Novell® Sentinel™

5.1.3

www.novell.com

Band I – INSTALLATIONSHANDBUCH

7. Juli 2006

Novell®

Rechtliche Hinweise

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

Online-Dokumentation: Zugriff auf die Online-Dokumentation für dieses und andere Novell-Produkte sowie auf Aktualisierungen erhalten Sie unter www.novell.com/documentation.

Novell-Marken

Informationen zu Novell-Marken finden Sie in der Liste der Marken und Dienstleistungsmarken von Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum der jeweiligen Inhaber.

Rechltliche Hinweise zu Drittanbieterprodukten

Sentinel 5 enthält möglicherweise folgende Drittanbietertechnologien:

- Apache Axis und Apache Tomcat, Copyright © 1999 bis 2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/
- ANTLR. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.antlr.org
- Boost, Copyright © 1999, Boost.org.
- Bouncy Castle, Copyright © 2000–2004, the Legion of Bouncy Castle. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.bouncycastle.org.
- Checkpoint. Copyright © Check Point Software Technologies Ltd.
- Concurrent, Dienstprogrammpaket. Copyright © Doug Lea. Wird ohne die Klassen CopyOnWriteArrayList und ConcurrentReaderHashMap verwendet.
- Crypto++ Compilation. Copyright © 1995–2003, Wei Dai, beinhaltet folgende durch Copyright geschützte Werke: mars.cpp von Brian Gladman und Sean Woods. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.eskimo.com/~weidai/License.txt.
- Crystal Reports Developer und Crystal Reports Server. Copyright © 2004 Business Objects Software Limited.
- DataDirect Technologies Corp. Copyright © 1991–2003.
- edpFTPj, lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, lizienziert unter der Lesser General Public License, verfügbar unter: http://shark.objectweb.org/license.html.
- ICEsoft ICEbrowser. ICEsoft Technologies, Inc. Copyright © 2003–2004.
- ILOG, Inc. Copyright © 1999–2004.
- Installshield Universal. Copyright © 1996–2005, Macrovision Corporation und/oder Macrovision Europe Ltd.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

  Java 2 Platform kann außerdem folgende Drittanbieterprodukte enthalten:

  - CoolServlets © 1999
  - DES and 3xDES © 2000, Jef Poskanzer
  - Crimson © 1999–2000, The Apache Software Foundation
  - Xalan J2 © 1999–2000, The Apache Software Foundation
  - NSIS 1.0j © 1999–2000, Nullsoft, Inc.
  - Eastman Kodak Company © 1992

- Lucinda, eine eingetragene Marke oder Marke von Bigelow and Holmes
- Taligent, Inc.
- IBM, einige Teile verfügbar unter: http://oss.software.ibm.com/icu4j/

Weitere Informationen zu diesen Drittanbietertechnologien und den zugehörigen Haftungssauschlüssen und Einschränkungen finden Sie unter: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javabeans/glasgow/jaf.html, klicken Sie auf "Download" > "License".
- JavaMail. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javamail/downloads/index.html, klicken Sie auf „Download“ > „License“.
- Java Ace von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University und Tao (mit ACE-Wrappers) von Douglas C. Schmidt und seiner Forschungsgruppe an der Washington University, University of California, Irvine, und Vanderbilt University. Copyright © 1993–2005. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html und http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Java Authentication and Authorization Service Modules, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://free.tagish.net/jaas/index.jsp.
- Java Network Launching Protocol (JNLP). Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.java.sun.com/products/javawebstart/download-jnlp.html, klicken Sie auf „Download“ > „License“.
- Java Service Wrapper. Teile wie folgt durch Copyright geschützt: Copyright © 1999, 2004 Tanuki Software und Copyright © 2001 Silver Egg Technology. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://wrapper.tanukisoftware.org/doc/english/license.html.
- JIDE. Copyright © 2002 bis 2005, JIDE Software, Inc.
- jTDS ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, lizenziert unter: Lesser General Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://web.ukonline.co.uk/mseries
- Monarch Charts. Copyright © 2005, Singleton Labs.
- Net-SNMP. Teile des Codes unterliegen dem Copyright verschiedener juristischer Personen, die sich alle Rechte vorbehalten. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 bis 2000, the Regents of the University of California; Copyright © 2001 bis 2003 Networks Associates Technology, Inc.; Copyright © 2001 bis 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc., und Copyright © 2003 bis 2004, Sparta, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://net-snmp.sourceforge.net.
- The OpenSSL Project. Copyright © 1998–2004, The Open SSL Project. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.openssl.org.
- Oracle Help für Java. Copyright © 1994–2006, Oracle Corporation.
- RoboHELP Office. Copyright © Adobe Systems Incorporated, vormals Macromedia.
- Skin Look and Feel (SkinLF). Copyright © 2000–2006 L2FProd.com. Lizenziert unter der Apache-Softwarelizenz. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter https://skinlf.dev.java.net/.
- Sonic Software Corporation. Copyright © 2003–2004. Die SSC-Software enthält Sicherheitssoftware, die von RSA Security, Inc., lizenziert wurde.
- Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © 2003 bis 2006. SecurityNexus, LLC. Alle Rechte vorbehalten.

- Xalan und Xerces, jeweils von der Apache Software Foundation lizenziert, Copyright © 1999–2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © 2003 bis 2006, yWorks.

HINWEIS: Zum Zeitpunkt der Veröffentlichung dieser Dokumentation waren die oben stehenden Links aktiv. Sollten Sie feststellen, dass einer der oben angegebenen Links unterbrochen oder die verlinkten Webseiten inaktiv sind, wenden Sie sich an Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Vorwort

Bei der Technischen Dokumentation von Sentinel handelt es sich um allgemeine, zweckorientierte Handbücher für den Betrieb und zur Referenz. Diese Dokumentation ist für Mitarbeiter des Bereichs Informationssicherheit konzipiert. Der Text in dieser Dokumentation gilt als Referenzquelle zum Enterprise Security Management System von Sentinel. Im Sentinel-Webportal steht weitere Dokumentation zur Verfügung.

