 程序檔密碼規則包含在正確的位置及正確的順序，如「驅動程式組態中所需的規則」，第 84 頁中所述。
- 比較 Identity Vault 中的密碼規則與已連接系統強制執行的任何密碼規則，以確定它們是相容的。

密碼失敗時未產生電子郵件

- 開啓 DSTrace 中的 *+DXML* 設定，查看 Identity Manager 規則處理。
- 將驅動程式的 Identity Manager 追蹤層級設爲 *3*。

- 驗證是否已選取產生電子郵件的規則。
- 驗證 Identity Vault 物件的 Internet EMail Address 屬性中是否包含正確的值。
- 在「通知組態」任務中，檢查 SMTP 伺服器和電子郵件範本。請參閱「設定電子郵件通知的組態」，第 132 頁。

電子郵件通知爲非侵入式，不會影響觸發電子郵件的 XML 文件處理。如果失敗，將不再重試，除非操作本身重試。電子郵件通知的除錯訊息會寫入追蹤檔案。

使用檢查密碼狀態時發生錯誤

iManager 中的「檢查密碼狀態」任務，會使驅動程式執行「檢查物件密碼」動作。

- 確定已連接系統支援檢查密碼。請參閱「已連接系統支援密碼同步化」，第 78 頁。

  如果驅動程式資訊清單未指出已連接系統支援密碼檢查功能，則無法透過 iManager 進行此操作。
- 如果「檢查物件密碼」動作傳回 -603，則 Identity Vault 物件不包含 nspmDistributionPassword 屬性。檢查 Identity Manager 屬性過濾器，以及密碼規則中的「將通用密碼同步化爲配送密碼」選項。
- 如果「檢查物件密碼」動作傳回「未同步化」，請驗證驅動程式組態是否包含適當的 Identity Manager 密碼同步化規則。
- 比較 Identity Vault 中的密碼規則與已連接系統強制執行的任何密碼規則，以確定它們是相容的。
- 「檢查物件密碼」動作會檢查「配送密碼」。如果「配送密碼」不在更新中，則「檢查物件密碼」可能不會回報化密碼已同步

實用的 DSTrace 指令

+DXML：檢視 Identity Manager 規則處理和潛在錯誤訊息。

+DVRS：檢視 Identity Manager 驅動程式訊息

+AUTH：檢視 NDS 密碼修改

+DCLN：檢視 NDS DCLient 訊息

5.8.6 案例 5：將應用程式密碼同步化到簡易密碼

此案例爲密碼同步化功能所專用。使用 Identity Manager 和 NMAS，即可從已連接系統取得密碼，並直接將它同步化到 Identity Vault「簡易密碼」。如果已連接系統僅提供雜湊密碼，則可以將它們同步化到「簡易密碼」，而無需回復雜湊。然後，其他應用程式可以透過 LDAP 或 Novell Client，使用相同的純文字或雜湊密碼向 Identity Vault 驗證，且已設定好 NMAS 元件的組態爲使用「簡易密碼」做爲登入方法。

如果已連接系統中的密碼是純文字格式，便可以從已連接系統發行到 Identity Vault「簡易密碼」儲存區中。

如果已連接系統僅提供雜湊密碼 (支援 MD5、SHA、SHA1 或 UNIX Crypt)，則您必須將它們發行至「簡易密碼」，並指出雜湊類型，例如 {MD5}。

如要另一個應用程式以相同密碼進行驗證，您需要自定其他應用程式，以使用 LDAP 取得使用者密碼並向「簡易密碼」驗證。

NMAS 會比較應用程式的密碼值和「簡易密碼」中的值。如果儲存在「簡易密碼」中的密碼是雜湊值，則 NMAS 會在比較之前，先使用應用程式密碼值來建立正確類型的雜湊值。如果應用程式的密碼和「簡易密碼」相同，則 NMAS 會驗證使用者。

在此案例中，「通用密碼」無法使用。

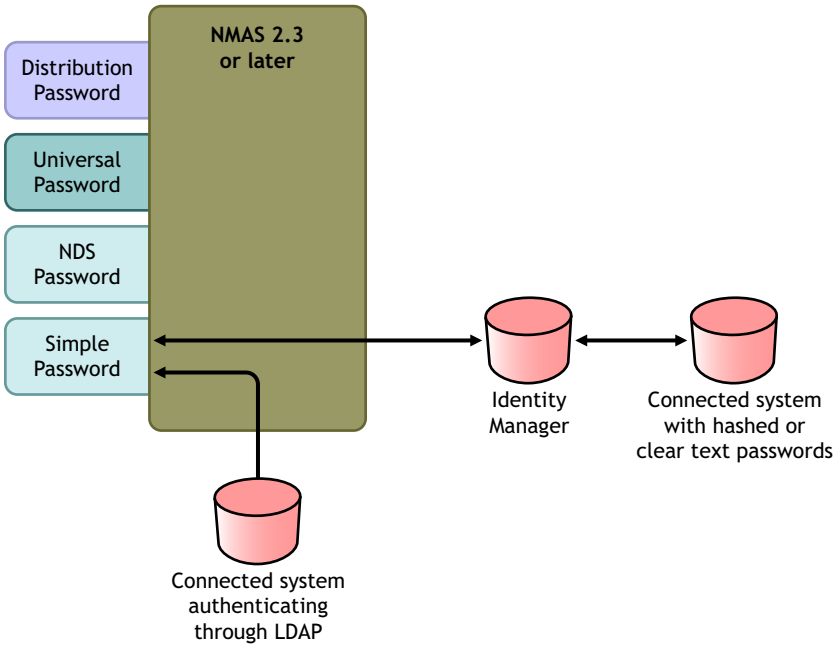
- 「同步化到 NDS 密碼的優點」，第 126 頁
- 「設定案例 5」，第 126 頁

同步化到 NDS 密碼的優點

表格 ***5-15*** 同步化到 *NDS* 密碼的優點

優點	缺點
◆ 可讓您直接更新「簡易密碼」。 ◆ 可讓您同步化雜湊密碼，並且使用它爲一個以上的應用程式進行驗證，而無需回復雜湊。	◆ 此案例不允許使用「通用密碼」。 ◆ 「忘記密碼」和「密碼自助服務」功能仍然受到「NDS 密碼」的支援，但不適用於「簡易密碼」。 ◆ 由於「設定通用密碼」任務取決於「通用密碼」，所以管理員無法使用該任務，在 Identity Vault 中設定使用者密碼。

特性 ***5-15*** 同步化到 *NDS* 密碼



設定案例 5

- 「密碼規則組態」，第 127 頁
- 「密碼同步化設定」，第 127 頁
- 「驅動程式組態」，第 127 頁

密碼規則組態

此案例的使用者不需要任何密碼規則。「通用密碼」無法使用。

密碼同步化設定

在此案例中，您可使用 Identity Manager 程序檔直接修改 SAS:Login Configuration 屬性。這表示，使用 iManager 中「密碼同步化」頁面設定的「密碼同步化」全域組態值 (GCV) 無效。

驅動程式組態

1 確定過濾器中的 SAS:Login Configuration 屬性具有「發行者」和「訂閱者」通道的「同步化」設定。

2 設定驅動程式規則的組態，發行已連接系統的密碼。

3 針對雜湊密碼，設定驅動程式規則的組態，以預加雜湊類型 (如果應用程式尚未提供)：

- {MD5}*hashed_password*

  此密碼以 Base 64 編碼。
- {SHA}*hashed_password*

  此密碼以 Base 64 編碼。
- {CRYPT}*hashed_password*

純文字密碼和 Unix Crypt 密碼雜湊不是以 Base64 編碼。

4 若要將密碼置入「簡易密碼」中，可設定驅動程式規則的組態，以修改 SAS:Login Configuration 屬性。

下列範例說明了如何在修改操作中使用 modify-attr 元素，將「簡易密碼」變更爲 MD5 雜湊密碼：

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-value> </
modify-attr>
```

針對純文字密碼，請遵循此範例。

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>clearpwd</value> </add-value> </modify-attr>
```

對於新增操作，add-attr 元素會包含下列其中一項：

```
<add-attr attr-name="SAS:Login Configuration>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-attr>
```

或

```
<add-attr attr-name="SAS:Login Configuration> <value>clearpwd</
value> </add-attr>
```

5.9 設定密碼過濾器

有些已連接系統可以提供使用者的實際密碼給 Identity Manager。

若要在 Active Directory、NIS 和 NT Domain 上擷取密碼，您必須執行某些次要設定，才能在已連接系統上安裝密碼過濾器。

- 「設定 Active Directory 和 NT Domain 的密碼同步化過濾器」，第 128 頁
- 「設定 NIS 的密碼同步化過濾器」，第 129 頁

5.9.1 設定 Active Directory 和 NT Domain 的密碼同步化過濾器

此資訊位於 Active Directory 和 NT Domain 之「Identity Manager 驅動程式」驅動程式實作指南中的「密碼同步化」一節，其網址爲 Identity Manager 驅動程式 (http://www.novell.com/documentation/dirxmldrivers/index.html)。

AD 或 NT Domain 的 Identity Manager 驅動程式只能安裝在一部 Windows 機器上。其他領域控制器不需要安裝驅動程式，但每個領域控制器都需要安裝 pwfilter.dll 檔案以擷取密碼，如此才能傳送至 Identity Manager。

爲了簡化設定和管理，您可使用所提供的公用程式，針對安裝驅動程式之 Windows 機器的所有領域控制器執行此動作。

5.9.2 設定 NIS 的密碼同步化過濾器

Identity Manager Driver for NIS 3.0 可以操作三種 UNIX 驗證資料儲存：檔案、NIS 和 NIS+。屆時將 PAM 模組來擷取密碼，並將它們傳送到 Identity Manager Driver for NIS。

「NIS 驅動程式」之 PAM 模組的部署會在 《*Identity Manager Driver for NIS* 實作指南》中說明，其網址爲 Identity Manager 驅動程式 (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)。

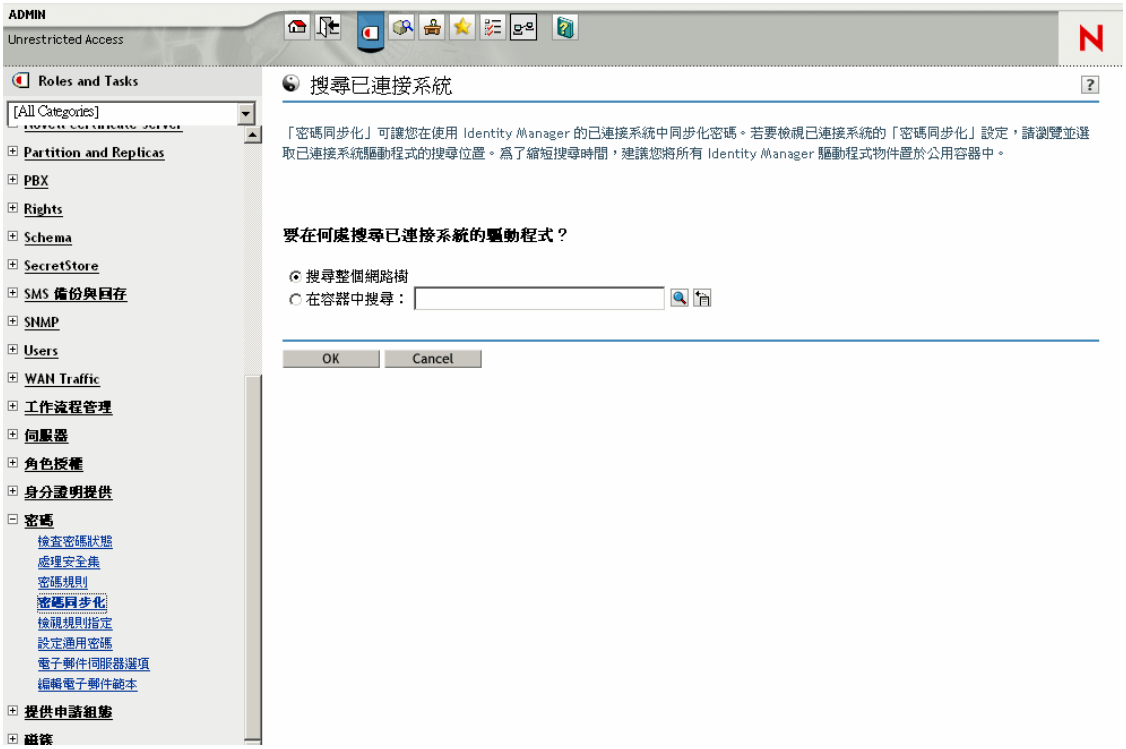
5.10 管理密碼同步化

- 「設定系統之間密碼的流程」，第 129 頁
- 「在已連接系統上強制執行密碼規則」，第 130 頁
- 「使 eDirectory 密碼與同步化密碼不相同」，第 131 頁

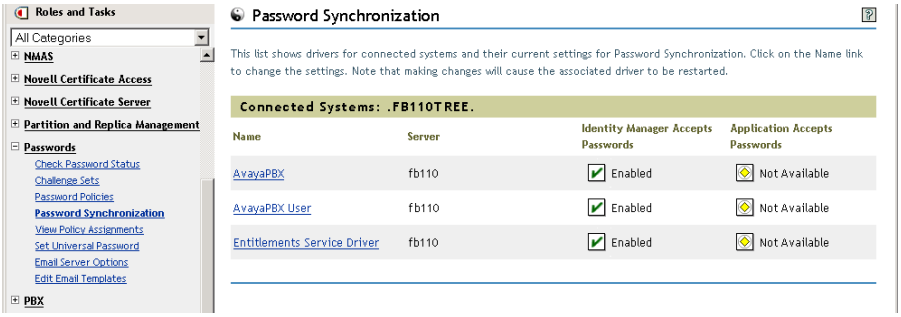
5.10.1 設定系統之間密碼的流程

若要檢視如何設定系統以接受或發行密碼的情形，請執行下列動作：

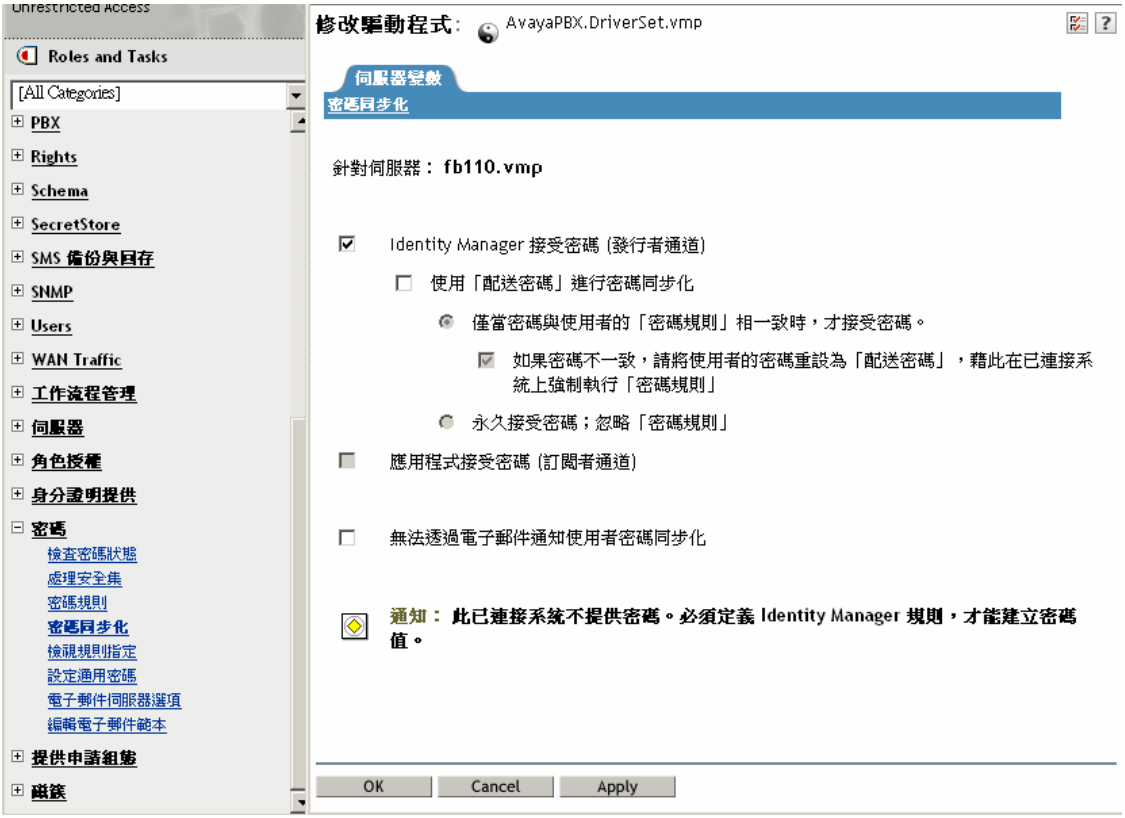
1. 在 iManager 中，選取「密碼」>「密碼同步化」。
2. 搜尋已連接系統的驅動程式。



搜尋結果會顯示流入和流出 Identity Manager 和已連接系統之密碼的設定。



若要變更這些設定，請按一下已連接系統驅動程式名稱。



在「修改驅動程式」頁面上，您可以設定是否針對送入 Identity Manager 的密碼強制執行密碼規則，以及是否可以藉由重新設定已連接系統密碼，在已連接系統上強制執行密碼規則。

此頁面上的設定是全域組態值 (GCV)，會儲存於每個伺服器。請參閱「使用全域組態值控制密碼同步化」，第 82 頁。

5.10.2 在已連接系統上強制執行密碼規則

如果使用「進階密碼規則」和「Identity Manager 密碼同步化」，建議您進行下列幾項操作：

1 研究所有已連接系統的密碼規則。

2 確定 「進階密碼規則」與已連接系統上的密碼規則相容。

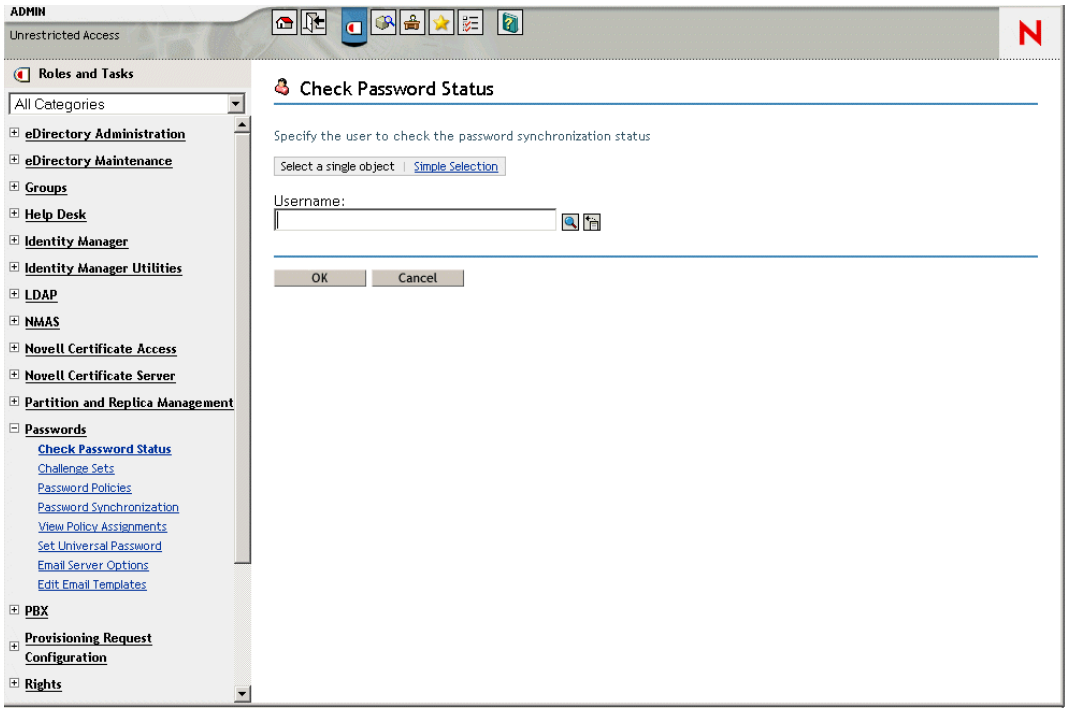
5.10.3 使 eDirectory 密碼與同步化密碼不相同

此案例描述於 「案例 4：Identity Manager 更新 「配送密碼」後，會通道封裝 --- 同步化 「已連接系統」，而不是 Identity Vault」，第 121 頁中。

5.11 檢查使用者的密碼同步化狀態

您可以判定特定使用者的 「配送密碼」是否與已連接系統中的密碼相同。

1 在 iManager 中，選取 「密碼」 > 「檢查密碼狀態」。



2 瀏覽並選取使用者。

「檢查密碼狀態」任務會使驅動程式執行 「檢查物件密碼」動作。

不是所有驅動程式都支援密碼檢查。支援密碼檢查的驅動程式，必須在驅動程式資訊清單中包含密碼檢查功能。iManager 不允許將密碼檢查操作，傳送到資訊清單中不包含此功能的驅動程式。

「檢查物件密碼」動作會檢查 「配送密碼」。如果 「配送密碼」不在更新中，則 「檢查物件密碼」可能會回報密碼沒有同步化。

如果發生下列任何一種情況，「配送密碼」將不會更新：

- 您正在使用 「案例 1：使用 NDS 密碼將兩個 Identity Vault 同步化」，第 101 頁中描述的同步化方法。

- 您正在同步化「通用密碼」(如「案例 2：使用通用密碼同步化」，第 103 頁中所述)，但是尚未啓用密碼規則組態選項，以將 「通用密碼」同步化到 「配送密碼」。

附註：請記住，對於 Identity Vault，「檢查密碼狀態」動作會檢查 「NDS 密碼」而不是「通用密碼」。因此，如果使用者的密碼規則未指定爲同步化 「NDS 密碼」與 「通用密碼」，則會一直將密碼報告爲未同步化。事實上，「配送密碼」和已連接系統上的密碼可能已同步化，但 「檢查密碼狀態」不會是正確的，除非 「NDS 密碼」和 「配送密碼」都與「通用密碼」同步化。

5.12 設定電子郵件通知的組態

iManager 任務可讓您指定電子郵件伺服器，並自定電子郵件通知的範本。

提供電子郵件範本的目的是讓 「密碼同步化」和 「密碼自助服務」將自動電子郵件傳送給使用者。

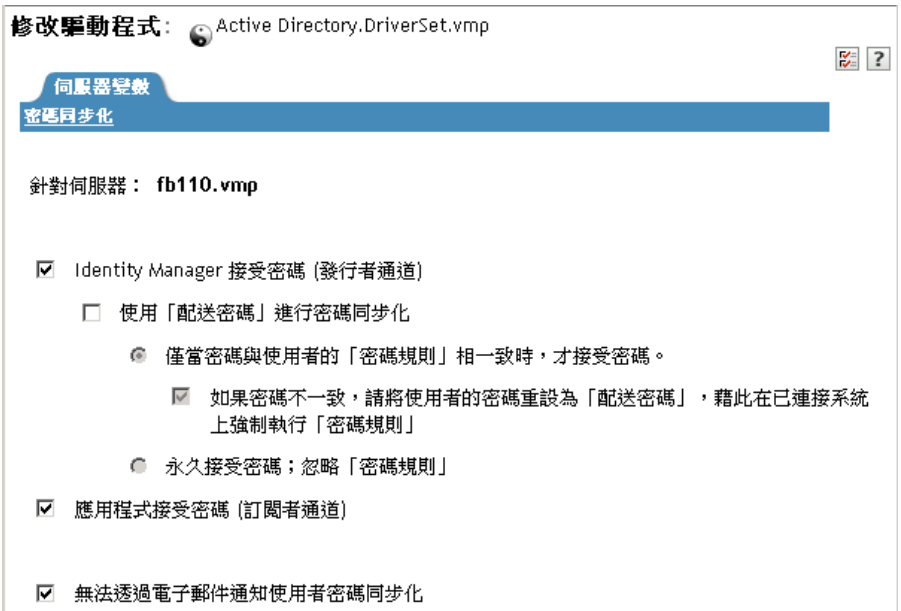
範本不需由您建立，而是由使用它們的應用程式提供。電子郵件範本是 Identity Vault 中的「範本」物件，放置在 「安全性」容器中，其通常位於網路樹的根部。雖然它們是 Identity Vault 物件，您只能透過 iManager 進行編輯。

這是一個模組化架構。由於已新增使用電子郵件範本的應用程式，因此範本可以與使用它們的應用程式一起安裝。

根據 iManager 中的選擇，控制是否傳送電子郵件訊息。對於 「忘記密碼」，只有在選擇使用其中一個會導致傳送電子郵件的 「忘記密碼」動作時，才會傳送電子郵件通知：以電子郵件傳送密碼給使用者，或者以電子郵件傳送密碼提示給使用者。請參閱 《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的 「爲使用者提供忘記密碼自助服務」。

選取 「透過電子郵件通知使用者密碼同步化失敗」時，會設定 「密碼同步化」的組態，僅針對失敗的密碼同步化操作和您指定的驅動程式來傳送電子郵件。

特性 ***5-16*** 設定密碼同步化的組態



另外，您還需要確定 SMTP 驗證資訊已包含在驅動程式規則中。

- 「先決條件」，第 133 頁
- 「設定 SMTP 伺服器以傳送電子郵件通知」，第 134 頁
- 「設定電子郵件通知範本」，第 135 頁
- 「提供驅動程式規則中的 SMTP 驗證資訊」，第 135 頁
- 「新增您自己的取代標籤至電子郵件通知範本」，第 137 頁
- 「傳送電子郵件通知給管理員」，第 143 頁
- 「當地語系化電子郵件通知範本」，第 143 頁

5.12.1 先決條件

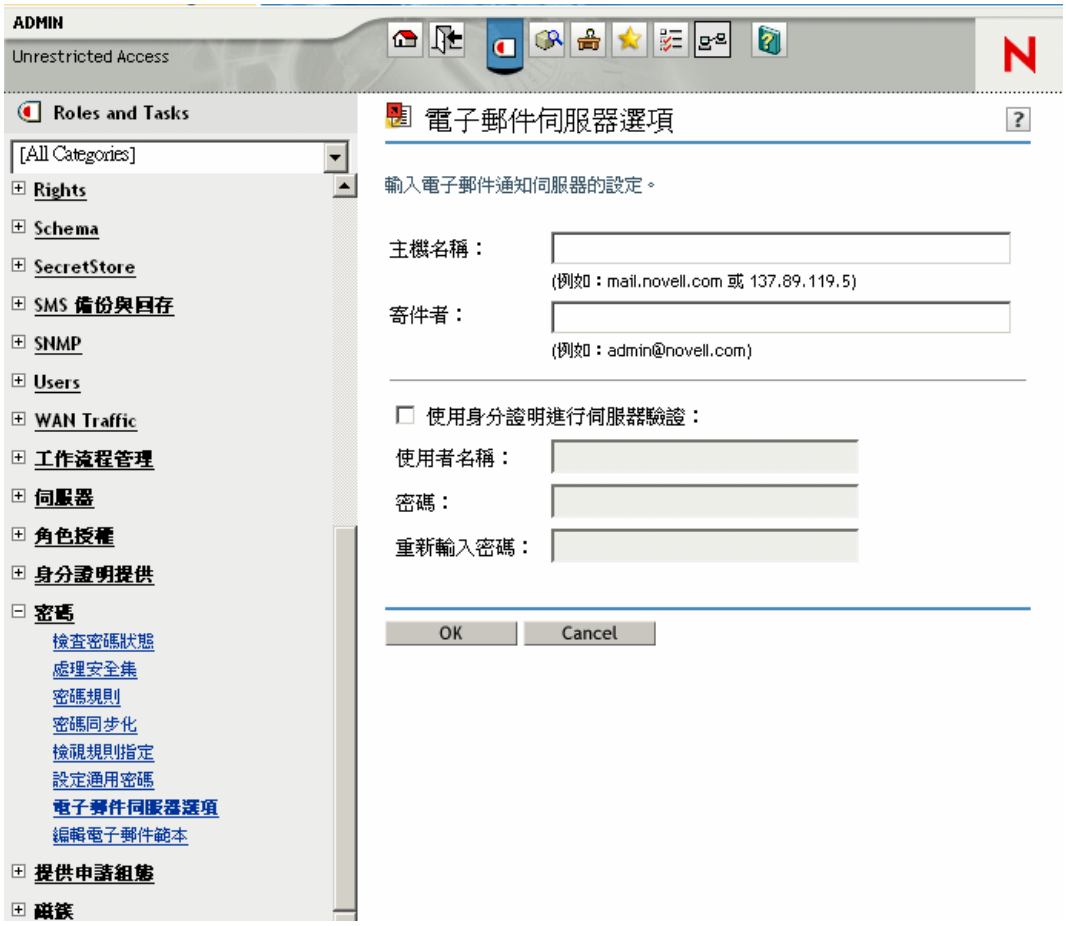
- 請確定 Identity Vault 使用者已填入 Internet EMail Address 屬性。
- 如果您使用「密碼同步化」的電子郵件通知，請確定「密碼同步化」驅動程式規則包含 SMTP 伺服器的密碼。請參閱「提供驅動程式規則中的 SMTP 驗證資訊」，第 135 頁。
- 如果您擔心某些使用者可能沒有填入電子郵件地址，或者需要所有失敗通知的電子郵件記錄，請考慮選擇所有電子郵件通知傳送到的密碼管理員帳戶 (除了使用者之外)。

  此電子郵件地址應該位於 Identity Manager 程序檔規則的「收件者」欄位。如需相關資訊，請參閱「傳送電子郵件通知給管理員」，第 143 頁。
- 如果 eDirectory 和 Identity Manager 在 UNIX 伺服器上，則該伺服器必須保留電子郵件範本物件的複製本。

  這些物件位於「安全性」容器根部。這表示，該伺服器需要根分割區的複製本。

5.12.2 設定 SMTP 伺服器以傳送電子郵件通知

1 在 iManager 中，選取「密碼」>「電子郵件伺服器選項」。



2 輸入下列資訊：

- 主機名稱
- 您想要在電子郵件訊息的「寄件者」欄位中顯示的名稱 (例如，「管理員」)
- 向伺服器驗證所需的使用者名稱和密碼 (必要時)。

3 按一下「確定」。

4 如果您將「密碼同步化」與 Identity Manager 驅動程式搭配使用，而且想要使用電子郵件通知功能時，還必須進行下列幾項操作：

4a 如果您的 SMTP 伺服器需要在傳送電子郵件之前進行驗證，請確定驅動程式規則包含密碼。如需指示，請參閱「提供驅動程式規則中的 SMTP 驗證資訊」，第 135 頁。

對於「忘記密碼」通知而言，在步驟 2 中指定「電子郵件伺服器選項」頁面的驗證資訊就夠了，但對於「密碼同步化」通知而言是不夠的。

4b 重新啓動需要以變更更新的 Identity Manager 驅動程式。

驅動程式僅會在啓動時間讀取範本和 SMTP 伺服器資訊。

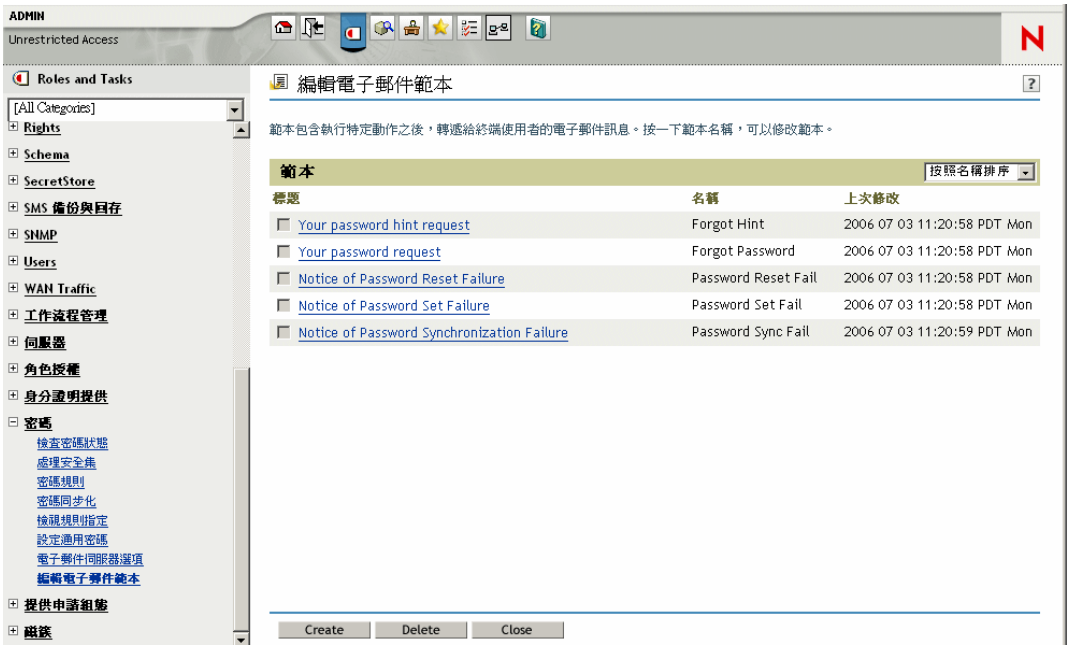
5 自定電子郵件範本，如「設定電子郵件通知範本」，第 135 頁中所述。

設定電子郵件伺服器之後，如果您使用可使訊息傳送的功能，則電子郵件訊息可以由使用它們的應用程式傳送。

5.12.3 設定電子郵件通知範本

您可以使用自己的文字自定這些範本。範本的名稱會指出它的用途。

1 在 iManager 中，選取「密碼」>「編輯電子郵件範本」。



2 視需要編輯範本。

請記住，如果想要新增取代標籤，則可能需要部份額外任務。請遵循「新增您自己的取代標籤至電子郵件通知範本」，第 137 頁中的指示。

3 重新啓動需要以變更更新的 Identity Manager 驅動程式。

驅動程式僅會在啓動時間讀取範本和 SMTP 伺服器資訊。

5.12.4 提供驅動程式規則中的 SMTP 驗證資訊

您會在「設定 SMTP 伺服器以傳送電子郵件通知」，第 134 頁中指定 SMTP 伺服器的使用者名稱和密碼。對於「忘記密碼」電子郵件通知而言，這已足夠。

然而，對於「密碼同步化」電子郵件通知而言，還會需要將密碼包含在驅動程式規則中。Metadirectory 引擎可以存取使用者名稱，但不可以存取密碼，其必須由驅動程式規則提供。

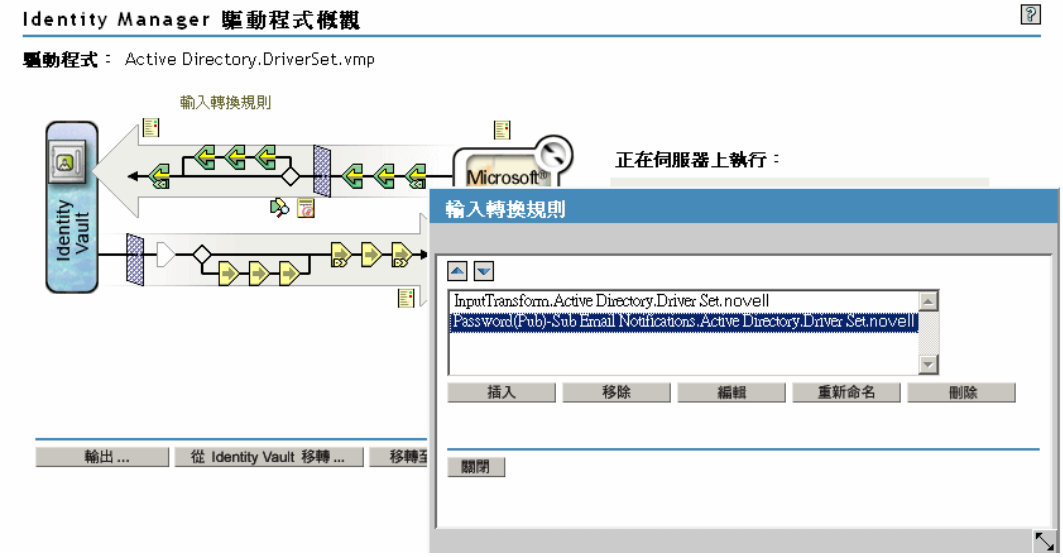
如果存在下列條件，則必須完成此程序：

- SMTP 伺服器是安全的，而且在傳送電子郵件之前需要驗證。
- 將「Identity Manager 密碼同步化」與 Identity Manager 驅動程式搭配使用
- 在驅動程式的「密碼同步化」設定中，您已選取「透過電子郵件通知使用者密碼同步化失敗」。

SMTP 伺服器密碼新增至驅動程式規則，請執行下列動作：

1. 確定驅動程式具有使用 「密碼同步化」所需的規則。

   範例驅動程式組態中有提供這些規則，或者也可以依 「升級現有的驅動程式組態以支援密碼同步化」，第 92 頁中所述來新增規則。
2. 在 iManager 中，選取 「*Identity Manager*」 > 「*Identity Manager* 概觀」。
3. 搜尋驅動程式集，或者瀏覽並選取保留驅動程式集的容器。
4. 在 「Identity Manager 驅動程式概觀」中，按一下驅動程式的圖示。
5. 選取 「輸入轉換」圖示或 「輸出轉換」圖示。

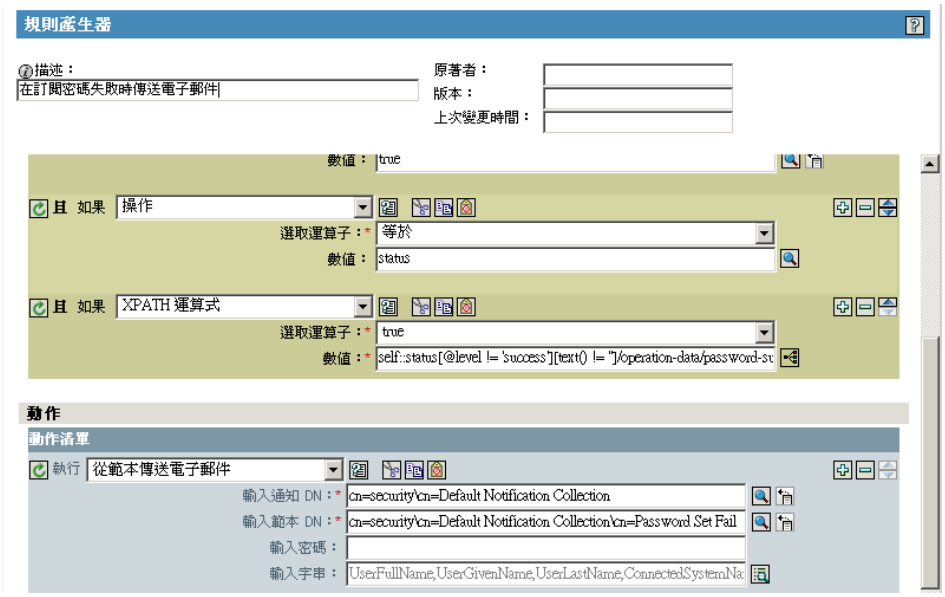


6. 選取規則，然後按一下 「編輯」。
7. 按一下規則。
8. 在包含 「請務必從範本傳送電子郵件」動作的規則中，指定 SMTP 伺服器的密碼。

   例如，如果您使用範例驅動程式組態，則需要修改下列 「密碼同步化」規則。

規則 (Policy) 集	規則 (Policy) 名稱	規則 (Rule) 名稱
輸入轉換	密碼 (發行者)- 訂閱電子郵件通知	◆ 訂閱密碼失敗時傳送電子郵件 ◆ 使用 Identity Manager 資料儲存密碼重設已連接系統密碼失敗時傳送電子郵件
輸出轉換	密碼 (訂閱者)- 發行電子郵件通知	◆ 發行密碼操作失敗時傳送電子郵件

下圖顯示需要密碼之 「請務必從範本傳送電子郵件」動作的範例。



密碼儲存在 Identity Vault 中時會經過混淆化處理。

9 選取 (標示) 規則，然後按一下 「確定」。

5.12.5 新增您自己的取代標籤至電子郵件通知範本

電子郵件通知範本具有一些預設即定義好的標籤，協助您個人化使用者訊息。您還可以新增自己的標籤。

是否能夠新增標籤，取決於正在使用電子郵件範本的應用程式。

- 「新增取代標籤至密碼同步化電子郵件通知範本」，第 137 頁
- 「新增取代標籤至忘記密碼電子郵件通知範本」，第 142 頁

新增取代標籤至密碼同步化電子郵件通知範本

您可以將取代標籤新增至用於 「密碼同步化」的電子郵件通知範本，但是除非您也在每個密碼同步化規則 (參考電子郵件通知範本) 中定義這些標籤，否則它們不會起作用。使用 DoSendEmailFromTemplate 動作時，在範本內宣告的所有取代標籤都必須定義爲動作的子 arg-string 元素。

例如，Identity Manager 會提供電子郵件通知範本包含的預設取代標籤。Identity Manager 還會在驅動程式組態中提供預設密碼同步化規則。電子郵件範本提供的每個預設標籤，也會在使用該電子郵件範本之密碼同步化規則 (Policy) 的每個規則 (Rule) 中定義。

例如，UserGivenName 標籤是在名爲 「密碼設定失敗」的電子郵件範本中定義的其中一個預設標籤。名爲 「訂閱密碼失敗時傳送電子郵件」的規則，會參考 DoSendEmailFromTemplate 動作中的電子郵件範本。此規則 (Rule) 在規則 (Policy) 中使用，會在密碼同步化失敗時通知使用者。在該規則中，相同的 UserGivenName 標籤定義爲 arg-string 元素。

與此範例類似，每個新增的標籤都必須在電子郵件範本和參考該範本的規則中定義，如此 Metadirectory 引擎才能瞭解當將電子郵件傳送至使用者時，如何在取代標籤的位置插入正確的資料。

您可以參考 Identity Manager 隨附 (做爲範例) 之 Identity Manager 驅動程式組態中的標籤。

請記住下列指示：

- 電子郵件範本中稱爲取代標籤的項目，在「規則產生器」的網路位置中稱爲記號。
- 您應該使用「規則產生器」，使定義取代標籤的引數字串更容易，如本節的步驟中所說明。
- 新增的標籤可以定義爲下列任何一項：
  - 用於使用者的任何「來源」或「目的」屬性

    與新增「忘記密碼」之電子郵件範本的標籤不同的是，只新增與 Identity Vault 中「使用者」物件上之屬性具有相同名稱的標籤，不會使標籤起作用。與密碼同步化電子郵件通知範本中使用的所有標籤一樣，您也必須在參考電子郵件範本的規則中定義標籤。
  - 全域組態值
  - XPATH 運算式

  這與「忘記密碼」之電子郵件範本的標籤形成對比，這些標籤限制爲 eDirectory 使用者屬性。
- 與新增「忘記密碼」之電子郵件範本的標籤 (需要使用 eDirectory 使用者屬性的名稱) 不同的是，只要符合用於定義參考電子郵件範本之規則中標籤的名稱，就可以選擇任意名稱來命名取代標籤。

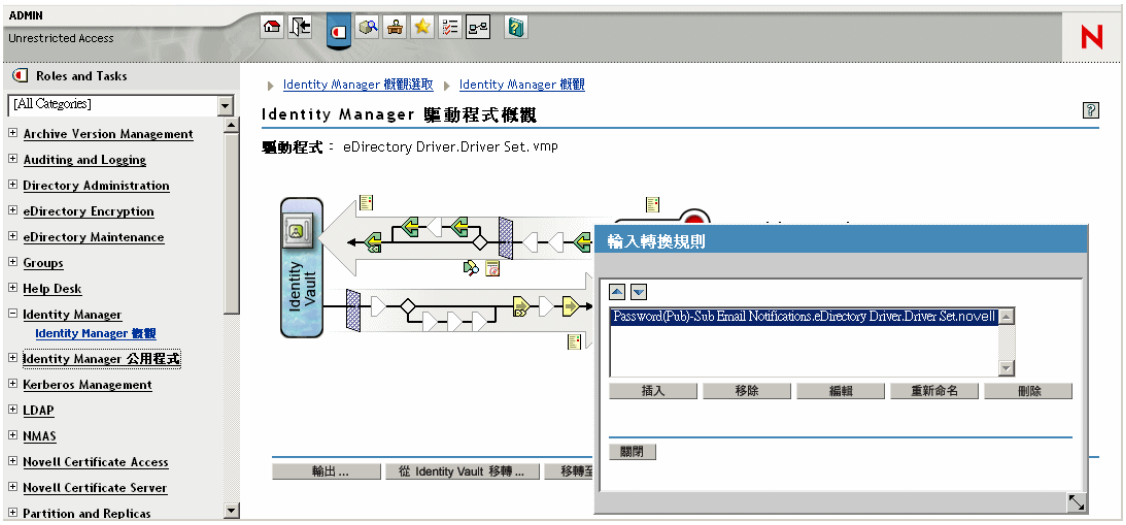
若要定義規則中的標籤，請找到參考電子郵件通知範本的所有規則，並使用「規則產生器」將標籤新增至規則。在每個規則 (Policy) 中，編輯參考範本的每個規則 (Rule)。

有一種方法可以確定會找到參考電子郵件通知範本之所有規則，就是輸出驅動程式組態，然後在 XML 中搜尋 do-send-e-mail 動作，該動作具有名稱與電子郵件通知範本名稱相同的範本。

1. 在 iManager 中，選取「*Identity Manager*」>「*Identity Manager* 概觀」。
2. 選取驅動程式集，其包含具有您要編輯之規則的驅動程式。
3. 按一下具有要編輯規則之驅動程式的圖示。
4. 在「發行者」或「訂閱者」通道上，按一下包含您要編輯之規則的規則集。

   例如，Identity Manager 隨附之 eDirectory 驅動程式的驅動程式組態，會在「輸入轉換」規則集中包含一個規則，該規則會同時參考兩個密碼同步化電子郵件通知範本。
5. 按一下規則，然後按一下「編輯」。

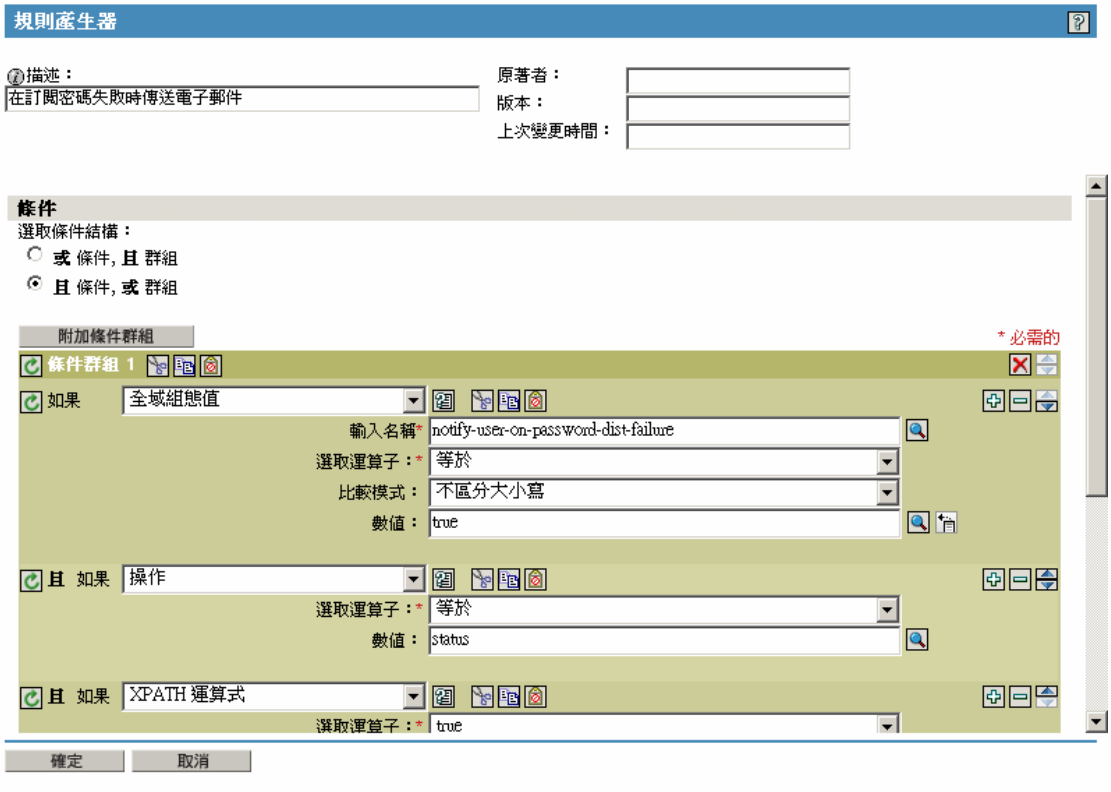
下圖說明如何編輯 eDirectory 驅動程式的「密碼 (發行者)- 訂閱電子郵件通知」規則：



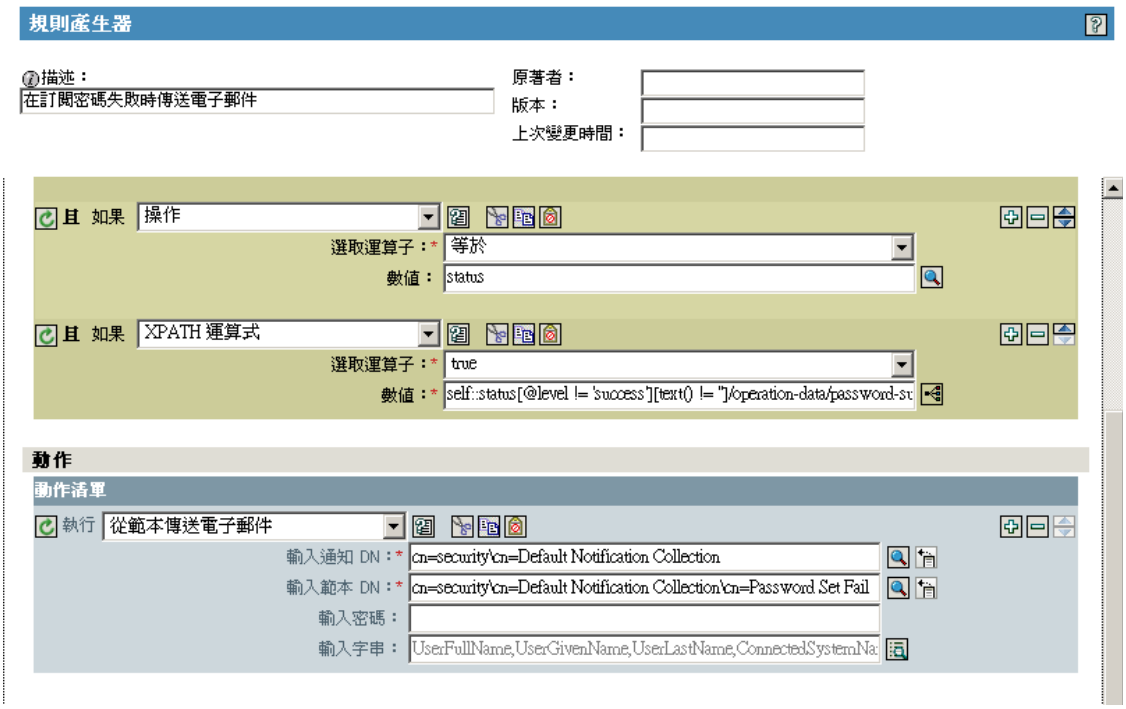
6 在開啓的規則清單中，按一下參考電子郵件通知範本的規則。

例如，在「密碼 (發行者)- 訂閱電子郵件通知」規則 (Policy) 中，您會看到此規則 (Rule) 清單。這兩個規則都參照其中一個密碼同步化電子郵件範本。如果您將標籤新增至範本，則需要編輯這兩個規則。

如果您按一下第一個規則，下列頁面即會出現：



7 捲動至「動作」區段。



8 針對 「請務必從範本傳送電子郵件」規則，按一下 「輸入字串」欄位的瀏覽按鈕。

這會開啓字串產生器。針對範例規則，下圖會顯示您將看到的字串清單。請註意，在做爲部份 Identity Manager 驅動程式組態的密碼同步化規則中，已定義用於電子郵件通知範本中的預設標籤 (如下圖)。您可以使用預設標籤做爲範例。

9 若要定義可用於電子郵件通知範本的標籤，請按一下 「附加新字串」，然後輸入標籤名稱。

請確定該名稱與用於電子郵件通知範本的名稱完全相同。

10 在 「字串值」欄位中，按一下瀏覽按鈕，以協助您定義標籤。

11 在 「引數產生器」頁面中，指定當此標籤用於電子郵件通知範本時應該引入的值。

您可以將標籤定義爲下列任何一項：

- 用於使用者的任何 「來源」或 「目的」屬性

  與新增 「忘記密碼」之電子郵件範本的標籤不同的是，只新增與 Identity Vault 中使用者物件上之屬性具有相同名稱的標籤，不會使標籤起作用。與密碼同步化電子郵件通知範本中使用的所有標籤一樣，您也必須在參考電子郵件範本的規則中定義標籤。

- 全域組態值
- XPATH 運算式

下圖說明如何定義標籤：

定義標籤之後，按一下「確定」，其會顯示爲「字串產生器」頁面中的其中一個字串。

12 務必按一下「確定」以完成所有頁面，如此才能儲存規則的變更。

13 重複步驟，以編輯參考電子郵件通知範本之所有規則 (Policy) 中的規則 (Rule)。

14 使用您在規則中使用的確實名稱，將規則中定義的標籤新增至電子郵件通知範本。

此時，您可以在電子郵件通知範本的本文中使用標籤名稱。

15 儲存變更，並重新啓動驅動程式。

新增取代標籤至忘記密碼電子郵件通知範本

使用下列指示，將標籤新增至「忘記密碼」的電子郵件通知範本：

- 您可以只新增對應於 LDAP 屬性的標籤，該屬性位於訊息傳送到的「使用者」物件上。
- 新增的標籤名稱，必須與使用者物件上的 LDAP 屬性名稱完全相同。

  若要查看 LDAP 屬性如何對應於 eDirectory 屬性名稱，您可以參考在 Identity Manager Driver for LDAP 中提供的「綱要映射規則」。
- 不需要任何其他組態。

5.12.6 傳送電子郵件通知給管理員

預設組態是僅將電子郵件通知傳送給使用者。Identity Manager 隨附的規則使用受影響使用者之 Identity Vault 物件的電子郵件地址。

然而，您可以設定密碼同步化規則的組態，以使電子郵件通知也傳送至管理員。若要這樣做，您必須針對其中一個規則修改 Identity Manager 程序檔。

藉由以管理員的電子郵件地址定義記號，將「隱藏副本」傳送給管理員。

若要複製管理員，請修改產生電子郵件的規則 (例如 PublishPasswordEmails.xml，規則會在其中查詢要傳送通知的電子郵件地址)，並新增具有管理員電子郵件地址的其他 <arg-string> 元素。

下列範例說明其他 arg-string 元素：

```
<arg-string name="to">

<token-text>Admin@company.com</token-text>

</arg-string>
```

進行這些變更之後，務必重新啓動驅動程式。

5.12.7 當地語系化電子郵件通知範本

請記住下列各項：

- 預設範本語言是英文，但是您可以編輯文字以使用其他語言。
- 取代標籤的名稱和定義必須保留爲英文，如此規則中的 arg-string 記號定義才會符合取代標籤的名稱。
- 以下指示僅限於「忘記密碼」電子郵件通知：若要指定郵件項目使用何種編碼，您需要在 portalservlet.properties 檔案中新增設定。例如：

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  如果此設定不存在，則郵件轉換不會使用任何編碼。
- 對於「密碼同步化」電子郵件訊息，可以在下列元素上指定名爲 charset 的 XML 屬性：<mail>、<message> 和 <‘>。

  如需使用這些元素的相關資訊，請參閱《手動任務服務的 *DirXML* 驅動程式實作指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)》，其中提供關於電子郵件範本的詳細資料。

5.13 疑難排解密碼同步化

- 請參閱 「實作密碼同步化」，第 100 頁中的祕訣。
- 確定「簡易密碼登入方法」有和 NMAS 一起安裝。

- 確定您具有伺服器上網路樹根部的副本。而在該伺服器上，您需要 NMAS 在 eDirectory 登入方法上，或在由 Identity Manager 同步化之已連接系統的密碼上，強制執行密碼規則。
- 在驅動程式同步化密碼的相同伺服器上，確定已複製要求密碼同步化的使用者。與其他驅動程式功能一樣，該驅動程式只可以管理相同伺服器上主複製本或讀 / 寫複製本中的使用者。
- 確定在 Web 伺服器和 Identity Vault 之間正確設定保全插槽層 (SSL) 的組態。
- 如果看到啓始建立使用者時密碼不一致的錯誤，但密碼在 Identity Vault 中的設定是正確的，則驅動程式規則中的預設密碼可能不符合該使用者套用的密碼規則。

  下列案例使用 Active Directory 驅動程式。然而，對於另一個驅動程式而言，可能也會發生同樣的問題。

  提供啓始密碼： 當驅動程式在 Identity Vault 中建立新的「使用者」物件時，您要讓 Active Directory 驅動程式爲使用者提供啓始密碼，以符合 Active Directory 中的使用者。Active Directory 驅動程式的範例組態會傳送啓始密碼，做爲與新增使用者不同的操作，而且範例組態也包含一個規則，即如果 Active Directory 沒有提供任何密碼，則會爲使用者提供預設密碼。

  新增使用者與設定密碼是分開進行的，因此，在此情況下，新使用者會一直接收預設密碼 (即使只是暫時如此)。Active Directory 驅動程式會在新增使用者之後立即傳送密碼，因此會很快更新預設密碼。如果預設密碼與使用者的 Identity Vault 密碼規則不一致，則會顯示錯誤。

  例如，如果透過使用者姓氏所建立的預設密碼太短，而與密碼規則不一致時，您可能會看到 –216 錯誤，指出密碼太短 。然而，如果 Active Directory 驅動程式隨後傳送相符的啓始密碼，則會很快更正該情況。

  無論您使用的驅動程式爲何，如果想要建立「使用者」物件的已連接系統提供啓始密碼，請考慮進行下列其中一項操作。如果啓始密碼不是源自 「新增」事件，而是源自後續事件，則這些方法尤爲重要。

  - 變更「發行者」通道上建立預設密碼的規則，以使預設密碼符合 Identity Vault 中已經針對您的組織定義的密碼規則 (選取「密碼」，然後選取「密碼規則」)。

    當啓始密碼來自授權應用程式時，它會取代預設密碼。

    有了預設密碼規則，才能維護系統內的高層次安全性，所以建議使用此選項。
  - 在「發行者」通道上，移除建立預設密碼的規則。在範例組態中，「指令轉換」規則集中有提供此規則。在 Identity Vault 中，允許新增沒有密碼的使用者。此選項的假設是，新建立之「使用者」物件的密碼終究會經過「發行者」通道，而且「使用者」物件沒有密碼的時間很短。
- 密碼規則是使用網路樹中心的方式指定的。相對地，「密碼同步化」是依每個驅動程式設定的。驅動程式會在每個伺服器上安裝，且僅可以管理主複製本或讀 / 寫複製本中的那些使用者。

  若要取得預期的「密碼同步化」結果，請確定執行「密碼同步化」驅動程式之伺服器上主複製本或讀 / 寫複製本中的容器，與您指定密碼規則且已啓用「通用密碼」的容器相符。將密碼規則指定給分割區根容器，可確保將密碼規則指定給該容器和次容器中的所有使用者。
- 實用的 DSTrace 指令：

  +DXML：檢視 Identity Manager 規則處理和潛在錯誤訊息。

  +DVRS：檢視 Identity Manager 驅動程式訊息

  +AUTH：檢視 NDS 密碼修改

+*DCLN*：檢視 NDS DCLient 訊息

建立並使用授權

6

Identity Manager 可讓您將已連接系統之間的資料同步化。授權可讓您爲個人或群組設定準則，一旦符合準則，即會啓始事件，以授予或撤銷對已連接系統內商務資源的存取權限。如此，您就會有多一層控制和自動化授予及撤銷資源的權限。

讓授權運作有兩種情況：建立授權與管理授權。您可以透過 iManager 或 Designer 建立授權。若要透過 iManager 建立授權，請選取 iManager 中「Identity Manager 公用程式」標題下的「建立授權」選項。如需相關資訊，請參閱「透過 iManager 以 XML 格式寫入授權」，第 151 頁。

您還可以使用 Designer 來建立授權，並將它們部署至現有的 Identity Manager 驅動程式。Designer 可讓您透過「授權精靈」建立授權，其中有圖形化介面讓您建立授權，並引導您逐步完成該程序。在 iManager 中，用來建立授權的介面很簡單，但要透過 XML 編輯器新增額外的內容。由於 Designer 具有圖形化介面，建議您使用它來建立和編輯授權。

在建立授權 (或使用某些 Identity Manager 驅動程式預先設定的授權) 之後，接下來是管理。授權由兩個套件或代辦來管理：透過做爲「角色授權規則」的 iManager，或透過工作流程供應的「使用者應用程式」。如需用於工作流程供應的授權相關資訊，請參閱「工作流程提供簡介」。如需「角色授權」的相關資訊，請參閱「管理角色授權綜覽」，第 164 頁。

「角色授權」規則可讓您在符合準則時授予商務資源。例如，如果使用者符合準則 1、2 和 3，則透過「角色授權」規則，使用者會成爲「群組 H」的成員；但是如果使用者符合 4 和 5，則該使用者會成爲「群組 I」的成員。爲了讓此授權透過工作流程供應來運作，首先需要經過核准。

6.1 術語

下列爲本章中使用的一些詞彙。

表格 *6-1* 術語

詞彙	解釋
授權	代表已連接系統中商務資源的 Identity Vault 物件。

詞彙	解釋
授權代辦	授予和撤銷授權。對於「角色授權」，代辦是「授權服務」驅動程式。
授予或撤銷	授予或撤銷授權的解譯，由 Identity Manager 驅動程式上的全域組態變數 (GCV) 來控制。
授權消費者	使用授權相關資訊的任何事物。授權對象包括 iManager、使用者應用程式和 Identity Manager 規則。

6.2 建立授權：綜覽

- 「支援授權且具預先設定組態的 Identity Manager 驅動程式」，第 148 頁
- 「在其他 Identity Manager 驅動程式上啓用授權」，第 149 頁

您必須事先瞭解要用授權來完成的作業。授權從您透過規則建立到 Identity Manager 驅動程式的功能進行運作。這些驅動程式規則 (Policy) 會實作規則 (Rule)，並處理 Identity Vault 與已連接系統之間的事件。如果 Identity Manager 驅動程式中的規則未指定您要執行的作業，則授權無法運作。例如，如果未指定「指令」規則 (Policy) 中「檢查群組成員資格的使用者修改」規則 (Rule) 的動作區段，則會忽略群組成員資格授權的授予或撤銷。

您需要確切瞭解要使用 Identity Manager 完成的動作，然後才可以正確設計任何已連接系統資源的授予和撤銷功能。下列四個步驟的程序，可協助您規劃對授權的建立和使用：

1. 瞭解您的業務要完成的作業。幾乎所有事項都可以透過 Identity Manager 來設計並實作，但是需要瞭解在實作未定義的某個事項之前要進行的動作。爲您要進行之動作建立有編號的清單。
2. 定義代表編號清單中某個點的授權。您可以建立無值授權和具值授權。具值授權可以從外部查詢取得值，可以由管理員來定義，也可以是自由格式。在「協助您建立自己授權的範例授權」，第 160 頁中有相關範例。
3. 將規則新增至「Identity Manager 驅動程式」，以實作設計的授權。若要建立 Identity Manager 驅動程式的規則，您需要非常熟悉 XSLT 或 DirXML 程序檔，熟悉已連接系統處理和接收資訊的方式，以及 Novell® eDirectory™ 儲存資訊的方式。除非您是一名優秀的 DirXML* 程式設計人員，否則這應該是顧問的工作。
4. 設定管理代辦以授予或撤銷授權。如果您想要自動處理，請使用「角色授權」；如果想要手動處理，請使用工作流程供應。

6.2.1 支援授權且具預先設定組態的 Identity Manager 驅動程式

Identity Manager 隨附若干驅動程式，其具有已包含授權、實作授權之規則，以及爲監聽授權活動而啓用之驅動程式的預先設定組態。您必須在啓始安裝驅動程式時啓用授權，以使預先設定組態元素成爲驅動程式的一部份。下列驅動程式具有支援授權的預先設定組態：

- Active Directory*
- Exchange
- GroupWise®
- LDAP
- NIS
- Lotus* Notes*

- NT Domain
- RACF

這些預先設定組態的驅動程式會完成上述之四個步驟中的前三個。驅動程式包含的範例授權類型可用於大多數常見案例：授予和撤銷使用者帳戶、群組和電子郵件配送清單。包含：

- Active Directory：授予和撤銷帳戶、群組成員資格、Exchange 信箱
- Exchange 5.5：授予和撤銷信箱與群組成員資格
- GroupWise：授予和撤銷帳戶，授予和撤銷配送清單的成員
- LDAP：授予和撤銷使用者帳戶
- Linux* 和 UNIX*：授予和撤銷帳戶
- Lotus Notes：授予和撤銷使用者帳戶與群組成員資格
- NT Domain：授予和撤銷使用者帳戶與群組成員資格
- RACF：授予和撤銷群組帳戶與群組成員資格

這些是您可以直接使用的範例授權和規則 (如果符合需求)；您還可以變更它們以符合需求，或者將它們當作範例使用，並透過 iManager 或 Designer 建立自己的範例。同樣的，如果您要使用預先設定組態之驅動程式的授權，就必須在 Designer 或 iManager 中啓始建立預先設定組態的驅動程式時啓用授權；不重新建立驅動程式，稍後就無法新增預先設定組態的授權。

如果您已搭配使用授權與 Identity Manager 2.x，並且想搭配使用那些授權與 Identity Manager 3，請執行 「*Identity Manager* 公用程式」下的 「升級授權」選項。

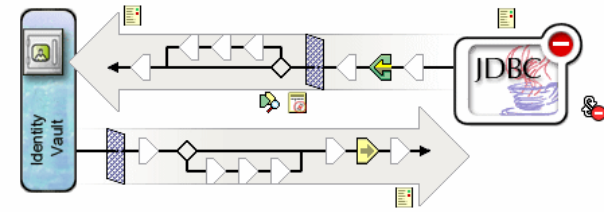
6.2.2 在其他 Identity Manager 驅動程式上啓用授權

您仍然可以在不包含授權預先設定組態的 Identity Manager 驅動程式上使用授權。若要啓用驅動程式以支援授權，請將 DirXML-EntitlementRef 屬性新增至驅動程式過濾器。若要這樣做，請執行下列動作：

1. 選取 「*Identity Manager*」 >「*Identity Manager* 概觀」。
2. 瀏覽至驅動程式所在的驅動程式集，然後按一下 「搜尋」。

3. 在「Identity Manager 概觀」畫面中，從呈現的「驅動程式集」中選取「驅動程式」物件。

4. 從「驅動程式集」連按兩下驅動程式，以帶出驅動程式畫面。按一下 Identity Vault 右側的「驅動程式過濾器」圖示 (紅圈者)。



5. 在「過濾器」頁面上，選取「新增屬性」，然後捲動至底部，選取「顯示所有屬性」。選取「*DirXML-EntitlementRef*」屬性，然後按一下「確定」。

6. 選取 「過濾器」頁面中的 「*DirXML-EntitlementRef*」。在 「訂閱者」標題下，選取 「通知」。按一下 「確定」。

7. 當您透過驅動程式上的 Designer 建立授權時，此程序會自動執行。

6.3 授權先決條件

- ❑ eDirectory 8.7.3 或更新版本
- ❑ Identity Manager 2 或 3
- ❑ 「授權服務」驅動程式

  要使用授權的每個驅動程式集中，都必須有 「授權服務」驅動程式。這需要爲每個驅動程式集做簡易的一次性設定。
- ❑ 支援授權的驅動程式組態

  在搭配使用授權與已連接系統之前，請進行下列其中一項操作：
  - 輸入驅動程式的 Identity Manager 驅動程式組態，並指定該驅動程式已啓用授權。
  - 啓用驅動程式以支援授權。若要這樣做，請執行下列動作：
    a. 使用 iManager 或 Designer (偏好使用 Designer) 建立授權。
    b. 將 DirXML-EntitlementRef 屬性新增至驅動程式過濾器，如 「在其他 Identity Manager 驅動程式上啓用授權」，第 149 頁中所述。
    c. 寫入規則，以實作您在 「步驟 1」中建立的授權。

6.4 透過 iManager 以 XML 格式寫入授權

爲協助您更加瞭解授權的相關內容，可在其中一個預先設定組態的驅動程式 (即已啓用授權的 Active Directory (AD)) 中查看授權和規則。這包含檢查 Novell 的授權文件類型定義 (Document Type Definition，DTD)，然後查看根據 DTD 寫入授權的 XML 範例。

本節內容：

6.4.1 Active Directory 驅動程式在授權啓用時新增的內容

已啓用授權的 AD 驅動程式包含下列結構變更：

- 將 DirXML-EntitlementRef 屬性新增至驅動程式過濾器。DirXML-EntitlementRef 屬性可讓驅動程式過濾器監聽授權活動。
- 建立使用者帳戶授權。「使用者帳戶」授權會針對使用者授予或撤銷 Active Directory 中的帳戶。當授予帳戶時，使用者會得到已啓用的登入帳戶。當撤銷帳戶時，視驅動程式組態設定方式停用或刪除登入帳戶。
- 建立群組成員資格授權。「群組授權」會授予或撤銷 Active Directory 中群組的成員資格。該群組必須與 Identity Vault 中的群組相關聯。當撤銷成員資格時，會從群組中移除使用者。群組成員資格授權不是在「發行者」通道上強制執行的。如果透過某些外部工具將使用者新增至 Active Directory 中的控制群組，驅動程式就不會移除該使用者。此外，如果從使用者物件移除授權，而不是只撤銷授權，則 AD 驅動程式不會採取任何動作。
- 建立 Exchange 信箱授權。「群組授權」會在 Microsoft Exchange 中授予或撤銷使用者的 Exchange 信箱。
- 將授權資訊新增至許多規則。

下列規則 (Policy) 包含可使授權正常運作的其他規則 (Rule)：

- InputTransform (驅動程式層級)。此規則 (Policy) 中的「檢查群組成員資格授權之新增關聯的目標」規則 (Rule) 會檢查用於群組成員資格授權之「新增關聯」的目標。除非該使用者已成功建立，否則無法處理指定給正在 Active Directory 中建立之使用者的群組成員資格授權。新增關聯表示，Active Directory 中的驅動程式已經建立物件。如果該物件也標示爲群組授權處理，它就會立即執行工作。
- 事件轉換 (「發行者」通道)。此規則 (Policy) 中的「不允許使用者帳戶刪除」規則 (Rule) 不允許使用者在 Identity Vault 中刪除使用者帳戶。當使用「使用者帳戶授權」時，受管理的使用者帳戶由 Identity Vault 中的授權來控制。Active Directory 中的刪除不會刪除 Identity Vault 中的控制物件。對 Identity Vault 中物件的未來變更或合併操作可能會重新建立 Active Directory 中的帳戶。
- 指令 (「訂閱者」通道)。「指令」規則 (Policy) 包含有關授權的下列規則 (Rule)：
  - 「使用者帳戶授權變更 (刪除選項)」規則。「使用者帳戶授權」會授予使用者已啓用的 Active Directory 帳戶。根據您爲「當撤銷帳戶授權時」全域變數所選取的值而定，撤銷授權會停用或刪除 Active Directory 帳戶。當授權變更且您已選取「刪除」選項時，會執行此規則。

- 「使用者帳戶授權變更 (停用選項)」規則。「使用者帳戶授權」會授予使用者已啓用的 Active Directory 帳戶。根據您爲「當撤銷帳戶授權時」全域變數所選取的值而定，撤銷授權會停用或刪除 Active Directory 帳戶。當授權變更且您已選取「停用」選項時，會執行此規則。
- 「檢查要授予或撤銷之群組成員資格的使用者修改」規則。
- 「檢查要授予或撤銷之 Exchange 信箱的使用者修改」規則。

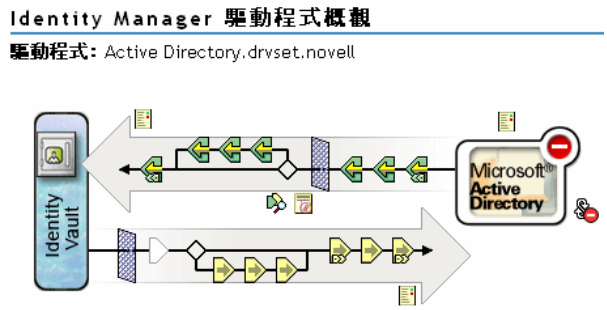
- 相符 (「訂閱者」通道)。這是「帳戶授權」：此規則 (Policy) 的「不符合現有帳戶」規則 (Rule)。當搭配使用「使用者帳戶」授權與 Identity Manager 使用者應用程式或「角色授權」時，帳戶是透過授予或撤銷授權來建立和刪除 (或停用)。如果使用者沒有 Active Directory 中帳戶的授權，則預設規則會與 Active Directory 中的現有帳戶不相符。如果您想要將授權規則套用至 Active Directory 中的相符帳戶，請修改或移除此規則。這可能會導致刪除或停用 Active Directory 帳戶。
- 建立 (「訂閱者」通道)。「建立」規則 (Policy) 包含有關授權的下列規則 (Rule)：
  - 帳戶授權：未授予授權時封鎖帳戶建立。當搭配使用「使用者帳戶」授權與 Identity Manager 使用者應用程式或「角色授權」時，僅會針對專門授予帳戶授權的使用者建立帳戶。在未授予授權時，此規則會否決使用者帳戶的建立。
  - 如果停用的帳戶不存在，則啓用 Identity Vault 帳戶。
  - 準備在新增之後檢查群組授權。因爲新增的物件必須存在以新增至群組，所以會在新增完成之後處理群組授權。當新增處理完成時，會以輸入轉換中核取的操作內容來對新增設旗標。
  - 發出在新增之後檢查 Exchange 授權的需求。
  - 將使用者名稱映射至 Windows 登入名稱。在設定 userPrincipalName 組態以遵循 eDirectory 使用者名稱時，請將 userPrincipalName 設爲 eDirectory 物件名稱加上 Active Directory 領域的名稱。

藉由在 iManager 中執行下列步驟，您可以查看每個規則實際的 XML 碼：

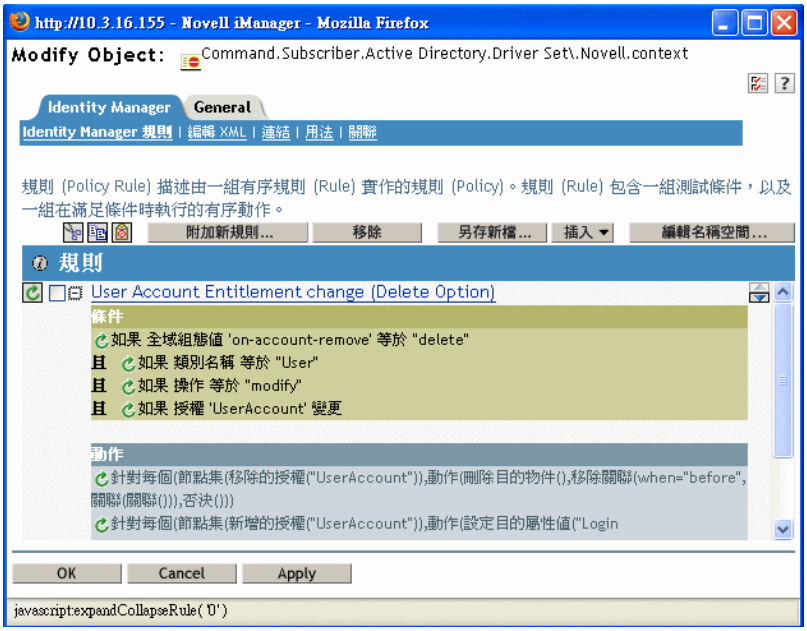
1. 選取「*Identity Manager*」>「*Identity Manager* 概觀」。
2. 瀏覽至驅動程式所在的驅動程式集，然後按一下「搜尋」。

3. 在「Identity Manager 概觀」頁上，從呈現的「驅動程式集」中選取「驅動程式」物件。

4. 從「驅動程式集」連按兩下驅動程式，以載上驅動程式頁面。按一下驅動程式中心 (以紅色線圈住) 的「檢視所有規則」圖示。

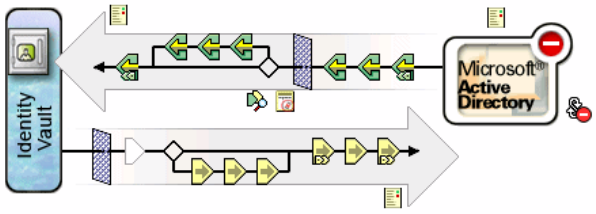


5. 從 「顯示所有規則」螢幕中選取規則之後，您可以檢視組成規則的條件和動作。



6. 若要檢視規則後面實際的 XML 碼，請從下拉式功能表 (此功能表預設爲 「Identity Manager 規則」) 中選取 「編輯 *XML*」。如需建立和編輯規則的相關資訊，請參閱 《規則產生器和驅動程式自訂指南》，以及選定的 《Identity Manager 驅動程式指南 (http://www.novell.com/documentation/dirxmldrivers/index.html)》，以建立該驅動程式特定的規則。

7. 若要檢視已啓用授權之預先設定驅動程式 (我們的範例是 Active Directory) 附帶的授權，請遵循步驟 1 至步驟 4。但是，請選取驅動程式中心 (以紅色線圈住) 的 「檢視所有授權」圖示。



8. 在 「管理授權」頁上，按一下授權名稱以在 XML 檢視器中載上授權。若要編輯授權的代碼，請按一下 「啓用 *XML* 編輯」。

已啓用授權的 Active Directory 驅動程式附帶三種授權：「使用者帳戶」、「群組」和「Exchange 郵件」。

特性 ***6-1*** *AD* 驅動程式附帶的授權

您可以查看這些授權的 XML 碼，做爲「協助您建立自己授權的範例授權」，第 160 頁中書面範例的一部份。

6.4.2 使用 Novell 的授權文件類型定義 (DTD)

部份授權在已啓用授權的驅動程式上預先定義。您可以使用這些授權，或者可以在 iManager 或 Designer 中建立自己的授權。使用下列 Novell 的授權文件類型定義 (DTD) 做爲建立授權的範例，可以協助您建立自己的授權。

此文件類型定義 (DTD) 說明之後是四個範例，說明如何透過 iManager 使用此 XML 格式寫入授權。如果您不想要擔心 XML 格式的相關問題，請使用 Designer 的「授權精靈」以一種更簡單的方式建立授權。

Novell 的授權文件類型定義 (DTD)

```
<!-********************************************************************->
<!-- DirXML Entitlements DTD <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a DirXML-
Entitlement object. --> <!ELEMENT entitlement (values?)> <!ATTLIST
entitlement conflict-resolution (priority | union) "priority" display-
name CDATA #REQUIRED description CDATA #REQUIRED > <!ELEMENT values
(query-app | value+)?> <!ATTLIST values multi-valued (true | false)
"true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app (query-xml,
result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set (display-
name, description, ent-value)> <!ELEMENT display-name(token-attr |
token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attribute of
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!-- Entitlement
```

```
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object. --> <!ELEMENT result(dn, src, id?,
param?, state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)>
<!ELEMENT state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg
ANY> <!ELEMENT timestamp (#PCDATA)> <!-- Cached query results stored
in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.
--> <!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!-- Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document. --> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 授權文件類型定義 (DTD) 說明

授權文件類型定義 (DTD) 分爲五個部份：定義、參考、結果、快取查詢和內部參考資訊。標題僅是備註，且是選擇性的。在文件類型定義 (DTD) 中，「授權定義」的標題是：

<!-- Entitlement definition stored in the XmlData attribute of a DirXML-Entitlement object. -->

標題後面是「元素 (ELEMENT)」和「屬性清單 (ATTLIST)」。以下是位於「授權定義」標題下面之元素和屬性的詳細說明。「授權定義」標題是您在建立授權時要特別注意的主要標題。

<!ELEMENT entitlement (values?)>

根層級元素是 <entitlement>，其可以包含單一、選擇性的子 <values> 元素。後面是「屬性」清單包含 conflict-resolution、display-name 和 description。衝突解析使用 Priority 或 Union 屬性值。

conflict-resolution (priority | union) "priority"

「角色授權」使用衝突解析來決定當多次將具值授權套用至相同的物件時，應該會發生的情況。例如，假設使用者 U 是「授權規則 A」和「授權規則 B」的成員，兩個規則都參考相同的具值授權 E，但是具有不同的值集。「授權規則 A」的授權 E 具有值 (a、b、c)。「授權規則 B」的授權 E 具有值集 (c、d、e)。

衝突解析屬性決定使用者 U 應該套用的值集。如果設爲 union，則會將兩個值集 (a、b、c、d、e) 都指定給使用者 U。如果設爲 priority，則根據優先程度較高的「授權規則」而定，使用者 U 僅會取得一個值集。

因爲值的集合會導致套用多個值，所以如果授權是單一值，則必須依 priority 解析衝突。目前，「角色授權」使用此屬性，而在以後，「工作流程授權」可能也會使用該屬性。

display-name CDATA #REQUIRED description CDATA #REQUIRED

授權不一定會顯示文字授權名稱。Display-name 和 Description 屬性用於一般使用者顯示 (在 Designer 中，您可以選擇授權的顯示名稱，而不需要使用實際的授權名稱)。

<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued (true | false) "true"

<values> 元素是選擇性的，表示是具值授權。如果您不使用此元素，則表示是無值授權。具值授權的範例是會授予配送清單的授權。無值授權的範例是在應用程式中授予帳戶的授權，例如 Active Directory 驅動程式附帶的「使用者帳戶」授權。

具值授權從三個來源接收值。一個來源是外部應用程式 (由 <query-app> 元素指定)。. 另一個來源是列舉值預先定義的清單 (一或多個 <value> 元素)。第三個來源是授權用戶端 (不具有 <value> 子代的 <values> 元素)。這些範例對於說明值的工作方式而言很有用。

具值授權可以是單一值的或多值的，預設值是多值的。強制執行此限制是授權用戶端的職責。

<!ELEMENT value (#PCDATA)>

授權值是不具類型的字串。

<!ELEMENT query-app (query-xml, result-set)>

如果值來自外部應用程式 (例如，電子郵件配送清單)，則您必須透過 < query-xml> 元素指定應用程式查詢。並透過 <result-set> 元素從查詢中擷取結果。我們在「範例 2：應用程式查詢授權：外部查詢」，第 161 頁中顯示了兩個範例。

<!ELEMENT query-xml ANY>

XML 查詢是 XDS 格式的。<query-xml> 指令用於從已連接的應用程式中尋找和讀取物件。DirXML 規則、物件移轉等功能根據驅動程式對查詢指令實作的結果而定。如需 XML 查詢的相關資訊，請參閱 Novell 關於查詢的開發人員文件 (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)。

<!ELEMENT result-set (display-name, description, ent-value)> <!ELEMENT display-name(token-attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-association | token-src-dn | token-attr)> <!ELEMENT description (token-association | token-src-dn | token-attr)> <!ELEMENT token-association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED

使用結果集元素，可以協助您解譯外部應用程式查詢的結果。相關資料有三種：值的顯示名稱 (display-name 子元素)、值的描述 (description 子元素) 和不會顯示的文字授權值 (ent-value 子元素)。

記號元素 <token-src-dn>、<token-association> 和 <token-attr> 實際上是 XPATH 運算式的預留位置，它們分別從 XDS 格式的 XML 文件擷取 src-dn 屬性值、關聯值或任何屬性值。文件類型定義 (DTD) 假設查詢結果是 XDS。

文件類型定義 (DTD) 中的其他標題

授權文件類型定義 (DTD) 中其餘的授權標題具有不同的功能，但它們不是您在建立授權時需要特別注意的項目。

<!-- Entitlement reference stored in the DirXML-EntitlementRef attribute of a DirXML-EntitlementRecipient or a DirXML-SharedProfile object. -->

文件類型定義 (DTD)「授權參考」部份中儲存的資訊指向授權物件。此資訊由管理代辦 (例如「角色授權」驅動程式 Entitlement.xml 或「核准流程」驅動程式 UserApplication.xml) 置於該處。這是已連接系統中使動作發生的觸發事件。您不需要對此標題下的文件類型定義 (DTD) 執行任何動作，但是可以使用此資訊來確定正在參考授權物件。

<!-- Entitlement result stored in the DirXML-EntitlementResult attribute of a DirXML-EntitlementRecipient object. -->

「授權結果」部份會報告授予或撤銷授權的相關結果。資訊包含事件的狀態，以及授予或撤銷事件的時間 (透過時戳)。您不需要對此標題下的元素和屬性執行任何動作。

<!-- Cached query results stored in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object. -->

「授權查詢」部份包含從外部應用程式蒐集的授權值。如果授權用戶端需要顯示此資訊，則可以再次使用此資訊。這些值儲存在 「授權」物件的 DirXML-SPCachedQuery 屬性中。您不需要對此標題下的元素和屬性執行任何動作。

<!-- Representation of a DirXML-EntitlementRef within the DirXML Script and within the operation-data of an operation in an XDS document. -->

因爲文件類型定義 (DTD) 定義多個文件的值，所以此 EntitlementRef 部份實際上不屬於「授權」定義。您不需要對此標題下的元素和屬性執行任何動作。

6.4.4 透過 Designer 建立授權

雖然「在 iManager 中建立和編輯授權」，第 159 頁中的範例顯示用於寫入授權的實際 XML 碼，但是寫入授權的一種更簡單的方法是使用 Identity Manager 隨附的 Designer 公用程式。將 Identity Manager 驅動程式新增至 Designer 模擬器中的 Identity Vault 之後，您可以從 「大綱檢視」中，在驅動程式上按一下滑鼠右鍵，並選取 「新增授權」。「授權精靈」會提示您指定想要的授權類型，然後精靈會指引您逐步完成建立程序。

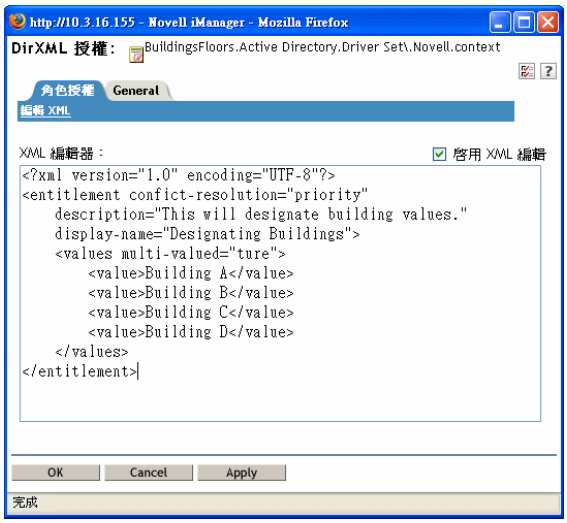
如需使用 「授權精靈」的相關資訊，請參閱 《Designer for Identity Manager 3：管理指南》。

6.4.5 在 iManager 中建立和編輯授權

雖然建議您使用 Designer 的 「授權精靈」來建立授權，但是您仍可以透過 iManager 建立授權。

1. 請選取 「Identity Manager 公用程式」標題下面的 「建立授權」選項。
2. 在 「建立授權」頁上，輸入想要的授權名稱，然後使用 「物件瀏覽器」尋找授權所屬的 「Identity Manager 驅動程式」物件。

3. 如果選取「定義額外的內容」，您會看到「XML 編輯器」頁，您可以在該頁針對此授權定義想要的元素。



4. 核取「啓用 XML 編輯」，以將元素新增至授權。

附註：不建議您變更授權的名稱。如果您稍後變更授權名稱，還需要變更規則中實作授權的所有參考。授權名稱儲存在規則內的 Ref 和 Result 屬性中。

6.4.6 協助您建立自己授權的範例授權

您可以建立兩種類型的授權：無值授權和具值授權。具值授權可以從外部查詢、管理員定義的清單或自由格式取得值。下面是您可以建立的四種授權範例。

附註：如果您看到某行中沒有「小於號 (<)」，這表示此行已換行，資訊通常顯示在一行，而不是兩行 (或三行)。另請注意，這些只是您可以針對每種具值授權建立的範例，而不是「帳戶授權」。

範例 **1**：帳戶授權：無值

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="This is an Account Entitlement"
display-name="Account Entitlement"/>
```