Die Technische Dokumentation von Sentinel umfasst fünf einzelne Ausgaben. Dazu gehören:

- Band I – Sentinel™ 5-Installationshandbuch
- Band II – Sentinel™ 5-Benutzerhandbuch
- Band III – Sentinel™ 5 Wizard-Benutzerhandbuch
- Band IV – Sentinel™ 5-Referenzhandbuch für Benutzer
- Band V – Sentinel™-Handbuch für Drittanbieter-Integration

Band I – Sentinel Installationshandbuch

In diesem Handbuch wird die Installation folgender Komponenten erläutert:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Wizard Collector Builder
- Wizard Collector Manager
- Advisor

Band II – Sentinel Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Verwendung der Sentinel Console
- Sentinel-Funktionen
- Sentinel Architektur
- Sentinel Kommunikation
- Herunterfahren/Starten von Sentinel
- Anfälligkeitsbewertung
- Ereignisüberwachung
- Ereignisfilterung
- Ereigniskorrelation
- Sentinel Data Manager
- Ereigniskonfiguration für Unternehmensrelevanz
- Zuordnungsservice
- Verlaufsberichte
- Wizard-Host-Verwaltung
- Vorfälle
- Szenarios
- Benutzerverwaltung
- Workflow

Band III – Wizard-Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Wizard Collector Builder-Operation
- Wizard Collector Manager
- Collectors
- Wizard-Host-Verwaltung
- Erstellen und Verwalten von Collectors

Band IV – Sentinel Referenzhandbuch für Benutzer

In diesem Handbuch werden die folgenden Themen behandelt:

- Wizard-Skriptsprache
- Wizard-Parsing-Befehle
- Wizard-Administratorfunktionen
- META-Tags für Wizard und Sentinel
- Benutzerberechtigungen
- Sentinel Correlations Engine
- Korrelations-Befehlszeilenoptionen
- Sentinel-Datenbankschema

Band V – Sentinel Handbuch für Drittanbieter-Integration

- Remedy
- HP OpenView Operations
- HP Service Desk

Inhalt

1 Einführung

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Dieses Handbuch führt Sie in Einzelschritten durch eine Standardinstallation. Das *Benutzerhandbuch zu Sentinel™ 5* enthält detailliertere Beschreibungen zu Architektur, Betrieb und Administrationsvorgängen.

In diesem Handbuch wird davon ausgegangen, dass Sie mit den Aspekten der Netzwerksicherheit, der Datenbankverwaltung sowie den Windows- und UNIX-Betriebssystemen vertraut sind.

Verwendete Konventionen

Hinweise und Warnhinweise

HINWEIS: Hinweise stellen zusätzliche Informationen bereit, die sich als hilfreich erweisen können.

ACHTUNG: Warnhinweise stellen zusätzliche Informationen bereit, mit denen sich Beschädigungen des Systems bzw. Datenverluste u. U. vermeiden lassen.

Befehle

Befehle sind in Courier-Schriftart angegeben. Beispiel:

```
useradd –g dba –d /export/home/oracle –m –s /bin/csh
   oracle
```

Überblick über Sentinel 5

Sentinel 5 legt die Messlatte in Bezug auf die Eigenschaften, die man von einem System für die Verwaltung von Sicherheitsinformationen erwarten kann, höher. Sentinel 5 beinhaltet Standardfunktionen zur Verwaltung von Sicherheitsinformationen, wie beispielsweise das Sammeln, Aggregieren, Korrelieren und Anzeigen von Ereignisdaten. Außerdem können Sie damit entschieden und angemessen auf Vorfälle reagieren, indem Sie die Verfahren zur Vorfallsidentifikation und -auflösung automatisieren und erzwingen.

Die wichtigsten Funktionen von Sentinel 5 sind iTRAC™, Active Views™ und iSCALE™. Mit diesen Funktionen können Verwaltung, Messung und Einhaltung von Bestimmungen effektiver durchgeführt werden. Sentinel 5 bietet folgende Möglichkeiten:

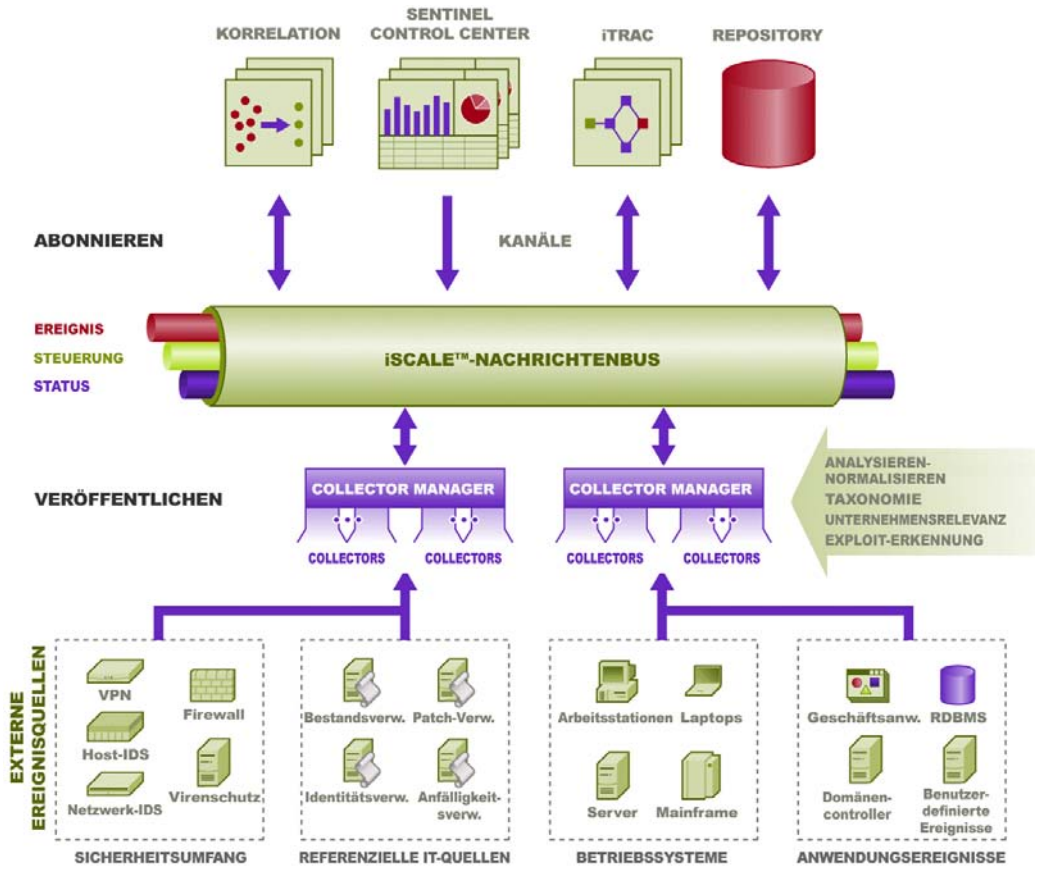
- Bereitstellung der Sichtbarkeit und Steuerungsmöglichkeiten, die erforderlich sind, um eine größere Kosteneffektivität der Sicherheitsumgebung zu erreichen
- Schnellere Erkennung und Auflösung von Vorfällen bei gleichzeitiger Senkung der Betriebskosten
- Bereitstellung geeigneter Berichte und Metriken zur fortlaufenden Bewertung Ihrer Position hinsichtlich Sicherheit und Einhaltung von Bestimmungen
- Erreichen und Überwachen der Einhaltung von internen Richtlinien und rechtlichen Vorschriften.