在此範例中，無值授權的名稱是 Account。其後接衝突解析行，預設設定爲 Priority，表示在大部份情況下，如果授權用於「角色授權」，則會由優先程度高的 RBE 設定其值 (然而，因爲這是無值授權的範例，所以不會套用值設定)。「授權」描述是 This is an Account Entitlement，顯示名稱是 Account Entitlement。這是您建立「帳戶授權」所需的全部資訊，之後您可以使用該資訊來在應用程式中授予帳戶。

啓用授權的 Active Directory 驅動程式具有 UserAccount 授權，Active Directory 會使用該授權來授予或撤銷使用者帳戶。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
```

```
resolution="union" description="The User Account entitlement grants or
denies an account in ActiveDirectory for the user. When granted, the
user is given an enabled logon account.When revoked, the logon account
is either disabled or deleted depending on how the drive is
configured."display-name="User Account Entitlement"
name="UserAccount"> </entitlement>
```

在此範例中，衝突解析是 Union，這可讓授權合併已指定的值 (同樣，值設定也不會套用至無值授權)。「描述」欄位說明此授權的用途及其建立的原因。此資訊對於以後要修改授權的人員很有用。授權的實際名稱是 UserAccount，然而 <display-name> 在管理代辦中顯示爲「使用者帳戶授權」。

範例 **2**：應用程式查詢授權：外部查詢

已啓用授權之 Active Directory 驅動程式附帶的「群組」和「Exchange 信箱」授權提供應用程式查詢的範例。當您需要已連接系統的外部資訊以執行事件時，請使用此授權類型。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Group Entitlement grants or denies
membership in a group in Active Directory. The group must be associated
with a group in the Identity Vault. When revoked, the user is removed
from the group. The group membership entitlement is not enforced on the
publisher channel: If a user is added to a controlled group in Active
Directory by some external tool, the user is not removed by the driver.
Further, if the entitlement is removed from the user object instead of
being simply revoked, the driver takes no action."   display-
name="Group Membership Entitlement" name="Group"> <values> <query-app>
<query-xml> <nds dtd-version="2.0"> <input> <query class-name="Group"
scope="subtree"> <search-class class-name="Group"/> <read-attr attr-
name="Description"/> </query> </input> </nds> </query-xml> <result-
set> <display-name> <token-src-dn/> </display-name> <description>
<token-attr attr-name="Description"/> </description> <ent-value>
<token-association/> </ent-value> </result-set> </query-app> </values>
</entitlement>
```

在此範例中，如果將授權多次套用至相同的物件，「群組」授權會使用 Union 來解決衝突。Union 屬性會合併所有相關「角色授權」規則的授權，因此，如果一個規則撤銷授權，而其他規則授予授權，則最終會授予授權。

因爲「群組」描述很詳細，所以很有用，它會說明透過驅動程式規則 (Policy) 中的規則 (Rule) 所設定的項目。此描述是您在定義授權時首先需要瞭解之詳細資料很好的範例。

<display-name> 是「群組成員資格授權」，顯示在管理代辦中，例如「角色授權」的 iManager 中。該名稱是授權的相對可辨識名稱 (Relative Distinguished Name，RDN)。如果您未定義顯示名稱，則授權的名稱是它的相對可辨識名稱 (RDN)。

啓始查詢值會在網路樹的頂端尋找「群組」的類別名稱，並會繼續搜尋其子網路樹。這些值來自已連接的 Active Directory 伺服器，以及從 <nds> 標籤開始的應用程式查詢。在 <query-xml> 標籤下面，此查詢會接收到類似於下列內容的資訊：

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
<association>o=Blanston,cn=group1</association> <attr attr-
```

```
name="Description"> the description for group1</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
<association>o=Blanston,cn=group2</association> <attr attr-
name="Description"> the description for group2</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
<association>o=Blanston, cn=group3</association> <attr attr-
name="Description"> the description for group3</attr> </instance> <!--
... ->
```

然後，在 <result-set> 標籤下面，從查詢中接收到的資訊會填入各種欄位。例如，<display-name> 欄位會收到 o=Blanston,cn=group1。<description> 欄位會收到 the description for group1，而 <ent-value> 欄位會收到 o=Blanston,cn=group1。因爲有多個群組存在且滿足查詢條件，所以還會收集此資訊，並將其顯示爲其他例項。

附註：關聯格式值對於每個外部系統都是唯一的，每個查詢到之外部系統的格式和語法也不同。

另一個範例是「Exchange 信箱」授權。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Exchange Mailbox Entitlement
grants or denies an Exchange mailbox for the user in Microsoft
Exchange." display-name="Exchange Mailbox Entitlement"
name="ExchangeMailbox"> <values> <query-app> <query-xml> <nds dtd-
version="2.0"> <input> <query class-name="msExchPrivateMDB" dest-
dn="CN=Configuration," scope="subtree"> <search-class class-
name="msExchPrivateMDB"/> <read-attr attr-name="Description"/> <read-
attr attr-name="CN"/> </query> </input> </nds> </query-xml> <result-
set> <display-name> <token-attr attr-name="CN"/> </display-name>
<description> <token-attr attr-name="Description"/> </description>
<ent-value> <token-src-dn/> </ent-value> </result-set> </query-app> </
values> </entitlement>
```

在此範例中，如果將授權多次套用至相同的物件，「Exchange 信箱」授權會使用 Union 來解決衝突。Union 屬性會合併所有相關「角色授權」規則的授權，因此，如果一個規則撤銷授權，而另一個規則授予授權，則最終會授予授權。

description 指出授權會針對 Microsoft Exchange 中的使用者授予或撤銷 Exchange 信箱，並會足夠詳細地說明授權作業。display-name 是「Exchange 信箱授權」，顯示在管理代辦中，例如「角色授權」的 iManager 中。該名稱是授權的相對可辨識名稱 (Relative Distinguished Name，RDN)。如果您未定義顯示名稱，則授權的名稱是它的相對可辨識名稱 (RDN)。

啓始查詢值會尋找 msExchPrivateMDB 的類別名稱，這是 Microsoft Exchange 函式呼叫，它會在容器「組態」中開始尋找，並會繼續搜尋其子網路樹。這些值來自已連接的 Active Directory 資料庫，以及從 <nds> 標籤開始的應用程式查詢。類別 msExchPrivateMDB 在 eDirectory 中沒有等同項目，因此您需要熟悉 Microsoft Exchange 函式呼叫，以進行此類查詢。但是因爲在 Active Directory 驅動程式中找到規則 (Rule) 和規則 (Policy)，所以查詢完成。

授權消費者使用由查詢擷取的資訊。例如，授權值 (ent-value) 透過 DirXML-EntitlementRef 屬性傳遞至 Identity Manager 規則。顯示名稱和描述資訊由 iManager 或「使用者應用程式」顯示，並儲存在 DirXML-SPCachedQuery 屬性中。

範例 **3**：管理員定義的授權：包含清單

第三個範例是管理員定義的授權，它會在您選取清單項目之後建立授予或撤銷事件。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="This will show Administrator-defined
Values"> <display-name="Admin-defined Entitlement"/> <values multi-
valued="true"> <value>Building A</value> <value>Building B</value>
<value>Building C</value> <value>Building D</value> <value>Building
E</value> <value>Building F</value> </values> </entitlement>
```

在此範例中，授權名稱是管理員定義的，並具有「管理員定義的授權」的已定義顯示名稱 (如果您想讓顯示名稱與授權的相對可辨識名稱 (RDN) 不同，只需輸入顯示名稱)。衝突解析行顯示 Union 的設定，可讓授權合併已指定的值。

「授權」描述是「*This will show Administrator-defined Values*」。多值屬性設爲 true，可讓授權多次指定值。在此範例中，values 是公司建築字母：Building A 到 Building F。然後，使用者或定義任務的管理員可以透過授權用戶端 (例如 iManager RBE 任務) 或透過「使用者應用程式」，指定建築資訊，然後將此資訊包含在外部應用程式 (例如 Novell eDirectory) 中。

範例 **4**：管理員定義的授權：不包含清單

第四個範例是管理員定義的授權，它會強制管理員輸入值，然後授權才可以授予或撤銷事件。如果您不具有啓始設定的所有資訊，而因此無法建立任務清單，則可以使用此類型的授權。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="There will be no pre-defined list">
<values multi-valued="false"/> </entitlement>
```

在此範例中，授權名稱是「管理員定義的 (不含清單)」，因爲沒有顯示名稱項目，所以它會使用授權名稱做爲顯示名稱。衝突解析會重新設爲預設值 Priority，這表示如果授權用於「角色授權」，則會由優先程度高的 RBE 設定值。您可以透過授權用戶端 (例如 iManager RBE 任務) 或透過「使用者應用程式」，指定建築資訊，然後將此資訊包含在外部應用程式 (例如 eDirectory) 中。

6.4.7 完成建立授權步驟

授權建立範例已顯示如何執行建立和使用授權的前兩個步驟，如「建立授權：綜覽」，第 148 頁中所述。這包含步驟 1：針對您想要使用授權達成的項目製作核對清單，以及步驟 2：撰寫授權，以處理核對清單中的項目。步驟 3：建立 Identity Manager 驅動程式的規則；這已超出本章的範圍。如需建立和編輯規則的相關資訊，請參閱《規則產生器和驅動程式自訂指南》和適當的 Identity Manager 驅動程式指南 (http://www.novell.com/documentation/idmdrivers/index.html)。

在建立授權 (或使用某些 Identity Manager 驅動程式預先設定的授權) 之後，您現在需要對它們進行管理，此爲步驟 4。授權由兩個套件或代辦進行管理：透過 iManager 做爲「角色授權規則」，或透過工作流程提供中的「使用者應用程式」。如需工作流程提供中使用的授權，請參閱「工作流程提供簡介」。本章的其餘部份重點放在「角色授權」上。

6.5 管理角色授權綜覽

- 「授權服務驅動程式的運作方式」，第 164 頁

傳統上是針對每個驅動程式來管理已連接系統上的授權，並且唯一的方式是建立並編輯驅動程式組態規則 (例如，使用「規則產生器」建立的此類規則)。在這種傳統分散式模型中，不同的管理員常常控制各自的 Identity Manager 驅動程式和已連接系統，而且決定使用者能否在該系統上取得資源的業務規則，會分別「硬式編碼」至每個已連接系統驅動程式的驅動程式組態規則中。

「角色授權」模型適合於一或多個管理員具有控制授權規則權限的環境。這樣的管理員需要大致瞭解 Identity Manager，但不需要太多 Identity Manager 或 XSLT 或 DirXML 程序檔的專門知識，即可使用「角色授權」介面。

「角色授權」規則可讓您在符合準則時自動授予或撤銷商務資源。授權類似於存取資源的許可憑單。利用許可憑單，您可以存取指定的資源；如果沒有此類許可憑單，您就沒有存取權限。舉一個工作範例而言，您可以指定如果使用者符合準則 1、2 和 3，則透過「角色授權」規則，使用者會成爲「群組 H」的成員，但是如果使用者符合準則 4 和 5，則會成爲「群組 I」的成員。

管理「角色授權」的設定是含有三個步驟的程序：

1. 如果您尚未進行此項操作，請啓用 Identity Manager 驅動程式物件上的 DirXML-EntitlementRef 屬性，如「在其他 Identity Manager 驅動程式上啓用授權」，第 149 頁中所述。
2. 安裝「授權服務」驅動程式 (Entitlement.xml)，如「建立授權服務驅動程式物件」，第 165 頁 中所述。
3. 在 iManager 中建立「角色授權規則」，如「建立授權規則」，第 166 頁中所述。

6.5.1 授權服務驅動程式的運作方式

「角色授權」依賴於「授權服務」驅動程式 (Entitlement.xml)。此驅動程式是監看使用者是否具有「授權規則」中成員資格的引擎服務。如果使用者符合「授權規則」動態群組的動態成員資格準則，或以靜態方式包含在其中，則「授權服務」驅動程式會更新「使用者」物件上 DirXML-EntitlementRef 屬性中的資訊。

對於「支援授權且具預先設定組態的 Identity Manager 驅動程式」，第 148 頁中列出的系統，您可以在輸入 Identity Manager 驅動程式組態時啓用授權。Identity Manager 隨附了一些驅動程式，其預先設定組態已包含授權、實作授權的規則，以及啓用以監聽授權活動的驅動程式。然後，您可以檢視所提供的規則。這些規則會監看 DirXML-EntitlementRef 屬性並授予或撤銷授權，以支援授權。

僅當發生下列其中一種狀況時，「授權服務」驅動程式才會更新 DirXML-EntitlementRef 屬性：

- 您使用「重新評估成員資格」任務
- 您指定應該在網路樹哪一部份重新評估使用者
- 移動使用者
- 重新命名使用者
- 修改「授權規則」中用於成員資格的任何屬性

授權規則可讓您授予已連接系統上的授權和 Identity Vault 中的權限。已連接系統上的授權可以是下列任何一項：

- 帳戶
- 電子郵件配送清單中的成員資格
- 群組成員資格
- 已連接系統中相對應物件的屬性，已對其填入您指定的值
- 佈置
- 您自定的其他授權

在已啓用授權的驅動程式組態中，會顯示您可以使用授權建立的部份選項。

因爲每個驅動程式集使用一個 「授權服務」驅動程式，所以 「授權規則」只能管理該驅動程式集相關聯之伺服器上讀 / 寫或主複製本中的使用者。

「角色授權」規則功能是以 Identity Manager 爲基礎。因此，若要管理已連接系統，您必須正確安裝和設定 Identity Manager 驅動程式的組態，並安裝 Identity Manager 外掛程式。

此外，爲避免 「授權規則」指定與 Identity Manager 驅動程式組態之間可能的衝突，您應該瞭解業務規則，以及透過 Identity Manager 管理這些規則的方式。 「Identity Manager 授權規則」和驅動程式組態中的規則在管理屬性時，不應該重疊或發生衝突。

6.6 建立授權服務驅動程式物件

您需要 「授權服務驅動程式」物件，才能建立 「授權規則」。您必須針對每個驅動程式集建立一個 「授權服務驅動程式」物件。

如果沒有物件，則系統會在您按一下 「角色授權」角色和任務時提示您建立一個。

1 查看是否已具有 「授權服務」驅動程式。

在 iManager 中，按一下 「角色授權 > 角色授權」，然後選取驅動程式集。

- 如果出現 「無授權服務驅動程式」頁面，請繼續步驟 2，以建立 「授權服務驅動程式」物件。
- 如果出現含有 「授權規則」清單的 「角色授權」頁面，則您已具有 「授權服務驅動程式」物件。您無需完成此程序。請繼續進行 「建立授權規則」，第 166 頁。

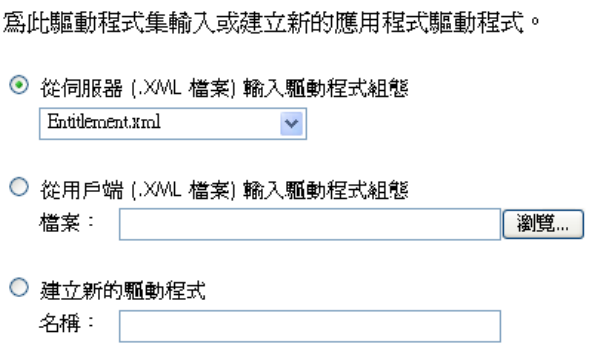
2 在 「無授權服務驅動程式」頁面中，按一下 「是」。

「建立驅動程式精靈」即會開啓。

您也可以按一下 「*DirXML* 公用程式 > 輸入驅動程式」。

3 在 「建立驅動程式精靈」頁面中，選取 「在現有的驅動程式集中」，然後按 「下一步」。

4 在「從伺服器 *(.XML 檔案)* 輸入驅動程式組態」下拉式清單中，選取 *Entitlement.xml*。



5 爲「授權服務驅動程式」物件命名 (或接受預設名稱)，然後按「下一步」。

系統會自動選擇正確的驅動程式組態檔案。您只需爲「驅動程式」物件指定一個名稱，或使用預設名稱。

6 建議您定義安全性等值並排除管理角色。將使用者 Admin 新增至這兩個選項，然後按「下一步」。

7 檢視摘要，然後按一下「完成」。

按照預設，安裝 Identity Manager 時，也會安裝「授權驅動程式」的驅動程式 Shim。在預設情況下，於 iManager 伺服器上安裝 Identity Manager 外掛程式時，會安裝「授權驅動程式」組態檔案。

完成「精靈」之後，您可以存取「授權」的外掛程式，並開始建立此驅動程式集的「角色授權規則」。

6.7 建立授權規則

- 「定義授權規則的成員資格」，第 168 頁
- 「選擇授權規則的授權」，第 169 頁

若要建立「授權規則」，您可以使用所提供的精靈。

1 確定已設定「授權服務驅動程式」，並已建立所需的驅動程式組態。

2 在 iManager 中，按一下「角色授權 > 角色授權」。

3 選取驅動程式集。

每個驅動程式集都會有一個授權規則。

即會開啓現有「授權規則」的清單，與下圖中的頁面類似。如果您是第一次使用「角色授權」，則不會列出任何規則。

4 按一下「新增」。

「授權規則精靈」即會開啓。

5 遵循精靈中的步驟 1 至步驟 6，以建立新規則。如需精靈中每個步驟的相關資訊，請參閱線上說明。

5a 在步驟 1 中，提供規則的名稱和描述。

5b 在步驟 2 中，定義成員資格過濾器的搜尋參數。

5c 在步驟 3 中，藉由在搜尋準則中包含和排除成員，來定義靜態成員。

5d 在步驟 4 中，選取 Identity Manager 驅動程式，並提供要包含的授權。您已在「透過 iManager 以 XML 格式寫入授權」，第 151 頁中建立授權。按一下「新增驅動程式」，然後選取要新增的授權。

5e 在步驟 5 中，瀏覽您要此授權規則做爲其託管者的物件。

5f 在步驟 6 中，閱讀摘要，以確保授權規則會進行您想要的操作。如果是這樣，請按一下「完成」；如果不是，請按一下「上一步」。

6 建立授權規則後，會關閉「授權服務」驅動程式。按一下「重新啓動」，以完成會期。

6.7.1 定義授權規則的成員資格

與 Identity Manager 驅動程式類似，每個「授權規則」只能管理其指定伺服器上主複製本或讀 / 寫複製本中的物件。每個「授權規則」都與指定給特定伺服器的單一「驅動程式集」物件相關聯。

只有「使用者」物件 (及其他衍生自「使用者」類別的物件類型) 可以是「授權規則」的成員。若要顯示「授權規則」的「成員資格」頁面，請選取「角色授權 > 角色授權」，然後將「授權規則清單」中您要編輯的「授權規則」反白，並選取「編輯」。在 Internet Explorer 瀏覽器中，選取「成員資格」索引標籤；在 Firefox 瀏覽器中，從下拉式功能表選取「編輯動態成員」。

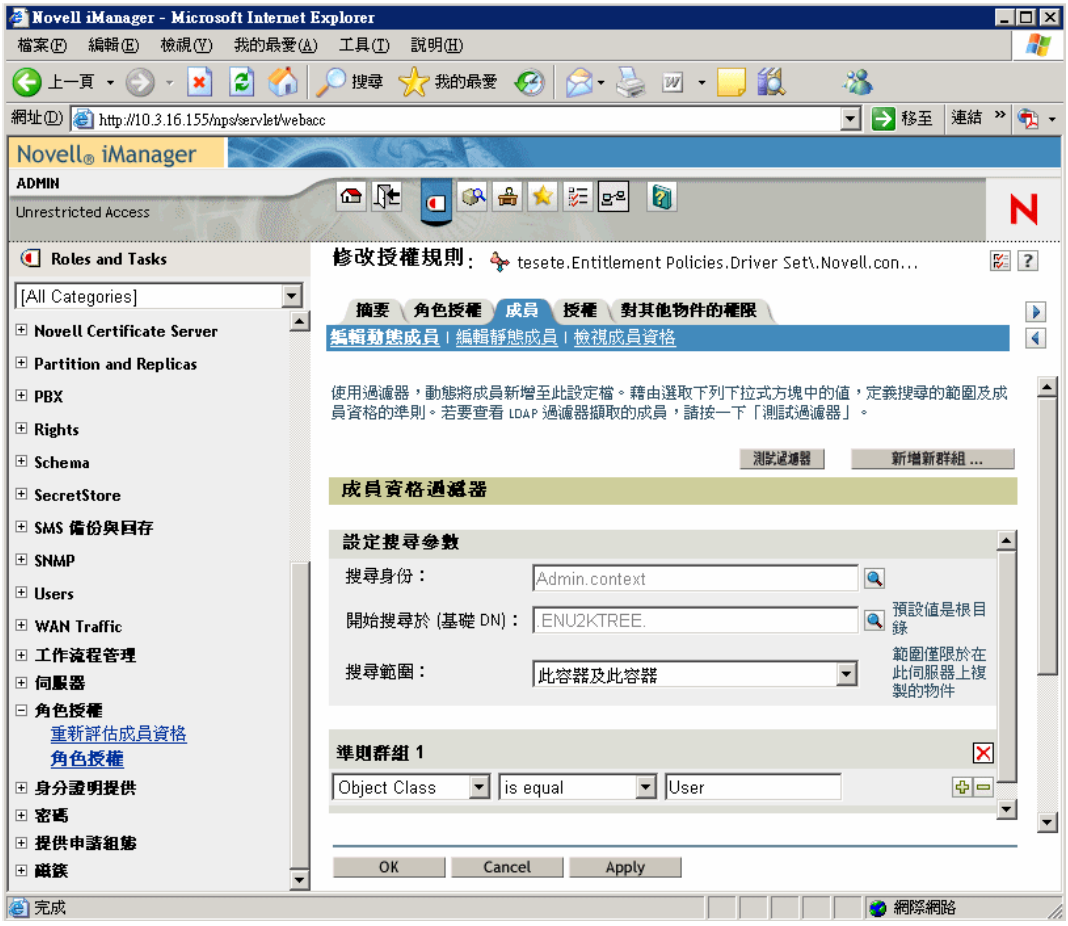
「授權規則」是動態的群組物件。您可以使用動態和靜態兩種方法，來定義「授權規則」的成員資格。您可以在同一「授權規則」中同時使用兩種方法。

- 動態： 您可以根據物件的屬性值，來定義成員資格的準則，例如，工作頭銜是否包含「管理員」一字。您指定的準則會轉換爲 LDAP 過濾器。

  符合該準則的使用者會自動成爲「授權規則」的一部份，而無需特別將每個使用者新增至規則。動態成員資格與「動態群組」物件相同。

如果某物件變更後不再符合動態成員資格的準則，則會自動撤銷授權。

特性 **6-2** 編輯動態和靜態成員



- 靜態： 除了建立動態成員資格的準則 (LDAP 過濾器) 之外，您還可以包含或排除特定的使用者。

  您可以靜態新增不符合過濾器準則的成員。您可以排除符合過濾器準則、但不應包含於「授權規則」中的成員。

6.7.2 選擇授權規則的授權

- 「已連接系統上的帳戶」，第 170 頁
- 「電子郵件配送清單和網路作業系統 (NOS) 清單中的成員資格」，第 171 頁
- 「已連接系統上的屬性值」，第 173 頁

授權可讓您授予或撤銷已連接系統上服務的存取權限和 Identity Vault 中的權限。

您在啓用授權後安裝的驅動程式隨附了授權清單，該清單可以使用「授權規則」加以指定。您可以建立自己的授權，以用於「授權規則」。驅動程式可以提供的授權是驅動程式的子物件，其由驅動程式開發人員建立，以代表驅動程式和已連接系統的功能。

Identity Vault 中物件的託管者權限會立即授予「授權規則」的成員。在預設狀態下，當下次針對使用者修改用於「授權規則」成員資格的屬性，或者將使用者移至其他容器或重新命名使用者時，會將已連接系統中的授權授予「授權規則」的每個成員。

已連接系統上的授權可以是下列任何一項：

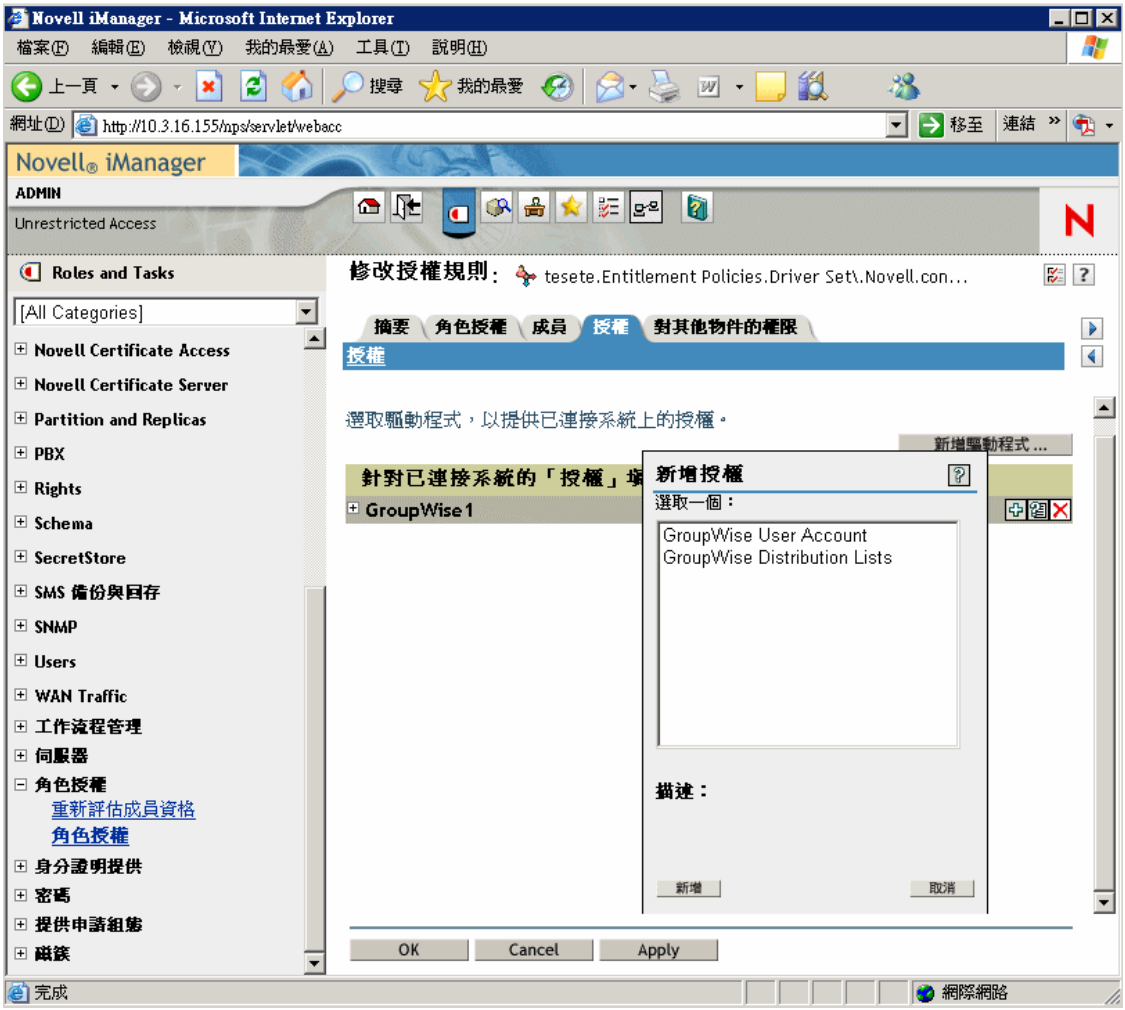
- 帳戶
- 電子郵件配送清單中的成員資格
- 網路作業系統 (Network Operating System，NOS) 清單中的群組成員資格
- 已連接系統中相對應物件的屬性，已對其填入您指定的值
- 您自定的其他授權

已連接系統上的帳戶

若要將授權新增至「授權規則」，請移至「授權」頁面並選取驅動程式。快顯視窗會顯示驅動程式提供的授權。

例如，在下圖中，您可以看到 GroupWise 驅動程式將提供的兩種授權，清單中的第一種授權是「GroupWise 使用者帳戶」。

特性 ***6-3*** 定義授權的介面



電子郵件配送清單和網路作業系統 **(NOS)** 清單中的成員資格

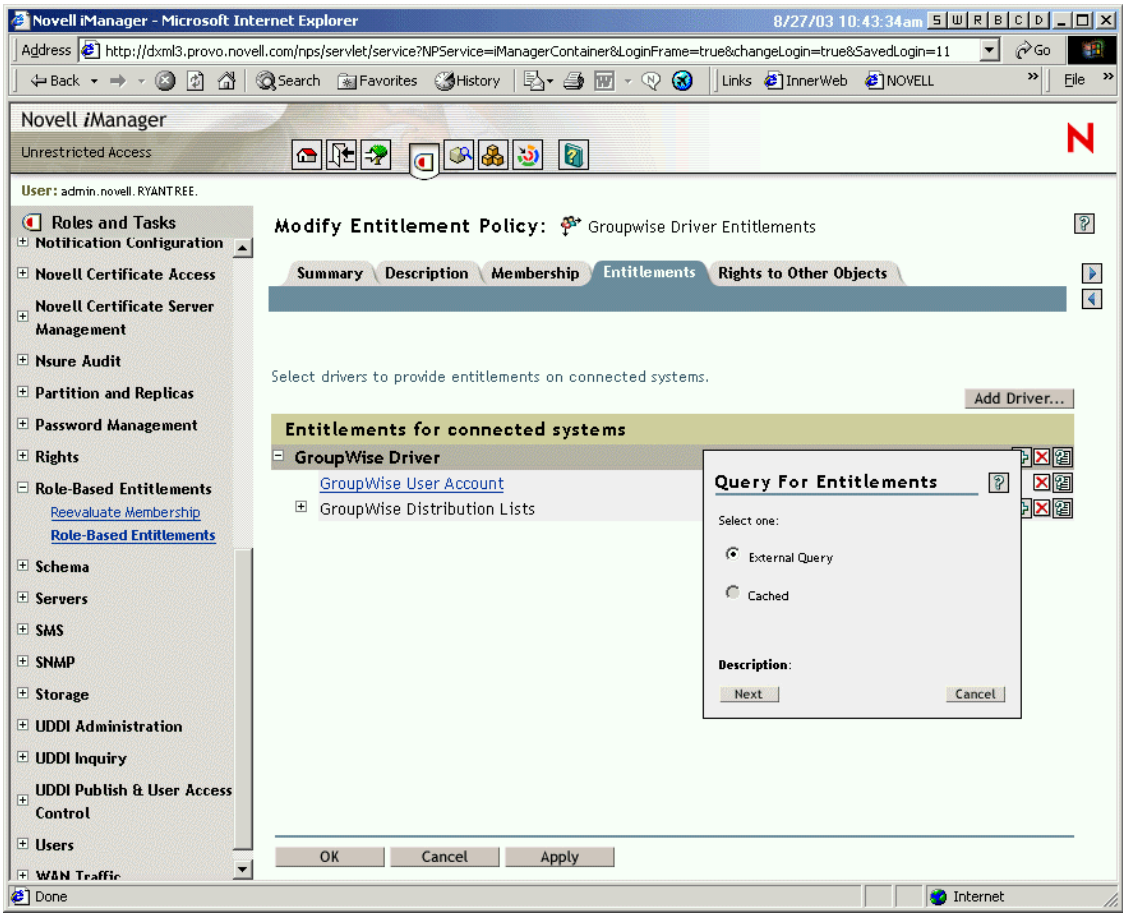
若要指定已連接系統上群組中的成員資格，請從驅動程式提供的授權清單中選擇成員資格授權。

下圖顯示一個範例，「GroupWise 配送清單」列在清單中的第二位。

特性 ***6-4*** 選取 *GroupWise* 配送清單

在此範例中，如果選擇 「*GroupWise* 配送清單」，則會顯示查詢快顯，如下圖中的範例所示。

特性 ***6-5*** 查詢授權



「授權規則」介面可讓您查詢電子郵件配送清單或網路作業系統 (NOS) 清單的清單。執行查詢之後，您可以選擇檢視快取清單。

驅動程式組態已設定爲傳回完整的清單，所以您可以在已連接系統上存在的清單中進行選擇。

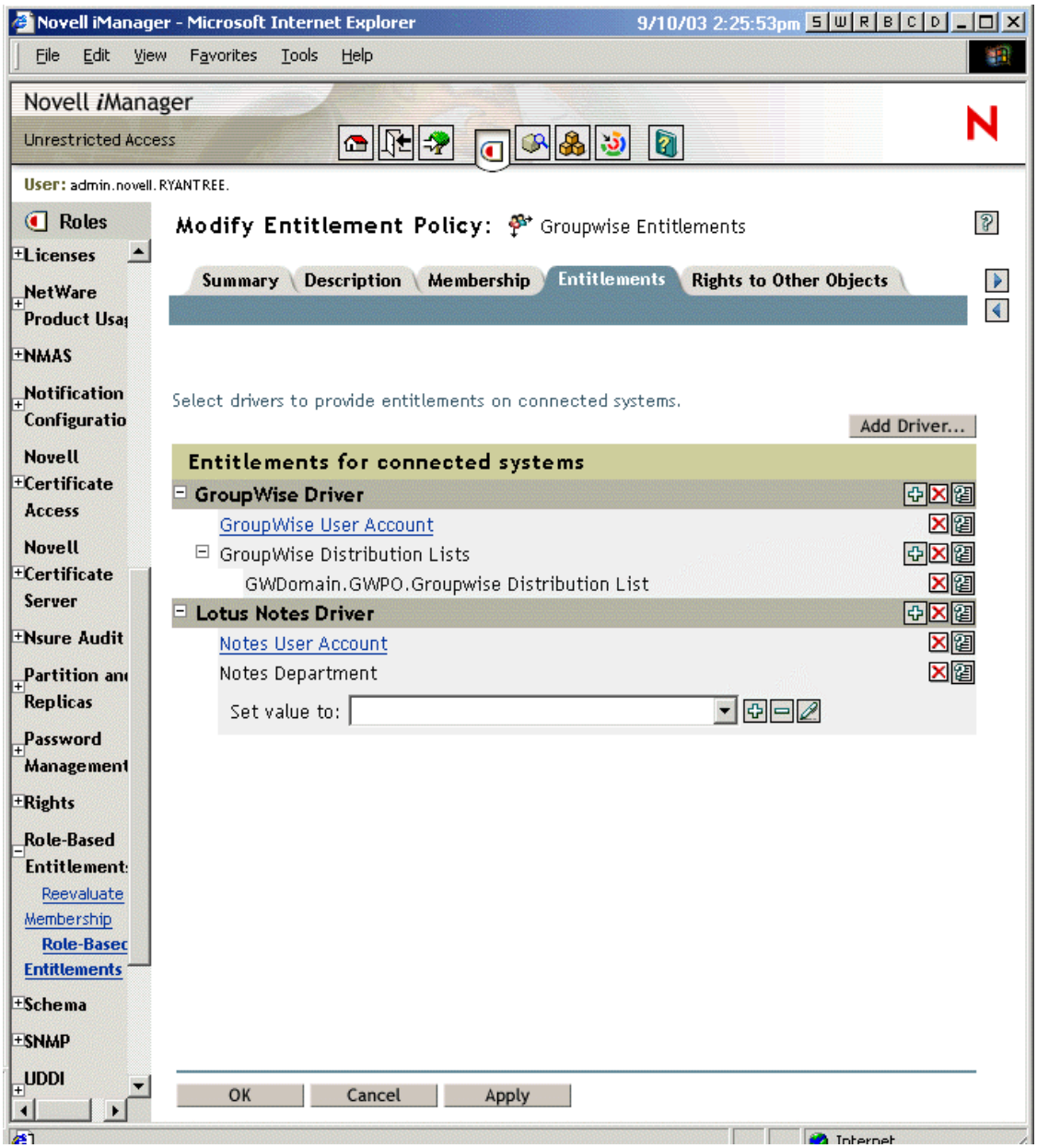
附註：您可以自定驅動程式，將清單限制爲只包含您指定的群組名稱，而非傳回完整清單的查詢。

已連接系統上的屬性值

您可以指定已連接系統上使用者帳戶的屬性值。該介面可讓您輸入想要使用者帳戶具有的值。

下圖顯示新增 Notes 屬性 Department 之屬性值的範例。

特性 ***6-6*** 新增屬性值



6.8 角色授權規則之間的衝突解析

- 「衝突綜覽」，第 175 頁
- 「變更個別授權的衝突解析方法」，第 176 頁
- 「設定授權規則的優先程度」，第 178 頁

6.8.1 衝突綜覽

當您建立「授權規則」時，影響特定使用者的多個規則在指定授權給該使用者時，可能會發生衝突。

以下是解析衝突的方式。您可以對某些授權變更衝突解析。

- 沒有值的授權是附加的。在大部份情況下，「帳戶」授權沒有值。如果有任何「授權規則」授予使用者一個已連接系統上的帳戶，則使用者會收到該系統上的帳戶。無論其他「授權規則」是否衝突，結果是累加的。

  這始終爲真；您無法變更授予帳戶之衝突解析的方法。

  您可以將沒有值的授權比喻爲燈的開關，開或關表示授予或不授予。

  例如，如果「管理員授權規則」授予 Jean Chandler 一個 Exchange 帳戶，但是已將 Jean Chandler 從亦授予 Exchange 帳戶的「收發室員工授權規則」中排除，則 Jean 仍會取得 Exchange 帳戶。

- 具有值的授權預設是累加的，但您可以選擇依優先程度來進行解析。授權 (如群組成員資格) 具有群組名稱清單做爲值，或具有帶值的屬性。在預設狀態下，這些類型的授權也會累加。

  必要的話，您可以變更這些類型之授權的衝突解析。

  在授權中定義控制每個授權之衝突解析的設定。驅動程式提供的每一種授權會分別列在資訊清單中。具有值的授權會具有針對每個授權分別設定的 conflict-resolution 屬性。預設設定爲 conflict-resolution="priority"。其他可能的值爲 conflict-resolution="union"。

  - **conflict-resolution="union" ---** 值爲 "union" 表示授權是累加的。授予使用者的授權包括任何規則中成員資格對使用者指定的所有授權。不同的授權僅僅是累加到一起，使用者會取得全部授權。

    例如，如果 Jameel 是「商展約聘規則」的成員 (該規則會授予名爲「商展郵寄清單」之 GroupWise 電子郵件配送清單中的成員資格)，但 Jameel 卻被從「商展管理員規則」(此規則亦指定名爲「商展郵寄清單」的電子郵件配送清單) 的成員資格中排除，則他仍會收到電子郵件配送清單中的成員資格。

    另一個範例是，如果「收發室規則」授予 Consuela「收發室員工」 AD 群組中的成員資格，並且「緊急自願者」規則還授予她「緊急回應」 AD 群組中的成員資格，則會授予 Consuela 兩個 AD 群組中的成員資格。

    此設定會讓規則清單中「授權規則」的順序對於授權而言不重要。

  - **conflict-resolution="priority" ---** 值爲 "priority" 表示，如果兩個不同規則中的值發生衝突，或者，如果一個規則包含某個使用者，而另一個規則排除該使用者，則授予該使用者的授權，只包括「授權規則」清單中具有較高優先程度之「授權規則」中的授權。

    先前的範例如果使用此設定，就會產生不同的結果。

    在以上 Jameel 的範例中，如果 GroupWise 電子郵件配送清單授權具有值 "priority"，並且在清單中「商展管理員規則」的優先程度高於「商展約聘規則」，則不會授予 Jameel「商展郵寄清單」中的成員資格。

    在以上 Consuela 的範例中，如果 AD 網路作業系統 (NOS) 群組成員資格授權具有值 "priority"，並且在清單中「收發室規則」的優先程度高於「緊急自願者規則」，則只會授予 Consuela「收發室員工」群組中的成員資格。因爲衝突解析是依優先程度而非累加式，所以不會授予她「緊急回應」群組中的成員資格。

在某些情況下，此功能很有用，例如，您設定環境的組態爲使用「角色授權」，將使用者置於其他系統的階層式結構中。您可能想要將使用者置於其中一個位置，而非同時置於兩個位置中。

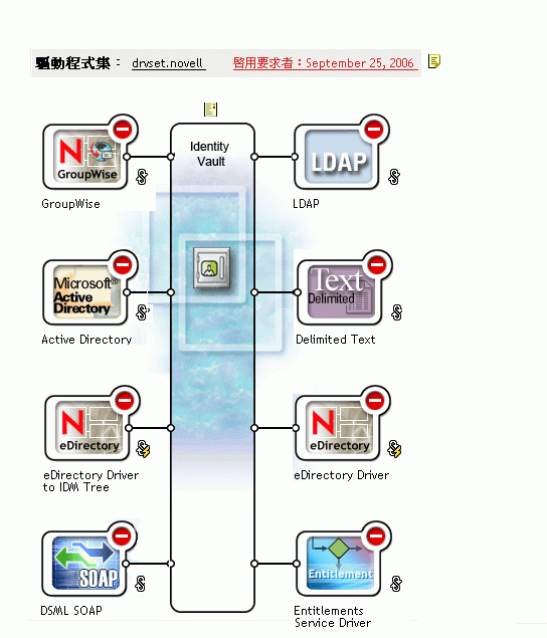
請記住，每個驅動程式提供的每個授權之設定都是獨立的。

一般而言，如果使用 "priority" 設定，則應在清單中將管理員規則置於一般使用者或個別顧問規則之上。您應該將成員資格較爲嚴格的群組，置於成員資格較爲寬鬆的群組之上。

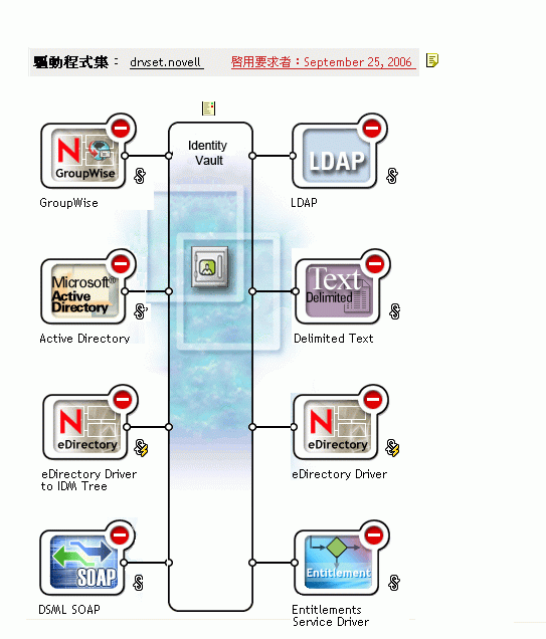
6.8.2 變更個別授權的衝突解析方法

1 在 iManager 中，按一下「*Identity Manager* > *Identity Manager* 概觀」，然後選取驅動程式集。

即會顯示含有驅動程式集中所有驅動程式之圖形化表示的頁面。



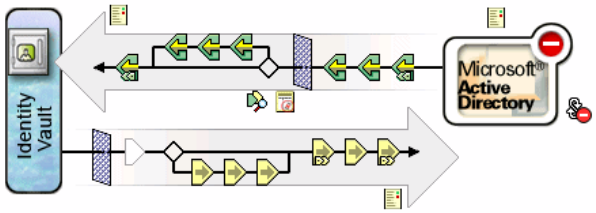
特性 **6-7** 驅動程式集



2 按一下「驅動程式」狀態按鈕，然後選取「停止驅動程式」。

3 按一下提供您要變更之授權的驅動程式圖示。

即會出現一個頁面，顯示驅動程式規則和驅動程式的圖示。在螢幕中間選取「檢視所有授權」圖示 (標有紅色圓圈)。



4 在「管理授權」頁面上，按一下授權名稱，以在 XML 檢視器中顯示授權。

5 選取「啓用 *XML* 編輯」核取方塊。

6 在 XML 中，尋找您要變更之授權的定義。

以下是您應尋找之指令行的範例：

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
Distribution Lists" name="gwDistLists">
```

7 變更 conflict-resolution 值。兩個可能的值如下：

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

如需這些值的相關資訊，請參閱「角色授權規則之間的衝突解析」，第 174 頁。

8 按一下「重新啓動」，以重新啓動「授權服務」驅動程式。

6.8.3 設定授權規則的優先程度

在預設狀態下，「授權規則」清單的順序無關緊要。這是因爲 Identity Manager 隨附的驅動程式組態使用 conflict-resolution="union"，做爲每個授權的衝突解析方法。

如果您將任何授權變更爲 conflict-resolution="priority,"，則「授權規則」清單的順序會變得重要，但只適用於已變更的那些授權。如需這些值的相關資訊，請參閱「角色授權規則之間的衝突解析」，第 174 頁。

您可以使用「授權規則」清單旁邊的箭頭按鈕，來變更「授權規則」的順序。清單中的第一個規則具有最高的優先程度。

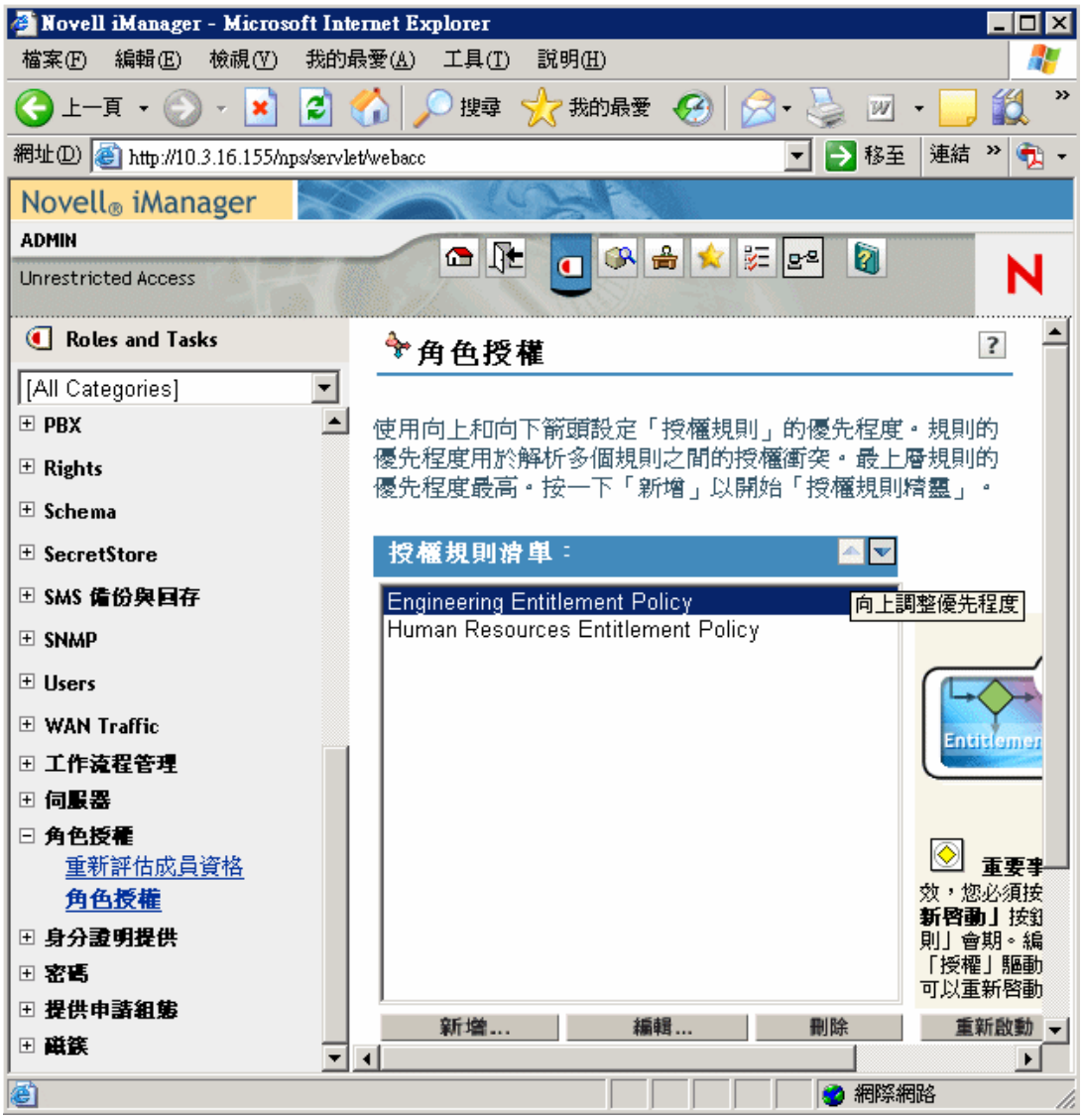
1 在 iManager 中，按一下「角色授權 > 角色授權」。

2 搜尋並選取驅動程式集。

即會出現含有「授權規則」清單的頁面。

3 藉由使用箭頭按鈕上下移動清單中的規則，來變更「授權規則」的優先程度。

將清單中的「授權規則」上移，可使其優先程度更高。



4 按一下「關閉」，以重新啟動驅動程式。

在重新啟動驅動程式之後，對優先程度的變更才會生效。

6.9 疑難排解角色授權

疑難排解時，請記住下列問題：

- 當在列出規則的頁面上按一下「新增」、「編輯」或「移除」，對規則進行任何變更時，「授權服務驅動程式」會停止。只有在該頁面上按一下「重新啟動」後，該驅動程式才會重新啟動。

  在未完成規則變更時，此功能可防止驅動程式授予或撤銷您生產環境中的授權。
- 同樣地，如果顯示有多人同時在編輯「授權規則」，則不會啟動「授權服務驅動程式」。

- 由於每個驅動程式集使用一個「授權服務驅動程式」，因此「授權規則」只能管理該驅動程式集相關聯之伺服器上讀 / 寫或主複製本中的使用者。

6.10 適用於角色授權和工作流程提供授權的授權元素

以下資訊適用於所有授權，而非特定的實作。

- 「控制授予或撤銷授權的意義」，第 180 頁
- 「防止資料遺失」，第 180 頁
- 「密碼同步化和授權」，第 181 頁

6.10.1 控制授予或撤銷授權的意義

您可以控制授予或撤銷授權的結果。每個驅動程式都提供控制「授予」或「撤銷」意義之支援選項的清單。

例如，在新增 GroupWise 帳戶時，您可以指定授予實際上是表示，授予使用者處於停用狀態的帳戶，如此一來，管理員必須進行干預，使用者才能存取該帳戶。或者，也可以選擇啓用該帳戶 (此爲預設值)。

在預設狀態下，驅動程式組態會使用最有可能保留資料的選項。例如，對於 GroupWise 帳戶，將移除的預設意義設爲「停用」，可以避免因管理員在變更規則時失誤而導致無意中遺失帳戶。另一個範例是，Identity Manager 驅動程式組態不會撤銷具有其他系統中使用者帳戶值的授權。如果授予使用者電子郵件配送清單中的成員資格，而稍後該使用者不再符合「授權規則」的準則，則只會將其從規則成員資格中刪除。雖然帳戶已停用，但不會移除群組成員資格和屬性值。如果您想要不同的結果，則 Identity Manager 專家可以自定驅動程式組態。

因爲「角色授權」功能可讓您在生產環境中對組織授權進行大規模變更，而無需在實驗室中測試結果，所以對撤銷授權的解釋尤爲重要。

藉由在預先設定組態的驅動程式上編輯「全域組態變數」，可以變更用於解釋授予或撤銷的設定。如果您是在建立自己的自定組態，則可以新增全域組態值 (GCV) 以解釋授予和撤銷授權。

6.10.2 防止資料遺失

「角色授權」是設計用來讓您根據規則中的成員資格，對授權 (例如帳戶) 進行大規模變更。然而，這意味著需要注意變更規則時發生的失誤。Identity Manager 隨附的驅動程式組態會使用最良性的設定。您應該瞭解如何使用全域組態值 (GCV) 來避免無意的資料遺失。

例如，建議您永不使用 delete，做爲解釋撤銷帳戶授權之全域組態值 (GCV) 的值。

在您編輯或建立新授權規則時保護資料的另一個方法是，關閉驅動程式，以便在未完成編輯規則操作時不進行任何變更。完成後，使用「授權規則」介面中的「重新啓動」按鈕，即可手動重新啓動驅動程式。同樣地，如果另一個使用者正在編輯「授權規則」，而您嘗試使用「重新啓動」按鈕重新啓動「授權服務」驅動程式，則會提示您不要重新啓動驅動程式，直到另一個使用者完成變更爲止。

6.10.3 密碼同步化和授權

對於使用「角色授權」的驅動程式，管理「密碼同步化」的方式與其他驅動程式相同，如「已連接系統間的密碼同步化」，第 69 頁中所述。

安全性：最佳作法

7

7.1 使用 SSL

爲所有傳輸啓用保全插槽層 (SSL) (如果可用的話)。爲 Metadirectory 引擎與 「遠端載入器」之間的通訊啓用保全插槽層 (SSL) (請參閱 「提供安全資料傳送」，第 43 頁)，以及爲 Metadirectory 引擎或 「遠端載入器」與已連接系統之間的通訊啓用 SSL。

如果未啓用保全插槽層 (SSL)，則會開放式地傳送資訊 (例如密碼)。

7.2 設定存取的安全性

務必設定對 Identity Vault 和 Identity Manager 物件存取的安全性。

實體安全性。 對於安裝 Identity Vault 的伺服器，保護其實體位置的存取安全性。

存取權限。建立 Identity Manager 物件和設定驅動程式組態都需要管理權限。監看和控制具有建立或修改下列項目之權限的人員：

- Identity Manager 驅動程式集
- Identity Manager 驅動程式
- 驅動程式組態物件 (過濾器、樣式表、規則)，尤其是用於取回或同步化密碼的規則
- 密碼規則物件 (和用於編輯這些物件的 iManager 任務)，因爲它們控制相互同步化哪些密碼，以及使用哪些 「密碼自助服務」選項

7.3 管理密碼

當您選擇在已連接系統之間交換資訊時，應小心確保交換是安全的。對於密碼而言更是如此。

- 「密碼提示」屬性 (nsimHint) 也是可公開讀取的，以允許忘記密碼的未經驗證使用者存取自己的提示。 「密碼提示」有助於減少 Help Desk 的電話。

  爲了安全起見，系統會檢查 「密碼提示」以確保其中不包含使用者的實際密碼。然而，使用者仍可能建立含有過多密碼相關資訊的 「密碼提示」。

  若要增加使用 「密碼提示」時的安全性，請執行下列動作：

  - 只允許在用於 「密碼自助服務」的 LDAP 伺服器上存取 nsimHint 屬性。

- 需要使用者先回答「處理安全問題」，然後才能收到「密碼提示」。
- 提醒使用者建立只有使用者本人能理解的「密碼提示」。密碼規則中的「密碼變更訊息」即爲這樣一種方式。請參閱《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「新增密碼變更訊息」。

如果您選擇根本不使用「密碼提示」，請確定不會在任何密碼規則中使用它。若要防止設定「密碼提示」，您可以進一步完全移除「提示設定」顯示裝置，如《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》的「移除提示顯示裝置以停用密碼提示」中所述。

- 「處理安全問題」是可公開讀取的，以允許忘記密碼的未經驗證使用者以另一種方法進行驗證。因爲使用者必須先提供正確的回應以證明其身份，才能收到忘記的密碼或「密碼提示」，所以要求「處理安全問題」可增加「忘記密碼自助服務」的安全性。

  由於系統會爲「處理安全問題」強制執行帳戶鎖定狀態設定，所以侵入者嘗試失敗的次數是受到限制的。

  然而，使用者可以建立保留密碼線索的「處理安全問題」。提醒使用者建立只有使用者本人能理解的「處理安全問題」和「回應」。密碼規則中的「密碼變更訊息」即爲這樣一種方式。請參閱《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》中的「新增密碼變更訊息」。
- 爲了安全起見，只有在您需要使用者回答「處理安全問題」時，才能使用「忘記密碼」動作：「將密碼以電子郵件傳送至使用者」和「允許使用者重設密碼」。
- 針對由管理員變更的「通用密碼」，已將安全性增強功能新增至 NMAS™ 2.3.4。其運作方式在本質上與先前提供給「NDS® 密碼」的功能相同。

  如果管理員變更使用者的密碼 (例如，在建立新使用者或回應 Help Desk 呼叫時)，則當您已啓用使密碼規則中的密碼過期的設定時，密碼會自動過期。密碼規則中的設定位於「進階密碼規則」中，名爲「密碼過期之前的天數 *(0-365)*」。對於此項特定功能，雖然天數並不重要，但是必須啓用該設定。

7.4 建立增強式密碼規則

密碼規則物件是可公開讀取的，以允許應用程式檢查密碼是否相符。這表示未經驗證的使用者可以查詢 Identity Vault，瞭解您所使用的密碼規則。如果您的密碼規則需要使用者建立增強式密碼，這不應該會造成風險，如《密碼管理管理指南 (http://www.novell.com/documentation/password_management/index.html)》的「建立增強式密碼規則」中所述。

「Identity Manager 密碼同步化」可讓您簡化使用者密碼，並減少 Help Desk 成本。雙向密碼同步化可讓您以多種方式在 eDirectory 與已連接系統之間共享密碼，如「實作密碼同步化」，第 100 頁的案例中所述。

使用「通用密碼」和密碼規則可讓您對使用者強制執行增強式密碼要求。使用密碼規則中的「進階密碼規則」，以遵循業界對密碼的最佳作法。

例如，您可以要求使用者密碼遵守下列規則：

- 需要唯一密碼。

  您可以防止使用者重複使用密碼，並控制系統應在歷程清單中儲存以供比較的密碼數目。
- 要求密碼的字元數不得少於某數目。

  要求較長的密碼是增強密碼的最佳方法之一。
- 要求密碼中至少需有幾個數字。

要求密碼中至少包含一個數值字元，有助於防止「字典攻擊」，即侵入者嘗試使用字典中的單字來登入。

- 排除您選擇的密碼。

  您可以排除您認爲有安全性風險的單字 (例如，公司名稱或地點)，或者單字 test 或 admin。雖然排除清單並非要您輸入整個字典中的單字，但是您排除的單字清單可能會很長。請記住，排除項目的清單太長會讓使用者登入速度緩慢。要求使用數字或特殊字元也許會是防止字典攻擊的更好方法。

請記住，如果您在網路樹的不同部份具有不同的密碼要求，則可以建立多個密碼規則。您可以將密碼規則指定至整個網路樹、分割區根容器、容器，甚至是個別使用者 (爲了簡化管理，我們建議您將密碼規則儘量指定至網路樹中的高層級)。

此外，您還可以使用帳戶鎖定狀態。此 eDirectory 功能始終可讓您指定在鎖定帳戶之前，允許的登入嘗試失敗次數。這是父容器上 (而非密碼規則中) 的設定。請參閱《*Novell eDirectory 8.7.3* 管理指南 (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv)》中的「管理使用者帳戶」。

7.5 設定已連接系統的安全性

請記住，您要同步化資料的已連接系統可能會以折衷的方式儲存或傳輸該資料。

請設定您要與其交換密碼之系統的安全性。例如，每個 LDAP、NIS 和 Windows 系統在啓用密碼同步化之前，都有您必須考量的安全性問題。

許多軟體廠商都會針對其產品提供您應遵循的特定安全性指示。

7.6 Designer for Identity Manager

在使用 Designer for Identity Manager 時，請考量下列問題：

- 監看和控制具有建立或修改 Identity Manager 驅動程式之權限的人員。

  建立 Identity Manager 物件和設定驅動程式組態都需要管理權限。

- 在將 Identity Vault 管理員密碼提供給顧問之前，請將指定給管理員的權限限制爲顧問必須存取的網路樹區域。
- 刪除專案檔案 (.proj)，或將其儲存至公司目錄。

  Designer .proj 檔案將保留在公司的專案網站上。顧問在完成專案之後不會取走這些檔案。

- 如果不再需要專案檔案、記錄檔案和追蹤檔案，請將它們刪除。
- 在丟棄或轉讓筆記型電腦之前，請驗證已清除專案檔案。
- 請確保從 Designer 到 Identity Vault 伺服器的連接實際上是安全的。

  否則，某些人可能會監看連接並獲取機密資訊。

- 使用「文件產生器」建立文件時，請謹慎操作文件。

  這些文件可能包含密碼和純文字的機密資料。

- 如果 Designer 需要讀取或寫入 eDirectory 屬性，請勿將該屬性標示爲加密。

  Designer 無法讀取或寫入加密屬性。

- 請勿儲存機密密碼。

目前，Designer 專案並未加密。只是對密碼進行了編碼。因此，請勿共享已儲存密碼的 Designer 專案。

若要儲存會期的密碼，但不將其儲存至專案，請執行下列動作：

a. 在展開的 「大綱」檢視窗中，在 Identity Vault 上按一下滑鼠右鍵。

b. 選取 「內容」。

c. 在 「組態」頁面上，輸入密碼，然後按一下 「確定」。

您可以針對每個會期輸入一次密碼。在結束專案之後，密碼會遺失。

若要將密碼儲存至硬碟，請完成步驟 1-3，選取 「儲存密碼」，然後按一下 「確定」。

特性 ***7-1*** 儲存密碼

7.7 安全性的產業最佳作法

請遵循安全措施的產業最佳作法，例如，封鎖伺服器上未使用的連接埠。

7.8 追蹤機密資訊的變更

- 「使用 iManager 記錄事件」，第 186 頁
- 「使用 Designer 記錄事件」，第 188 頁

7.8.1 使用 iManager 記錄事件

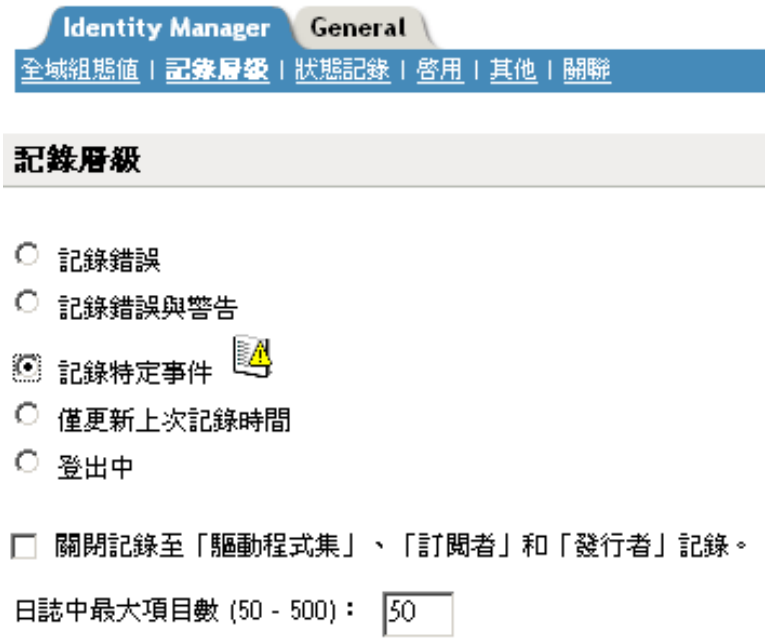
您可以使用 Novell Audit 來記錄您認爲對安全性重要的事件。如需 Novell Audit 的相關資訊，請參閱第 10 章 「使用 Novell Audit 記錄和報告」, 第 209 頁。

例如，您可以藉由執行下列操作，來記錄特定 Identity Manager 驅動程式 (或驅動程式集) 的密碼變更：

1 選取 「*eDirectory* 管理」 > 「修改物件」 > 「記錄層級」。

從下拉式清單中選取或選取索引標籤，這視您的 iManager 版本而定。

2 選取「記錄特定事件」。



3 若要選取特定事件，請按一下記錄事件圖示。

4 在「事件」頁面上，選取下列項目：

- 在「操作事件」中，選取「變更密碼」。
  此項目會監看對 NDS 密碼的直接變更。
- 在「轉換事件」中，選取「密碼設定」和「密碼同步化」。這兩個項目都會監看「通用密碼」和「配送密碼」的事件。

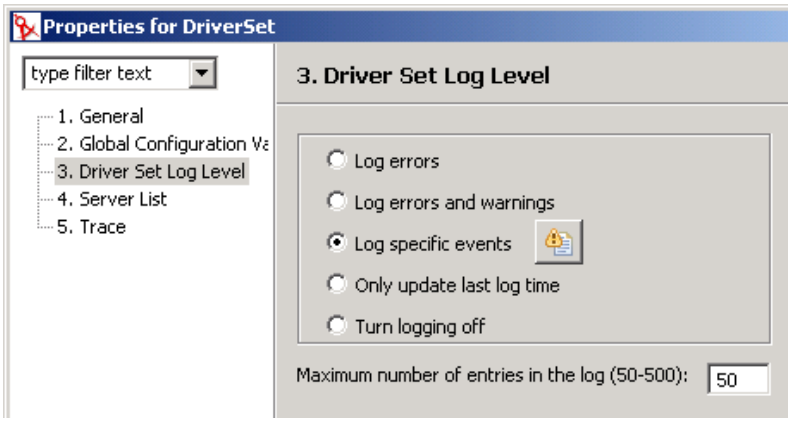
5 按兩次「確定」。

7.8.2 使用 Designer 記錄事件

您可以記錄套用至驅動程式集或驅動程式的事件。

記錄驅動程式集的事件

1 在 Designer 中，在驅動程式集上按一下滑鼠右鍵，然後選取「內容」。



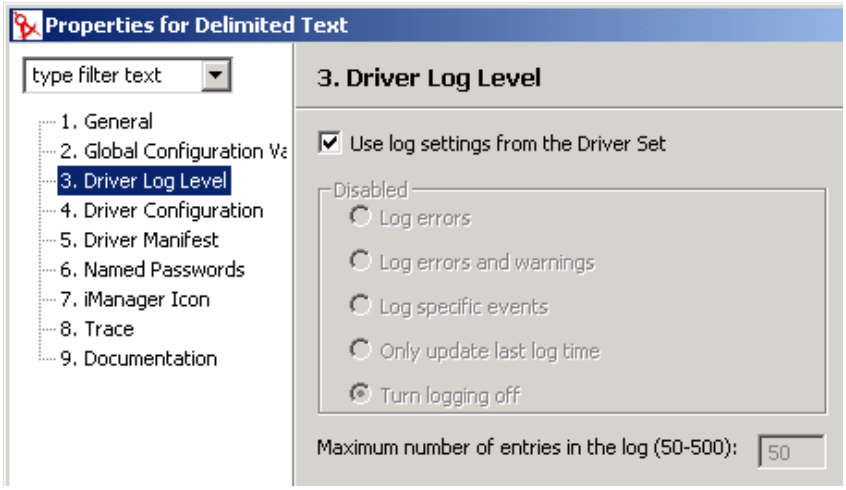
2 選取「驅動程式集記錄層級」，然後選取「記錄特定事件」。

3 按一下「選取要記錄的事件」圖示。

4 選取要記錄的事件，然後按一下「確定」。

記錄驅動程式的事件

1 在 Designer 中，在驅動程式上按一下滑鼠右鍵，然後選取「內容」。



2 選取「驅動程式記錄層級」，然後選取「記錄特定事件」。

您可以視需要接受驅動程式集的設定，然後按一下「確定」。否則，取消選取「使用驅動程式集的記錄設定」，選取「記錄特定事件」，然後按一下「確定」。

3 按一下「選取要記錄的事件」圖示。

4 選取要記錄的事件，然後按一下「確定」。

管理引擎服務 8

下列驅動程式僅用於 Metadirectory 引擎服務，而不能用於外部已連接系統。安裝 Identity Manager 時，會自動安裝這些驅動程式。

8.1 授權服務驅動程式

請參閱第 6 章 「建立並使用授權」, 第 147 頁。

8.2 手動任務服務驅動程式

「手動任務服務驅動程式」是設計用來通知一或多個使用者已發生的資料事件，以及是否需要使用者採取任何動作。在員工提供案例中，資料事件可能是建立新的 「使用者」物件，且使用者動作可能包含：藉由在 eDirectory 中輸入資料，或在應用程式中輸入資料，來指定辦公室電話號碼。其他案例包含：通知管理員已建立新的使用者物件，通知管理員使用者已變更物件上的資料等等。

設定 「手動任務服務驅動程式」組態通常包括設定兩個獨立但相關之子系統的組態： 「訂閱者」通道規則和電子郵件範本，以及 「發行者」通道 Web 伺服器範本和規則。

此外，還必須設定驅動程式參數，例如，SMTP 伺服器名稱、Web 伺服器連接埠號碼等。

本節內容：

8.2.1 安裝

- 安裝：使用 Identity Manager 安裝程式安裝 「*Metadirectory* 伺服器」選項時，會自動安裝 「手動任務服務的驅動程式」。
- 平台： 驅動程式在 Identity Manager 和 「遠端載入器」支援的平台上執行。
- 啓用： 驅動程式不需要個別啓用。啓用 Metadirectory 引擎時，也會啓用此驅動程式。

8.2.2 綜覽

在本節中，您會找到各種驅動程式功能如何運作的相關資訊。

- 「取代記號」，第 195 頁
- 「取代資料」，第 195 頁
- 「範本動作元素」，第 195 頁
- 「訂閱者通道電子郵件」，第 196 頁
- 「發行者通道 Web 伺服器」，第 196 頁

操作模式

支援兩種主要操作模式：

- 直接申請資料： 系統會傳送電子郵件訊息，要求使用者在 eDirectory 中輸入資料 (可能是供另一個應用程式使用)。電子郵件收件者按一下訊息中的 URL，即可回應該訊息。該 URL 指向在 「手動任務服務驅動程式」之 「發行者」通道中執行的 Web 伺服器。然後，使用者可與 Web 伺服器產生的動態網頁互動，以進行 eDirectory™ 驗證，並輸入申請的資料。
- 事件通知：無需透過 「發行者」通道，傳送電子郵件訊息至使用者。該電子郵件訊息可能只是通知在 eDirectory 中發生了事件，也可能是透過 「發行者」通道之 Web 伺服器以外的方法 (例如 Novell iManager、其他應用程式或自定介面) 來申請資料。

範例：訂閱者通道電子郵件、發行者通道 **Web** 伺服器回應

在下面的員工提供範例案例中，新員工的管理員會對員工指定房間號碼：

1. 在 eDirectory 中已建立新的 「使用者」物件 (例如，透過公司 HR 系統的 DirXML 驅動程式)。
2. 「手動任務服務驅動程式訂閱者」將 SMTP 訊息傳送至使用者的管理員和管理員助理。該 SMTP 訊息包含參考 「發行者」通道 Web 伺服器的 URL。這個 URL 也包含資料項目，用於識別使用者和識別具有提交申請資料權限的人員。
3. 管理員或管理員助理按一下電子郵件訊息中的 URL，在網頁瀏覽器中顯示 HTML 表單。然後，管理員或助理進行下列操作：
   - 選取其 eDirectory 「使用者」物件的 DN，做爲識別回應電子郵件訊息之人員的方法。
   - 輸入其 eDirectory 密碼。
   - 輸入新員工的房間號碼。
   - 按一下 「提交」按鈕。
4. 新員工的房間號碼會透過 「手動任務服務驅動程式發行者」通道提交至 eDirectory。

範例：訂閱者通道電子郵件、無發行者通道回應

在下面的範例案例中，新員工的管理員會在資產管理系統中對員工指定電腦：

1. 在 eDirectory 中已建立新的 「使用者」物件 (例如，透過公司 HR 系統的 DirXML 驅動程式)。
2. 「手動任務服務驅動程式訂閱者」將 SMTP 訊息傳送至使用者的管理員和管理員助理。該 SMTP 訊息包含在資產管理系統中輸入資料的指示。
3. 管理員或助理在資產管理系統中輸入資料。
4. (選擇性) 電腦識別資料會透過資產管理系統的 DirXML 驅動程式送入 eDirectory 中。

手動任務服務驅動程式建立電子郵件訊息和網頁的方式

電子郵件訊息、HTML 網頁和 XDS 文件均可視爲文件。「手動任務服務驅動程式」會根據提供給驅動程式的資訊，動態地建立文件。

範本是 XML 文件，其包含文件的模板或固定部份，以及指出最終建構文件之動態或取代部份出現位置的取代記號。

「手動任務服務驅動程式」的「訂閱者」通道和「發行者」通道，都會使用範本來建立文件。「訂閱者」通道會建立電子郵件訊息，而「發行者」通道會建立網頁和 XDS 文件。

透過取代資料，提供文件的動態部份。「訂閱者」通道上的取代資料由「訂閱者」通道規則 (例如「指令轉換」規則) 提供。「發行者」通道上的取代資料由 Web 伺服器的 HTTP 資料 (URL 資料和 HTTP POST 資料) 提供。「手動任務服務驅動程式」可以自動提供「手動任務服務驅動程式」已知的某些資料 (例如 Web 伺服器位址)。

XSLT 樣式表會處理範本。這些處理範本的樣式表不同於「訂閱者」或「發行者」通道中做爲 DirXML 規則的樣式表。

取代資料會做爲參數提供給 XSLT 樣式表。樣式表處理的輸出，是用做電子郵件訊息本文、網頁或提交至「發行者」通道上 DirXML 之內容的 XML、HTML 或文字文件。

取代資料會透過電子郵件訊息中的 URL，從「訂閱者」通道傳遞至「發行者」通道。該 URL 包含具有取代資料項目的查詢部份。

「手動任務服務驅動程式」隨附足以處理範本的預先定義樣式表，以便建立電子郵件文件、HTML 文件和 XDS 文件。需要的話，可以寫入其他自定樣式表以提供其他處理選項。

您也可以使用進階方法來建立文件，該方法僅使用 XSLT 樣式表和取代資料。不涉及任何範本。不過，因爲範本方法易於設定組態和維護，不需要 XSLT 程式設計知識，所以本指南假設使用的是這種方法。

範本

本節描述在「手動任務服務驅動程式」中使用的文件建立範本。

範本是由樣式表處理以產生輸出文件的 XML 文件。輸出文件可以是 XML、HTML 或純文字 (或可使用 XSLT 產生的任何其他格式)。

範本可用於在「訂閱者」通道上產生電子郵件訊息文字，以及在「發行者」通道上產生動態網頁和 XDS 文件。

範本包含文字、元素和取代記號。輸出文件中的取代記號會由提供給處理範本之樣式表的資料取代。

以下是數個用於各種用途的範本範例。在範例中，取代記號是兩個 $ 字元之間的字元字串，並以粗體顯示。

範本也可以包含動作元素。動作元素是由處理範本之樣式表解釋的控制元素。動作元素會在附錄 F 「手動任務服務驅動程式：範本動作元素參考」，第 277 頁 中進行描述。在下列範例中，動作元素也會以粗體顯示。

下列範例範本是用來產生 HTML 電子郵件訊息本文：

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head> <body> Dear $manager$,<p/> <p> This message is to inform
```

```
you that your new employee <b>$given-name$ $surname$</b> has been
hired. <p> You need to assign a room number for this individual. Click
<a href="$url$">Here</a> to do this. </p> <p> Thank you,<br/> HR
Department </p> </body> </html>
```

下列範例範本是用來產生純文字電子郵件訊息本文：

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
Dear $manager$,

This message is to inform you that your new employee $given-name$
$surname$ has been hired.

p> You need to assign a room number for this individual. Use the
following link to do this:

$url$

Thank you,[XXX]

The HR Department

</form:text>
```

因爲範本必須是 XML 文件，所以需要 <form:text> 元素。處理範本時，會刪除 <form:text> 元素。

下列範本是用來產生做爲網頁的 HTML 表單，以輸入資料：

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Enter room number for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet" type="text/css"/>
<br/><br/><br/><br/> <form class="myform" METHOD="POST" ACTION="$url-
base$/process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input TYPE="hidden"
name="association" value="$association$"/> <input TYPE="hidden"
name="response-style sheet" value="process_template.xsl"/> <input
TYPE="hidden" name="response-template" value="post_response.xml"/>
<input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> You are:<br/>
<form:if-single-item name="responder-dn">           <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/> $responder-
dn$           </form:if-single-item>          <form:if-multiple-items
name="responder-dn">          <form:menu name="responder-dn"/>
</form:if-multiple-items> </td></tr> <tr><td> Enter your password:
<br/> <input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/
> </td></tr> <tr><td> Enter room number for $subject-name$:<br/>
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
```

```
value="$query:roomNumber$"/> </td></tr> <tr><td> <input TYPE="submit"
value="Submit"/> <input TYPE="reset" value="Clear"/> </td></tr> </
table> </form> </body> </html>
```

下列範本是用來產生 XDS 文件：

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

取代記號

在以上範例範本中，以 $ 分隔的項目是取代記號。例如，$manager$ 會由管理員的實際名稱取代。

取代記號可以出現在文字中或 XML 屬性值 (請注意，上面第一個範例中 <a> 元素上的 href 值) 中。

取代資料

取代資料包含取代從範本產生之輸出文件中取代記號的字串。取代資料由「訂閱者」通道資料、「發行者」通道 HTTP 資料提供，或由驅動程式自動提供。取代資料的其他類型是透過 Identity Manager 從 eDirectory 擷取的資料 (查詢資料)。附錄 D 「手動任務服務驅動程式：取代資料」，第 269 頁 中包含對取代資料更爲全面的描述。

訂閱者通道資料：「訂閱者」通道取代資料有兩個類型。第一個類型在用於建立電子郵件訊息的範本中用作取代記號的取代值。第二個類型放置在 URL 的查詢部份，以便在 URL 提交給 「發行者」 Web 伺服器時，可以在 「發行者」通道上使用資料。

HTTP 資料： 取代資料會做爲 URL 查詢字串資料、HTTP POST 資料 (或兩者)，提供給「發行者」通道 Web 伺服器。

自動資料：「手動任務服務驅動程式」會提供自動資料。在附錄 E 「手動任務服務驅動程式：自動取代資料項目」，第 275 頁 中包含對自動資料項目的描述。

查詢資料：以 query: 開頭的取代記號會視爲從 eDirectory 取得目前資料的申請。query: 後面的記號部份是 eDirectory 物件屬性的名稱。要查詢的物件由其中一個取代資料項目指定：association、src-dn 或 src-entry-id。以項目在之前句子中呈現的順序來考量這些項目。

範本動作元素

動作元素是範本中名稱空間合法的元素，用於簡單邏輯控制，或用於建立 HTML 表單的 HTML 元素。用來使元素合法的名稱空間爲 http://www.novell.com/dirxml/manualtask/form。在此文件與隨 「手動任務服務驅動程式」提供的範例範本中，使用 form 做爲字首。

上面範例中以粗體顯示的元素是動作元素。

在附錄 F 「手動任務服務驅動程式：範本動作元素參考」，第 277 頁 中包含對動作元素的詳細描述。

訂閱者通道電子郵件

「手動任務服務驅動程式」的「訂閱者」通道是設計用來傳送電子郵件訊息。爲完成此操作，驅動程式支援名爲 <mail> 的自定 XML 元素。「訂閱者」通道上的規則會建構 <mail> 元素，以回應部份 eDirectory 事件 (例如，建立使用者)。<mail> 元素的一個範例如下所示：

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe"> <to>JStanley@novell.com</
to> <cc>carol@novell.com</cc> <reply-to>HR@novell.com</reply-to>
<subject>Room Assignment Needed for: Joe the Intern</subject> <message
mime-type="text/html"> <stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> <resource cid="css-1">novdocmain.css</resource> </message>
<message mime-type="text/plain">
<stylesheet>process_text_template.xsl</stylesheet>
<template>txt_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> </message> <attachment>HR.gif</attachment> </mail>
```

「手動任務服務驅動程式」的「訂閱者」會使用 <mail> 元素中包含的資訊，來建構 SMTP 電子郵件訊息。您可以建構 URL，並將其插入電子郵件訊息，電子郵件收件者可以透過它回應電子郵件訊息。URL 可以指向「發行者」通道 Web 伺服器，或者也可以指向某個其他 Web 伺服器。

在附錄 G 「手動任務服務驅動程式：<mail> 元素參考」，第 281 頁 中包含對 <mail> 元素及其內容的詳細描述。

發行者通道 **Web** 伺服器

「手動任務服務驅動程式」的「發行者」通道會執行已設定組態的 Web 伺服器，以便使用者可以透過網頁瀏覽器將資料輸入 eDirectory。Web 伺服器是設計用來與從 「手動任務服務驅動程式」之「訂閱者」通道傳送的電子郵件訊息搭配運作。

「發行者」通道 Web 伺服器可以提供靜態檔案和動態內容。靜態檔案的範例包含 .css 樣式表、影像等。動態內容的範例是根據 URL 或 HTTP POST 資料中包含之取代資料變更的網頁。

「發行者」通道 Web 伺服器組態通常會設定爲允許使用者將資料輸入 eDirectory，以回應「訂閱者」通道傳送的電子郵件。使用者與 Web 伺服器的一般互動如下所示：

1. 使用者會使用網頁瀏覽器，從電子郵件訊息提交 URL 至 Web 伺服器。URL 會指定用來建立動態網頁 (一般包含 HTML 表單) 的樣式表、範本和取代資料。
2. Web 伺服器會處理含樣式表和取代資料的範本，以建立 HTML 頁面。HTML 頁面會做爲 URL 參考的資源，傳回至使用者的網頁瀏覽器。
3. 瀏覽器會顯示 HTML 頁面，並且使用者會輸入申請的資訊。
4. 瀏覽器會傳送包含輸入之資訊，以及來自電子郵件 URL 之其他資訊的 HTTP POST 申請。回應電子郵件的使用者 DN 和使用者密碼必須位於 POST 資料中。
5. Web 伺服器會利用使用者 DN 和密碼來驗證使用者。如果驗證失敗，則包含失敗訊息的網頁會做爲 POST 申請的結果傳回。您可以使用 POST 資料中指定的樣式表和範本來建構失敗訊息。如果驗證成功，則會繼續處理。
6. Web 伺服器會使用 POST 資料中指定的樣式表和範本來建構 XDS 文件。將該 XDS 文件提交至「發行者」通道上的 Identity Manager。
7. 使用 XDS 文件提交的結果，以及 POST 資料中指定的樣式表和範本，可以建構網頁以對使用者指出資料提交的結果。此網頁會做爲 POST 申請的結果傳送至瀏覽器。

8.2.3 設定組態

本節描述如何設定「手動任務服務驅動程式」參數和範本的組態。

驅動程式設定

本節描述驅動程式物件使用者介面之「驅動程式設定」區段中出現的參數。

這些參數中的許多參數實際上是用於「發行者」通道 Web 伺服器。因爲「手動任務服務驅動程式發行者」也需要存取它們，所以它們會出現在「驅動程式設定」區域下。

文件基礎的 DN

此參數是容器物件的 eDirectory DN。「手動任務服務驅動程式」可以從 eDirectory 和磁碟下載 XML 文件 (包含 XSLT 樣式表)。如果應該從 eDirectory 下載 XML 文件，則此參數會識別從其中下載文件的根容器。

從 eDirectory 下載的文件位於 eDirectory 物件的屬性值中。如果沒有指定，則屬性是 XmlData。藉由將 # 字元和屬性名稱附加至包含文件之物件的名稱，可以指定該屬性。

例如，假設指定文件的基礎 DN 爲 "novell\Manual Task Documents"，並且在 "Manual Task Documents" 下方有一個名爲 "templates" 的容器。

如果名爲 "e-mail _template" 的 DirXML 樣式表物件位於 "templates" 目錄下，則下列資源識別碼可以用來參考 XML 文件："templates/e-mail _template" 或 "templates/e-mail _template#XmlData"。

您可以提供資源識別碼做爲取代資料、URL 資料或 HTTP POST 資料。例如，下列元素可能會出現在「訂閱者」通道上的 <message> 元素下：