Erzielen größerer Leistungen mit den vorhandenen Ressourcen durch Reduzieren der manuellen Vorgänge

Sentinel 5 besteht aus mehreren Komponenten, die in ihrem Zusammenspiel die führende Lösung auf dem Markt ergeben:

- Sentinel Control Center
- Sentinel Server
- Sentinel Advisor
- Sentinel Data Manager
- Sentinel Wizard
  - Wizard Collector Builder
  - Wizard Collector Manager
  - Wizard Engine

Im Folgenden wird die **konzeptionelle Architektur** von Sentinel 5 erörtert und es werden die Sentinel-Komponenten beschrieben, die an der Durchführung des Sicherheitsmanagements beteiligt sind.



Sentinel-Produktmodule

Sentinel 5 besteht aus drei Hauptmodulen – Sentinel Control Center, Sentinel Wizard (Collector Builder und Collector Manager) und Sentinel Advisor.

Sentinel Control Center

Sentinel Control Center bietet eine integrierte Sicherheitsverwaltungskonsole, mit der Analysten schnell neue Trends oder Angriffe erkennen, grafische Informationen in Echtzeit bearbeiten und damit interagieren sowie auf Vorfälle reagieren können. Sentinel Control Center beinhaltet folgende wichtige Funktionen:

- Active Views – Analysefunktionen und Visualisierung in Echtzeit
- Vorfälle – Erstellung und Verwaltung von Vorfällen
- Admin – Definition und Verwaltung von Korrelationsregeln
- iTRAC – Prozessverwaltung für Dokumentation, Erzwingung und Verfolgung von Prozessen zur Vorfallsauflösung.
- Berichterstellung –Verlaufsberichte und Metriken

Sentinel Wizard

Sentinel Wizard sammelt Daten aus Quellgeräten und bietet einen umfangreicheren Ereignisstream durch Einfügen von Taxonomie, Exploit-Erkennung und Geschäftsrelevanz in den Datenstrom, bevor die Ereignisse korreliert und analysiert und an die Datenbank gesendet werden. Ein umfangreicherer Ereignisstrom bedeutet, dass die Daten mit dem erforderlichen Geschäftskontext korreliert werden, um interne bzw. externe Bedrohungen und Richtlinienverletzungen erkennen und beheben zu können. In jeder Konfiguration können ein oder mehrere Instanzen von Wizard bereitgestellt werden, sodass die Kunden die Möglichkeit erhalten, Produktkomponenten auf der Grundlage ihrer Netzwerktopologie in ihrer Infrastruktur bereitzustellen.

Mit Wizard können Sie Collectors effizient entwickeln und anpassen. Dadurch kann Sentinel Daten aus vielen verschiedenen Geräten in einem Unternehmen sammeln. Bei diesen Geräten handelt es sich unter anderem um folgende:

- Intrusion Detection-Systeme (Host)
- Intrusion Detection-Systeme (Netzwerk)
- Firewalls
- Betriebssysteme
- Richtlinienüberwachung
- Authentifizierung
- Router & Switches
- VPN
- Virenschutz
- Webserver
- Datenbanken
- Mainframe
- Anfälligkeitsbewertung
- Directory Services
- Netzwerk-Management
- Proprietäre Systeme

Zu den Hauptkomponenten von Sentinel Wizard gehören folgende Elemente:

- Collector – ein Rezeptor, der unverarbeitete (rohe) Ereignisse aus Sicherheitsgeräten und -systemen sammelt und normalisiert.
- Collector Engine – Komponente, die die Schablonenlogik für die einzelnen Ports verarbeitet.
- Collector Manager – die Back-End-Komponente, die Collectors und Meldungen über den Systemstatus verwaltet und eine globale Filterung der Ereignisse durchführt.
- Collector Builder – eine eigenständige Anwendung, mit der Sie Collectors erstellen und konfigurieren können.

Sentinel Advisor

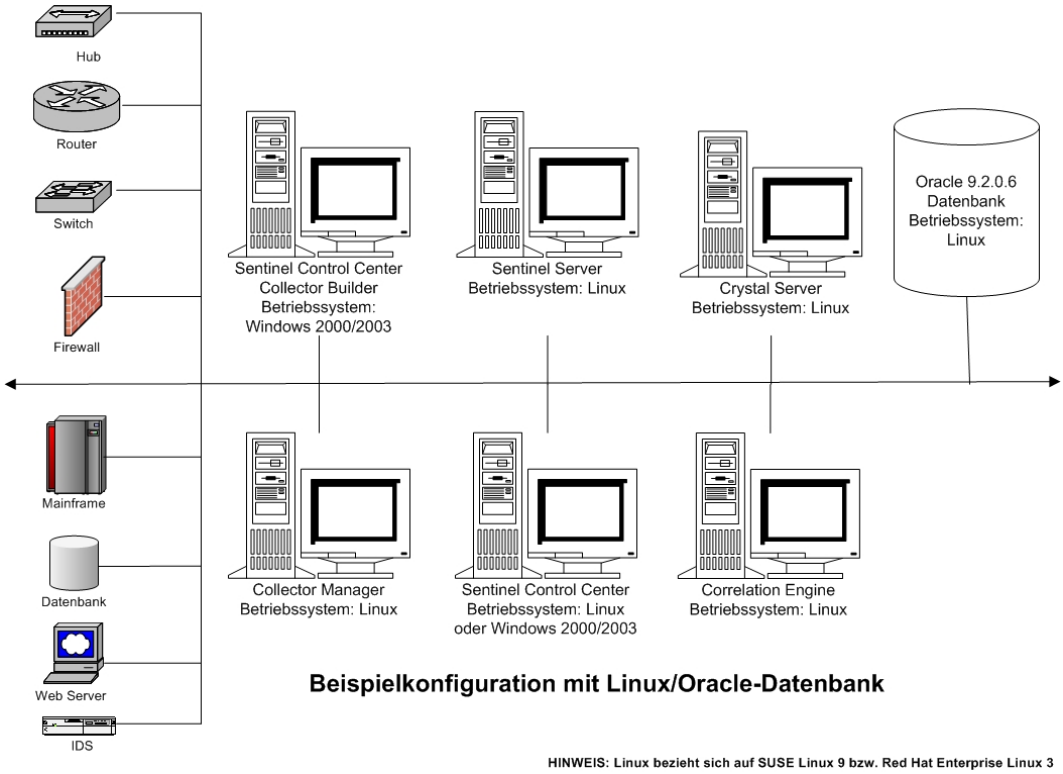
Sentinel Advisor ist ein optionales Zusatzmodul, das Querverweise zwischen Echtzeit-Alarmdaten von Sentinel und Informationen über bekannte Anfälligkeiten und Gegenmaßnahmen bietet.

Typische Konfiguration

Im Folgenden finden Sie typische Konfigurationen von Sentinel 5 sowie eine Erläuterung zur Durchführung des Sicherheitsmanagements. Ihre Implementierung kann je nach Ort und Art der Installation abweichen.

HINWEIS: Genauere Informationen zu EPS (Ereignisse pro Sekunde), Plattformen, RAM, Anforderungen für den Festplattenspeicher und CPU finden Sie in *Kapitel 2 – Optimale Verfahren*.