```
<template>templates/e-mail _template#XmlData</template>
```

文件目錄

此參數會識別做爲基礎目錄使用的檔案系統目錄，該基礎目錄用於尋找資源，如範本、XSLT 樣式表和其他由「發行者」通道 Web 伺服器提供服務的檔案資源。範例值如下：

Windows	c:\Novell\Nds\mt_files
NetWare	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

使用 HTTP 伺服器 (true|false)

此參數指出「發行者」通道是否應該執行 Web 伺服器。如果 Web 伺服器應該執行，則設定此參數爲 true；如果不應該執行，則設定此參數爲 false。

如果「手動任務服務驅動程式」僅用來傳送具有無回應 URL 或指向另一個應用程式之 URL 的電子郵件，則不應該執行 HTTP 伺服器，以節省系統資源。

HTTP IP 位址或主機名稱

此參數可讓您指定「發行者」通道 Web 伺服器，將在多個本地 IP 位址中的哪個 IP 位址上監聽 HTTP 申請。

保留 HTTP IP 位址或主機名稱參數值爲空白，會導致「發行者」通道 Web 伺服器在預設 IP 位址上監聽。對於具有單一 IP 位址的伺服器，這已足夠。將以點標記的 IP 位址做爲參數值，會導致「發行者」通道 Web 伺服器在指定的位址上監聽 HTTP 申請。

請注意，如果在郵件指令元素中未指定主機名稱或位址，則「訂閱者」通道郵件處理器會使用指定的 HTTP IP 位址或主機名稱值來建構 URL。如果「使用 HTTP 伺服器 (true|false)」參數設爲 false，則 HTTP IP 位址或主機名稱可用來指定 Web 伺服器的位址或名稱，以在建構郵件訊息的 URL 時使用。

HTTP 連接埠

此參數是整數值，其指出「發行者」通道 Web 伺服器應在哪個 TCP 連接埠上監聽內送申請。如果未指定此值，則連接埠號碼預設爲 80 或 443，視保全插槽層 (SSL) 是否用於 Web 伺服器連接而定。

如果「手動任務服務驅動程式」在 Identity Manager 伺服器上執行 (即未在遠端機器上的「遠端載入器」下執行)，則 HTTP 連接埠應該設爲 80 或 443 以外的其他號碼。這是因爲 iMonitor 或其他程序一般會使用連接埠 80 和 443。

KMO 的名稱

如果不爲空白，則此參數是「eDirectory 金鑰材料物件」的名稱，該物件包含「發行者」通道 Web 伺服器用於保全插槽層 (SSL) 的伺服器證書和金鑰。

設定此參數，會導致「發行者」通道 Web 伺服器使用保全插槽層 (SSL) 來回應 HTTP 申請。

此參數會優先於任何 Java* KeyStore 參數 (請參閱下文)。

因爲使用「發行者」通道 Web 伺服器時，eDirectory 密碼會在 HTTP POST 資料中傳遞，所以基於安全理由，建議使用保全插槽層 (SSL)。

KeyStore 檔案名稱

此參數與「KeyStore 密碼」、「證書名稱 (金鑰別名)」和「證書密碼 (金鑰密碼)」一起，用來指定包含「發行者」通道 Web 伺服器用於保全插槽層 (SSL) 之證書和金鑰的 Java KeyStore 檔案。

設定此參數，會導致「發行者」通道 Web 伺服器使用保全插槽層 (SSL) 來回應 HTTP 申請。

如果已設定「KMO 的名稱」參數，則會忽略此參數及其相關參數。

因爲使用「發行者」通道 Web 伺服器時，eDirectory 密碼會在 HTTP POST 資料中傳遞，所以基於安全理由，建議使用保全插槽層 (SSL)。

KeyStore 密碼

此參數指定以「KeyStore 檔案名稱」參數指定之 Java KeyStore 檔案的密碼。

證書名稱 (金鑰別名)

此參數指定以「KeyStore 檔案名稱」參數指定之 Java KeyStore 檔案中使用的證書名稱。

證書密碼 (金鑰密碼)

此參數指定使用「證書名稱 (金鑰別名)」參數指定之證書的密碼。

訂閱者設定

本節描述「訂閱者」通道的設定。

SMTP 伺服器

此參數指定「訂閱者」通道將用來傳送電子郵件訊息之 SMTP 伺服器的名稱。

SMTP 帳戶名稱

如果使用 SMTP 伺服器參數指定的 SMTP 伺服器需要驗證，則此參數會指定要用於驗證的帳戶名稱。所使用的密碼是與驅動程式「驗證」參數相關聯的「應用程式」密碼。

預設 "From" 地址

如果指定，則這是「訂閱者」通道傳送之電子郵件 SMTP 寄件者欄位中使用的電子郵件地址。如果未指定，則傳送給「訂閱者」的 <mail> 元素必須包含 <from> 元素。

傳送給「訂閱者」之 <mail> 元素下的 <from> 元素會置換此參數。

其他處理器

如果指定，則這是一個空格分隔的 Java 類別名稱清單。每個類別名稱都是一個自定類別，其會實作 com.novell.nds.dirxml.driver.manualtask.CommandHandler 介面，並處理自定 XDS 元素 (<mail> 的處理器是內建處理器)。

在附錄 I「手動任務服務驅動程式：訂閱者通道的自定元素處理器」，第 295 頁 中可找到自定處理器的其他相關資訊。

發行者設定

本節描述「發行者」通道的設定。

其他伺服器常式

如果不爲空白，則這是一個空格分隔的 Java 類別名稱清單。每個類別名稱都是一個自定類別，其會延伸 javax.servlet.http.HttpServer。自定伺服器常式可用來延伸「發行者」通道 Web 伺服器的功能。

在附錄 J「手動任務服務驅動程式：發行者通道的自定伺服器常式」，第 297 頁中可找到自定伺服器常式的其他相關資訊。

訂閱者通道規則

「訂閱者」通道規則的組態視特定安裝要使用「手動任務服務驅動程式」完成的項目而定。然而，某些指示可能會有用。

一般而言，建構 <mail> 元素 (傳送給「訂閱者」) 的最佳位置是在「指令轉換」規則中。原因是在指令到達「指令轉換」規則時，大部份 DirXML 引擎處理已完成。這表示已針對新增事件處理「建立規則」(例如，對於不具有建構電子郵件所需之全部屬性的物件，允許否決新增事件)。這也表示已將沒有關聯之物件的修改事件轉換爲新增事件。

建構電子郵件訊息的 XSLT 樣式表可能 (也可能不) 需要查詢 eDirectory，以取得其他資訊。

例如，如果電子郵件訊息只是對新員工的歡迎訊息，則新增指令可以包含所有必要的資訊：名、姓和網際網路電子郵件地址。藉由在「建立」規則中指定「名」、「姓」和「網際網路電子郵件地址」爲必要的屬性，可以完成上述作業。這可確保只有包含所需資訊的新增指令才會到達「指令轉換」。

然而，如果電子郵件訊息是傳送給某員工之管理員的訊息，則樣式表需要查詢 eDirectory。管理員 DN 可透過員工之「使用者」物件的新增事件取得，但是因爲管理員的電子郵件地址是管理員之「使用者」物件的一個屬性，所以必須進行查詢以取得此項資訊。

此外，如果由於修改與驅動程式相關之物件的指令，會產生電子郵件通知，則必須進行查詢，以取得修改指令中未包含的資訊。

阻止指令到達訂閱者

如果將從新增事件以外的其他事件產生電子郵件訊息，則必須允許新增事件到達要監看之物件的「訂閱者」。允許新增事件到達「訂閱者」，會使產生的關聯值從「訂閱者」傳回至 Identity Manager。

「手動任務服務驅動程式」規則監看的 eDirectory 物件應該與「手動任務服務驅動程式」相關聯，這很重要。只有建立關聯的物件才會將刪除、重新命名和移動事件報告給驅動程式。另外，沒有關聯之物件上的修改事件會在「訂閱者」通道事件轉換後轉換成新增事件。

所有其他指令 (修改、移動、重新命名和刪除) 都應該由「指令轉換」規則阻擋，防止它們到達「訂閱者」。「訂閱者」僅處理 <add> 指令和 <mail> 指令。其他指令會讓「訂閱者」傳回錯誤。

產生電子郵件訊息

電子郵件訊息由「訂閱者」傳送，以回應接收到描述要傳送之電子郵件訊息的 <mail> 元素。如需 <mail> 元素及其內容的描述，請參閱附錄 G「手動任務服務驅動程式：<mail> 元素參考」，第 281 頁。

產生電子郵件訊息以回應任何 Identity Manager 事件 (新增、修改、重新命名、移動、刪除)。

提供給 <mail> 元素之 <message> 元素子代的取代資料視兩個主要因素而定：

- 用來產生訊息本文的範本。電子郵件範本使用的取代項目會顯示爲 <replacement-data> 元素的子代。
- 「發行者」通道上網頁範本所需要的資訊 (如果電子郵件在 「發行者」通道上產生回應的話)。網頁範本使用的取代項目會顯示爲 <url-query> 元素的子代，該元素是 <url-data> 的子代，而 <url-data> 又是 <replacement-data> 的子代。

如果電子郵件訊息應該包含指向 「發行者」通道 Web 伺服器的 URL，並用來請求使用者的資訊，則取代資料必須至少包含一個 responder-dn 項目。responder-dn 項目的值必須是要向其傳送訊息之使用者的 「使用者」物件 DN。

如果在範本中使用查詢取代記號 (請參閱 「取代資料」，第 195 頁)，則 <message> 元素的取代資料必須包含名爲 src-dn、src-entry-id 或 association 且具有適當值的項目。關聯項目只能在要查詢的 eDirectory 物件與 「手動任務服務驅動程式」建立關聯後使用。因爲查詢發生時，「訂閱者」對未關聯物件產生的關聯尚未寫入 eDirectory 物件，所以無法使用該關聯。

<message> 元素可以指定訊息本文的多用途網際網路郵件延伸標準 (Multipurpose Internet Mail Extensions，MIME) 類型。如果已指定 MIME 類型，但未指定樣式表 (即沒有 <message> < 的 stylesheet> 元素子代)，則會使用兩個預設樣式表名稱的其中一個。如果 MIME 類型爲 text/plain，則預設樣式表名稱爲 process_text_template.xsl。如果 MIME 類型爲 text/plain 以外的其他任何類型，則預設樣式表名稱爲 process_template.xsl。

訂閱者通道電子郵件範本

電子郵件範本是包含模板和取代記號的 XML 文件。電子郵件範本是用來產生電子郵件訊息本文文字。如需範本的一般資訊，請參閱 「範本」，第 193 頁。

電子郵件範本中使用的取代記號指示必須做爲 <replacement-data> 元素子代提供的 <item> 元素，而 <replacement-data> 元素是由建構 <mail> 元素的 「訂閱者」通道規則建構而成。例如，如果電子郵件範本具有取代記號 $employee-name$，則 <message> 元素的取代資料中必須有 <item name="employee-name"> 元素。如果員工名稱項目不存在，則所產生之電子郵件訊息本文在範本中取代記號佔用的位置上沒有任何文字。

電子郵件範本可用來產生純文字、HTML 或 XML 格式的訊息本文。

如果電子郵件範本產生純文字訊息，則必須由指定純文字做爲其輸出類型的樣式表來進行處理。如果樣式表未指定純文字做爲其輸出類型，則會發生不想要的 XML 逸出。預設 「手動任務服務驅動程式」樣式表 process_text_template.xsl 一般用來處理產生純文字的範本。

發行者通道規則

在大部份 「手動任務服務驅動程式」的實作中，不需要 「發行者」通道規則。這是因爲可能會建構網頁和 XDS 範本，以便準確地產生所需的 XDS，而且不需要由規則進一步處理 XDS。

如果需要規則，則它們將是專門針對某個安裝。

發行者通道網頁範本

網頁範本是包含模板和取代記號的 XML 文件。網頁範本是用來產生網頁文件 (通常是 HTML 文件)。如需範本的一般資訊，請參閱 「範本」，第 193 頁。

網頁範本中的取代記號指示「訂閱者」通道上做爲 URL 查詢資料提供的取代資料。「發行者」通道上的取代資料會從 HTTP GET 申請的 URL 查詢字串取得，並從 HTTP POST 申請的 URL 查詢字串和 POST 資料取得。

做爲從「訂閱者」通道至電子郵件訊息，然後至「發行者」通道 Web 伺服器的取代資料流程範例，請考量下列案例。

設定「手動任務服務驅動程式」的組態，以便請求新員工管理員指定新員工的房間號碼。對新「使用者」物件的 <add> 指令 (由「訂閱者」通道「指令轉換」規則處理) 是傳送至管理員之電子郵件的觸發。

當管理員按一下電子郵件訊息中的 URL 時，即會在管理員的網頁瀏覽器中顯示網頁。該網頁必須指出管理員正在爲何人輸入房間號碼。

若要完成此項操作，「訂閱者」通道上的 <url-query> 元素會包含依名稱識別新使用者的取代資料項目：

```
<item name=”subject-name”>Joe the Intern</item>
```

這會讓 URL 查詢字串除其他內容外，還特別包含了 "subject-name=Joe%20the%20Intern" (其中 "%20" 是 URL 編碼空間)。

當管理員按一下電子郵件訊息中的 URL 時，其網頁瀏覽器會提交 URL 至「發行者」通道 Web 伺服器。Web 伺服器會建構名爲 subject-name 且值爲 Joe the Intern 的取代資料項目。

同樣由 URL 指定的網頁範本會包含取代記號 $subject-name$。在樣式表處理網頁範本以建構網頁時，取代記號由 Joe the Intern 取代，其會針對因建立「使用者」物件而導致傳送電子郵件的員工自定網頁。

如需完整「訂閱者」通道至「發行者」通道異動的其他資訊，請參閱附錄 H 「手動任務服務驅動程式：新員工的資料流程案例」，第 285 頁 。

發行者通道 **XDS** 範本

XDS 範本是包含模板和取代記號的 XML 文件。XDS 範本是用來產生 XDS 文件，這些文件會提交至「手動任務服務驅動程式」之「發行者」通道上的 Identity Manager。如需範本的一般資訊，請參閱「綜覽」一節下的「範本」。

XDS 範本中的取代記號指示做爲 HTTP POST 申請中的資料提供給 Web 伺服器的部份取代資料。

例如，請考量下列 XDS 範本：

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

範本中的取代記號指示 HTTP POST 資料必須提供關聯值和房間號碼值。

關聯值一般會在「訂閱者」通道中產生。「訂閱者」通道電子郵件會將 association=some 值置於電子郵件訊息中包含之 URL 的查詢字串內。在將 URL 提交至 Web 伺服器時用來產生網頁的網頁範本，通常會將關聯值置於隱藏的 INPUT 元素中：

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

將關聯值置於隱藏的 INPUT 元素，會導致將 "association=some value" 配對做爲 HTTP POST 資料的一部份來進行提交。

使用類似於下列內容的 INPUT 元素，在網頁中輸入 room-number 值：

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

如果管理員輸入 1234，並按一下「提交」，則網頁瀏覽器會將 "room-number=1234" 做爲 HTTP POST 資料的一部份來進行傳送。

然後，Web 伺服器會產生 <item name="association"> 取代資料項目和 <item name="room-number"> 取代資料項目，以供在處理 XDS 範本時使用。

使用 POST 資料中指定的樣式表處理 XDS 範本，以產生 XDS 文件。然後將 XDS 文件提交至「手動任務服務驅動程式」之「發行者」通道上的 Identity Manager。

追蹤設定

「手動任務服務驅動程式」會輸出各種追蹤層級的訊息：

層級	追蹤訊息描述
0	無追蹤訊息
1	追蹤基本操作的單行訊息
2	無其他訊息 (「DirXML 引擎」會追蹤此層級和更高層級的 XML 文件)
3	無其他訊息
4	與使用範本和樣式表建構之文件相關的訊息
5	追蹤的取代資料文件

8.2.4 其他資訊

如需「手動任務服務驅動程式」設定的其他資訊，請參閱下列附錄部份：

- 附錄 D 「手動任務服務驅動程式：取代資料」，第 269 頁
- 附錄 E 「手動任務服務驅動程式：自動取代資料項目」，第 275 頁
- 附錄 F 「手動任務服務驅動程式：範本動作元素參考」，第 277 頁
- 附錄 G 「手動任務服務驅動程式：<mail> 元素參考」，第 281 頁
- 附錄 H 「手動任務服務驅動程式：新員工的資料流程案例」，第 285 頁
- 附錄 I 「手動任務服務驅動程式：訂閱者通道的自定元素處理器」，第 295 頁
- 附錄 J 「手動任務服務驅動程式：發行者通道的自定伺服器常式」，第 297 頁

高可用性

9

您可以搭配共享儲存區使用 Identity Manager，以提供高可用性。若要在叢集環境中使用 Novell® eDirectory™ 和 Identity Manager，需要執行一些步驟。

本節內容：

9.1 設定 eDirectory 和 Identity Manager 組態以與 Linux 和 UNIX 上的共享儲存區搭配使用

本節提供設定 eDirectory 和 Identity Manager 組態，以便在使用共享儲存區之高可用性叢集中進行容錯移轉的步驟。本節中的資訊對任何 Linux 或 UNIX 平台上的共享儲存區高可用性叢集而言是通用的；此項資訊並非專門針對特定的叢集管理員。

您需要瞭解的基本概念是，eDirectory 和 Identity Manager 的狀態資料必須位於共享儲存區上，才能提供給目前執行服務的叢集節點使用。實際上，這表示 eDirectory 資料儲存 (通常位於 /var/nds/dib 中) 必須重新定位至叢集共享儲存區。Identity Manager 狀態資料也位於 /var/nds/dib 中。叢集節點上的每個 eDirectory 例項都必須設爲使用共享儲存區上的資料儲存。其他 eDirectory 組態資料也必須位於共享儲存區上。

除了 eDirectory 資料儲存之外，還需要共享 Novell 國際密碼基礎結構 (Novell International Cryptographic Infrastructure，NICI) 資料，以便在叢集節點間複製伺服器特定的金鑰。通常會建議將 Novell 國際密碼基礎結構 (NICI) 資料複製到每個叢集節點上的本地儲存區，而不是將 NICI 資料移至共享儲存區。這樣做更爲可取，如此一來，即使叢集節點處於次要狀態，並未代管共享儲存區，用戶端 Novell 國際密碼基礎結構 (NICI) 功能也可以在該節點上使用。

下列各節會討論共享 eDirectory 和 Novell 國際密碼基礎結構 (NICI) 資料，並基於以下假設：

- 您對於 Novell 國際密碼基礎結構 (NICI)、eDirectory 和 Identity Manager 資料與組態，使用預設的安裝位置。

  因爲相關 Identity Manager 資料與 eDirectory 資料位於相同的位置，所以並未將 Identity Manager 資料與 eDirectory 資料分開來討論。
- 您熟悉 eDirectory 和 Identity Manager 安裝程序。
- 您使用的是兩個節點的叢集。

  到目前爲止，兩個節點的叢集是高可用性最常用的組態。然而，本節中的概念可以輕鬆地延伸至 *n* 個節點的叢集。

本節內容：

- 「共享 eDirectory 和 Identity Manager 資料」，第 207 頁
- 「Identity Manager 驅動程式考量」，第 208 頁

9.1.1 安裝 eDirectory

附註：做爲 eDirectory 安裝程序的一部份安裝 Novell 國際密碼基礎結構 (NICI)。

1. 在主要叢集節點上安裝 eDirectory。
2. 在主要叢集節點上設定 eDirectory 的組態。在主要叢集節點上建立新的網路樹，或將伺服器安裝至現有的網路樹。針對 eDirectory 伺服器名稱，請使用 UNIX 伺服器名稱以外的其他名稱。使用對叢集通用的名稱，而不是其中一個叢集節點特定的名稱。
3. 在次要叢集節點上安裝相同版本的 eDirectory。請勿在次要叢集節點上設定 eDirectory 的組態。

   次要節點沒有單獨的網路樹。

9.1.2 安裝 Identity Manager

1. 使用「*Metadirectory* 伺服器」選項，在主要叢集節點上安裝 Identity Manager。

   安裝程序會安裝 Identity Manager 檔案，並設定 eDirectory 網路樹的組態，以與 Identity Manager 搭配使用。
2. 使用次要叢集切換在次要叢集節點上安裝相同版本的 Identity Manager，方法是輸入

   ```
   dirxml_platform.bin -DCLUSTER_INSTALL="true"
   ```

   在安裝期間，選擇「*Metadirectory* 伺服器」選項。

   使用次要叢集切換會安裝 Identity Manager 檔案，但不會嘗試執行任何其他 eDirectory 組態設定。因爲次要節點沒有單獨的網路樹，所以不需要任何組態設定。

9.1.3 共享 NICI 資料

Novell 國際密碼基礎結構 (NICI) 會提供 eDirectory、Identity Manager 和 Novell 用戶端應用程式使用的加密服務。與 eDirectory 搭配使用時，Novell 國際密碼基礎結構 (NICI) 會提供伺服器特定的金鑰。在執行 eDirectory 做爲叢集服務的所有叢集節點上，這些伺服器特定金鑰必須相同。

可用來共享 Novell 國際密碼基礎結構 (NICI) 資料的方法有兩種：

- 將 Novell 國際密碼基礎結構 (NICI) 資料置於叢集共享儲存區上。

  此方法的缺點是當叢集節點未代管共享儲存區時，該叢集節點上依賴 Novell 國際密碼基礎結構 (NICI) 的應用程式將失敗。
- 將 Novell 國際密碼基礎結構 (NICI) 資料從主要伺服器複製到次要伺服器的本地儲存區。

若要複製 Novell 國際密碼基礎結構 (NICI) 資料，請執行下列動作：

1. 將次要叢集節點上的 /var/novell/nici 重新命名爲其他名稱 (如 /var/novell/nici.sav)。

2 將 /var/novell/nici 目錄從主要叢集節點複製到次要叢集節點。

使用 scp，或者藉由在主要節點上建立 /var/novell/nici 目錄的 tar 檔案、將其傳送至次要節點，並在次要節點上還原目錄，可以完成此項操作。

9.1.4 共享 eDirectory 和 Identity Manager 資料

在預設狀態下，eDirectory 會在 /var/nds/dib 中儲存其資料儲存。組態和狀態的其他項目也會儲存在 /var/nds 及其子目錄中。eDirectory 的預設組態目錄爲 /etc。您必須執行下列步驟，以設定 eDirectory 和 Identity Manager 的組態與高可用性叢集中的共享儲存區搭配使用。這些步驟假設共享儲存區裝在 /shared 上。

- 「在主要節點上」，第 207 頁
- 「在次要節點上」，第 208 頁

在主要節點上

1 將 /var/nds 目錄子網路樹複製到 /shared/var/nds。

2 重新命名 /var/nds 目錄 (例如，命名爲 /var/nds.sav)。

此動作不是必要的，但是在此階段建立備份，可讓您無需重新安裝 eDirectory，即可重新開始 (必要的話)。

3 建立從 /var/nds 至 /shared/var/nds 的符號鏈結 (例如 ln -s /shared/var/nds /var/nds)。

4 建立下列符號鏈結：

連結自	連結至
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf
/shared/var/nds/macaddr	/etc/macaddr

5 建立 /etc/nds.conf 的備份。

6 將 /etc/nds.conf 移至 /shared/var/nds。

7 編輯 /shared/var/nds/nds.conf，並將下列項目置於檔案中 (覆寫任何目前同名的項目)：

- n4u.nds.dibdir=/shared/var/nds/dib
- n4u.server.configdir=/shared/var/nds
- n4u.server.vardir=/shared/var/nds
- n4u.nds.preferred-server=localhost

針對下列項目，請以叢集共享乙太網路介面的介面名稱取代 eth0:0。同時，以本地主機乙太網路介面的介面名稱取代 lo。

- n4u.nds.server.interfaces=eth0:0@524,lo@524

- http.server.interfaces=eth0:0@8008,lo@8008
- https.server.interfaces=eth0:0@8009,lo@8009

8 建立從 /etc/nds.conf 至 /shared/var/nds/nds.conf 的符號鏈結。

9 啓動 ndsd 並驗證 ndsd 會與共享儲存區一起執行。

10 停止 ndsd。

11 將 ndsd 放入叢集管理員要代管的資源清單。

12 將 ndsd 從開機時啓始化程序要啓動的精靈清單中移除。

在次要節點上

1 重新命名 /var/nds 目錄 (例如，命名爲 /var/nds.sav)。嚴格來說，此動作不是必要的，但是備份讓您能夠在 eDirectory 安裝程序之外的某個時候重新開始。

2 建立從 /var/nds 至 /shared/var/nds 的符號鏈結。

3 製作 /etc/nds.conf 的備份。

4 移除 /etc/nds.conf。

5 建立從 /etc/nds.conf 至 /shared/var/nds/nds.conf 的符號鏈結。

6 將 ndsd 放入叢集管理員要代管的資源清單。

7 將 ndsd 從開機時啓始化程序要啓動的精靈清單中移除。

完成主要和次要節點的步驟之後，啓動叢集服務。eDirectory 和 Identity Manager 將在主要節點上啓動。

9.1.5 Identity Manager 驅動程式考量

大部份 Identity Manager 驅動程式都可以在叢集組態中執行。然而，您需要考量下列項目：

- 必須在每個叢集節點上都安裝驅動程式可執行檔 (.jar 檔案和 / 或共享物件)。
- 如果驅動程式必須與其支援的應用程式在同一伺服器上執行，則必須設定應用程式的組態，以做爲叢集服務的一部份來執行。
- 如果驅動程式有驅動程式特定狀態資料的可設定組態位置，則該位置必須位於叢集共享儲存區上。

  在沒有變更記錄的情況下使用的 LDAP 驅動程式，或在無觸發模式中使用的 JDBC 驅動程式，就是這樣一個範例。
- 如果驅動程式的組態資料儲存在 eDirectory 外部，則該組態資料必須位於共享儲存區，或者必須在每個叢集節點上複製該資料。「手動任務驅動程式」的範本目錄就是這樣一個範例。

9.2 SuSE Linux 的個案研討

如需在 SUSE LINUX Enterprise Server 8 的共享儲存區上執行 Identity Manager 的描述，請參閱 TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm).

使用 Novell Audit 記錄和報告 10

Identity Manager 已配備以使用 Novell® Audit 進行稽核和報告。

10.1 綜覽

Novell Audit 是一組技術，可提供監看、記錄、報告和通知功能。透過與 Novell Audit 整合，Identity Manager 可提供驅動程式和引擎活動之目前和歷程狀態的詳細資訊。此項資訊會以一組預先設定組態的報告、標準通知服務和使用者定義的資料記錄的方式提供。

您可以使用 Novell Audit 監看即時 Identity Manager 事件、傳送任何 Identity Manager 事件的電子郵件通知，以及產生 Identity Manager 活動的報告。

使用一些外掛程式 (類似於隨 「報告和通知服務 (Reporting and Notification Service，RNS)」 提供的外掛程式)，以控制傳送至 Novell Audit 的訊息類型。將其他層級新增至這些外掛程式，以選取您要追蹤的操作或除錯資訊類型，如狀態、新增項目、搜尋等等。

報告和通知服務

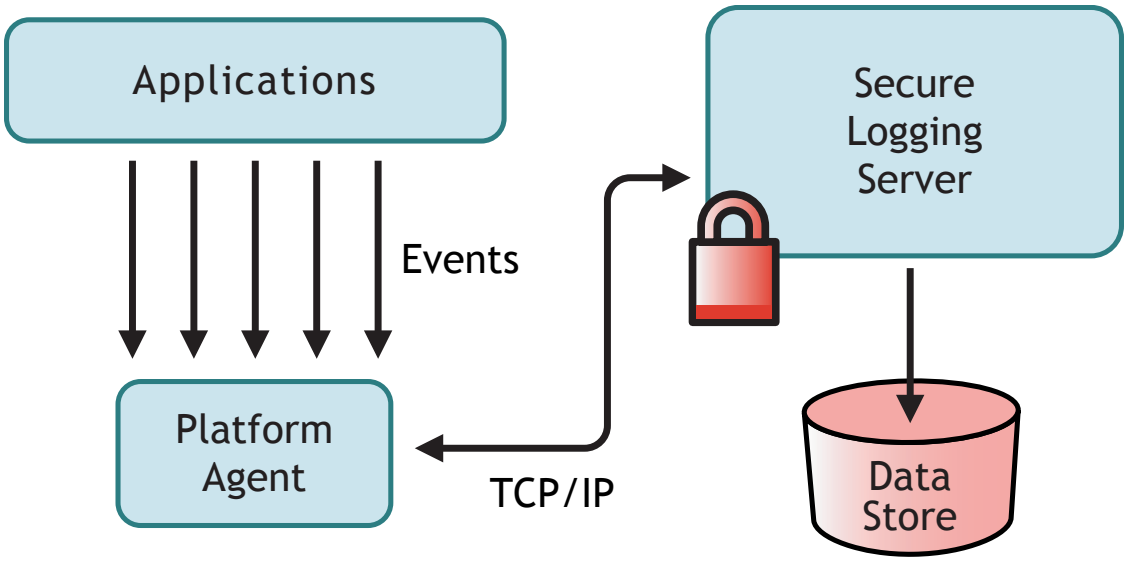
如果您目前正在使用報告和通知服務 (Reporting and Notification Service，RNS)，Metadirectory 引擎仍會繼續處理報告和通知服務 (RNS) 功能，但不建議使用。因爲 Novell Audit 會擴充報告和通知服務 (RNS) 提供的功能，並且在 Identity Manager 以後的版本中可能不再支援 RNS，所以您應該計劃採用 Novell Audit。如需報告和通知服務 (RNS) 文件，請參閱 《*DirXML 1.1a* 管理指南 (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html)》。

10.2 Novell Audit

Novell Audit 是集中式的跨平台記錄服務，可以將多個應用程式的資料記錄至集中式資料儲存。在記錄事件資料之後，您可以根據記錄的事件來執行詳細的報告、自定查詢和觸發通知。

下圖顯示 Novell Audit 的高層結構：

特性 ***10-1*** 結構綜覽



在此圖例中，Identity Manager 是其中一個應用程式，其會使用 「平台代辦」將事件報告至「Novell Audit 安全記錄伺服器」。

10.3 設定 Novell Audit

如「綜覽」中所述，Novell Audit 包含兩個基本元件：

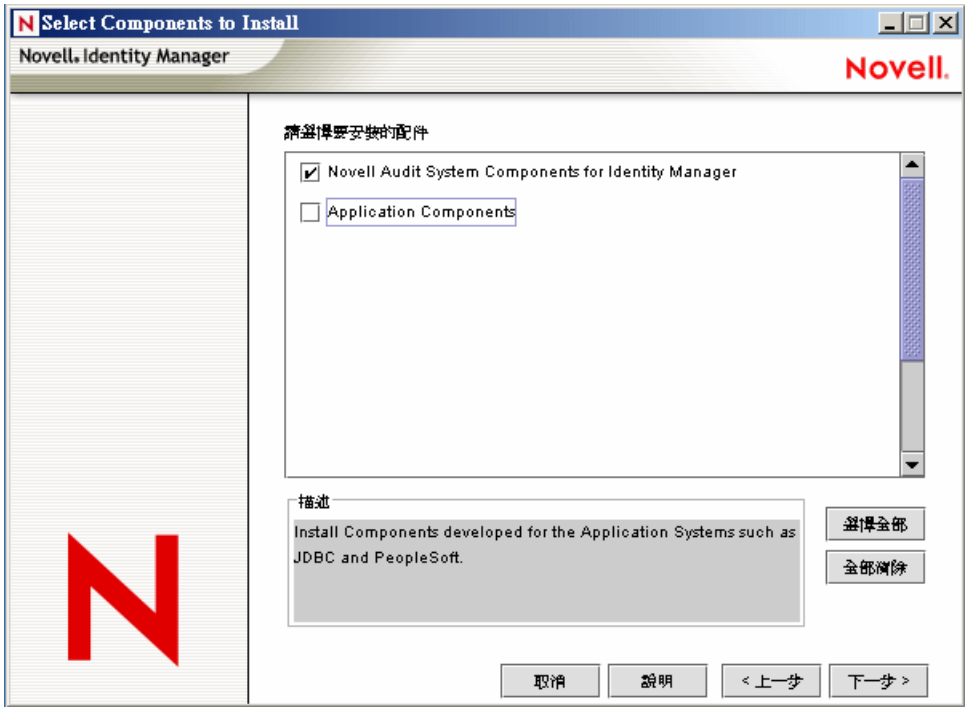
- 平台代辦
- 安全記錄伺服器

「平台代辦」是與 Identity Manager 一起執行的元件，其會將事件告知「安全記錄伺服器」，且會與 Identity Manager 一起安裝。「安全記錄伺服器」是會從 Identity Manager 及其他應用程式接收事件資料的元件，且會做爲 Novell Audit 1.0.3 的一部份，與 Identity Manager 分開來安裝。

10.3.1 設定平台代辦

藉由在安裝期間選取 Identity Manager 的 「Novell Audit 系統元件」選項，可以安裝 「平台代辦」。

特性 ***10-2*** *Identity Manager* 的安裝



在安裝 Identity Manager 期間可以安裝 「平台代辦」，也可以在稍後安裝。

附註：如果在啓動 Metadirectory 引擎後安裝 「平台代辦」，則必須在連結 「平台代辦」與 Identity Manager 之前重新啓動 Identity Manager。Identity Manager 會嘗試僅在啓動期間連接至 「平台代辦」。

安裝 「平台代辦」之後，請完成下列步驟以設定其組態：

1 在文字編輯器中開啓 Novell Audit 組態檔案 logevent.cfg。此檔案的預設位置如下：

作業系統	路徑
NetWare®	sys:\etc\logevent.cfg
Windows	*windows_directory*\logevent.cfg
Linux\Solaris	/etc/logevent.conf

2 將 LogHost 參數的值變更爲您 「安全記錄伺服器」的 IP 位址或 DNS 名稱。

3 重新啓動 Identity Manager。

10.3.2 設定安全記錄伺服器

附註：「Novell Audit 安全記錄伺服器」並非隨附於 Identity Manager。「安全記錄伺服器」是 Novell Audit 1.0.3 的一部份。如需下載 Novell Audit 1.0.3 的相關資訊，請參閱 Novell Audit 產品頁面 (http://www.novell.com/products/nsureaudit)。

「安全記錄伺服器」可以在下列作業系統上執行：NetWare 5.1 或更新版本、Windows* NT 4.0、Windows 2000 Server、Windows 2003 Server、Solaris* 8 或 9，以及 Linux* 的數個版本，包括 SUSE® Enterprise Linux Server 8 和 SUSE 9.0。

「安全記錄伺服器」可以將事件記錄至 MySQL*、Oracle*、Microsoft* SQL Server、Java* 應用程式，以及數個其他位置 (包括平面檔)。Novell Audit 包含設計用來查詢資料庫中事件資料的自定應用程式，稱爲 Novell Audit Report。您需要具有 ODBC 連接器的資料儲存，才能使用此進階報告工具。

每個平台都有內含「安全記錄伺服器」設定指示的「快速入門指南」可供使用，該指南隨附於 Novell Audit 1.0.3 安裝程式中。您可以在 Web 上檢視「快速入門」指南，並且在 Novell Audit 文件網站 (http://www.novell.com/documentation/nsureaudit) 上可找到《*Novell Audit 1.0.3* 管理指南》。

10.4 記錄組態

Identity Manager 可讓您使用數個預先定義的層級，或個別選取每個要記錄的事件，來設定所記錄事件的組態。組態設定的變更也會一併記錄下來。

只要啓用記錄，「使用者定義的事件」，第 217 頁中所討論的使用者定義事件就會被記錄下來，而且 Metadirectory 引擎永遠不會過濾這些事件。

記錄的組態會在驅動程式集或個別驅動程式上設定。驅動程式可以承襲驅動程式集的記錄組態。如需包含記錄資訊之 eDirectory™ 屬性的相關資訊，請參閱「eDirectory 物件」，第 219 頁。

在預設狀態下，僅會記錄重要事件和使用者定義事件。

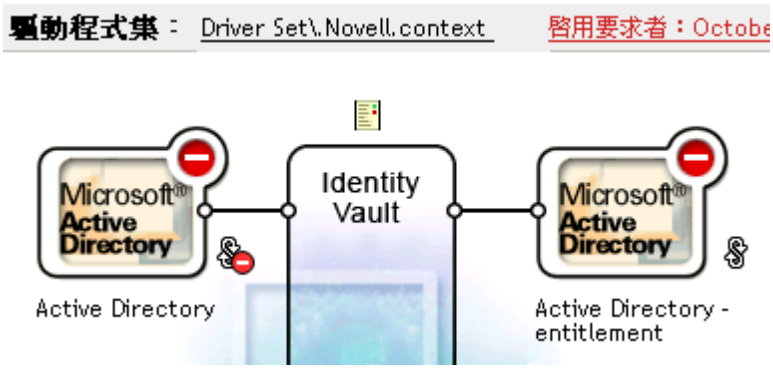
10.4.1 選取要記錄的事件

您可以選取驅動程式集或特定驅動程式的事件。

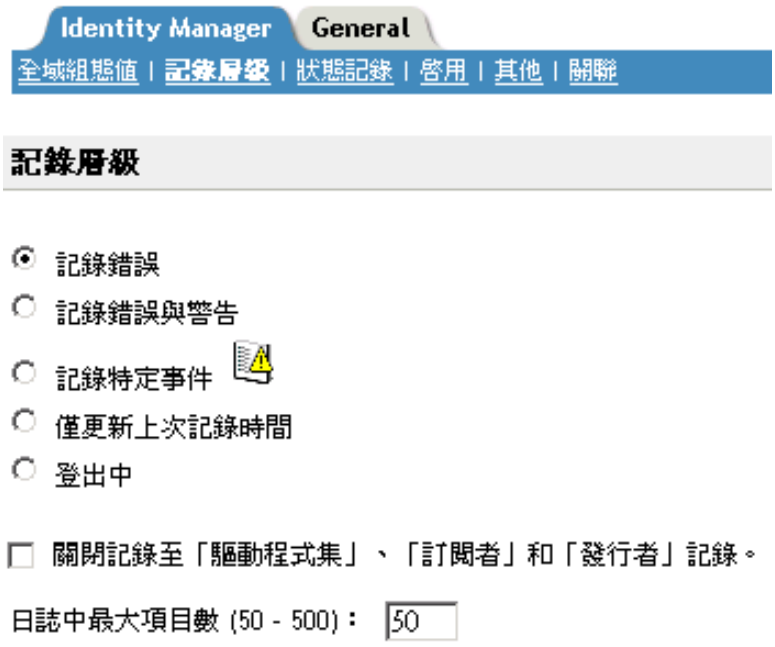
記錄驅動程式集的事件：

1. 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」，然後按「下一步」。
2. 瀏覽至並選取「驅動程式集」物件，然後按一下「搜尋」。

3 按一下 「驅動程式集」名稱，「修改物件」頁面即會出現。



4 選取 「*Identity Manager*」索引標籤上的 「記錄層級」。



5 選取您環境所需要的記錄選項。

選項	描述
記錄錯誤	這是預設的記錄層級。此選項會記錄狀態爲錯誤的所有事件和使用者定義事件。 選取此選項後，您只會收到十進位 ID 爲 196646 的事件，且第一個文字欄位中會有一則儲存的錯誤訊息。
記錄錯誤與警告	此選項會記錄狀態爲錯誤或警告的所有事件和使用者定義事件。 選取此選項後，您只會收到十進位 ID 爲 196646 和 196647 的事件，且第一個文字欄位中會有一則儲存的錯誤或警告訊息。

選項	描述
記錄特定事件	此選項可讓您從清單中選取要記錄的特定事件。按一下 圖示以選取事件。使用者定義事件固定會被記錄下來。 若要記錄錯誤或警告以外的任何事件，您必須從此清單中選取該事件。選取此選項後，如果您要繼續記錄錯誤和警告，還必須選取它們。如需所有可用事件的清單，請參閱 「Identity Manager 事件」，第 216 頁。
僅更新上次記錄時間	只有使用者定義的事件會記錄下來。當事件發生時，會更新上次記錄時間，以便您可以檢視狀態記錄中上次錯誤的時間和日期。
記錄功能關閉	僅記錄使用者定義的事件。
關閉記錄至「驅動程式集」、「訂閱者」和「發行者」記錄。	關閉記錄至「驅動程式集」物件記錄、「訂閱者」和「發行者」記錄。
記錄中的最大項目數	此設定可讓您指定狀態記錄中記錄的最大項目數。如需詳細資訊，請參閱 「檢視狀態記錄」，第 223 頁。

6 選取您要記錄的事件之後，請按一下「確定」。

記錄驅動程式的事件：

1 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」，然後按「下一步」。

2 瀏覽至並選取「驅動程式集」物件，然後按一下「搜尋」。

3 按一下驅動程式圖示的右上角，然後選取「編輯內容」。

4 選取「*Identity Manager*」索引標籤上的「記錄層級」。

5 (選擇性) 在預設狀態下，「驅動程式」物件會設定爲承襲「驅動程式集」物件的記錄設定。若要只選取此驅動程式的記錄事件，請取消選取使用「驅動程式集」的記錄設定。

6 選取您環境所需要的記錄選項。

選項	描述
記錄錯誤	這是預設的記錄層級。此選項會記錄狀態爲錯誤的所有事件和使用者定義事件。 選取此選項後，您只會收到十進位 ID 爲 196646 的事件，且第一個文字欄位中會有一則儲存的錯誤訊息。
記錄錯誤與警告	此選項會記錄狀態爲錯誤或警告的所有事件和使用者定義事件。 選取此選項後，您只會收到十進位 ID 爲 196646 和 196647 的事件，且第一個文字欄位中會有一則儲存的錯誤或警告訊息。
記錄特定事件	此選項可讓您從清單中選取要記錄的特定事件。按一下 圖示以選取事件。使用者定義事件固定會記錄下來。 若要記錄錯誤或警告以外的任何事件，您必須從此清單中選取該事件。選取此選項後，如果您要繼續記錄錯誤和警告，就必須同時加以選取。如需所有可用事件的清單，請參閱「Identity Manager 事件」，第 216 頁。
僅更新上次記錄時間	只有使用者定義的事件會記錄下來。當事件發生時，會更新上次記錄時間，以便您可以檢視狀態記錄中上次錯誤的時間和日期。

選項	描述
記錄功能關閉	只有使用者定義的事件會記錄下來。
關閉記錄至「驅動程式集」、「訂閱者」和「發行者」記錄。	關閉記錄至「驅動程式集」物件記錄、「訂閱者」和「發行者」記錄。
記錄中的最大項目數	此設定可讓您指定狀態記錄中記錄的最大項目數。如需詳細資訊，請參閱「檢視狀態記錄」，第 223 頁。

7 選取您要記錄的事件之後，請按一下「確定」。

Identity Manager 事件

Identity Manager 記錄之所有事件的清單都包含在附錄 C 「Identity Manager 事件和報告」，第 243 頁中。

驅動程式啓動和停止事件

驅動程式每次啓動或停止，Identity Manager 都會產生事件。下表包含這些事件的詳細資料：

表格 ***10-1*** 驅動程式啓動和停止事件

事件	記錄層級	資訊
EV_LOG_DRIVER_START	LOG_INFO	若要記錄驅動程式啓動，必須使用「*記錄特定事件*」選項，並選取此事件。
EV_LOG_DRIVER_STOP	LOG_WARNING	若要記錄驅動程式停止，請選取「*記錄錯誤與警告*」，或使用「*記錄特定事件*」選項，並選取此事件。

如需根據這些事件建立 Novell Audit 通知的詳細資訊，請參閱「根據事件傳送通知」，第 220 頁。

錯誤和警告事件

無論何時遇到錯誤或警告，Identity Manager 都會產生事件。下表包含這些事件的詳細資料：

表格 ***10-2*** 錯誤和警告事件

事件	記錄層級	資訊
DirXML_Error	LOG_ERROR	所有 Identity Manager 錯誤都會記錄此事件。遇到的實際錯誤碼會儲存在事件中。 若要記錄錯誤，請選取「*記錄錯誤*」、「*記錄錯誤與警告*」，或使用「*記錄特定事件*」選項，並選取此事件。

事件	記錄層級	資訊
DirXML_Warning	LOG_WARNING	所有 Identity Manager 警告都會記錄此事件。遇到的實際警告碼會儲存在事件中。 若要記錄警告，請選取「*記錄錯誤與警告*」，或使用「*記錄特定事件*」選項，並選取此事件。

如需根據這些事件建立 Novell Audit 通知的詳細資訊，請參閱「根據事件傳送通知」，第 220 頁。

遠端載入器事件

以下是從遠端載入器記錄的事件：

表格 ***10-3*** 遠端載入器事件

事件	記錄層級	資訊
遠端載入器啓動	LOG_INFO	若要在「遠端載入器」啓動時記錄，必須使用「*記錄特定事件*」選項，並選取此事件。
遠端載入器停止	LOG_INFO	若要在「遠端載入器」停止時記錄，必須使用「*記錄特定事件*」選項，並選取此事件。
遠端載入器連接已建立	LOG_INFO	若要在「遠端載入器」連接已建立時記錄，必須使用「*記錄特定事件*」選項，並選取此事件。
遠端載入器連接已中斷	LOG_INFO	若要在「遠端載入器」連接已中斷時記錄，必須使用「*記錄特定事件*」選項，並選取此事件。

如需根據這些事件建立 Novell Audit 通知的詳細資訊，請參閱「根據事件傳送通知」，第 220 頁。

10.4.2 使用者定義的事件

Identity Manager 可讓您設定自己的事件，使其記錄 Novell Audit。事件可以藉由在「規則產生器」中使用動作加以記錄，或者也可以在樣式表中記錄。定義規則時您可以存取的任何資訊均可加以記錄。

事件 **ID**

1000 至 1999 之間的事件 ID 會分配給使用者定義的事件。定義您自己的事件時，必須指定此範圍內的值做爲事件 ID。在 Novell Audit 中，此 ID 會與 Identity Manager 應用程式 ID 003 結合。

記錄層級

記錄層級可讓您根據要記錄的事件類型來分組事件。您可以使用下列預先定義的記錄層級：

表格 *10-4* 記錄層級

記錄層級	描述
log-emergency	導致 Metadirectory 引擎或驅動程式關閉的事件。
log-alert	需要立即注意的事件。
log-critical	可導致部份 Metadirectory 引擎或驅動程式故障的事件。
log-error	描述可由 Metadirectory 引擎或驅動程式處理之錯誤的事件。
log-warning	不代表問題的負面事件。
log-notice	管理員可用來瞭解或改善使用和操作的正面或負面事件。
log-info	任何重要的正面事件。
log-debug	可讓支援或工程師除錯 Metadirectory 引擎或驅動程式操作的相關事件。

使用規則產生器產生事件

在「規則產生器」中，藉由選取「產生事件」動作，可以記錄事件。

1. 選取產生事件之前要滿足的條件，然後選取「產生事件」動作。
2. 指定事件 ID。
3. 選取記錄層級。
4. 按一下「輸入字串」欄位旁邊的 圖示，以啓動「具名字串產生器」。
5. 使用「具名字串產生器」建構對應於自定資料欄位的具名字串：

6. 按一下「確定」，以返回「規則產生器」來建構規則的其餘部份。

如需如何設定規則組態以記錄事件的相關資訊，請參閱《規則產生器和驅動程式自訂指南》中的「產生事件」。

使用狀態文件產生事件

透過使用 <xsl:message> 元素之樣式表產生的狀態文件會傳送至 Novell Audit，其事件 ID 與狀態文件的層級屬性相對應，如下表中所指定：

表格 *10-5* 狀態文件

狀態層級	狀態事件 ID
成功	EV_LOG_STATUS_SUCCESS (1)
重試	EV_LOG_STATUS_RETRY (2)
警告	EV_LOG_STATUS_WARNING (3)

狀態層級	狀態事件 ID
錯誤	EV_LOG_STATUS_ERROR (4)
嚴重	EV_LOG_STATUS_FATAL (5)
使用者定義	EV_LOG_STATUS_OTHER (6)

下列範例會產生層級爲 EV_LOG_STATUS_ERROR 的 Novell Audit 事件 0x004 和 value1=7777：