Unterstützte Plattformen für Sentinel Server unter Linux



HINWEIS: Informationen zu den einzelnen Betriebssystemen finden Sie in den folgenden Tabellen.

Sentinel Server		
Betriebssystem	**Version**	**Patch-Stufe**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	Update 5 ES (x86)

Datenbank		
Datenbank	**Version**	**Patch-Stufe**
Oracle 64-Bit Enterprise Edition	9i	▪ 9.2.0.6 2617419 oder ▪ 9.2.0.7

HINWEIS: Weitere Informationen zum wichtigen Patch 2617419 finden Sie auf der Oracle-Website und im Novell-Kundenportal.

Sentinel Control Center (Benutzerschnittstelle)		
Betriebssystem	**Version**	**Patch-Stufe**
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

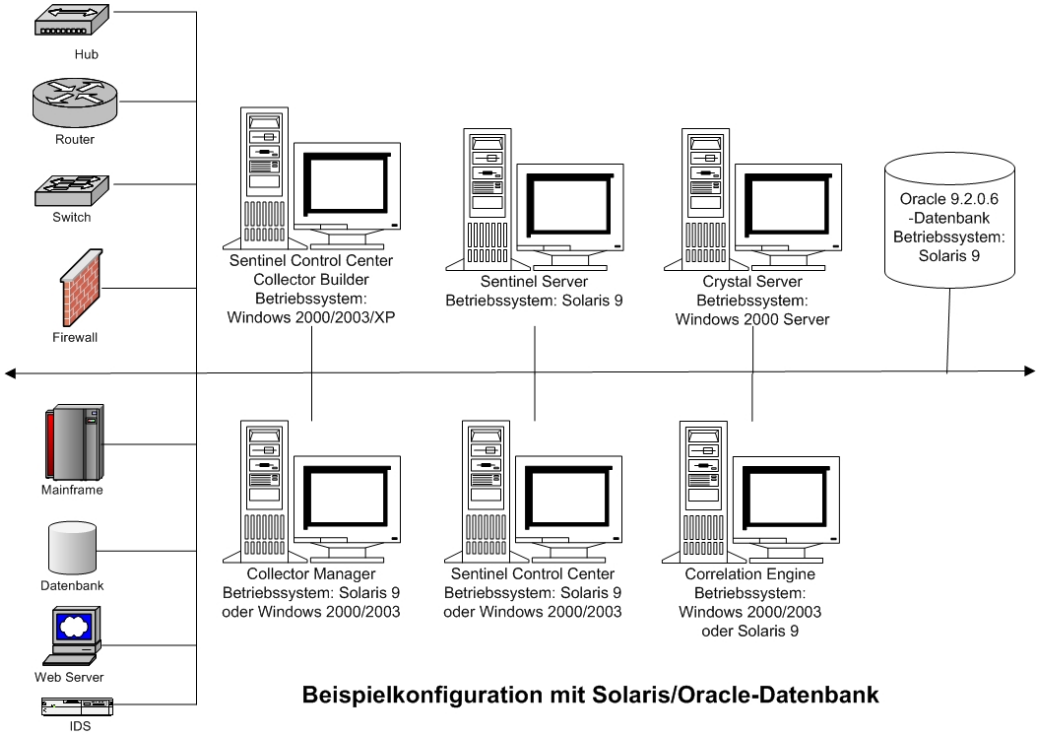
Collector Builder		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1

Collector Manager		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATUM: 03. Mai 2005
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server (Auswahl aus zwei Versionen [Linux (SLES/Red Hat) und Windows])			
Crystal Version	**Betriebssystem**	**Betriebssystem-Version**	**Betriebssystem-Patch-Stufe**
Crystal BusinessObjects Enterprise™ 11	SuSE Linux Enterprise Server 9 (SLES 9)	9	
Crystal BusinessObjects Enterprise™ 11	Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Crystal BusinessObjects Enterprise™ 11	Windows mit MS SQL 2000. Sentinel 5 unterstützt MSDE nicht.	Windows 2003 Server.	SP1

HINWEIS: Sentinel 5 unterstützt Crystal XI auf Windows® 2000 Server und MSDE nicht.

Unterstützte Plattformen für Sentinel Server unter Solaris



Beispielkonfiguration mit Solaris/Oracle-Datenbank

HINWEIS: Informationen zu den einzelnen Betriebssystemen finden Sie in den folgenden Tabellen.

Sentinel Server		
Betriebssystem	**Version**	**Patch-Stufe**
Solaris Enterprise Edition	9	Solaris 9 Recommended Patch Cluster DATUM: 03. Mai 2005

Datenbank		
Datenbank	**Version**	**Patch-Stufe**
Oracle 64-Bit	9i	▪ 9.2.0.6 2617419 oder ▪ 9.2.0.7

HINWEIS: Weitere Informationen zum wichtigen Patch 2617419 finden Sie auf der Oracle-Website und im Novell-Kundenportal.

Sentinel Control Center (Benutzerschnittstelle)		
Betriebssystem	**Version**	**Patch-Stufe**
Solaris	9	Solaris 9 Recommended Patch Cluster DATUM: 03. Mai 2005

Sentinel Control Center (Benutzerschnittstelle)		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Collector Builder		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1

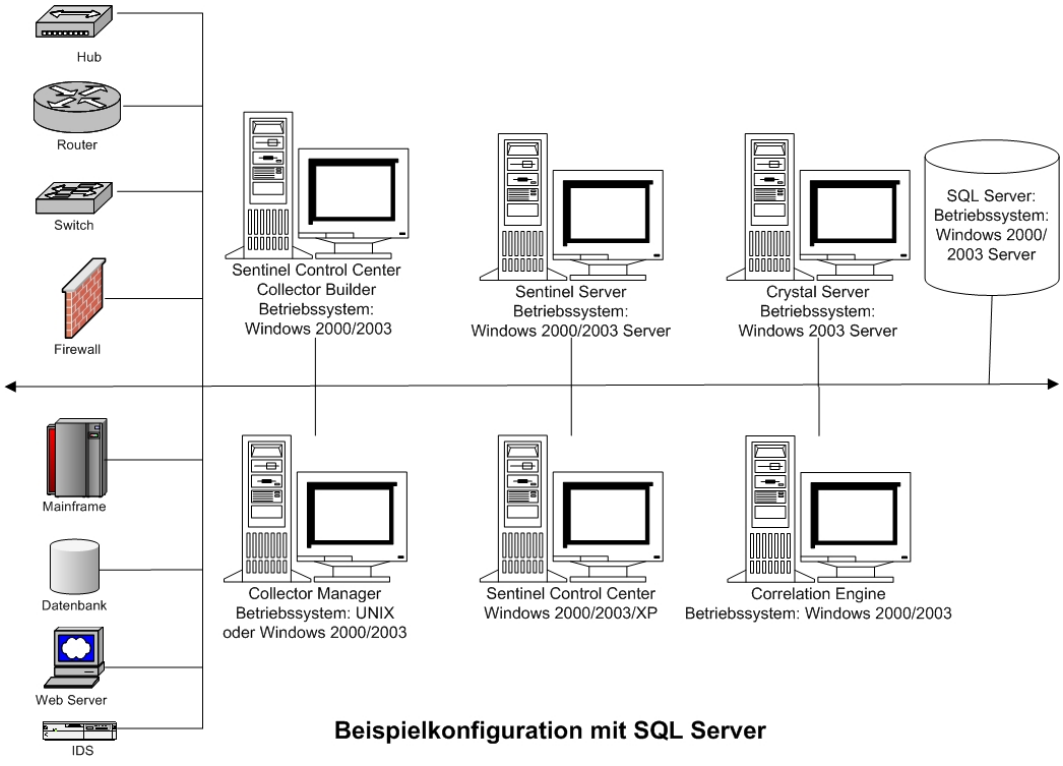
Collector Manager		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATUM: 03. Mai 2005
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Crystal Version	**Betriebssystem**	**Betriebssystem-Version**	**Betriebssystem-Patch-Stufe**
Crystal BusinessObjects Enterprise™ 11	Windows mit MS SQL 2000. Sentinel 5 unterstützt MSDE nicht.	Windows 2003 Server	SP1