```
<xsl:message> <status level="error" text1="This would be text1"
value="7777">This data would be in the blob and in text 2, since no
value is specified for text2 in the attributes.</status> </
xsl:message>
```

下列範例會產生層級爲 EV_LOG_STATUS_ERROR 的 Novell Audit 事件 0x004 和 value1=7778：

```
<xsl:message> <status level="error" text1="This would be text1"
text2="This would be text2" value1="7778">This data would be in the
blob only for this case, since a value for text2 is specified in the
attributes.</status> </xsl:message>
```

10.4.3 eDirectory 物件

本節提供儲存記錄資料之 Novell eDirectory 屬性的詳細資料。因爲這些物件的組態會根據您在 iManager 中的選項自動設定，所以您無需直接修改這些屬性。

您要記錄的 Identity Manager 事件儲存在「驅動程式集」物件或「驅動程式」物件上的 DirXML-LogEvent 屬性中。該屬性是多值整數，每個值都識別一個要記錄的事件 ID。

記錄事件之前，引擎會根據此屬性的內容檢查目前事件類型，以決定是否應該記錄該事件。

先前版本的 Identity Manager 是使用 DirXML-DriverTraceLevel 屬性來設定記錄層級。記錄層級是在每個「驅動程式」物件上指定，且不支援承襲。在 Identity Manager 2 以後的版本中，「驅動程式」物件可以從「驅動程式集」物件承襲此資訊。決定記錄設定時，驅動程式物件的 DirXML-DriverTraceLevel 屬性具有最高優先順序。如果「驅動程式」物件不包含 DirXML-DriverTraceLevel 屬性，則引擎會使用父驅動程式集物件的記錄設定。

10.5 查詢與報告

Novell Audit 提供兩種工具，可在 Novell Audit 資料庫中查詢事件：Novell Audit iManager 外掛程式和 Novell Audit Report (LReport)。

Novell Audit iManager 外掛程式是 Web 型態的 JDBC 資料庫查詢應用程式，可讓您使用下拉式清單和巨集快速建立和儲存查詢。

Novell Audit Report 是 Windows 型態的 ODBC 相容應用程式，可使用 SQL 查詢陳述式或 Crystal Decisions Reports 查詢 Oracle 和 MySQL 資料儲存 (或具有 ODBC 驅動程式支援的任何其他資料庫)。

請遵循 《*Novell Audit* 管理指南》中的指示，存取 Novell Audit iManager 外掛程式或設定 Novell Audit Report。在 Novell Audit 文件網站 (http://www.novell.com/documentation/nsureaudit) 上可找到此指南。

10.5.1 Identity Manager 報告

Identity Manager 提供一些 Crystal Decisions Reports (*.rpt)，這些報告可簡化 Identity Manager 中執行之一般操作相關資訊的收集。這些報告包含在 Identity Manager 安裝 CD 上。

設定 Novell Audit Report 的組態之後，即可執行這些報告，以及已定義的任何自定查詢和報告。如需使用 Novell Audit Report 中這些報告的相關資訊，請參閱 《*Novell Audit 1.0.3* 管理指南》中的 「使用 Novell Audit Report 中的報告 (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html)」。如需這些報告的範例，請參閱附錄 C 「Identity Manager 事件和報告」，第 243 頁 中的 「報告」，第 260 頁。

10.5.2 檢視 Identity Manager 事件

1. 在 「Novell Audit Report 工作空間」中，按一下 「事件」索引標籤，然後展開 「*DirXML*」資料夾。

   此清單包含所有預先定義的 Identity Manager 事件。連按兩下清單中的任何事件，以檢視事件內容。
2. 若要查詢 Identity Manager 事件，請以滑鼠右鍵按一下 「工作空間」中的事件，然後選取 「定義查詢」。
3. 當 「查詢專家」出現時，指定時間框架並驗證事件。
4. 若要執行此查詢，請選取 「工作空間」中的 「查詢」索引標籤，並以滑鼠右鍵按一下查詢名稱，然後選取 「執行」。

使用 SQL 陳述式，也可以建立查詢。所有 Identity Manager 事件都具有介於 109608 和 262144 之間的十進位 「事件 ID」。

10.6 根據事件傳送通知

Novell Audit 可在發生或未發生特定事件時傳送通知。通知可以根據一或多個事件和包含於這些事件中的任何值來傳送，而且可以傳送至任何記錄通道，讓您能夠將通知記錄至資料庫、Java 應用程式、SNMP 管理系統或數個其他位置。

如需建立通知的相關資訊，請參閱 *Novell Audit 1.0.3* 管理指南中的 「設定過濾器和事件通知的組態」(http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lg08.html#al0lg08)

10.7 使用狀態記錄

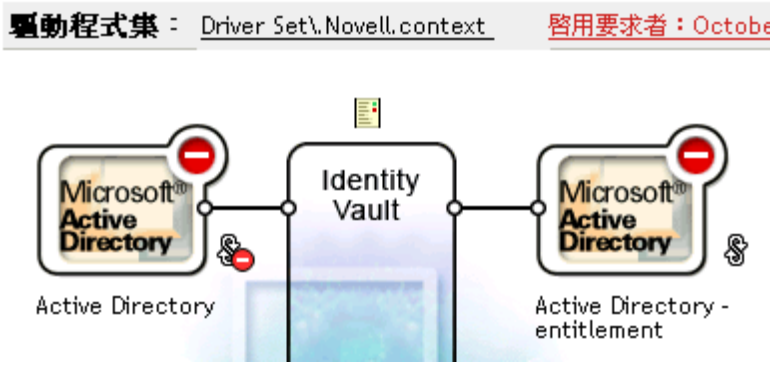
除了 Novell Audit 提供的功能之外，Identity Manager 還會記錄 「驅動程式集」物件和 「驅動程式」物件上指定數目的事件。這些狀態記錄可讓您檢視最近 Identity Manager 的活動。在記錄到達設定大小之後，時間最早的一半記錄會永久移除，以清理空間供較新的事件使用。因此，您應該將想要長時間追蹤的任何事件記錄至 Novell Audit 或報告和通知服務 (RNS)。

10.7.1 設定最大記錄大小

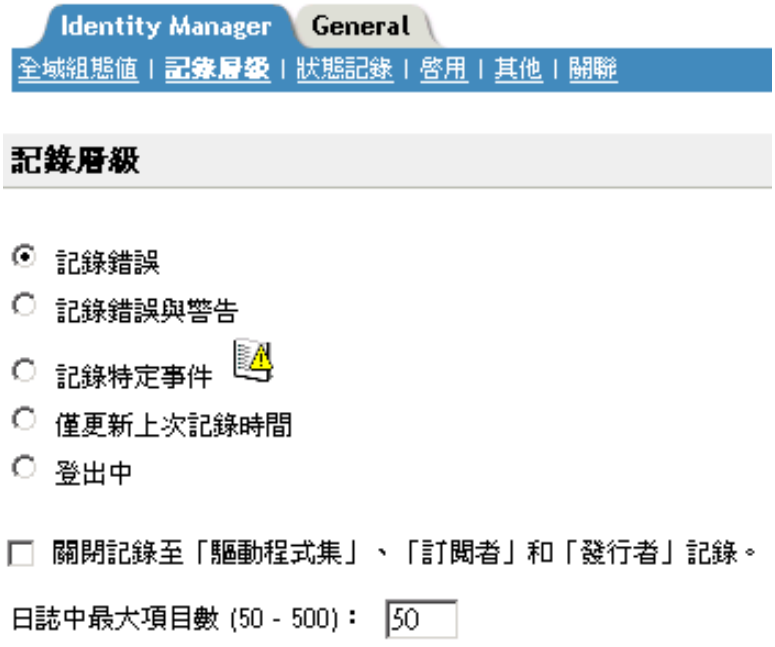
您可以設定狀態記錄的組態爲保留 50 至 500 個事件。此設定的組態可以在 「驅動程式集」物件上設定，使其由該驅動程式集內的所有驅動程式承襲，也可以針對該驅動程式集內的每個驅動程式設定。最大記錄大小獨立運作於您選取要記錄的事件之外，所以您可以設定要在「驅動程式集」上記錄的事件，然後針對其中的每個驅動程式指定不同的記錄大小。

在驅動程式集上設定記錄大小

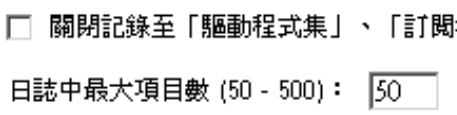
1. 在 iManager 中，選取 「*Identity Manager* > *Identity Manager* 概觀」，然後按 「下一步」。
2. 瀏覽至並選取 「驅動程式集」物件，然後按一下 「搜尋」。
3. 按一下 「驅動程式集」名稱，「修改物件」視窗即會出現。



4. 選取 「*Identity Manager*」索引標籤上的 「記錄層級」。



5 在「記錄中的最大項目數」欄位中，指定最大記錄大小：



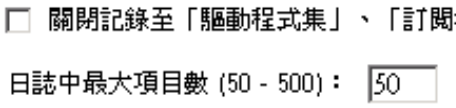
6 指定最大數目之後，按一下「確定」。

在驅動程式上設定記錄大小

1 在 iManager 中，選取「*Identity Manager* > *Identity Manager* 概觀」，然後按「下一步」。
2 瀏覽至並選取「驅動程式集」物件，然後按一下「搜尋」。
3 按一下驅動程式圖示的右上角，然後選取「編輯內容」。

4 選取「*Identity Manager*」索引標籤上的「記錄層級」。

5 在「記錄中的最大項目數」欄位中，指定最大記錄大小：



6 指定最大數目之後，按一下「確定」。

10.7.2 檢視狀態記錄

在 iManager 中，狀態記錄項目是以狀態記錄圖示  來代表。在 iManager 中，只要是看到此圖示的地方，您都可以於其中檢視短期記錄。您可以使用下列狀態記錄：

- 針對驅動程式集。
- 針對驅動程式集中每個驅動程式的「發行者」通道。
- 針對驅動程式集中每個驅動程式的「訂閱者」通道。

「發行者」和「訂閱者」通道的狀態記錄會報告驅動程式產生的通道特定訊息，例如未關聯物件的操作否決。

驅動程式集的狀態記錄僅包含引擎產生的訊息，例如驅動程式集中任何驅動程式的狀態變更。所有引擎訊息都會記錄下來。

DirXML 命令列公用程式

A

在 Identity Manager 安裝期間，公用程式和程序檔會安裝在所有平台上。公用程式的安裝位置如下：

- Windows：\Novell\Nds\dxcmd.bat
- NetWare：sys:\system\dxcmd.ncf
- UNIX：/usr/bin/dxcmd

有兩種不同的方法可以使用 「DirXML 命令列公用程式」。

- 「互動模式」，第 225 頁
- 「指令行模式」，第 233 頁

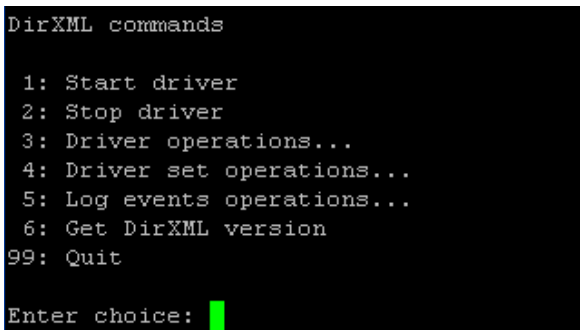
A.1 互動模式

互動模式提供文字介面，以便控制和使用 「DirXML 命令列公用程式」。

1. 在主控台輸入 dxcmd。
2. 輸入對 Identity Manager 物件具有足夠權限之使用者的名稱。

   範例：admin.novell
3. 輸入上面指定的使用者密碼。

   範例：novell



4. 輸入您要執行的指令編號。

   表格 A-1 頁上 226 包含選項和可用功能的清單。
5. 輸入 99 結束公用程式。

附註：如果您是在 Unix 或 Linux 上執行 eDirectory™ 8.8，則必須指定 -host 和 -port 參數，例如 dxcmd -host 10.0.0.1 -port 524。如果不指定這些參數，會發生 jclient 錯誤。

```
novell.jclient.JCException: connect (to address) 111 UNKNOWN ERROR
```

在預設狀態下，eDirectory 8.8 不會監聽本地主機。「DirXML 命令列公用程式」需要解析伺服器 IP 位址 (或主機名稱) 和連接埠，才能進行驗證。

表格 ***A-1*** 互動模式選項

選項	描述
1: *Start Driver*	啓動驅動程式。如果存在多個驅動程式，則每個驅動程式都會以編號列出。輸入驅動程式的編號，以啓動驅動程式。
2: *Stop Driver*	停止驅動程式。如果存在多個驅動程式，則每個驅動程式都會以編號列出。輸入驅動程式的編號，以停止驅動程式。
3: *Driver operations*	列出驅動程式可用的操作。如果存在多個驅動程式，則每個驅動程式都會以編號列出。輸入驅動程式的編號，以查看可用的操作。如需可用的操作，請參閱表格 A-2 頁上 226。
4: *Driver set operations*	列出驅動程式集可用的操作。 ◆ 1: Associate driver set with server ◆ 2: Disassociate driver set from server ◆ 99: Exit
5: *Log events operations*	列出可用來透過 Novell Audit 記錄事件的操作。如需這些選項的描述，請參閱表格 A-5 頁上 231。
6: *Get DirXML version*	列出已安裝之 Identity Manager 的版本。
99: *Quit*	離開「DirXML 命令列公用程式」。

特性 ***A-1*** 驅動程式選項

```
 1: Start driver
 2: Stop driver
 3: Get driver state
 4: Get driver start option
 5: Set driver start option
 6: Resync driver
 7: Migrate from application into DirXML
 8: Submit XDS command document to driver
 9: Check object password
10: Initialize new driver object
11: Passwords operations
12: Cache operations
99: Exit

Enter choice:
```

表格 ***A-2*** 驅動程式選項

選項	描述
1: *Start driver*	啓動驅動程式。

選項	描述
2: *Stop driver*	停止驅動程式。
3: *Get driver state*	列出驅動程式的狀態。 ◆ 0 - 驅動程式已停止 ◆ 1 - 驅動程式正在啓動 ◆ 2 - 驅動程式正在執行 ◆ 3 - 驅動程式正在停止
4: *Get driver start option*	列出目前的驅動程式啓動選項。 ◆ 1 - 停用 ◆ 2 - 手動 ◆ 3 - 自動
5: *Set driver start option*	變更驅動程式的啓動選項。 ◆ 1 - 停用 ◆ 2 - 手動 ◆ 3 - 自動 ◆ 99 - 結束
6: *Resync driver*	強制重新同步化驅動程式。此操作會提示您輸入時間延遲：*Do you want to specify a minimum time for resync? (yes/no).* 如果輸入 yes，請指定重新同步化發生的日期和時間：*Enter a date/time (format 9/27/05 3:27 PM).* 如果輸入 no，則會立即發生重新同步化。
7: *Migrate from application into DirXML*	處理包含查詢指令的 XML 文件：*Enter filename of XDS query document:* 使用 Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)，建立包含查詢指令的 XML 文件。 範例： NetWare：sys:\files\query.xml Windows：c:\files\query.xml Linux：/files/query.xml

選項	描述
8: *Submit XDS command document to driver*	處理 XDS 指令文件： *Enter filename of XDS command document:* 範例： NetWare：sys:\files\user.xml Windows：c:\files\user.xml Linux：/files/user.xml *Enter name of file for response:* 範例： NetWare：sys:\files\user.log Windows：c:\files\user.log Linux：/files/user.log
9: *Check object password*	驗證已連接系統中物件的密碼是否與驅動程式相關聯。此操作會比對物件的 eDirectory 密碼 (「配送密碼」，與「通用密碼」搭配使用)。 輸入使用者名稱：
10: *Initialize new driver object*	將新「驅動程式」物件上的資料進行內部啓始化，僅用於測試目的。
11: *Password operations*	「密碼」選項有九個。如需這些選項的描述，請參閱表格 A-3 頁上 229。
12: *Cache operations*	「快取」操作有五個。如需這些選項的描述，請參閱表格 A-4 頁上 230。
99: *Exit*	離開驅動程式選項。

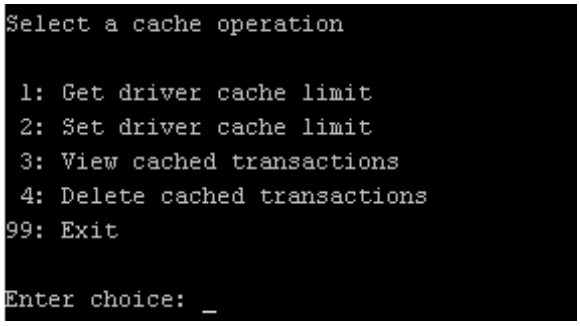
特性 ***A-2*** 密碼操作

```
Select a password operation

 1: Set shim password
 2: Clear shim password
 3: Set Remote Loader password
 4: Clear Remote Loader password
 5: Set named password
 6: Clear named password(s)
 7: List named passwords
 8: Get passwords state
99: Exit