HINWEIS: Crystal Reports v9 wird unter Sentinel v5.1 und früher sowie unter Sentinel v5.1.1 SP1 und höher unterstützt. Es wird nicht unter Sentinel v5.1.1 ohne SP1 unterstützt. Wenn Sie Crystal Reports v9 und Sentinel v5.1.1 verwenden, müssen Sie Sentinel v5.1.1 Service Pack 1 anwenden oder auf v5.1.2.bzw.v5.1.3 aufrüsten.

HINWEIS: Sentinel 5 unterstützt Crystal XI auf Windows® 2000 Server nicht.

Unterstützte Plattformen für Sentinel Server unter Windows



Beispielkonfiguration mit SQL Server

HINWEIS: Informationen zu den einzelnen Betriebssystemen finden Sie in den folgenden Tabellen.

Sentinel Server		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000 Server – Enterprise Edition	SP4
Windows	2003 Server – Enterprise Edition	SP1

Datenbank		
Datenbank	**Version**	**Patch-Stufe**
SQL Server	2000 Enterprise	SP3a
SQL Server	2005 Enterprise (Sentinel v5.1.1 SP1 und höher)	

Sentinel Control Center (Benutzerschnittstelle)		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Collector Builder		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1

Collector Manager		
Betriebssystem	**Version**	**Patch-Stufe**
Windows	2000	SP4
Windows	2003	SP1
Solaris	9	Solaris 9 Recommended Patch Cluster DATUM: 03. Mai 2005
SuSE Linux Enterprise Server 9 (SLES 9)	9	
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Crystal Version	**Betriebssystem**	**Betriebssystem-Version**	**Betriebssystem-Patch-Stufe**
Crystal BusinessObjects Enterprise™ 11	Windows mit MS SQL 2000. Sentinel 5 unterstützt MSDE nicht.	Windows 2003 Server	SP1

HINWEIS: Crystal Reports v9 wird unter Sentinel v5.1 und früher sowie unter Sentinel v5.1.1 SP1 und höher unterstützt. Es wird nicht unter Sentinel v5.1.1 ohne SP1 unterstützt. Wenn Sie Crystal Reports v9 und Sentinel v5.1.1 verwenden, müssen Sie Sentinel v5.1.1 Service Pack 1 anwenden oder auf v5.1.2.bzw.v5.1.3 aufrüsten.

HINWEIS: Sentinel 5 unterstützt Crystal XI auf Windows® 2000 Server nicht.

Weitere Novell-Referenzen

Folgende Handbücher sind auf den Sentinel-Installations-CDs enthalten:

- Sentinel™-Installationshandbuch
- Sentinel™-Benutzerhandbuch
- Sentinel™ 5 Wizard-Benutzerhandbuch
- Sentinel™-Referenzhandbuch für Benutzer
- Sentinel™-Handbuch für Drittanbieter-Integration
- Versionshinweise

Kontaktaufnahme mit Novell

- Website: http://www.novell.com
- Technischer Support von Novell: http://www.novell.com/support/index.html
- Internationaler technischer Support von Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self-Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Für Support rund um die Uhr: +1 800-858-4000

2 Optimale Verfahren

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

In diesem Kapitel werden optimale Verfahren erörtert und Empfehlungen zur bestmöglichen Nutzung von Sentinel abgegeben. Es enthält folgende Themen:

- Optimale Verfahren für die Installation
  - Hardware-Empfehlungen
  - Konfiguration für Disk-Array
  - Netzwerkkonfiguration
  - Installation von Oracle und MS SQL Server
  - Sentinel-Datenbank-Patches
  - Empfohlene UNIX-Kernel-Einstellungen
  - Konfigurationsparameter beim Erstellen der eigenen Datenbankinstanz
  - Installation von Sentinel
  - Maximieren der Ereignisberichterstellung für Crystal Reporting
  - Von Sentinel bereitgestellte Berichte
  - Tipps für die Entwicklung benutzerdefinierter Crystal-Berichte
- Optimale Verfahren für die Wartung
  - Datenbankanalyse
  - Database Health CheckCorrelation Engine
  - Transaktionsprotokoll Speicherorte der Sentinel-Protokolldateien

Installation Best Practices

In der folgenden Tabelle finden Sie die Leistungs-Ratings für bestimmte Attribute von Sentinel.

Attribut	Rating	Kommentare
▪ EPS zum Einfügen der Ereignisdatenbank	1250	Das Einfügen wird durch Korrelationsregeln und den Zuordnungsservice beeinflusst.
▪ EPS für jeden Collector Manager	350	
▪ EPS pro Collector (Checkpoint, Win2K, etc...)	300	
▪ Maximale Anzahl an pro Collector Manager unterstützten Collectors	10	
▪ Maximale Anzahl von Collector Managers pro Sentinel-Instanz	20	
▪ Anzahl der pro Correlation Engine bereitgestellten Regeln	20-80	Niedrige EPS (150 EPS) = 80 Hohe EPS (1250 EPS) = 20
▪ Wie viele Active Views™ pro Sentinel-Instanz	35-50	

- Maximale Anzahl gleichzeitiger Benutzer 20
- Maximle Anzahl von Ansichten pro Sentinel Control Center 10
- Maximum Anzahl von Zuordnungen pro Sentinel-Instanz 10
- Maximale Größe der einzelnen Zuordnungen 10 MB
- Maximale Anzahl an Zeilen pro Zuordnung 350k

CPU-Referenzspezifikation beruht auf:

- Windows – 3,2 GHz Xeon
- SuSE Linux – 3.2 GHz Xeon
- Solaris – 1,1 GHz Sparc-3
- Linux – 3,2 GHz Xeon

Die Konfiguration gilt für folgende Betriebssysteme:

- Windows 2003 Server mit SP4
- Windows 2003 Server mit SP1
- SuSE Linux Enterprise Server 9 (SLES 9)
- Solaris 9 mit Patches und Version Generic_112233-11 des Recommended Patch Cluster
- Red Hat Enterprise Linux 3 Update 5 ES (x86)

Bei der Datenbank handelt es sich um eine der folgenden:

- MSSQL 2000 mit SP3a
- Oracle 9i Enterprise Edition 9.2.0.6 bzw. 9.2.0.7 mit Partitionierung

Einfache Konfiguration – Einzelplatzbetrieb (Demo)

Bei dieser Installation werden alle Komponenten (einschließlich der Datenbank) auf einer einzelnen Plattform installiert. Dies dient vorrangig zu Demonstrationszwecken. Es ist nicht für die aktuelle Verwendung zu empfehlen. Es gelten folgende Hardware-Voraussetzungen:

Komponenten	**Minimum**		**Empfohlen**	
	RAM (GB)	**CPU**	**RAM (GB)**	**CPU**
Computer 1 ▪ Alle Sentinel-Komponenten ▪ Collector Manager ▪ Collectors ▪ Datenbank ▪ Disk-Array Für Windows: ▪ Crystal Server ▪ Collector Builder Für Linux: ▪ Crystal Server	2	2	4	2

Komponenten	Minimum RAM (GB)	CPU	Empfohlen RAM (GB)	CPU
Computer 2 (nur für UNIX-Installationen) Für Solaris: ▪ Crystal Server ▪ Collector Builder (Windows) Für Linux: ▪ Collector Builder (Windows)	1.0	1	2.0	2

Proof of Concept (POC) – Einzelplatzkonfiguration

Bei dieser Installation werden alle Komponenten mit Ausnahme der Datenbank) auf einer einzelnen Plattform installiert. Diese Konfiguration wird normalerweise verwendet, um die prinzipielle Machbarkeit zu beweisen und die Funktiosfähigkeit bei normaler Belastung zu testen. In diesem Fall befindet sich die Datenbank auf einem anderen Rechner als die übrige Sentinel-Installation.

Komponenten	Minimum RAM (GB)	CPU	Empfohlen RAM (GB)	CPU
Computer 1 ▪ Alle Sentinel-Komponenten ▪ Collector Manager ▪ Collectors Für Windows: ▪ Crystal Server ▪ Collector Builder Für Linux: ▪ Crystal Server	4.0	2	4	4
Computer 2 ▪ Datenbank ▪ Disk-Array	4	2	4	4
Computer 3 (nur für UNIX-Installationen) Für Solaris: ▪ Crystal Server ▪ Collector Builder (Windows) Für Linux: ▪ Collector Builder (Windows)	2.0	2	4.0	2

Produktion – Verteilte Konfiguration

Bei einer verteilten Konfiguration handelt es sich um eine Benutzerdefinierte Installation die für Standard und Enterprise Systems verwendet wird.

Da Sentinel neben Crystal Reports 8 gesonderte Komponenten aufweist, können viele verschiedene Konfigurationen erstellt werden. Die folgenden Ausführungen behandeln zwei verschiedene Konfigurationen.

Da Datenbanken E/A-abhängig sind, sollten Sie Ihre Datenbanken auf einem gesonderten Computer speichern. Für den DB-Server ist ein Hochgeschwindigkeits-Speicher-Array erforderlich, der die E/A-Anforderungen auf der Grundlage der Einfügegeschwindigkeit für Ereignisse erfüllen.

Die verteilten Hosts müssen mit den anderen Sentinel Server-Hosts über einen einzelnen Hochgeschwindigkeits-Switch (GIGE) verbunden sein, um Engpässe im Netzwerkverkehr zu vermeiden.

Produktion – Verteilte Konfiguration (Option 1)

Konfiguration mit 4 Computern

Komponenten	**Minimum**		**Empfohlen**	
	RAM (GB)	**CPU**	**RAM (GB)**	**CPU**
Computer 1 ▪ Correlation Engine ▪ DAS ▪ iSCALE (Nachrichtenbus) ▪ „Advisor“	4.0	4	8.0	8
Computer 2 ▪ Collector Manager ▪ „Collectors“	1.0	2	2.0	2
Computer 3 ▪ Crystal Server	2.0	2	4.0	4
Computer 4 ▪ Datenbank ▪ Disk-Array	4	4	16	8

Produktion – Verteilte Konfiguration (Option 2)

Konfiguration mit 5 Computern

Komponenten	**Minimum**		**Empfohlen**	
	RAM (GB)	**CPU**	**RAM (GB)**	**CPU**
Computer 1 ▪ DAS ▪ iSCALE (Nachrichtenbus) ▪ „Advisor“	4.0	4	8.0	8
Computer 2 ▪ Correlation Engine	1.0	2	2.0	2

Komponenten	Minimum		Empfohlen	
	RAM (GB)	CPU	RAM (GB)	CPU
Computer 3 ▪ Collector Manager ▪ „Collectors“	1.0	2	2.0	2
Computer 4 ▪ Crystal Server	2.0	2	4.0	4
Computer 5 ▪ Datenbank ▪ Disk-Array	4	4	16	8

Richtlinie für Patch-Unterstützung

Sentinel zertifiziert Betriebssystem- und Datenbank-Patches innerhalb von 60 Tagen nach ihrer Herausgabe.

Hardware-Empfehlungen

Sentinel Server Correlation Engine			
EPS	**RAM**	**Speicher**	**CPU**
250	2 GB	72 GB	Windows – 2 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 2 x 3.0 GHz Xeon Solaris – V280 2 x 1,1 GHz Ultra Sparc III
500	4 GB	72 GB	Windows – 4 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 4 x 3.0 GHz Xeon Solaris – V480 4 x 1,1 GHz Ultra Sparc III
1000+	8 GB	72 GB	Windows – 8 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 8 x 3.0 GHz Xeon Solaris – V880 8 x 1,1 GHz Ultra Sparc III

Collector Manager			
EPS	**RAM**	**Speicher**	**CPU**
250	2 GB	36 GB	Windows – 2 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 2 x 3.0 GHz Xeon Solaris – V280 2 x 1,1 GHz Ultra Sparc III
350+	4 GB	36 GB	Windows – 4 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 4 x 3.0 GHz Xeon Solaris – V480 4 x 1,1 GHz Ultra Sparc III

Sentinel Control Center Collector Builder (nur Windows) Sentinel Data Manager		
RAM	**Speicher**	**CPU**
2 GB	15 GB	Windows 2000 oder 2003 – 2 x 3,0 GHz Xeon Windows XP (nur Control Center) – 2 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 2 x 3.0 GHz Xeon Sun Solaris 9 – V280 2 x 1,1 GHz Ultra Sparc III

		Datenbank	
EPS	**RAM**	**Speicher**	**CPU**
250	8 GB	500 GB	Windows – 4 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 4 x 3.0 GHz Xeon Solaris – V480 4 x 1,1 GHz Ultra Sparc III
500	12 GB	1,0 TB	Windows – 4 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 4 x 3.0 GHz Xeon Solaris – V880 6 x 1,1 GHz Ultra Sparc III
1000+	16 GB	2,0 TB	Windows – 8 x 3,0 GHz Xeon SuSE Linux oder Redhat Linux – 8 x 3.0 GHz Xeon Solaris – V880 8 x 1,1 GHz Ultra Sparc III

Konfiguration für Disk-Array

Bei Novell Sentinel 5 Server im Produktionskontext ist ein Hochgeschwindigkeits-Disk-Array für die Datenbank und die Sentinel-Hosts erforderlich. In diesem Abschnitt werden Konfigurationsempfehlungen für typische Datenträger (RAID) abgegeben. Folgende Komponenten werden in erster Linie von der Leistung der Datenträgerhardware beeinflusst:

- Database-Komponente (MSSQL/Oracle): Die Ereignisrate (EPS) und Query-Funktionen (Quick Query / Crystal-Leistung) sind betroffen.
- DAS-RT (Data Access Service Real Time-Komponente): Funktion Active View ist betroffen.
- DAS-Aggregation: Die Anzahl der Zusammenfassungen, die aktiviert werden können, ist betroffen.

Mindestanforderung für die Enterprise-Installation (mindestens 1000 EPS)

Es sollte mindestens eine RAID 5-Konfiguration verwendet werden. RAID 5 kann am kosteneffektivsten sein. Allerdings bringt diese Konfiguration gewisse Einbußen bei Leistung und Redundanz zugunsten des besseren Kostenverhältnisses mit sich. Beachten Sie, dass es sich hierbei lediglich um Empfehlungen handelt, die als Richtschnur verwendet werden sollten. Für die meisten groß angelegten produktionsfähigen Unternehmensinstallationen ist eine detailliertere Analyse der Anforderungen an Geschwindigkeit, Durchsatz und Redundanz erforderlich.

- RAID-Gruppe 1 – Datanbank (Daten, Indizes, Transaktionsprotokolle usw.)
- RAID-Gruppe 2 – Sentinel Server DAS (Datenverzeichnis, Temp DIR*)
- Mindestanzahl an Datenträgern: 13 pro RAID-Gruppe
- Festplattentyp: 12k+ RPM, Glasfaserkanal or SCSI
- LUN 1 (RAID-Gruppe 1): 5–144 GB+ pro Festplatte
- LUN 2 (RAID-Gruppe 2): 5–144 GB+ pro Festplatte

Optimale Konfiguration

Für eine Konfiguration mit optimaler Leistung und Redundanz kann ein RAID 1+0 mit denselben Einstellungen wie oben verwendet werden. Es können jedoch unter Einhaltung derselben Richtlinien wie oben weitere RAID-Gruppen und LUNs erforderlich sein, um für bestimmte Datenbanken größeren Parallelismus und bessere E/A-Werte zu erreichen.

HINWEIS: Im Abschnitt Installation von Sentinel finden Sie Anweisungen dazu, wie Sie DAS TEMP DIR auf einen anderen Speicherort verweisen lassen können.

Beispielspeicherkonfiguration für eine MS SQL-Installation

In diesem Beispiel wird das Speichersubsystem EMC^2 CLARiiON mit folgenden Eigenschaften verwendet:

- 1 TB Speicherplatz
- 60 Laufwerke, 36 GB, 15 K RPM

RAID-Gruppen

Array	RAID-Gruppe	Anzahl der Laufwerke	Zugewiesene Laufwerke (Bus-Gehäuse-Festplatte)	Name
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	RAID-Gruppe 0
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	RAID-Gruppe 1
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	RAID-Gruppe 2
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	RAID-Gruppe 3
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	RAID-Gruppe 4
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	RAID-Gruppe 5
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	RAID-Gruppe 6

LUN-Zuweisungen

Array	LUN	RAID-Typ	RAID-Gruppe	Größe (GB)	Speicher-prozessor	Name
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

Speichergruppen

Array	Speichergruppe	LUN	Host	Laufwerk-buchstabe	Name
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H:	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I:	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J:	SQLIndex1

Array	Speichergruppe	LUN	Host	Laufwerk-buchstabe	Name
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

Beispielspeicherkonfiguration für eine Oracle-Konfiguration

Volume 1	RAID 1	Oracle-Basisverzeichnis
Volume 2	RAID 1	Redo-Protokoll – Mitglied a
Volume 3	RAID 1	Redo-Protokoll – Mitglied b
Volume 4	RAID 0+1 oder RAID 5	Undo- und Temp-Tabellenbereiche
Volume 5	RAID 0+1 oder RAID 5	Tabellenbereiche für Sentinel-Daten
Volume 6	RAID 0+1 oder RAID 5	Tabellenbereiche für Sentinel-Index
Volume 7	RAID 0+1 oder RAID 5	Tabellenbereiche für Sentinel-Zusammenfassungsdaten
Volume 8	RAID 0+1 oder RAID 5	Tabellenbereiche für Sentinel-Zusammenfassungsindex
Volume 9	RAID 1	Archiv-Protokolldateien

Netzwerkkonfiguration

Komponenten für Sentinel Server: Diese Komponenten sollten miteinander über einen einzelnen 1 GB-Switch verbunden sein. Dazu gehören Datenbank, Kommunikationsserver, Advisor, Sentinel-Basisservices, Correlation Engine und DAS.

Sentinel Control Center, Collector Builder und Collector Service (Collector Manager): Diese Komponenten müssen über FULL DUPLEX-Switches mit mindestens 100 Mbit mit Sentinel Serververbunden sein.

Installation von Oracle und MS SQL Server

HINWEIS: Die meisten Datenbankinstallationsparameter können nach der Datenbankinstallation über Enterprise Manager bzw. über die Befehlszeile geändert werden.

1. Um eine möglichst hohe Leistung zu erreichen sollten, sofern die Installation in RAID vorgenommen wird und sofern es die RAID-Umgebung zulässt folgende Protokolle auf der Festplatte mit der höchsten Schreibgeschwindigkeit installiert werden, die verfügbar ist.
   - Redo-Protokoll (Oracle)
   - Transaction Log (MS SQL)
2. Um die Größe Ihrer Datenbank genau zu bestimmen, sollten Sie ursprünglich mit einer kleinen Datenbank anfangen und die Datenbankgröße erweitern, nachdem das System eine kurze Zeit ausgeführt wurde. So können Sie das Wachstum Ihrer Datenbank auf der Grundlage Einfügegeschwindigkeit für Ereignisse beobachten, um die Speicherplatzanforderungen für die Systemdatenbank zu ermitteln.
3. Um die Wiederherstellung zu erleichtern, sollten regelmäßige geplante Sicherungen der Datenbank durchgeführt werden.