Enter choice: _
```

表格 ***A-3*** 密碼操作

操作	描述
1: *Set shim password*	設定應用程式密碼。這是您用來驗證進入已連接系統所使用的使用者帳戶密碼。
2: *Clear shim password*	清除應用程式密碼。
3: *Set Remote Loader password*	「遠端載入器」密碼用於控制對「遠端載入器」例項的存取。如需相關資訊，請參閱第 3 章 「設定已連接系統。」，第 41 頁。 輸入「遠端載入器」密碼，然後重新輸入該密碼以進行確認。
4: *Clear Remote Loader password*	清除「遠端載入器」密碼，如此「驅動程式」物件上便不會設定任何「遠端載入器」密碼。
5: *Set named password*	可讓您將密碼或其他安全性資訊儲存在驅動程式上。如需相關資訊，請參閱「使用具名密碼」，第 27 頁。 您需要填入四個提示： ◆ Enter password name: ◆ Enter password description: ◆ Enter password: ◆ Confirm password
6: *Clear named passwords*	清除驅動程式物件上儲存的指定具名密碼或所有具名密碼：*Do you want to clear all named passwords? (yes/no).* 如果輸入 yes，則會清除所有具名密碼。如果輸入 no，則會提示您指定要清除的密碼名稱。
7: *List named passwords*	列出驅動程式物件上儲存的所有具名密碼。此操作會列出密碼名稱和密碼描述。
8: *Get password state*	列出是否已設定下列密碼： ◆ Driver Object password: ◆ Application password: ◆ Remote loader password: dxcmd 公用程式可讓您設定「應用程式」密碼和「遠端載入器」密碼。您無法使用此公用程式設定「驅動程式物件」密碼。程式會顯示是否已設定該密碼。
99: *Exit*	離開目前的功能表，返回「驅動程式」選項。

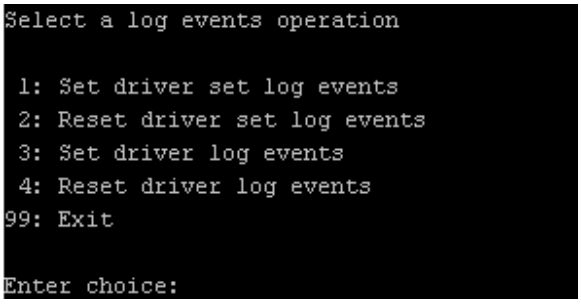
特性 ***A-3*** 快取操作



表格 ***A-4*** 快取操作

操作	描述
1: *Get driver cache limit*	顯示對驅動程式設定的目前快取限制。
2: *Set driver cache limit*	設定驅動程式快取限制 (以 KB 爲單位)。值爲 0 表示沒有限制。
3: *View cached transactions*	文字檔會建立，檔案內含快取中儲存的事件。您可以選取要檢視的異動數目。 ◆ Enter option token (default=0): ◆ Enter maximum transactions records to return (default=1): ◆ Enter name of file for response:
4: *Delete cached transactions*	刪除快取中儲存的異動。 ◆ Enter position token (default=0): ◆ Enter event-id value of first transaction record to delete (optional): ◆ Enter number of transaction records to delete (default=1):
99: *Exit*	離開目前的功能表，返回「驅動程式」選項。

特性 ***A-4*** 記錄事件操作



表格 ***A-5*** 記錄事件操作

操作	描述
1: *Set driver set log events*	可讓您透過 Novell Audit 記錄驅動程式集事件。有 49 個可選取記錄的項目。如需這些選項的清單，請參閱表格 A-6 頁上 231。 輸入您要記錄之項目的編號。選取項目之後，輸入 99 以接受選項。
2: *Reset driver set log events*	重設所有的記錄事件選項。
3: *Set driver log events*	可讓您透過 Novell Audit 記錄驅動程式事件。有 49 個可選取記錄的項目。如需這些選項的清單，請參閱表格 A-6 頁上 231。 輸入您要記錄之項目的編號。選取項目之後，輸入 99 以接受選項。
4: *Reset driver log events*	重設所有的記錄事件選項。
99: *Exit*	離開記錄事件操作功能表。

表格 ***A-6*** 驅動程式集和驅動程式記錄事件

選項
1: Status success
2: Status retry
3: Status warning
4: Status error
5: Status fatal
6: Status other
7: Query elements
8: Add elements
9: Remove elements
10: Modify elements
11: Rename elements
12: Move elements
13: Add-association elements
14: Remove-association elements
15: Query-schema elements
16: Check-password elements
17: Check-object-password elements

選項
18: Modify-password elements
19: Sync elements
20: Pre-transformed XDS document from shim
21: Post input transformation XDS document
22: Post output transformation XDS document
23: Post event transformation XDS document
24: Post placement transformation XDS document
25: Post create transformation XDS document
26: Post mapping transformation <inbound> XDS document
27: Post mapping transformation <outbound> XDS document
28: Post matching transformation XDS document
29: Post command transformation XDS document
30: Post-filtered XDS document <Publisher>
31: User agent XDS command document
32: Driver resync request
33: Driver migrate from application
34: Driver start
35: Driver stop
36: Password sync
37: Password request
38: Engine error
39: Engine warning
40: Add attribute
41: Clear attribute
42: Add value
43: Remove value
44: Merge entire
45: Get named password
46: Unknown
47: Unknown
48: User defined IDs
99: Accept checked items

A.2 指令行模式

指令行模式可讓您使用程序檔或批次檔案。表格 A-7 頁上 233 包含不同的可用選項。

若要使用指令行選項，請決定您想要使用的項目並將其串在一起。

範例：dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters

該指令會啓動驅動程式。

表格 ***A-7*** 指令行選項

選項	描述
組態	
-user *<user name>*	指定對您要測試之驅動程式具有管理權限的使用者名稱。
-host *<name or IP address>*	指定安裝驅動程式之伺服器的 IP 位址。
-password *<user password>*	針對上面指定的使用者指定密碼。
-port *<port number>*	如果不使用預設連接埠，請指定連接埠號碼。
-q *<quiet mode>*	執行指令時顯示極少的資訊。
-v *<verbose mode>*	執行指令時顯示詳細資訊。
-? *<show this message>*	顯示說明功能表。
-help *<show this message>*	顯示說明功能表。
動作	
-start *<driver dn>*	啓動驅動程式。
-stop *<driver dn>*	停止驅動程式。
-getstate *<driver dn>*	顯示驅動程式的狀態爲執行中或已停止。
-getstartoption *<driver dn>*	顯示驅動程式的啓動選項。
-setstartoption *<driver dn>* *<disabled|manual|auto>* *<resync|noresync>*	設定重新啓動伺服器時驅動程式的啓動方式。設定重新啓動驅動程式時是否重新同步化物件。
-getcachelimit *<driver dn>*	列出對驅動程式設定的快取限制。
-setcachelimit *<driver dn>* *<0 or positive integer>*	設定驅動程式的快取限制。
-migrateapp *<driver dn>* *<filename>*	處理包含查詢指令的 XML 文件。 藉由使用 Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html)，建立包含查詢指令的 XML 文件。
-setshimpassword *<driver dn>* *<password>*	設定應用程式密碼。這是您用來驗證進入已連接系統所使用的使用者帳戶密碼。
-clearshimpassword *<driver dn>* *<password>*	清除應用程式密碼。

選項	描述
-setremoteloaderpassword *<driver dn> <password>*	設定「遠端載入器」密碼。 「遠端載入器」密碼是用來控制對「遠端載入器」例項的存取。如需相關資訊，請參閱第 3 章 「設定已連接系統。」，第 41 頁。
<clearremoteloaderpassword *<driver dn>*	清除「遠端載入器」密碼。
-sendcommand *<driver dn> <input filename> <output filename>*	處理 XDS 指令文件。 將 XDS 指令文件指定爲輸入檔案。 範例： NetWare：sys:\files\user.xml Windows：c:\files\user.xml Linux：/files/user.log 指定輸出檔案名稱，以查看結果。 範例： NetWare：sys:\files\user.log Windows：c:\files\user.log Linux：/files/user.log
-setlogevents *<dn> <integer ...>*	設定驅動程式上的 Novell Audit 記錄事件。整數是要記錄之項目的選項。如需輸入之整數的清單，請參閱表格 A-6 頁上 231。
-clearlogevents *<dn>*	清除驅動程式上設定的所有 Novell Audit 記錄事件。
-setdriverset *<driver set dn>*	將驅動程式集與伺服器相關聯。
-cleardriverset	清除驅動程式集與伺服器的關聯。
-getversion	顯示已安裝之 Identity Manager 的版本。
-initdriver object *<dn>*	將新「驅動程式」物件上的資料進行內部啓始化，僅用於測試目的。
-setnamedpassword *<driver dn> <name> <password> [description]*	在驅動程式物件上設定具名密碼。指定具名密碼的名稱、密碼和描述。
-clearnamedpassword *<driver dn> <name>*	清除指定的具名密碼。
-clearallnamedpaswords *<driver dn>*	清除特定驅動程式上設定的所有具名密碼。

設定遠端載入器組態的選項

B

下表中的選項可讓您設定 「遠端載入器」的組態。

表格 ***B-1*** 遠端載入器選項

選項	次要名稱	參數	描述
address		IP address	選擇性參數。指定 「遠端載入器」在特定本地 IP 位址上監聽。如果代管 「遠端載入器」的伺服器具有多個 IP 位址，並且 「遠端載入器」必須僅在其中一個位址上監聽，此選項便很有用處。 有三個選項：address=*address number* address= 捻 ocalhost' Don't use this parameter. 如果不使用 -address，則 「遠端載入器」會在所有本地 IP 位址上監聽。 範例：address=137.65.134.83
-class	-cl	Java class name	指定要裝載之 Identity Manager 應用程式 Shim 的 Java 類別名稱。 例如，針對 Java 驅動程式，輸入下列其中一項： -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java 會使用 KeyStore 來讀取證書。-class 選項與 -module 選項互斥。 若要查看 Java 類別名稱的清單，請參閱表格 B-2 頁上 240。
-commandport	-cp	port number	指定 「遠端載入器」例項用於控制的 TCP/IP 連接埠。如果 「遠端載入器」例項正在裝載應用程式 Shim，則指令連接埠是另一個 「遠端載入器」例項與裝載 Shim 之例項進行通訊的連接埠。如果 「遠端載入器」例項正在將指令傳送至裝載應用程式 Shim 的例項，則指令連接埠是裝載例項正在其上監聽的連接埠。如果未指定，則預設指令連接埠爲 8000。藉由指定不同的連接埠和指令連接埠，「遠端載入器」的多個例項可以在裝載不同驅動程式例項的同一伺服器上執行。 範例： -commandport 8001 -cp 8001

選項	次要名稱	參數	描述
-config	無	filename	指定組態檔案。組態檔案可以包含除 config 之外的任何指令行選項。在指令行上指定的選項會置換組態檔案中指定的選項。 範例： -config config.txt
-connection	-conn	connection configuration string	指定用於連接執行 Identity Manager 遠端介面 Shim 之 Metadirectory 伺服器的連接參數。「遠端載入器」的預設連接方法是使用保全插槽層 (SSL) 的 TCP/IP。此連接的預設 TCP/IP 連接埠是 8090。多個「遠端載入器」例項可以在相同的伺服器上執行。每個「遠端載入器」例項會裝載一個個別的 Identity Manager 應用程式 Shim 例項。藉由指定不同的連接埠和指令連接埠給每個「遠端載入器」例項，區分多個「遠端載入器」例項。 範例： -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
-description	-desc	short description	指定要用於追蹤視窗標題和 Novell® Audit 記錄的簡短描述字串 (例如 SAP)。 範例： -description SAP -desc SAP 「遠端載入器主控台」在組態檔案中使用的是完整格式。您可以使用完整格式 (例如 -description) 或簡短格式 (例如 -desc)。
-help	-?	無	顯示說明。 範例： -help -?
-java	-j	無	指定要爲 Java Shim 例項設定密碼。只有在與 setpasswords 選項一起使用時，此選項才有用處。如果指定 -class 的同時也指定了 苦 etpasswords，則不需要此選項。
-javadebugport	-jdp	Port number	指定「遠端載入器」例項要在指定的連接埠上啓用 Java 除錯。此選項對於 Identity Manager 應用程式 Shim 的開發人員而言很有用處。 範例： -javadebugport 8080 -jdp 8080

選項	次要名稱	參數	描述
keystore			條件參數。僅用於 .jar 檔案中包含的 Identity Manager 應用程式 Shim。 指定 Java KeyStore 的檔名，該 Java KeyStore 包含遠端介面 Shim 使用之證書發證者的託管根部證書。這通常是裝載遠端介面 Shim 之 eDirectory™ 網路樹的「證書權限」。 如果您正在執行保全插槽層 (SSL)，並需要「遠端載入器」來與 Java 驅動程式通訊，請輸入鍵值配對： keystore='*keystorename*' storepass='*password*'
-module	-m	modulename	指定包含要裝載之 Identity Manager 應用程式 Shim 的模組。 例如，針對原生驅動程式，輸入下列其中一項： -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" 或 -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module 選項會使用根部檔案證書。-module 選項與 -class 選項互斥。
-password	-p	password	指定用於指令驗證的密碼。此密碼必須與第一個密碼 (即使用 setpasswords 對接受指令之載入器例項指定的密碼) 相同。如果已指定指令選項 (例如 unload 或 tracechange)，但未指定 password 選項，則會提示使用者輸入指令的目標載入器密碼。 範例： -password novell4 -p novell4
port		decimal port number	必要的參數。它會指定 TCP/IP 連接埠，「遠端載入器」會在該連接埠上監聽遠端介面 Shim 的連接。 範例： port=8090
rootfile			條件參數。如果您正在執行保全插槽層 (SSL)，並需要「遠端載入器」來與原生驅動程式通訊，請輸入 rootfile='*trusted certname*'

選項	次要名稱	參數	描述
-service	-serv	無或 install/ uninstall	若要安裝例項做爲服務，請將 install 引數與裝載應用程式 Shim 所需的任何其他引數搭配使用。例如，所使用的引數必須包含 -module，但是任何引數都可以包含 -connection、- commandport 等等。 此選項會安裝 Win32 服務，但是不會啓動該服務。 若要解除安裝做爲服務執行的例項，請將 uninstall 引數與裝載應用程式 Shim 所需的任何其他引數搭配使用。 僅針對做爲 Win32 服務執行的例項，才會在指令行上使用此選項的無引數版本。安裝例項做爲服務時，會自動進行設定。 範例： -service install -serv uninstall 在 rdxml 或「Java 遠端載入器」上無法使用此選項。
-setpasswords	-sp	password password	指定「遠端載入器」例項的密碼，以及與「遠端載入器」通訊之遠端介面 Shim 的「Identity Manager 驅動程式」物件密碼。引數中的第一個密碼是「遠端載入器」的密碼。選擇性引數中的第二個密碼是「Identity Manager 驅動程式」物件的密碼，該物件與 Metadirectory 伺服器上的遠端介面 Shim 相關聯。您必須不指定密碼，或是兩個密碼都指定。如果不指定密碼，則「遠端載入器」會提示您指定密碼。這是組態選項。使用此選項可以設定「遠端載入器」例項指定密碼，但不載入 Identity Manager 應用程式 Shim 或與其他載入器例項通訊。 範例： -setpasswords novell4 staccato3 -sp novell4 staccato3
-storepass		storepass	僅用於 .jar 檔案中包含的 Identity Manager 應用程式 Shim。指定由 KeyStore 參數所指定的 Java KeyStore 密碼。 範例： storepass=mypassword 此選項僅適用於「Java 遠端載入器」。
-trace	-t	integer	指定追蹤層級。這僅在裝載應用程式 Shim 時使用。追蹤層級對應 Metadirectory 伺服器上使用的追蹤層級。 範例： -trace 3 -t 3

選項	次要名稱	參數	描述
-tracechange	-tc	integer	指示裝載應用程式 Shim 的「遠端載入器」例項變更其追蹤層級。追蹤層級對應 Metadirectory 伺服器上使用的追蹤層級。 範例： -tracechange 1 -tc 1
-tracefile	-tf	filename	指定要在其中寫入追蹤訊息的檔案。如果追蹤層級大於零，追蹤訊息就會寫入該檔案。即使追蹤視窗未開啓，追蹤訊息也會寫入檔案。 範例： -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	-tfc	無或 filename	指示裝載應用程式 Shim 的「遠端載入器」例項開始使用追蹤檔案，或者關閉使用中的追蹤檔案並使用新的追蹤檔案。使用此選項的無引數版本，會導致裝載的例項關閉任何正在使用的追蹤檔案。 範例： -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt
-tracefilemax	-tfm	size	指定追蹤檔案資料可在磁碟上佔用的大約大小上限。如果指定此選項，則會產生具有以 tracefile 選項指定之名稱的追蹤檔案，並會有最多 9 個額外的「延展」檔案。延展檔案是以使用主追蹤檔名加上 "*_n*" 爲其命名基礎，其中 n 是 1 至 9 的數字。 size 參數是位元組的數目。使用字尾 K、M 或 G 來代表千位元組、百萬位元組或十億位元組，以指定大小。 「遠端載入器」啓動時，如果追蹤檔案資料大於指定的最大值，則在所有 10 個檔案都完成延展之前，追蹤檔案資料會保持大於指定的最大值。 範例： -tracefilemax 1000M -tfm 1000M 在此範例中，追蹤檔案可以只有 1 GB。
-unload	-u	無	卸載「遠端載入器」例項。如果「遠端載入器」正在做爲 Win32 服務執行，則此指令會停止該服務。 範例： -unload -u

選項	次要名稱	參數	描述
-window	-w	On/Off	在「遠端載入器」例項中開啓或關閉追蹤視窗。 範例： -window on -w off 此選項只能用於 Windows 平台。在「Java 遠端載入器」上無法使用它。
-wizard	-wiz	無	啓動「組態精靈」。執行不帶指令行參數的 dirxml_remote.exe 亦會啓動該精靈。如果同時指定了組態檔案，則此選項會很有用處。在這種情況下，精靈啓動時會使用組態檔案中的值，並且您可以使用精靈來變更組態，而無需直接編輯組態檔案。 範例： -wizard -wiz 只有 Windows 平台上才有此選項可用，在「Java 遠端載入器」上則無從使用。

表格 ***B-2*** *Java* 類別名稱

Java 類別名稱	驅動程式
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX 驅動程式
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	分隔文字驅動程式
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory 驅動程式
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	授權服務驅動程式
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise 驅動程式
com.novell.nds.dirxml.jdbc.JDBCDriverShim	JDBC 驅動程式
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP 驅動程式
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	迴路驅動程式
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手動任務驅動程式
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS 驅動程式
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes 驅動程式
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft 驅動程式
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR 驅動程式
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	SAP 使用者管理驅動程式
com.novell.nds.dirxml.driver.sifagent.SIFShim	SIF 驅動程式
com.novell.nds.dirxml.driver.soap.SOAPDriver	Soap 驅動程式

Java 類別名稱	驅動程式
com.novell.idm.driver.ComposerDriverShim	使用者應用程式
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	補救 ARS 的驅動程式

Identity Manager 事件和報告

C

本節包含 Identity Manager 記錄之所有 Novell® Audit 事件的清單，還包含可使用 Novel Audit 執行之報告的範例。「報告」，第 260 頁包含報告的範例。

每個事件上都有下列儲存資訊：事件 ID、描述、策劃者標題、目標標題、子目標標題、文字 1 標題、文字 2 標題、文字 3 標題、值 1 標題、值 1 類型、值 2 標題、值 2 類型、值 3 標題、值 3 類型、群組標題、群組類型、資料標題、資料類型、顯示綱要。

下列元件的事件位於表格中。

C.1 引擎事件

該表格包含可透過 Novell Audit 稽核之引擎事件的清單。

表格 *C-1* 引擎事件欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	目標標題	子目標標題
30001	狀態成功	通道	src-dn (dest-dn)	層級
30002	狀態重試	通道	src-dn (dest-dn)	層級
30003	狀態警告	通道	src-dn (dest-dn)	層級
30004	狀態錯誤	通道	src-dn (dest-dn)	層級
30005	狀態嚴重錯誤	通道	src-dn (dest-dn)	層級
30006	狀態其他	通道	src-dn (dest-dn)	層級
30007	搜尋	通道	dest-dn 或關聯	範圍
30008	新增項目	通道	dest-dn 或關聯	屬性名稱
30009	刪除項目	通道	dest-dn 或關聯	屬性名稱

事件 ID	描述	策劃者標題	目標標題	子目標標題
3000A	修改項目	通道	dest-dn 或關聯	屬性名稱
3000B	重新命名項目	通道	dest-dn 或關聯	物件類型
3000C	移動項目	通道	dest-dn 或關聯	移動目的
3000D	新增關聯	通道	dest-dn	屬性名稱
3000E	移除關聯	通道		屬性名稱
3000F	查詢綱要	通道		
30010	檢查密碼	通道	驅動程式	
30011	檢查物件密碼	通道	dest-dn 或關聯	
30012	變更密碼	通道	dest-dn 或關聯	
30013	Sync	通道	dest-dn 或關聯	屬性名稱
30014	輸入 XML 文件	通道		屬性名稱
30015	輸入轉換文件	通道		
30016	輸出轉換文件	通道		
30017	事件轉換文件	通道		
30018	佈置規則轉換文件	通道		
30019	建立規則轉換文件	通道		
3001A	輸入映射規則轉換文件	通道		
3001B	輸出映射規則轉換文件	通道		
3001C	相符規則轉換文件	通道		
3001D	指令轉換文件	通道		
3001E	發行者過濾器轉換文件	通道		
3001F	使用者代辦申請	通道		
30020	重新同步化驅動程式	通道	驅動程式	
30021	移轉	通道	關聯	屬性名稱
30022	驅動程式啓動	驅動程式集	驅動程式	
30023	驅動程式停止	驅動程式停止	驅動程式	
30024	密碼同步化	通道	物件	屬性名稱
30025	密碼重設	通道	dest-dn 或關聯	屬性名稱
30026	DirXML 錯誤	通道	物件	
30027	DirXML 警告	通道	物件	
30028	自定操作	通道		
30029	清除屬性	通道	dest-dn 或關聯	屬性名稱

事件 ID	描述	策劃者標題	目標標題	子目標標題
3002A	新增值 - 修改項目	通道	dest-dn 或關聯	屬性名稱
3002B	移除值	通道	dest-dn 或關聯	屬性名稱
3002C	合併項目	通道	物件	屬性名稱
3002D	取得具名密碼	驅動程式或通道	物件	
3002E	重設屬性	通道	物件	通道
3002F	新增值 - 新增項目	通道	dest-dn 或關聯	屬性名稱

表格 ***C-2*** 引擎事件欄位：文字 *1* 標題、文字 *2* 標題和文字 *3* 標題

事件 ID	描述	文字 1 標題	文字 2 標題	文字 3 標題
30001	狀態成功	類型	狀態文件	事件 ID
30002	狀態重試	類型	狀態文件	事件 ID
30003	狀態警告	類型	狀態文件	事件 ID
30004	狀態錯誤	類型	狀態文件	事件 ID
30005	狀態嚴重錯誤	類型	狀態文件	事件 ID
30006	狀態其他	類型	狀態文件	事件 ID
30007	搜尋	物件類型		事件 ID
30008	新增項目	物件類型	src-dn	事件 ID
30009	刪除項目	物件類型	src-dn	事件 ID
3000A	修改項目	物件類型	src-dn	事件 ID
3000B	重新命名項目	新名稱	src-dn	事件 ID
3000C	移動項目	移動關聯	src-dn	事件 ID
3000D	新增關聯	關聯		事件 ID
3000E	移除關聯	關聯		事件 ID
3000F	查詢綱要			事件 ID
30010	檢查密碼			
30011	檢查物件密碼			事件 ID
30012	變更密碼	物件類型	src-dn	事件 ID
30013	同步化	物件類型	關聯	類型
30014	輸入 XML 文件			警告訊息
30015	輸入轉換文件			警告訊息
30016	輸出轉換文件			警告訊息
30017	事件轉換文件			警告訊息

事件 ID	描述	文字 1 標題	文字 2 標題	文字 3 標題
30018	佈置規則轉換文件			警告訊息
30019	建立規則轉換文件			警告訊息
3001A	輸入映射規則轉換文件			警告訊息
3001B	輸出映射規則轉換文件			警告訊息
3001C	相符規則轉換文件			警告訊息
3001D	指令轉換文件			警告訊息
3001E	發行者過濾器轉換文件			警告訊息
3001F	使用者代辦申請			
30020	重新同步化驅動程式			錯誤訊息
30021	移轉	物件類型		警告訊息
30022	驅動程式啓動			驅動程式訊息
30023	驅動程式停止			驅動程式訊息
30024	密碼同步化			
30025	密碼重設		src-dn	
30026	DirXML 錯誤	錯誤訊息		
30027	DirXML 警告	警告訊息		
30028	自定操作			
30029	清除屬性		src-dn	事件 ID
3002A	新增值 - 修改項目	值	src-dn	事件 ID
3002B	移除值	值	src-dn	事件 ID
3002C	合併項目	物件類型	通道	關聯
3002D	取得具名密碼	密碼名稱		事件 ID
3002E	重設屬性			
3002F	新增值 - 新增項目	值	src-dn	事件 ID

表格 ***C-3*** 引擎事件欄位：值 *1* 標題、值 *2* 標題和值 *3* 標題

事件 ID	描述	值 1 標題	值 2 標題	值 3 標題
30001	狀態成功			
30002	狀態重試			
30003	狀態警告			
30004	狀態錯誤			
30005	狀態嚴重錯誤			

事件 ID	描述	值 1 標題	值 2 標題	值 3 標題
30006	狀態其他			
30007	搜尋			結果
30008	新增項目			結果
30009	刪除項目			結果
3000A	修改項目			結果
3000B	重新命名項目			結果
3000C	移動項目			結果
3000D	新增關聯			結果
3000E	移除關聯			結果
3000F	查詢綱要			結果
30010	檢查密碼			
30011	檢查物件密碼			
30012	變更密碼			結果
30013	同步化			結果
30014	輸入 XML 文件			
30015	輸入轉換文件			
30016	輸出轉換文件			
30017	事件轉換文件			
30018	佈置規則轉換文件			
30019	建立規則轉換文件			
3001A	輸入映射規則轉換文件			
3001B	輸出映射規則轉換文件			
3001C	相符規則轉換文件			
3001D	指令轉換文件			
3001E	發行者過濾器轉換文件			
3001F	使用者代辦申請			結果
30020	重新同步化驅動程式			結果
30021	移轉			
30022	驅動程式啓動	狀態		
30023	驅動程式停止	狀態		
30024	密碼同步化			結果
30025	密碼重設			

事件 ID	描述	值 1 標題	值 2 標題	值 3 標題
30026	DirXML 錯誤	程式碼		
30027	DirXML 警告	程式碼		
30028	自定操作			
30029	清除屬性			結果
3002A	新增值 - 修改項目			結果
3002B	移除值			結果
3002C	合併項目			
3002D	取得具名密碼			結果
3002E	重設屬性			
3002F	新增值 - 新增項目			結果

表格 ***C-4*** 引擎事件欄位：資料類型和觸發

事件 ID	描述	資料類型	觸發
30001	狀態成功	XML 文件	許多不同的事件可以引起狀態成功事件發生。該事件通常表示操作已順利完成。
30002	狀態重試	XML 文件	許多不同的事件可以引起狀態重試事件發生。該事件表示操作未完成，必須稍後再試。
30003	狀態警告	XML 文件	許多不同的事件可以引起狀態警告事件發生。該事件通常表示操作已完成，但存在次要問題。
30004	狀態錯誤	XML 文件	許多不同的事件可以引起狀態錯誤事件發生。該事件通常表示未順利完成操作。
30005	狀態嚴重錯誤	XML 文件	許多不同的事件可以引起狀態嚴重錯誤事件發生。該事件通常表示未順利完成操作，且引擎或驅動程式無法繼續。
30006	狀態其他	XML 文件	如果處理任何狀態文件的層級不在先前定義的五個層級之內，就會建立狀態其他事件。這些事件僅可以在樣式表或規則內產生。
30007	搜尋	XML 文件	發生於查詢文件傳送至 IDM 引擎或驅動程式時。
30008	新增項目	XML 文件	發生於新增物件時。
30009	刪除項目	XML 文件	發生於刪除物件時。
3000A	修改項目	XML 文件	發生於修改物件時。

事件 ID	描述	資料類型	觸發
3000B	重新命名項目	XML 文件	發生於重新命名物件時。
3000C	移動項目	XML 文件	發生於移動物件時。
3000D	新增關聯	XML 文件	發生於新增關聯時。該事件可能會在新增或相符時發生。
3000E	移除關聯	XML 文件	刪除物件時，沒有移除關聯事件。在不同的應用程式中刪除「使用者」物件，並隨後將刪除轉換成會移除關聯的修改時，移除關聯就會發生。
3000F	查詢綱要	XML 文件	發生於查詢綱要操作傳送至 IDM 引擎或驅動程式時。
30010	檢查密碼		透過 iManager 啓始的手動功能
30011	檢查物件密碼	XML 文件	發生於發出申請以檢查物件密碼 (而非驅動程式) 時。
30012	變更密碼	XML 文件	發生於發出申請以檢查「驅動程式」密碼時。
30013	同步化	XML 文件	發生於申請「同步化」事件時。
30014	輸入 XML 文件	XML 文件	只要引擎或驅動程式建立輸入文件，就會產生。
30015	輸入轉換文件	XML 文件	產生於輸入轉換規則處理之後，可讓使用者檢視轉換過的文件。
30016	輸出轉換文件	XML 文件	產生於輸出轉換規則處理之後，可讓使用者檢視轉換過的文件。
30017	事件轉換文件	XML 文件	產生於事件轉換規則處理之後，可讓使用者檢視轉換過的文件。
30018	佈置規則轉換文件	XML 文件	產生於佈置規則處理之後，可讓使用者檢視轉換過的文件。
30019	建立規則轉換文件	XML 文件	產生於建立規則處理之後，可讓使用者檢視轉換過的文件。
3001A	輸入映射規則轉換文件	XML 文件	產生於綱要映射規則處理之後，而規則會將文件轉換成 eDirectory 綱要。
3001B	輸出映射規則轉換文件	XML 文件	產生於綱要映射規則處理之後，而規則會將文件轉換成應用程式綱要。
3001C	相符規則轉換文件	XML 文件	產生於相符規則處理之後，可讓使用者檢視轉換過的文件。
3001D	指令轉換文件	XML 文件	產生於指令轉換規則處理之後，可讓使用者檢視轉換過的文件。
3001E	發行者過濾器轉換文件	XML 文件	產生於發行者通道的通知過濾器處理之後，可讓使用者檢視轉換過的文件。

事件 ID	描述	資料類型	觸發
3001F	使用者代辦申請	XML 文件	發生於「使用者代辦 XDS」指令文件傳送至訂閱者通道上的「驅動程式」時。
30020	重新同步化驅動程式		發生於發出重新同步化申請時。
30021	移轉		發生於發出移轉申請時。
30022	驅動程式啓動	XML 文件	發生於啓動驅動程式時。
30023	驅動程式停止	XML 文件	發生於停止驅動程式時。
30024	密碼同步化		產生於設定物件的配送或簡易密碼時。
30025	密碼重設		產生於密碼同步化操作失敗之後重設已連接應用程式密碼時。
30026	DirXML 錯誤		只要引擎發生內部錯誤，就會產生。
30027	DirXML 警告		只要引擎發生內部警告，就會產生。
30028	自定操作	XML 文件	發生於輸入文件中出現不明操作時。已知操作的範例是新增、刪除或修改。
30029	清除屬性		發生於修改操作包含 remove-all-value 元素時。
3002A	新增值 - 修改項目	值	發生於在物件的修改期間新增值時。
3002B	移除值	值	發生於修改操作包含 remove-value 元素時。
3002C	合併項目	XML 文件	發生於合併兩個物件時。
3002D	取得具名密碼	XML 文件	產生於「取得具名密碼」操作時。
3002E	重設屬性	XML 文件	發生於在發行者或訂閱者通道上發出「重設」文件時。
3002F	新增值 - 新增項目	值	發生於在物件的建立期間新增值時。

C.2 伺服器事件

下列表格包含可以透過 Novell Audit 進行稽核之伺服器事件的清單。

表格 ***C-5*** 伺服器事件欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	目標標題	子目標標題
307D0	組態：記錄事件	伺服器	驅動程式	屬性名稱

事件 ID	描述	策劃者標題	目標標題	子目標標題
307D1	組態：驅動程式快取限制	伺服器	驅動程式	屬性名稱
307D2	組態：驅動程式集	伺服器	伺服器	屬性名稱
307D3	組態：驅動程式啓動選項	伺服器	驅動程式	屬性名稱
307D4	驅動程式重新同步化	伺服器	驅動程式	
307D5	移轉應用程式伺服器	伺服器	驅動程式	
307D6	Shim 密碼設定	伺服器	驅動程式	屬性名稱
307D7	鍵入密碼設定	伺服器	驅動程式	
307D8	遠端載入器密碼設定	伺服器	驅動程式	屬性名稱

表格 ***C-6*** 伺服器事件欄位：文字 *1* 標題、文字 *2* 標題和文字 *3* 標題

事件 ID	描述	文字 1 標題	文字 2 標題	文字 3 標題
307D0	組態：記錄事件			操作
307D1	組態：驅動程式快取限制			
307D2	組態：驅動程式集	驅動程式集	類型	
307D3	組態：驅動程式啓動選項			訊息
307D4	驅動程式重新同步化			
307D5	移轉應用程式伺服器			
307D6	Shim 密碼設定			
307D7	鍵入密碼設定		類型	
307D8	遠端載入器密碼設定			

表格 ***C-7*** 伺服器事件欄位：值 *1* 標題、值 *2* 標題和值 *3* 標題

事件 ID	描述	值 1 標題	值 2 標題	值 3 標題
307D0	組態：記錄事件			結果
307D1	組態：驅動程式快取限制	限制		結果

事件 ID	描述	值 1 標題	值 2 標題	值 3 標題
307D2	組態：驅動程式集			結果
307D3	組態：驅動程式啓動選項	啓動選項		結果
307D4	驅動程式重新同步化			結果
307D5	移轉應用程式伺服器			結果
307D6	Shim 密碼設定		版本	結果
307D7	鍵入密碼設定			結果
307D8	遠端載入器密碼設定		版本	結果

表格 ***C-8*** 伺服器事件欄位：資料類型和觸發

事件 ID	描述	資料類型	觸發
307D0	組態：記錄事件	輸入緩衝區	發生於「驅動程式」或「驅動程式集」物件上的記錄事件屬性變更時。
307D1	組態：驅動程式快取限制		發生於「驅動程式」物件上的「驅動程式快取限制」屬性變更時。
307D2	組態：驅動程式集	輸入緩衝區	發生於「驅動程式集」/「伺服器」關聯變更時。
307D3	組態：驅動程式啓動選項	輸入緩衝區	發生於「驅動程式」物件的「驅動程式啓動選項」變更時。
307D4	驅動程式重新同步化		發生於發出驅動程式重新同步化要求時。
307D5	移轉應用程式伺服器	XML 文件	發生於應用程式伺服器發生移轉時。
307D6	Shim 密碼設定		發生於設定「應用程式」密碼時。
307D7	鍵入密碼設定		
307D8	遠端載入器密碼設定		發生於設定「遠端載入器」密碼時。

C.3 遠端載入器事件

表格包含可以透過 Novell Audit 稽核之「遠端載入器」事件的清單。

表格 ***C-9*** 遠端載入器事件欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	觸發
30BB8	遠端載入器啓動	例項	發生於「遠端載入器」啓動時。
30BB9	遠端載入器停止	例項	發生於「遠端載入器」停止時。
30BBA	遠端載入器連接已建立	例項	發生於「遠端載入器」連接建立時。
30BBB	遠端載入器連接已中斷	例項	發生於「遠端載入器」連接中斷時。

C.4 詳細資料入口網站應用程式

表格 ***C-10*** 詳細資料入口網站應用程式欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	目標標題	子目標標題
31400	Delete_Entity	使用者名稱	實體 DN	實體定義
31401	Update_Entity	使用者名稱	實體 DN	實體定義

表格 ***C-11*** 詳細資料入口網站應用程式欄位：群組標題、群組類型和觸發

事件 ID	描述	群組標題	群組類型	觸發
31400	Delete_Entity	群組號碼	數字	發生於刪除物件時。
31401	Update_Entity	群組號碼	數字	發生於修改物件時。

C.5 變更密碼入口網站應用程式

表格 ***C-12*** 變更密碼入口網站應用程式欄位：策劃者標題、目標標題和文字 *3* 標題

事件 ID	描述	策劃者標題	目標標題	文字 3 標題
31420	Change_Password_Failure	啓始者 ID	目標 DN	錯誤訊息
31421	Change_Password_Success	啓始者 ID	目標 DN	

表格 ***C-13*** 變更密碼入口網站應用程式欄位：值 *3* 標題、值 *3* 類型和觸發

事件 ID	描述	值 3 標題	值 3 類型	觸發
31420	Change_Password_Failure	錯誤編號	布林值	發生於密碼變更失敗時。
31421	Change_Password_Success			發生於密碼變更成功時。

C.6 忘記密碼變更密碼入口網站應用程式

表格 *C-14* 忘記密碼變更密碼入口網站應用程式欄位：策劃者標題、目標標題和文字 *3* 標題

事件 ID	描述	策劃者標題	目標標題	文字 3 標題
31420	Forgot_Password_Change_Failure	啓始者 ID	目標 DN	錯誤訊息
31421	Forgot_Password_Change_Success	啓始者 ID	目標 DN	

表格 *C-15* 忘記密碼變更密碼入口網站應用程式欄位：值 *3* 標題、值 *3* 類型和群組標題

事件 ID	描述	值 3 標題	值 3 類型	群組標題
31420	Forgot_Password_Change_Failure	錯誤編號	布林值	群組編號
31421	Forgot_Password_Change_Success			群組編號

表格 *C-16* 忘記密碼變更密碼入口網站應用程式欄位：群組類型和觸發

事件 ID	描述	群組類型	觸發
31420	Forgot_Password_Change_Failure	數字	發生於「忘記密碼」變更失敗時。
31421	Forgot_Password_Change_Success	數字	發生於「忘記密碼」變更成功時。

C.7 搜尋清單入口網站應用程式

表格 *C-17* 搜尋清單入口網站應用程式欄位：策劃者標題、目標標題和群組標題

事件 ID	描述	策劃者標題	目標標題	群組標題
31430	Search_Request	使用者 ID	搜尋鍵	使用者 ID
31431	Search_Saved	使用者 ID	搜尋鍵	使用者 ID

表格 *C-18* 搜尋清單入口網站應用程式欄位：群組類型、資料標題和資料類型

事件 ID	描述	群組類型	資料標題	資料類型
31430	Search_Request	數字	搜尋 XML	字串
31431	Search_Saved	數字	搜尋 XML	字串

表格 ***C-19*** 搜尋清單入口網站應用程式欄位：觸發

事件 ID	描述	觸發
31430	Search_Request	發生於使用者執行搜尋申請時。
31431	Search_Saved	發生於使用者選取「我已儲存的搜尋」時。

C.8 建立入口網站應用程式

表格 ***C-20*** 建立入口網站應用程式欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	目標標題	子目標標題
31440	Create_Entity	使用者名稱	實體 DN	實體定義

表格 ***C-21*** 建立入口網站應用程式欄位：觸發

事件 ID	描述	觸發
31440	Create_Entity	發生於建立物件時。

C.9 安全性網路位置

表格包含可以透過 Novell Audit 稽核之安全性事件的清單。

表格 ***C-22*** 安全性網路位置欄位：策劃者標題、目標標題和文字 *1* 標題

事件 ID	描述	策劃者標題	目標標題	文字 1 標題
31540	Create_Proxy_Definition_Success	啓始者 ID	定義	詳細資料
31541	Create_Proxy_Definition_Failure	啓始者 ID	定義	詳細資料
31542	Update_Proxy_Definition_Success	啓始者 ID	定義	詳細資料
31543	Update_Proxy_Definition_Failure	啓始者 ID	定義	詳細資料
31544	Delete_Proxy_Definition_Success	啓始者 ID	定義	詳細資料
31545	Delete_Proxy_Definition_Failure	啓始者 ID	定義	詳細資料
31546	Create_Delegatee_Definition_Success	啓始者 ID	定義	詳細資料
31547	Create_Delegatee_Definition_Failure	啓始者 ID	定義	詳細資料
31548	Update_Delegatee_Definition_Success	啓始者 ID	定義	詳細資料
31549	Update_Delegatee_Definition_Failure	啓始者 ID	定義	詳細資料
3154A	Delete_Delegatee_Definition_Success	啓始者 ID	定義	詳細資料
3154B	Delete_Delegatee_Definition_Failure	啓始者 ID	定義	詳細資料

事件 ID	描述	策劃者標題	目標標題	文字 1 標題
3154C	Create_Availability_Success	啓始者 ID	目標	
3154D	Create_Availability_Failure	啓始者 ID	目標	詳細資料
3154E	Delete_Availability_Success	啓始者 ID	目標	詳細資料
3154F	Delete_Availability_Failure	啓始者 ID	目標	詳細資料

表格 ***C-23*** 安全性網路位置欄位：文字 *3* 標題、資料標題和資料類型

事件 ID	描述	文字 3 標題	資料標題	資料類型
31540	Create_Proxy_Definition_Success			
31541	Create_Proxy_Definition_Failure	錯誤訊息	stacktrace	字串
31542	Update_Proxy_Definition_Success			
31543	Update_Proxy_Definition_Failure	錯誤訊息	stacktrace	字串
31544	Delete_Proxy_Definition_Success			
31545	Delete_Proxy_Definition_Failure	錯誤訊息	stacktrace	字串
31546	Create_Delegatee_Definition_Success			
31547	Create_Delegatee_Definition_Failure	錯誤訊息	stacktrace	字串
31548	Update_Delegatee_Definition_Success			
31549	Update_Delegatee_Definition_Failure	錯誤訊息	stacktrace	字串
3154A	Delete_Delegatee_Definition_Success			
3154B	Delete_Delegatee_Definition_Failure	錯誤訊息	stacktrace	字串
3154C	Create_Availability_Success			
3154D	Create_Availability_Failure	錯誤訊息	stacktrace	字串
3154E	Delete_Availability_Success			
3154F	Delete_Availability_Failure	錯誤訊息	stacktrace	字串

表格 ***C-24*** 安全性網路位置欄位：觸發

事件 ID	描述	觸發
31540	Create_Proxy_Definition_Success	發生於建立代理定義成功時。
31541	Create_Proxy_Definition_Failure	發生於建立代理定義失敗時。
31542	Update_Proxy_Definition_Success	發生於更新代理定義成功時。
31543	Update_Proxy_Definition_Failure	發生於更新代理定義失敗時。
31544	Delete_Proxy_Definition_Success	發生於刪除代理定義成功時。
31545	Delete_Proxy_Definition_Failure	發生於刪除代理定義失敗時。

事件 ID	描述	觸發
31546	Create_Delegatee_Definition_Success	發生於建立受托者定義成功時。
31547	Create_Delegatee_Definition_Failure	發生於建立受托者定義失敗時。
31548	Update_Delegatee_Definition_Success	發生於更新受托者定義成功時。
31549	Update_Delegatee_Definition_Failure	發生於更新受托者定義失敗時。
3154A	Delete_Delegatee_Definition_Success	發生於刪除受托者定義成功時。
3154B	Delete_Delegatee_Definition_Failure	發生於刪除受托者定義失敗時。
3154C	Create_Availability_Success	發生於建立可用性狀態成功時。
3154D	Create_Availability_Failure	發生於建立可用性狀態失敗時。
3154E	Delete_Availability_Success	發生於刪除可用性狀態成功時。
3154F	Delete_Availability_Failure	發生於刪除可用性狀態失敗時。

C.10 工作流程

表格包含可以透過 Novell Audit 稽核之「使用者應用程式」事件的清單。

表格 ***C-25*** 工作流程欄位：策劃者標題、目標標題和子目標標題

事件 ID	描述	策劃者標題	目標標題	子目標標題
31520	Workflow_Error	啓始者 ID		
31521	Workflow_Started	啓始者 ID		
31522	Workflow_Forwarded	啓始者 ID	收件者	程序名稱
31523	Workflow_Reassigned	啓始者 ID	收件者	程序名稱
31524	Workflow_Approved	啓始者 ID	收件者	程序名稱
31525	Workflow_Refused	啓始者 ID	收件者	程序名稱
31526	Workflow_Ended	啓始者 ID	收件者	程序名稱
31527	Workflow_Claimed	啓始者 ID	收件者	程序名稱
31528	Workflow_Unclaimed	啓始者 ID	收件者	程序名稱
31529	Workflow_Denied	啓始者 ID	收件者	程序名稱
3152A	Workflow_Completed	啓始者 ID	收件者	程序名稱
3152B	Workflow_Timedout	啓始者 ID	收件者	程序名稱
3152C	User_Message	啓始者 ID	原著者	
3152D	Provision_Error	啓始者 ID	收件者	程序名稱
3152E	Provision_Submitted	啓始者 ID	收件者	程序名稱
3152F	Provision_Success	啓始者 ID	收件者	程序名稱

事件 ID	描述	策劃者標題	目標標題	子目標標題
31530	Provision_Failure	啓始者 ID	收件者	程序名稱
31531	Provision_Granted	啓始者 ID	收件者	程序名稱
31532	Provision_Revoked	啓始者 ID	收件者	程序名稱
31533	Workflow_Retracted	啓始者 ID	收件者	程序名稱

表格 ***C-26*** 工作流程欄位：文字 *1* 標題、文字 *2* 標題和文字 *3* 標題

事件 ID	描述	文字 1 標題	文字 2 標題	文字 3 標題
31520	Workflow_Error	活動	程序 ID	錯誤訊息
31521	Workflow_Started	活動	程序 ID	
31522	Workflow_Forwarded	活動	程序 ID	
31523	Workflow_Reassigned	活動	程序 ID	
31524	Workflow_Approved	活動	程序 ID	次要使用者
31525	Workflow_Refused	活動	程序 ID	次要使用者
31526	Workflow_Ended	活動	程序 ID	
31527	Workflow_Claimed	活動	程序 ID	次要使用者
31528	Workflow_Unclaimed	活動	程序 ID	次要使用者
31529	Workflow_Denied	活動	程序 ID	次要使用者
3152A	Workflow_Completed	活動	程序 ID	
3152B	Workflow_Timedout	活動	程序 ID	
3152C	User_Message		訊息	
3152D	Provision_Error	活動	程序 ID	錯誤訊息
3152E	Provision_Submitted	活動	程序 ID	
3152F	Provision_Success	活動	程序 ID	
31530	Provision_Failure	活動	程序 ID	
31531	Provision_Granted	活動	程序 ID	
31532	Provision_Revoked	活動	程序 ID	
31533	Workflow_Retracted	活動	程序 ID	次要使用者

表格 ***C-27*** 工作流程欄位：值 *3* 標題、值 *3* 類型和資料標題

事件 ID	描述	值 3 標題	值 3 類型	資料標題
31520	Workflow_Error	錯誤編號	布林值	stacktrace
31521	Workflow_Started			

事件 ID	描述	值 3 標題	值 3 類型	資料標題
31522	Workflow_Forwarded			
31523	Workflow_Reassigned			
31524	Workflow_Approved			次要使用者類型
31525	Workflow_Refused			次要使用者類型
31526	Workflow_Ended			
31527	Workflow_Claimed			次要使用者類型
31528	Workflow_Unclaimed			次要使用者類型
31529	Workflow_Denied			次要使用者類型
3152A	Workflow_Completed			
3152B	Workflow_Timedout			
3152C	User_Message			
3152D	Provision_Error	錯誤編號	布林值	stacktrace
3152E	Provision_Submitted			
3152F	Provision_Success			
31530	Provision_Failure			
31531	Provision_Granted			
31532	Provision_Revoked			
31533	Workflow_Retracted			次要使用者類型

表格 ***C-28*** 工作流程欄位：資料類型和觸發

事件 ID	描述	資料類型	觸發
31520	Workflow_Error	字串	許多項目都可導致此事件。
31521	Workflow_Started		發生於工作流程啓動時。
31522	Workflow_Forwarded		發生於轉遞工作流程時。
31523	Workflow_Reassigned		發生於重新指定工作流程時。
31524	Workflow_Approved	字串	發生於核准工作流程時。
31525	Workflow_Refused	字串	發生於拒絕工作流程時。
31526	Workflow_Ended		發生於工作流程結束時。
31527	Workflow_Claimed	字串	發生於要求工作流程時。
31528	Workflow_Unclaimed	字串	
31529	Workflow_Denied	字串	發生於拒絕工作流程時。
3152A	Workflow_Completed		發生於工作流程完成時。

事件 ID	描述	資料類型	觸發
3152B	Workflow_Timedout		發生於工作流程逾時時。
3152C	User_Message		
3152D	Provision_Error	字串	許多項目都可導致此事件。
3152E	Provision_Submitted		
3152F	Provision_Success		
31530	Provision_Failure		
31531	Provision_Granted		
31532	Provision_Revoked		
31533	Workflow_Retracted	字串	發生於工作流程收回時。

C.11 報告

下面是 Novell Audit 報告的範例。下列爲可執行的報告清單。

- 管理動作報告
- 歷程核准流程報告
- 資源提供報告
- 特定使用者稽核追尋
- 特定使用者提供
- 使用者提供

特性 ***C-1*** 管理動作報告

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

Total # Events: 121

Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5 Administrative Action Report

Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Novell® Audit Report for Identity Manager

Resource Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

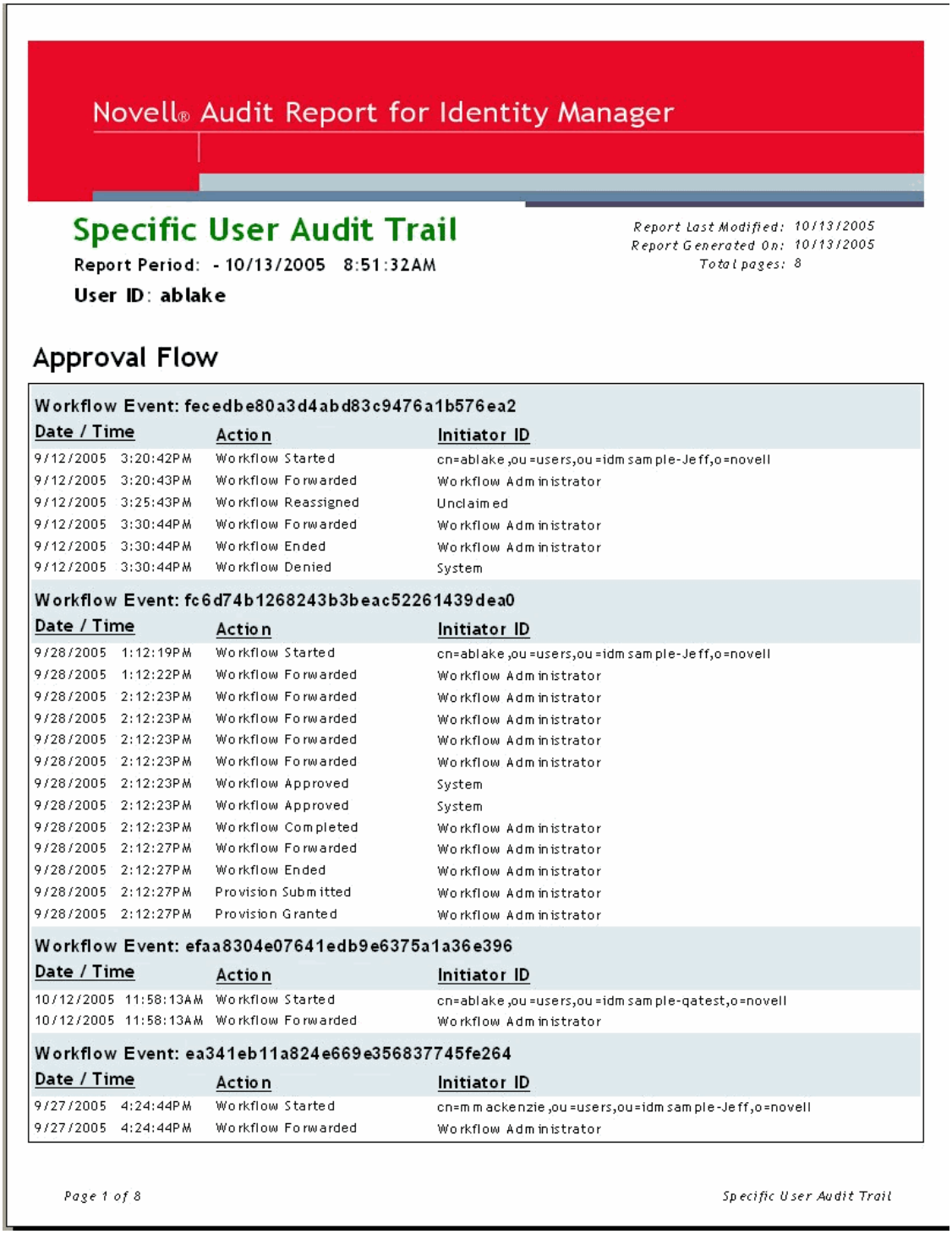
Total # Events: 42

Report Period: - 10/13/2005 8:47:18AM

Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	**Date / Time**	**User Name**	**Action**
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3 *Resource Provisioning Report*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

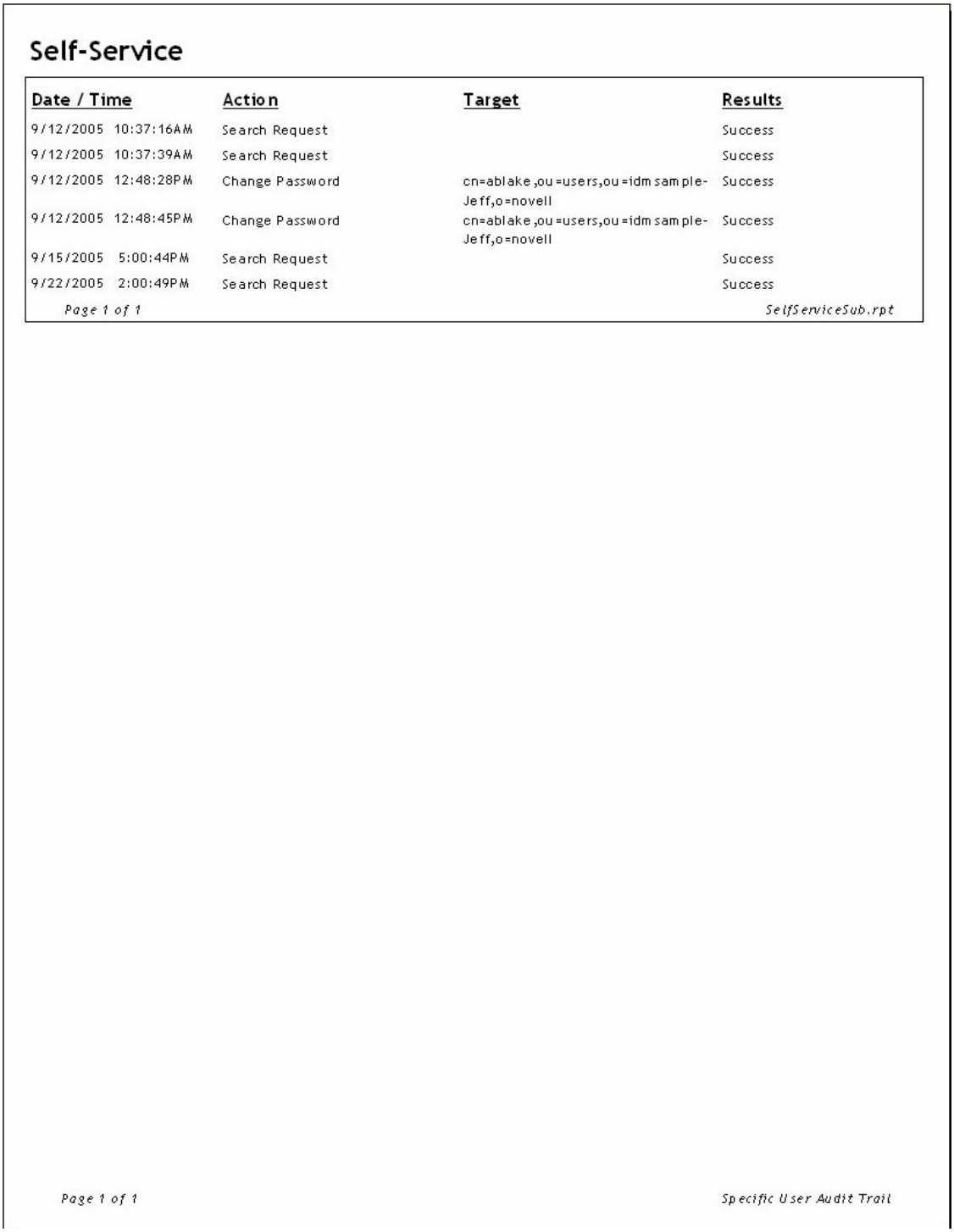
Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8

Specific User Audit Trail

特性 ***C-5*** 特定使用者稽核追尋 *2*



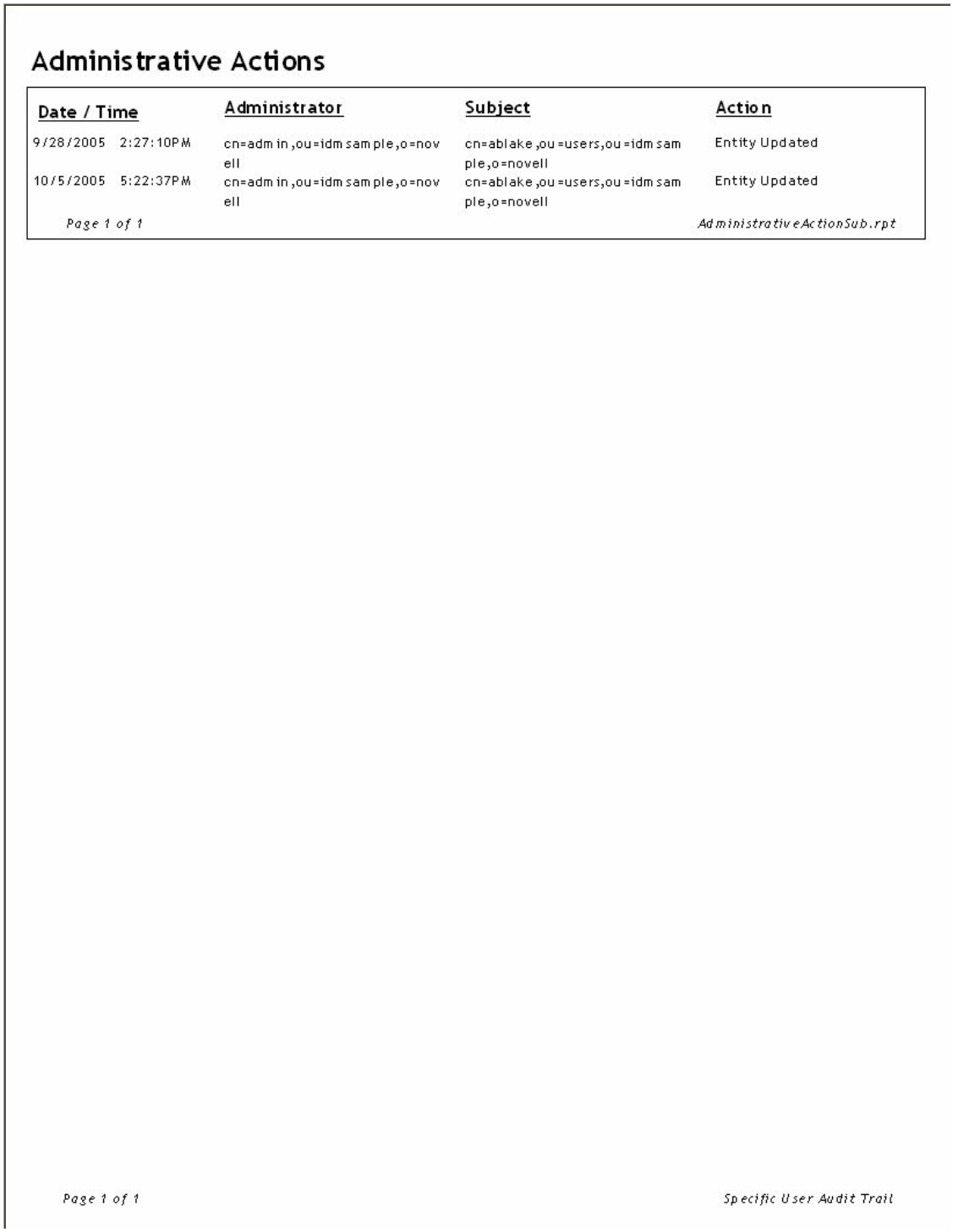
Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 *SelfServiceSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

特性 ***C-6*** 特定使用者稽核追尋 *3*



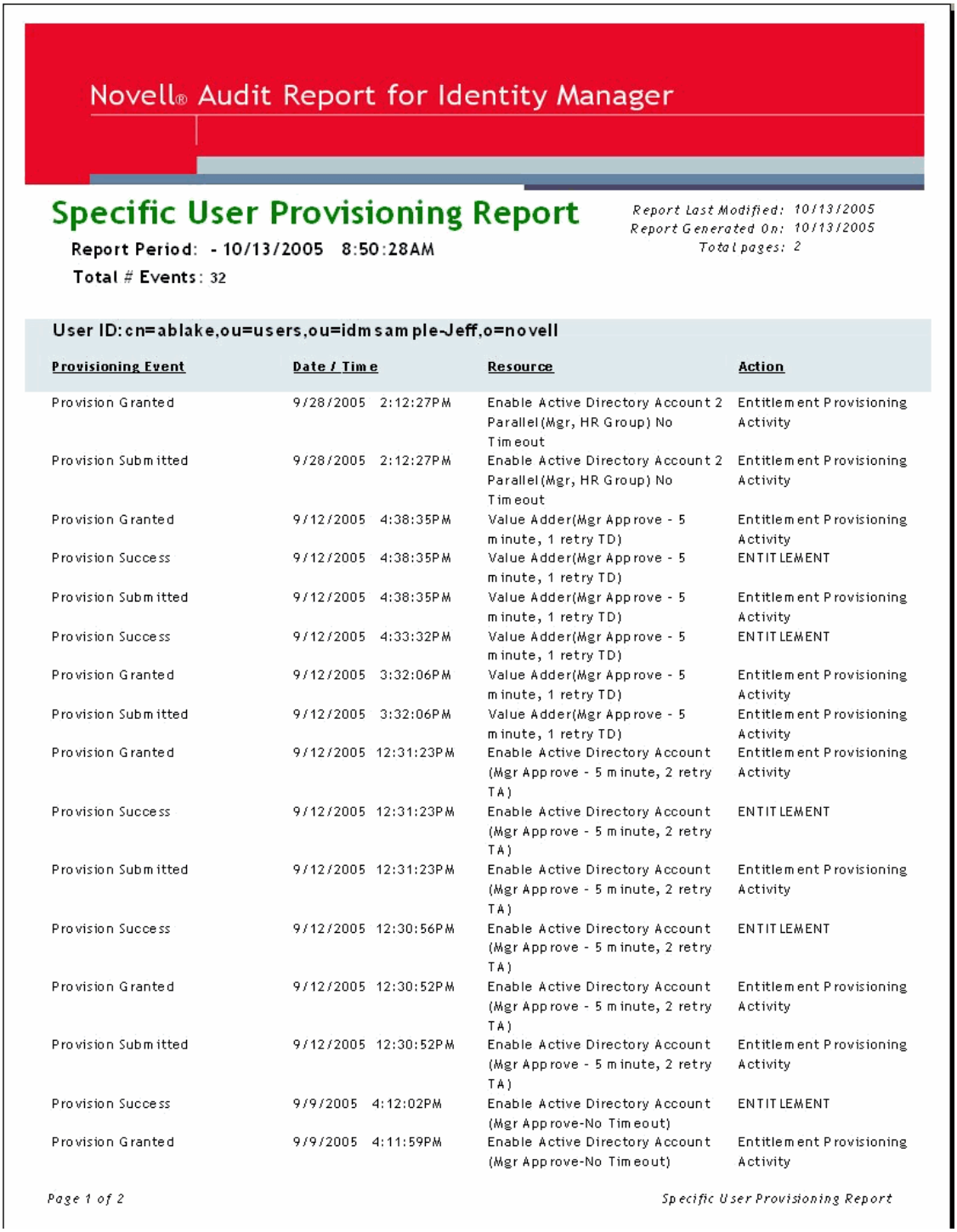
Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 *AdministrativeActionSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

特性 ***C-7*** 特定使用者提供報告



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2 *Specific User Provisioning Report*

Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3 *User Provisioning Report*

手動任務服務驅動程式：取代資料

D

取代資料用於與用做範本的 XML 文件搭配，來建構電子郵件訊息、網頁和 XDS 文件。以 XSLT 樣式表處理範本文件會做爲建構輸出文件的一部份來執行取代，從而完成實際取代。

透過「訂閱者」和「發行者」通道上的不同機制，取代資料會提供給「手動任務服務驅動程式」。

訂閱者通道

- 取代資料是做爲 <mail> 元素的一部份提供。
- 所提供的部份取代資料可以是 URL 資料。如果 URL 資料已提供，則資料會以自動資料項目來處理、完成和取代 (請參閱附錄 E 「手動任務服務驅動程式：自動取代資料項目」，第 275 頁)。
- 如果 <mail> 元素指定應建構關聯值 (即 <mail> 元素具有 src-dn 屬性)，則名爲 "association" 的自動資料項目會新增至取代資料。

發行者通道

- 取代資料會在 HTTP URL 資料和 HTTP POST 資料中提供。
- 取代資料用於範本處理之前，自動 URL 取代資料項目會先新增至該取代資料。

範本處理期間，取代資料會以 XML 文件呈現。取代資料文件會以名爲 replacement-data 的參數傳遞至處理範本的樣式表。如果沒有使用任何範本，則會使用樣式表直接處理 XML 文件。

D.1 資料安全性

資料項目會透過「訂閱者」通道傳送之電子郵件中包含的 URL，從「訂閱者」通道傳遞至「發行者」通道。變更 URL 中的某些資料項目代表會有安全威脅。例如，如果 URL 中「訂閱者」通道所提供之 URL 中的 responder-dn 值，由提交至「發行者」通道 Web 伺服器之 URL 中另一個使用者的 DN 取代，則會允許未授權使用者變更 eDirectory 中的資料。

爲了確保已提交之 URL 中的資料與原來由「訂閱者」通道提供的資料相同，會提供受保護的資料。受保護的資料是由於安全性原因而無法變更的資料。此資料根據組態不同而各不相同，但固定會包含 responder-dn 資料項目，以及對應於任何要變更其值之 eDirectory 物件的資料項目。

加密原始值並將加密的值置於 URL 查詢字串，如此便可保護資料項目。當「發行者」 Web 伺服器接收到加密的值時，「發行者」會解密該值，並使用該值來比較由 HTTP GET 或 POST 申請所提供的未加密資料項目。

如果資料項目的例項顯示在加密資料中，則未加密的資料項目值必須符合其中一個加密的資料項目值。如果未加密的資料項目值不符合其中一個加密的資料項目值，則「發行者」通道 Web 伺服器會拒絕 HTTP 申請。

此外，還會拒絕不包含受保護資料的所有 HTTP POST 申請。

範例

在 HTTP POST 申請中，「發行者」通道 Web 伺服器會使用名爲 responder-dn 的未加密 POST 資料來檢查由 POST 資料提供的密碼。這樣做是爲了針對使用者的 eDirectory 物件驗證回應使用者。

假設 「訂閱者」通道 <url-query> 元素內容指定下列兩個資料項目：

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>


<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

由 「訂閱者」通道產生的 URL 將包含受保護資料中的兩個 responder-dn 值。

假設某位惡意使用者取得了電子郵件訊息中產生和傳送的 URL，該惡意使用者會使用該 URL 取得可讓使用者變更 eDirectory 物件資料的 HTML 表單。

在提交至 Web 伺服器的 HTTP POST 申請中，該惡意使用者會使用其 eDirectory DN (responder-dn=\PERIN-TAO\novell\wally) 做爲未加密的 responder-dn 值，同時在 POST 資料中提交自己的密碼，如此 Web 伺服器所執行的授權便會成功。

不過，當 「發行者」通道 Web 伺服器接收 HTTP POST 資料時，會找不到已加密受保護資料中的 "\PERIN-TAO\novell\wally" 並拒絕 POST 申請。

D.2 XML 元素

構成取代資料文件的元素如下所述。如果沒有描述元素的任何 XML 屬性，則任何元素均不得使用。

D.2.1 <replacement-data>

<replacement-data> 元素可出現在下列位置：

1. 做爲 「訂閱者」通道 <mail> 元素下，<message> 元素的子代。

   「手動任務服務驅動程式」會將提供的 <replacement-data> 元素處理成獨立的 <replacement-data> 元素，以用於範本處理。會發生下列處理：

   a. 如果所含 <mail> 元素的關聯值已建立，則 <item name="association"> 元素會新增至取代資料。已建立元素的值是傳回至 Identity Manager 的關聯值。

   b. 如果 <replacement-data> 元素有 <url-data> 元素子代，則 <url-data> 元素會取代爲包含已建構之 URL 資料的數個 <item> 元素。請見 <url-data> 和 <url-query>。

2. 使用 「訂閱者」或 「發行者」通道上的樣式表建構文件時，用來做爲取代資料文件的獨立頂層元素。

D.2.2 <item>

<item> 元素可以是 <replacement-data> 元素、<url-data> 元素或 <url-query> 元素的子代。<item> 元素的內容是用於範本中替代取代記號的文字。<item> 元素固定會使用 name 屬性來命名。

<item> 屬性

name： name 屬性的值會指定名稱，取代記號會使用該名稱參照此資料項目。例如，如果 name 屬性的值是 manager，則取代記號 $manager$ 會取代爲 <item name="manager"> 元素中包含的值。name 屬性是必要的。

protect： 對於做爲 <url-query> 元素子代的 <item> 元素，protect 屬性會指定是否該項目會新增至 URL 查詢字串的受保護資料區段 (請見 <url-query>)。如果 protect 屬性存在，則其必須具有值 yes。

預先定義的 **<item>** 名稱

特定 <item> 元素針對 「訂閱者」通道、「發行者」通道，或者這兩個通道都具有預先定義的意義。

template：「發行者」通道會將 template 項目的值視爲範本文件的名稱，用於產生對 HTTP GET 申請的回應。

當 <item name="template"> 做爲 「訂閱者」通道上 <url-query> 元素的子代出現時，該值會置於 URL 查詢資料中，以將在回應 HTTP GET 申請時要使用的範本文件名稱指定給 「發行者」通道 Web 伺服器。

responder-dn：「發行者」通道會使用 HTTP POST 資料中 responder-dn 項目的值做爲 eDirectory 物件的 DN，而 HTTP POST 資料中提供的密碼會依據該 DN 來驗證。

Web 伺服器會拒絕不包含 responder-dn 值和 password 值的所有 HTTP POST 申請。此外，如果 HTTP POST 資料不包含 protected-data 項目，申請就會受到拒絕。

「訂閱者」通道會提供 <url-query> 元素下的一或多個 <item name="responder-dn" protect="yes"> 元素。因爲 responder-dn 項目用於使用者驗證，所以該項目必須是受保護的。

password： 透過 HTTP POST 資料提供給 「發行者」通道 Web 伺服器。項目內容是密碼，且該密碼會以 POST 資料中 responder-dn 項目指定的 eDirectory 物件加以驗證。password 項目通常會在用於產生 HTTP POST 申請的 HTML 表單中輸入。

範例：

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template：透過 HTTP POST 資料提供給 Web 伺服器，用於產生做爲 POST 回應所使用的網頁。response-template 項目通常會透過用於產生 HTTP POST 申請之 HTML 表單中，隱藏的 INPUT 元素加以指定。

範例：

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet： 透過 HTTP POST 資料提供給 Web 伺服器，用於產生做爲 POST 回應所使用的網頁。response-stylesheet 項目通常會透過用於產生 HTTP POST 申請之 HTML 表單中，隱藏的 INPUT 元素加以指定。

範例：

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
VALUE="process_template.xsl"/>
```

auth-template：透過 HTTP POST 資料提供給 Web 伺服器，用於產生網頁。該網頁用於使用者驗證失敗時，對 POST 的回應。auth-template 項目通常會透過用於產生 HTTP POST 申請之 HTML 表單中，隱藏的 INPUT 元素加以指定。

範例：

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet：透過 HTTP POST 資料提供給 Web 伺服器，用於產生網頁。該網頁用於使用者驗證失敗時，對 POST 的回應。auth-template 項目通常會透過用於產生 HTTP POST 申請之 HTML 表單中，隱藏的 INPUT 元素加以指定。

範例：

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data： protected-data 項目包含「訂閱者」通道所建構的加密資料。在「訂閱者」通道上，protected-data 項目是自動提供的項目。

在「發行者」通道上，protected-data 項目會從 HTTP GET 申請的 URL 查詢字串，以及 HTTP POST 申請的 POST 資料取得。

protected data 項目通常會透過用於建構 HTTP GET 回應之範本中的取代記號，從 HTTP GET 申請傳遞至用於產生 HTTP POST 的網頁。

範例：

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

<url-data> 元素是「訂閱者」通道上的 <message> 元素下，<replacement-data> 元素的子代。該元素包含用於建構 URL 和相關資料項目 (會提供給建構電子郵件訊息所使用的範本) 的 <item> 元素，而且還包含 <url-query> 元素。

就「手動任務服務」驅動程式的用途而言，URL 由下列五個部份組成：

1. 規劃，如 http、https 或 ftp。
2. 主機，如 www.novell.com 或 192.168.0.1。
3. 連接埠號碼。冒號後接十進位整數。例如，:80 或 :8180。
4. 檔案或資源指定器。這通常是檔名且可以包括路徑資訊。例如，stylesheets/process_template.xsl。
5. 查詢字串。此爲名稱值配對的集合，以 & 字元分隔。例如，template=form_template.xml&protected-data=AabABJKEL=

<url-data> 下預先定義的 **<item>** 名稱

除非 <url-data> 元素下的 <item> 元素是下列其中一項，否則會忽略。以下所有元素都是選擇性的。

file： 指定 URL 的檔案部份。如果 file 項目與「發行者」通道 Web 伺服器搭配使用，則會指定用於建構因回應 URL 而傳回之啓始 HTML 頁面的樣式表。如果 file 項目與非「發行者」通道 Web 伺服器的其他伺服器搭配使用，則會指定 URL 參照之資源的名稱。

如果 file 項目未顯示，則 URL 檔案部份預設會爲 process_template.xsl。

scheme： <url-data> 元素下的選擇性項目。如果存在，則其會指定 URL 的規劃部份 (如 http 或 ftp)。通常只有在 URL 指向非「發行者」之 Web 伺服器的伺服器時，才會使用 scheme 項目。

如果 scheme 項目未顯示，則 URL 規劃會視「發行者」通道 Web 伺服器的組態而定，預設爲 http 或 https。

host：<url-data> 元素下的選擇性項目。如果存在，則會指定 URL 的主機部份 通常只有在 URL 指向非「發行者」之 Web 伺服器的伺服器時，才會使用 host 項目。

如果 host 項目未顯示，則 URL 主機會預設爲執行「手動任務服務驅動程式」之伺服器的 IP 位址 (即「發行者」通道之 Web 伺服器的 IP 位址)。

port： <url-data> 元素下的選擇性項目。如果存在，則會指定 URL 的連接埠部份 通常只有在 URL 指向非「發行者」之 Web 伺服器的伺服器時，才會使用 port 項目。

如果 port 項目未顯示，則 URL 連接埠會預設爲「發行者」通道 Web 伺服器執行的連接埠。

D.2.4 <url-query>

<url-query> 元素是 <url-data> 元素的子代，包含用於建構電子郵件訊息中使用之 URL 查詢部份的 <item> 元素。

顯示爲 <url-query> 元素子代的每個項目都會以 name="value" 的形式置於查詢字串中，其中 name 是 <item> 元素的 name 屬性值，value 是 <item> 元素的字串內容。

出現在 <url-query> 下的項目元素可以有具有值爲 "yes" 的 protect 屬性。如果是這種情況，項目的名稱和值就會加密，並置於 URL 查詢字串中產生的名稱值配對。已產生之值的名稱是 protected-data。該值爲 Base64 編碼，且爲多值屬性的加密名稱值配對。

資料的保護可以確保 URL 提交至「發行者」通道 Web 伺服器時，資料無法變更。例如，responder-dn 資料項目需要受到保護，以確保只有那些具有回應電子郵件訊息之授權的使用者才能夠變更 eDirectory 資料。

如果產生的 URL 將與「發行者」通道 Web 伺服器搭配使用，則 <url-query> 元素必須至少包含一個 <item name="responder-dn" protect="yes"> 元素，否則 Web 伺服器會拒絕最終的 HTTP POST 申請。

手動任務服務驅動程式：自動取代資料項目

E

「手動任務服務驅動程式」會自動提供特定的取代資料項目元素。本節描述下列資料項目。

E.1 訂閱者通道自動取代資料

下列資料項目會在「訂閱者」通道處理期間自動新增至取代資料文件：

association：如果 <mail> 元素有 <association> 元素子代，或者如果「訂閱者」傳回 <add-association> 元素，則 <item name="association"> 元素會新增至取代資料文件。<item> 元素的內容是 eDirectory 物件的關聯值，該物件則與正在處理的電子郵件訊息相關聯。關聯值可能尚未寫入 eDirectory 物件，因此無法用於查詢中。

url： 該 <item> 元素的內容是用於電子郵件訊息中的完整 URL。在「訂閱者」通道上，url 項目會從 <url-data> 元素下的下列項目建立：scheme、host、port、file 和 <url-query> 元素下的項目。如果找不到 scheme、host 或 port，則使用預設值。預設值由「發行者」通道 Web 伺服器的組態決定。

url-base：該 <item> 元素的內容是已產生之 URL 的部份，不包含資源識別碼 (檔案) 和查詢字串。

url-query： 該 <item> 元素的內容是從 <url-query> 元素下之 <item> 元素產生的 URL 查詢字串。

url-file： 該 <item> 元素的內容是 URL 的資源識別碼。

protected-data： 該 <item> 元素的內容是從 <url-query> 元素下 <item> 元素取得之名稱值配對的加密形式。只有 protect 屬性設爲 "yes" 的 <item> 元素會新增至受保護的資料值。如需受保護資料的相關資訊，請參閱附錄 D 「手動任務服務驅動程式：取代資料」，第 269 頁中的「資料安全性」。

E.2 發行者通道自動取代資料

下列資料項目會在「發行者」通道 Web 伺服器處理期間自動新增至取代資料文件：

post-status：「訂閱者」通道 Web 伺服器會在 HTTP POST 申請處理期間建立 <item name="post-status"> 元素，並將其新增至取代資料文件。Web 伺服器的 HTTP POST 申請是將 XDS 文件提交至 Identity Manager 的申請。Identity Manager 會傳回做爲 XDS 提交結果的狀態文件。<item name="post-status"> 元素的內容是 <status> 元素層級屬性的值，該值會做爲 Identity Manager 的提交結果由 Identity Manager 傳回。

post-status 項目通常用於建構做爲 HTTP POST 申請結果傳回的網頁。

post-status-message：「訂閱者」通道 Web 伺服器會在 HTTP POST 申請處理期間建立 <item name="post-status-message"> 元素，並將其新增至取代資料文件。Web 伺服器的 HTTP POST 申請是將 XDS 文件提交至 Identity Manager 的申請。Identity Manager 會傳回做爲 XDS 提交結果的狀態文件。<item name="post-status-message"> 元素的內容是 <status> 元素的內容，該內容會做爲 Identity Manager 的提交結果由 Identity Manager 傳回。僅當由 Identity Manager 傳回的 <status> 元素有內容時，post-status-message 項目才會建立。

post-status-message 項目通常用於建構做爲 HTTP POST 申請結果傳回的網頁。

url：「訂閱者」通道 Web 伺服器會在 HTTP GET 和 HTTP POST 申請處理期間建立 <item name="url"> 元素，並將其新增至取代資料文件。使用取代資料文件建構任何文件之前，會先新增該 <item> 元素。URL 規劃、主機和連接埠由 Web 伺服器組態決定。

url-base：「訂閱者」通道 Web 伺服器會在 HTTP GET 和 HTTP POST 申請處理期間建立 <item name="url-base">，並將其新增至取代資料文件。使用取代資料文件建構任何文件之前，會先新增該 <item> 元素。「發行者」通道上 url-base <item> 元素的內容與 url <item> 元素相同。

手動任務服務驅動程式：範本動作元素參考

F

動作元素是範本文件中名稱空間合法的元素，用於簡單的邏輯控制，或用於建立 HTML 表單的 HTML 元素。用於使元素合法的名稱空間是 http://www.novell.com/dirxml/manualtask/form。在此文件和隨「手動任務服務」驅動程式所提供的範例範本中，使用的字首是 form。

只要是任何本節中沒有專門涵蓋的動作元素，範本處理樣式表均已將其從輸出文件中刪除 (除非已自定樣式表)。例如，此舉可讓您使用 form:text 元素括住純文字電子郵件訊息的資料，從而讓範本成爲有效的 XML。

F.1 <form:input>

<form:input> 元素用於根據一或多個取代資料項目的存在情況，產生一或多個 HTML INPUT 元素。已建立的 INPUT 元素數量與具有 <form:input> 元素名稱屬性指定之名稱的取代資料項目數量相對應。

屬性

Name： 指定用於建立 INPUT 元素之取代資料項目的名稱。該屬性值會做爲已建立 INPUT 元素之名稱屬性的值來使用。

type 或 **TYPE**： 指定已建立 INPUT 元素之 type 屬性的值。

value： 如果 value 屬性的值等於 "yes,"，則會將 value 屬性新增至值爲取代資料項目之字串值的已建立 INPUT 元素。如果 value 屬性的值不是 "yes,"，則已建立 INPUT 元素的內容會設爲取代資料項目的字串值。

範例

```
<form:input name="responder-dn" TYPE="hidden" value="yes"/>
```

會建立一或多個 INPUT 元素，其類似於

```
<INPUT name="responder-dn" TYPE="hidden" value="\PERIN-
TAO\novell\phb"/>
```

F.2 <form:if-item-exists>

<form:if-item-exists> 元素用於有條件地將資料插入輸出文件。僅當指定的項目出現在取代資料中時，才會處理 <form:if-item-exists> 的內容。

屬性

Name： 指定取代資料項目的名稱。如果存在一或多個取代資料項目的範例，則會處理 <form:if-item-exists> 元素的內容。

範例

```
<form:if-item-exists name="post-status-message"> <tr> <td> Status
message was: $post-status-message$ </td> </tr> </form:if-item-exists>
```

僅當有名爲 post-status-message 的取代資料項目時，此範例才會將列插入 HTML 表格。

F.3 <form:if-multiple-items>

form:if-multiple-items 元素用於有條件地將資料插入輸出文件。僅當指定的項目在取代資料中多次出現時，才會處理 form:if-multiple-items 的內容。

屬性

name： 指定取代資料項目的名稱。如果存在多個取代資料項目的範例，則會處理 form:if-multiple-items 的內容。

範例

```
<form:if-multiple-items name="responder-dn"> <form:menu
name="responder-dn"/> </form:if-multiple-items>
```

如果有多個名爲 responder-dn 的取代資料項目，則此範例會建置 HTML SELECT 元素 (請參閱 <form:menu>)。

F.4 <form:if-single-item>

form:if-single-item 元素用於有條件地將資料插入輸出文件。僅當指定的項目在取代資料中正好只出現一次時，才會處理 form:if- single -item 的內容。

屬性

name： 指定取代資料項目的名稱。如果具名項目在取代資料中正好只出現一次，則會處理 form:if-single-item 的內容。

範例

```
<form:if-single-item name="responder-dn"> <input TYPE="hidden"
name="responder-dn" value="$responder-dn$"/> $responder-dn$ </form:if-
single-item>
```

如果取代資料中正好只有一個名爲 "responder-dn" 的取代資料項目，則此範例會將 HTML INPUT 元素和部份取代文字插入輸出文件。

F.5 <form:menu>

form:menu 元素用於產生具有一或多個 OPTION 元素子代的 HTML SELECT 元素。第一個 OPTION 元素子代標示爲選取。

屬性

name： 指定取代資料項目的名稱。如果具名項目出現在取代資料中，則 HTML SELECT 元素會在輸出文件中建立。針對取代資料中取代資料項目的每個例項，都會建立 HTML OPTION 元素做爲 SELECT 元素的子代。

範例

```
<form:menu name="responder-dn"/>
```

此範例會產生類似下列內容的 HTML 元素：

```
<SELECT name="responder-dn"> <OPTION selected>\PERIN-TAO\big-org\php</
OPTION> <OPTION>\PERIN-TAO\big-org\carol</OPTION> </SELECT>
```

手動任務服務驅動程式：<mail> 元素參考

G

本節詳細描述 <mail> 元素及其內容。如果未列出元素屬性，則表示該元素未定義屬性。

G.1 <mail>

<mail> 元素及其內容描述建構 SMTP 訊息所需的資料。

<mail> 屬性

src-dn： 包含觸發電子郵件之 eDirectory 物件的 DN 值。如果物件資料要透過 「發行者」通道的 Web 伺服器修改以回應電子郵件，則需要此屬性。

G.2 <to>

<to> 元素是 <mail> 元素的子代。一或多個 <to> 元素包含 SMTP 訊息之主要收件者的電子郵件地址。至少需要一個 <to> 元素。每個 <to> 元素必須只包含單一電子郵件地址。

G.3 <cc>

<cc> 元素是 <mail> 元素的子代。零或多個 <cc> 元素包含 SMTP 訊息之副本收件者的電子郵件地址。<cc> 元素並非必要元素。每個 <cc> 元素必須只包含單一電子郵件地址。

G.4 <bcc>

<bcc> 元素是 <mail> 元素的子代。零或多個 <bcc> 元素包含 SMTP 訊息之密件副本收件者的電子郵件地址。<bcc> 元素並非必要元素。每個 <bcc> 元素必須只包含單一電子郵件地址。

G.5 <from>

<from> 元素是 <mail> 元素的子代。<from> 元素包含電子郵件寄件者的電子郵件地址。<from> 元素並非必要元素。如果 <from> 元素不存在，則會使用做爲「手動任務服務驅動程式」參數一部份提供的預設寄件者地址。

G.6 <reply-to>

<reply-to> 元素是 <mail> 元素的子代。<reply-to> 元素包含要向其傳送 SMTP 訊息回覆之實體的電子郵件地址。<reply-to> 元素並非必要元素。

G.7 <subject>

<subject> 元素是 <mail> 元素的子代。其字串內容用於設定 SMTP 標題欄位。<subject> 元素並非必要，但是由於一些顯而易見的原因建議您使用。

G.8 <message>

<message> 元素是 <mail> 元素的子代。其內容用於建構 SMTP 訊息的訊息本文。至少需要一個 <message> 元素。以訊息本文的替代表示 (例如純文字和 HTML，或者英文和其他語言) 建構 SMTP 訊息時，可以提供多個 <message> 元素。

<message> 屬性

mime-type： 選擇性地指定 <message> 元素建構之訊息本文的 MIME 類型 (例如 text/plain 或 text/html)。如果 mime-type 屬性不存在，則驅動程式會嘗試自動探查 MIME 類型。

當 SMTP 訊息具有替代表示以便選擇顯示最佳的表示時，電子郵件用戶端可以使用 MIME 類型。

language： 選擇性地指定 <message> 元素建構之訊息本文的語言。此值應遵循 SMTP 規格。如果 language 屬性不存在，則不會提供預設值。

當 SMTP 訊息具有替代表示以便選擇顯示最佳的表示時，電子郵件用戶端可以使用語言規格。

G.9 <stylesheet>

<stylesheet> 元素是 <message> 元素的子代。<stylesheet> 元素的內容是用於建構訊息本文之 XSLT 樣式表的名稱。如果 <stylesheet> 元素不存在，則會使用 process_template.xsl 做爲樣式表。

G.10 <template>

<template> 元素是 <message> 元素的子代。<template> 元素的內容是用於建構訊息本文之 XML 文件的名稱。如果 <template> 元素不存在，則訊息樣式表會處理取代資料文件以建構訊息本文。

G.11 <filename>

<filename> 元素是 <attachment> 元素的子代。<filename> 元素的內容是檔名。filename 值用於將檔名指定給已建構的附件。

G.12 <replacement-data>

<replacement-data> 元素是 <message> 元素的子代。該元素的內容會做爲處理訊息範本之樣式表的參數來使用；沒有範本時，則由訊息樣式表直接處理。附錄 D 「手動任務服務驅動程式：取代資料」，第 269 頁 和附錄 E 「手動任務服務驅動程式：自動取代資料項目」，第 275 頁 中描述了 <replacement-data> 元素的內容。

G.13 <resource>

<resource> 元素是 <message> 元素的子代。該元素的內容會視爲要合併到 SMTP 訊息中的檔案名稱，做爲訊息本文的資源。例如，HTML 訊息本文的 .css 樣式表可以提供做爲資源。

<resource> 屬性

cid： 指定用於參考訊息本文內 URL 中資源的內容 ID。例如，如果 .css 樣式表是資源，則 cid 值可能是 css-1。在 HTML 訊息本文中，下列元素可以用來參考 .css 樣式表：

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

<attachment> 元素是 <mail> 元素的子代。該元素與 <message> 具有相同的內容，或者其可以使用檔名做爲內容。零或多個 <attachment> 元素可以顯示爲 <mail> 元素的子項。

<attachment> 屬性

mime-type： 選擇性地指定附件的 MIME 類型。如果 mime-type 屬性不存在，則驅動程式會嘗試自動探查 MIME 類型。

language： 選擇性地指定附件的語言。如果語言屬性不存在，則不會提供預設值。

手動任務服務驅動程式：新員工的資料流程案例

H

本節提供在雇用新員工而導致電子郵件訊息傳送至員工管理員的範例情況中，對資料流程的逐步檢查。電子郵件訊息要求管理員在訊息中使用 URL 輸入員工的房間號碼值。

範例案例之「手動任務服務驅動程式」的組態如下所示。

H.1 訂閱者通道組態

過濾器

類別：User

屬性：Given Name、manager、Surname

規則

建立規則：需要 Given Name、manager 和 Surname 屬性。

指令轉換規則：將 <add> 轉換成 <mail> 元素。

H.2 發行者通道組態

過濾器

類別：User

屬性：roomNumber

規則

無。

H.3 資料流程描述

在下列清單中，流經整個程序的最重要資料項目是 responder-dn 和 association。responder-dn 項目用於驗證透過 Web 伺服器輸入資料的使用者。association 項目會識別資料要變更的 eDirectory 物件。

1. 公司雇用了新員工。新員工的資料會輸入到公司的人力資源 (Human Resource，HR) 系統。
2. 人力資源 (HR) 系統的 Identity Manager 驅動程式會在 eDirectory 中建立新的「使用者」物件。使用者屬性包括 Given Name、Surname 和 manager。
3. 新「使用者」物件的下列 <add> 事件會提交至「手動任務服務驅動程式訂閱者」通道：

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <add class-
name="User" src-dn="\PERIN-TAO\novell\Provo\Joe" src-entry-
id="281002" timestamp="1023314433#2"> <add-attr attr-
name="Surname"> <value type="string">the Intern</value> <add-attr>
<add-attr attr-name="Given Name"> <value type="string">Joe</value>
<add-attr> <add-attr attr-name="manager"> <value type="dn">\PERIN-
TAO\novell\Provo\phb</value> <add-attr> </add> </input> </nds>
```

a. 「訂閱者指令轉換」規則會使用管理員 DN 值將查詢發出至 eDirectory，以取得管理員電子郵件地址和管理員助理的 DN。

b. 如果管理員有助理，則「訂閱者指令轉換」會將查詢發出至 eDirectory，以取得助理的電子郵件地址。

c. 「訂閱者指令轉換」會建構 <mail> 元素，並以 <mail> 元素取代 <add> 指令元素。在下面的範例中，取代資料項目以粗體表示。

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <mail src-
dn="\PERIN-TAO\novell\Provo\Joe"> <to>phb@company.com</to>
<cc>carol@company.com</cc> <bcc>HR@company.com</bcc> <reply-
to>HR@company.com</reply-to> <subject>Room Assignment Needed
for: Joe the Intern</subject> <message mime-type="text/html">
<stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data>
<item name="manager">JStanley</item>           <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query>   <item
name="template">form_template.xml</item>               <item
name="responder-dn" protect="yes">\PERIN-TAO\novell\Provo\phb</
item>               <item name="responder-dn"
protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item> </url-query> </
url-data> </replacement-data> <resource cid="css-
1">novdocmain.css</resource> </message> </mail> </input> </nds>
```

d. 「手動任務服務驅動程式訂閱者」會從 Nsure™ Identity Manager 接收 <mail> 元素。

e. 因爲 <mail> 元素具有 src-dn 屬性，所以「訂閱者」會產生一個 association 值。

f. 「訂閱者」會從 <mail> 元素中的資料建構取代資料文件，以用於建構電子郵件訊息。URL 的查詢部份中有各種資料項目 (URL 中 '?' 字元後面以粗體表示的部份)。URL 做爲 HTTP GET 申請提交至 Web 伺服器時，「發行者」通道 Web 伺服器會使用這些資料項目。

```
<replacement-data> <item name="manager">JStanley</item> <item
name="given-name">Joe</item> <item name="surname">the Intern</
item> <item name="template">form_template.xml</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\carol</item> <item
name="subject-name">Joe the Intern</item> <item
name="association">1671b2:ee4246a561:-7fff:192.168.0.1</item>
<item name="url-base">https://192.168.0.1:8180</item> <item
name="url-file">process_template.xsl</item> <item
```

```
name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="url"> https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV </item> </
replacement-data>
```

g. 「訂閱者」會使用 process_template.xsl 處理 html_msg_template.xml。取代資料文件會做爲參數傳遞至樣式表，再來是 html_msg_template.xml 文件。請注意以粗體表示的取代記號。取代記號會由取代資料文件中相對應之 <item> 元素的值取代。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> </head> <body> <link href="cid:css-1" rel="style
sheet" type="text/css"/> <p> Dear $manager$, </p> <p> This
message is to inform you that your new employee <b>$given-name$
$surname$</b> has been hired. </p> <p> Please assign a room
number for this individual. Click <a href="$url$">Here</a> to
do this. </p> <p> Thank you,<br/> HR<br/> HR Department </p> </
```

```
body> </html>
```

接下來是產生的電子郵件文件。取代記號已由取代資料文件中，相對應之 <item> 元素的值取代。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> </head> <body> <link href="cid:css-1"
rel="style sheet" type="text/css"> <p> Dear J Stanley, </p> <p>
This message is to inform you that your new employee <b>Joe the
Intern</b> has been hired. </p> <p> Please assign a room number
for this individual. Click <a href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this. </p> <p> Thank you,<br> HR<br> HR Department </p> </
body> </html>
```

h. SMTP 電子郵件訊息會傳送至管理員和管理員的助理。

i. 「訂閱者」會將包含 <status> 元素和 <add-association> 元素的 XML 文件傳回至 Identity Manager。

4. 管理員會開啓電子郵件訊息，並按一下「按一下此處」連結。

5. 管理員的 Web 瀏覽器會將 URL 做爲 HTTP GET 申請提交至「發行者」通道 Web 伺服器。

   a. Web 伺服器會建構下列取代資料文件。大部份資料項目來自 URL 的查詢部份。自動產生的項目 url 和 url-base 則是例外。

```
<replacement-data> <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="template">form_template.xml</item> <item name="responder-
```

```
dn">\PERIN-TAO\novell\Provo\phb</item> <item name="responder-
dn">\PERIN-TAO\novell\Provo\carol</item> <item name="subject-
name">Joe the Intern</item> <item name="url-base">https://
192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> </replacement-data>
```

Web 伺服器會使用 process_template.xsl 樣式表處理 form_templates.xml 文件。取代記號和動作元素以粗體表示。請注意，各種資料項目是放置在隱藏的 INPUT 元素中，如此該資料項目便會做爲 HTML POST 資料的一部份傳遞至 Web 伺服器。

此外還有 $query:roomNumber$ 取代記號，其會擷取員工 roomNumber 屬性 (如果有的話) 的目前值。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> <title>Enter room number for $subject-name$</
title> </head> <body> <link href="novdocmain.css" rel="style
sheet" type="text/css"/> <br/><br/><br/><br/> <form
class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input
TYPE="hidden" name="association" value="$association$"/> <input
TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/> <input TYPE="hidden"
name="response-template" value="post_response.xml"/> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> <form:if-
single-item name="responder-dn">   You are:<br/> <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
$responder-dn$  </form:if-single-item>          <form:if-
multiple-items name="responder-dn"> Indicate your identity:<br/
>  <form:menu name="responder-dn"/>         </form:if-multiple-
items> </td></tr> <tr><td> Enter your password: <br/><input
name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/> </
td></tr> <tr><td> Enter room number for $subject-name$:<br/>
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
value="$query:roomNumber$"/> </td></tr> <tr><td> <input
TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/> </td></tr> </table> </form> </body> </html>
```

下列 HTML 頁面是結果：

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Enter room number for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <form
class="myform" METHOD="POST" ACTION="https://192.168.0.1:8180/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr> <td> <input TYPE="hidden"
name="template" value="post_form.xml"> <input TYPE="hidden"
```

```
name="subject-name" value="Joe the Intern"> <input
TYPE="hidden" name="association" value="45f0e3:ee45e07709:-
7fff:192.168.0.1"> <input TYPE="hidden" name="response-style
sheet" value="process_template.xsl"> <input TYPE="hidden"
name="response-template" value="post_response.xml"> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"> <input TYPE="hidden"
name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT"> Indicate your
identity:<br> <SELECT name="responder-dn"> <OPTION
selected>\PERIN-TAO\novell\Provo\phb</OPTION> <OPTION>\PERIN-
TAO\novell\Provo\carol</OPTION> </SELECT> </td> </tr> <tr> <td>
Enter your password: <br>

    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40"> </td> </tr> <tr> <td> Enter room number for Joe
the Intern:<br> <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value=""> </td> </tr> <tr> <td> <input
TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear"> </td> </tr> </table> </form> </body> </html>
```

b. 管理員會從網頁功能表中選取其 eDirectory DN，輸入密碼並輸入新員工的房間號碼，然後按一下「提交」。

c. Web 瀏覽器會將 HTTP POST 申請提交至 Web 伺服器。

d. Web 伺服器會從 POST 資料建構下列取代資料文件。請注意各種隱藏 <INPUT> 元素中的資料。管理員輸入表單中的資料以粗體表示。

```
<replacement-data>   <item name="room-number">cubicle 1234</
item> <item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive="true"><-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
```

```
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>  <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> </replacement-data>
```

e. Web 伺服器會驗證 responder-dn 項目的值是否符合受保護資料中包含的 responder-dn 值。如果值不符合，則 Web 伺服器會中止申請。如果值相符，則會繼續處理。

f. Web 伺服器會將 <check-object-password> XDS 申請提交至「發行者」通道上的 Identity Manager，以驗證提交 HTTP POST 申請的使用者。

```
<nds dtdversion="1.0" ndsversion="8.6"> <source> <product
build="20020606_0824" instance="Manual Task Service Driver"
version="1.1a">DirXML Manual Task Service Driver</product>
<contact>Novell, Inc.</contact> </source> <input> <check-
object-password dest-dn="\PERIN-TAO\novell\Provo\phb" event-
id="chkpwd"> <password><!- content suppressed </password> </
check-object-password> </input> </nds>
```

g. Identity Manager 會傳回 <status level="success">。如果 Identity Manager 傳回 success 之外的項目，則 auth_template 資料項目指定的範本和 auth_stylesheet 資料項目指定的樣式表會用於建構做爲 POST 結果傳回的網頁。

h. Web 伺服器會使用 process_template.xsl 樣式表處理 post_form.xml 範本，以產生 XDS 文件。取代記號以粗體表示。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>$association$</association>
<modify-attr attr-name="roomNumber"> <remove-all-values/> <add-
value> <value>$room-number$</value> </add-value> </modify-attr>
</modify> </input> </nds>
```

i. 「發行者」會將已建立的 XDS 文件提交至 Identity Manager。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>45f0e3:ee45e07709:-
7fff:192.168.0.1</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value>
<value>cubicle 1234</value> </add-value> </modify-attr> </
modify> </input> </nds>
```

j. Identity Manager 會傳回結果文件。

```
<nds dtdversion="1.1" ndsversion="8.6"> <source> <product
version="2.0">Identity Manager</product> <contact>Novell,
Inc.</contact> </source> <output> <status event-id="wfmod"
```

```
level="success"></status> </output> </nds>
```

k. Web 伺服器會將取代資料項目 post-status (可能還有取代資料項目 post-status-message) 新增至取代資料文件。新增的資料項目以粗體表示：

```
<replacement-data> <item name="room-number">cubicle 1234</item>
<item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive=”true”><!-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> <status event-id="" level="success"></
status>   <item name="post-status">success</item> </
replacement-data>
```

l. Web 伺服器會使用 process_template.xsl 樣式表處理 post_response.xml 範本。取代記號和動作元素以粗體表示。

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Result of post for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet"
type="text/css"/> <br/><br/><br/><br/> <table class="formtable"
cellpadding="5" cellspacing="20" border="1" align="center">
<tr> <td> DirXML reported status = $post-status$ </td> </tr>
<form:if-item-exists name="post-status-message"> <tr> <td>
Status message was: $post-status-message$ </td> </tr> </
form:if-item-exists> </table> </body> </html>
```

m. 產生的網頁會做爲 HTTP POST 的結果傳回。因爲取代資料文件中不存在 <form:if-item-exists> 元素參考的 post-status-message，所以表格的第二列不存在。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Result of post for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <table
```

```
class="formtable" cellpadding="5" cellspacing="20" border="1"
align="center"> <tr> <td> DirXML reported status = success </
td> </tr> </table> </body> </html>
```

手動任務服務驅動程式：訂閱者通道的自定元素處理器

驅動程式會提供延伸機制，以使用簡易郵件傳輸協定 (SMTP) 以外的方法來傳送使用者通知。例如，客戶可能需要使用訊息應用程式介面 (Messaging Application Programming Interface，MAPI) 來傳送通知，而不是使用 SMTP。

若要使用 SMTP 以外的機制傳送通知，您必須寫入 Java 類別，以處理驅動程式之「訂閱者」通道上提交的自定 XML 元素。

Java 自定元素處理器必須實作 com.novell.nds.dirxml.driver.manualtask.CommandHandler Java 介面。自定元素類別的名稱是在「訂閱者」組態參數的「其他處理器」項目中指定。

「訂閱者」通道遇到指令元素時，會在其表格中搜尋處理器。通道找到報告會處理指令元素的處理器時，該指令元素便會傳遞至處理器。然後，處理器會執行任何必要的處理。

驅動程式中有兩個內建指令元素處理器：<mail> 元素的處理器和 <add> 元素的處理器。

自定指令元素定義由自定處理器的原著者決定。若要設計自定指令元素，比較合理的著手處是從設計 <mail> 元素開始。

自定元素是由規則以在「訂閱者」通道上建立 <mail> 元素的相同方式建立。

在驅動程式隨附的 javadoc 中包含 com.novell.nds.dirxml.driver.manualtask.CommandHandler 的文件，以及許多公用程式和支援類別的文件。javadoc 位於配送影像檔之名爲 manual_task_docs.zip 的檔案中。

I.1 建構與發行者通道 Web 伺服器搭配使用的 URL

若要安全地使用驅動程式的「發行者」通道 Web 伺服器，您需要使用公用程式類別建構要隨附於通知訊息中的 URL。com.novell.nds.dirxml.driver.manualtask.URLData 設計用於此任務。

在 SampleCommandHandler.java 中找到的範例程式碼會說明此程序。

I.2 使用樣式表和範本文件建構訊息文件

使用 SMTP 處理器所使用的相同方法建構文件很方便，該方法是樣式表、範本文件和取代資料的結合。若要執行此動作，您必須取得樣式表和範本文件，並使用程式叫用樣式表處理器。

在 SampleCommandHandler.java 中找到的範例程式碼會說明此程序。

I.3 SampleCommandHandler.java

範例自定指令處理器的原始碼隨附於驅動程式配送中。原始碼位於配送影像檔之 manual_task_docs.zip 的檔案中。

處理器是在 com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler 類別中實作。

範例處理器僅會使用樣式表和範本產生文件，並將產生的文件寫入檔案。

I.3.1 編譯 SampleCommandHandler 類別

您可以使用任何 Java 2 編譯器編譯 SampleCommandHandler 類別。您必須將 nxsl.jar、dirxml.jar、collections.jar 和 ManualTaskServiceBase.jar 置於 Java 編譯器 classpath 中。

I.3.2 嘗試使用 SampleCommandHandler 類別

從輸入驅動程式的 「房間號碼」範例組態開始。

編譯 SampleCommandHandler 類別，並將產生的類別檔案置於 .jar 檔案中。將 .jar 檔案置於適合於您執行驅動程式之平台的 DirXML .jar 檔案目錄中。

新增下列在驅動程式內容之 「驅動程式參數 XML」區段中找到的 <subscriber-options> 元素下的 XML 元素：

```
<output-path display-name="Sample Output Path"></output-path>
```

編輯 「驅動程式參數」。在標示爲 「範例輸出路徑」的項目中，將路徑放置到 SampleCommandHandler 要寫入其已建立之文件的目錄中。在標示爲 「其他處理器」的項目中，新增 com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler 字串。

使用在與 SampleCommandHandler.java 檔案相同的目錄中找到的 CommandXform.xsl 置換 「訂閱者」通道指令轉換規則。

建立 「使用者」物件，並將管理員參考新增至 「使用者」物件。如果管理員具有電子郵件地址值，則 <sample> 指令元素會傳送至 「訂閱者」，且 SampleCommandHandler 會於您在上面指定的位置寫入檔案。

手動任務服務驅動程式：發行者通道的自定伺服器常式

J

驅動程式會提供延伸機制，其他功能可以透過該機構新增至「發行者」通道 Web 伺服器。藉由在標示爲「其他伺服器常式」的「驅動程式」組態項目中指定伺服器常式類別名稱，「發行者」可以載入自定伺服器常式。

J.1 使用發行者通道

如果自定伺服器常式需要將資料提交至 Identity Manager，則伺服器常式必須使用驅動程式的「發行者」通道。com.novell.nds.dirxml.driver.manualtask.ServletRegistrar 和 com.novell.nds.dirxml.driver.manualtask.PublisherData 類別會提供給您，以便使此操作進行更順利。在 SampleServlet.java 中找到的範例程式碼會說明此程序。

J.2 驗證

自定伺服器常式必須驗證提交資訊的使用者。在 SampleServlet.java 中找到的範例程式碼會說明此程序。不過，使用 <check-object-password> 元素執行的驗證類型不會檢查 eDirectory™ 權限。如果「驅動程式」物件具有執行變更的權限，則無論提交變更的使用者是否具有權限，「發行者」通道上提交的變更都會准許進行。

如果您在「訂閱者」通道上使用指令處理器產生的 URL，則必須使用 com.novell.nds.dirxml.driver.manualtask.URLData 類別驗證該 URL，以確保 responder-dn 資料項目未被篡改。如需完成此操作的相關資訊，請參閱 javadoc。

J.3 SampleServlet.java

範例伺服器常式的原始碼隨附於驅動程式配送中。該原始碼位於配送影像檔的 manualtask_driver_docs.zip 檔案中。

伺服器常式是在 com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet 類別中實作。

範例伺服器常式接受以 .sample 結束之任何資源的 HTTP GET 申請。HTTP URL 的查詢字串必須包含 dest-dn 項目、attr-name 項目和 value 項目。

伺服器常式會驗證使用者，然後透過驅動程式的「發行者」通道將修改申請提交至 Identity Manager。

J.3.1 編譯 SampleServlet 類別

您可以使用任何 Java 2 編譯器編譯 SampleServlet 類別。您必須將 nxsl.jar、dirxml.jar、collections.jar 和 ManualTaskServiceBase.jar 置於 Java 編譯器 classpath 中。

J.3.2 嘗試使用 SampleServlet 類別

從輸入驅動程式的「房間號碼」範例組態開始。

編譯 SampleServlet 類別，並將產生的類別檔案置於 .jar 檔案中。將 .jar 檔案置於適合於您執行驅動程式之平台的 DirXML .jar 檔案目錄中。

編輯「驅動程式參數」。在標示爲「其他伺服器常式」的項目中，新增 com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet 字串。

將「電話號碼」新增至「發行者」通道過濾器。

在瀏覽器中提交下列 URL (假設瀏覽器和驅動程式在相同的機器上執行)：

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telephone%20Number&value=555-1212

使用網路樹中使用者的 DN 置換 *username.container*。