4. Bei Oracle-Installationen wird die Archivprotokollierung standardmäßig deaktiviert. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank keine Ereignisse mehr entgegen, wenn die Kapazitätsgrenze des Protokollziels erreicht ist.
5. Zugunsten einer möglichst hohen Leistung sollten die Speicherorte auf verschiedene Orte verweisen, um E/A-Konflikte zu vermeiden.
   - Datenverzeichnis
   - Indexverzeichnis
   - Zusammenfassungsdatenverzeichnis
   - Zusammenfassungsindexverzeichnis
   - Protokollverzeichnis (Nur MS SQL)
   - Temporäres Verzeichnis und Tabellenbereichs-Verzeichnis zum Rückgängigmachen (nur Oracle)
   - Verzeichnis für Redo-Protokollmitglied A (nur Oracle)
   - Verzeichnis für Redo-Protokollmitglied B (nur Oracle)

Sentinel-Datenbank-Patches

Nur bei MS SQL gilt: Wenn Patches für die Sentinel-Datenbank angewendet werden, fügt das Installationsprogramm neue Indizes nur zu *_P_MAX hinzu. Bereits bestehende Partitionen werden nicht akutalisiert. Sie müssen Indizes manuell zu bereits bestehenden Partitionen hinzufügen, wenn die neuen Indizes die Leistungsfähigkeit für Abfragen erhöhen sollen, die für bestehende Partitionen ausgeführt werden.

Empfohlene UNIX-Kernel-Einstellungen

Im Folgenden finden Sie die vorgeschlagenen Mindestwerte. Weitere Informationen finden Sie in der Dokumentation zu Ihrem System und zu Oracle.

Mindestwerte für Kernel-Parameter für Linux

Weitere Informationen zur Anzeige und Festlegung von Kernel-Parametern unter Linux finden Sie in *Kapitel 3 – Installation von Sentinel 5 für Oracle – Vor der Installation von Oracle unter Linux*.

```
shmmax=2147483648 (Mindestwert)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Mindestwerte für Kernel-Parameter für Solaris

Überprüfen Sie die UNIX-Kernel-Parameters für Oracle unter /etc/system und legen Sie folgende Werte fest:

```
shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

Konfigurationsparameter beim Erstellen der eigenen Datenbankinstanz

Folgende Einstellungen werden für das Erstellen Ihrer Eigenen Datenbankinstanz empfohlen. Die Einstellungen können je nach Systemkonfiguration und Anforderungen variieren.

In der Oracle-Instanz müssen Sie folgende Elemente erstellen:

- Oracle-Initialisierungsparameter (diese Werte hängen von Systemgröße und Konfiguration ab)
- Für Sentinel erforderliche Tabellenbereichs-Konfigurationsparameter für Solaris und Linux

Empfohlene Mindestwerte für die Konfigurationsparameter	
Parameter	**Größe (in Byte, wenn nicht anders angegeben)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Empfohlene Mindestgröße für den Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
REDO	3 x 100 M	▪ Dies ist ein Mindestwert. Bei einem hohen EPS-Wert sollten größere Redo-Protokolle erstellt werden.
SYSTEM	500 M	▪ Mindestwert
TEMP	1 G	▪ Mindestwert
UNDO	1 G	▪ Mindestwert

Empfohlene Mindestgröße für den Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
ESENTD	5 G	▪ Mindestwert ▪ Für Ereignisdaten
ESENTD2	500 M	▪ Mindestwert ▪ Daten für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
ESENTWFD	250 M	▪ Für iTRAC-Daten (autoextend aktiviert)
ESENTWFX	250 M	▪ Für iTRAC-Index (autoextend aktiviert)
ESENTX	3 G	▪ Mindestwert ▪ Für Ereignisindex
ESENTX2	500 M	▪ Mindestwert ▪ Index für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
SENT_ADVISORD	200 M	▪ Mindestwert ▪ Für Advisor-Daten (autoextend aktiviert)
SENT_ADVISORX	100 M	▪ Mindestwert ▪ Für Advisor-Index (autoextend aktiviert)
SENT_LOBS	100 M	▪ Mindestwert ▪ Für große Datenbankobjekte (autoextend aktiviert)
SENT_SMRYD	3 G	▪ Mindestwert ▪ Für die Aggregation, Zusammenfassungsdaten
SENT_SMRYX	2 G	▪ Mindestwert ▪ Für die Aggregation, Zusammenfassungsindex

Installation von Sentinel

Bei der Installation von Sentinell sollten Sie zugunsten von Leistung und Sicherungsmöglichkeiten folgende Punkte bedenken.

1. Wenn Sie eine Neuinstallation von Sentinel durchführen möchten, nachdem bereits eine frühere Version installiert wurde, sollten Sie UNBEDINGT bestimmte Dateien und Systemeinstellungen aus der früheren Installation entfernen. Wenn Sie diese Dateien nicht entfernen, kann die Neuinstallation scheitern. Dieser Vorgang sollte auf jedem Computer durchgeführt werden, auf dem eine Neuinstallation erfolgen soll. Weitere Informationen zu den zu entfernenden Dateien finden Sie in *Anhang E*.
2. Die Leistung von Active Views und der Zuordnung kann enorm verbessert werden, indem das temporäre Verzeichnis der DAS_RT- und DAS_Query-Prozesse auf eine schnelle Festplatte (z. B. ein Disk-Array) verwiesen wird. Um das temporäre Verzeichnis dieser Prozesse auf eine schnelle Festplatte zu verweisen, gehen Sie auf dem Rechner, auf dem DAS installiert ist, wie folgt vor:
   a. Erstellen Sie auf der schnellen Festplatte ein Verzeichnis für die temporären Dateien. Unter UNIX müssen der Benutzer esecadm und die Gruppe esec Inhaber dieses Verzeichnisses sein und über Schreibrechte dafür verfügen.
   b. Erstellen Sie eine Sicherungskopie der Datei %ESEC_HOME%\configuration.xml.

c. Öffnen Sie die Datei %ESEC_HOME%\configuration.xml in einem Texteditor.

d. Fügen Sie für die DAS_RT- und DAS_Query-Prozesse das JVM-Argument java.io.tmpdir hinzu und setzen Sie es auf das soeben erstellte Verzeichnis.

e. Um diese Änderung für den DAS_RT-Prozess vorzunehmen, suchen Sie nach der Zeile mit dem Text

```
-Dsrv_name=DAS_RT
```

und fügen Sie genau danach das Argument

```
-Djava.io.tmpdir=<tmp-verzeichnis>
```

ein. Hier ein Beispiel für die Zeile aussehen sollte (die Argumennte –Xmx, -Xms, und –XX können abweichen):

```
<process component=„DAS“
   image=„&quot;$(ESEC_JAVA_HOME)/java&quot; -server -
   Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2 -Xmx310m
   -Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/BaseMetaDat
   a.xml -
   Djava.util.logging.config.file=../config/das_rt_log
   .prop -
   Dcom.esecurity.configurationfile=../../configuratio
   n.xml -
   Djava.security.auth.login.config=../config/auth.log
   in -Djava.security.krb5.conf=../../lib/krb5.conf -
   jar ../../lib/ccsbase.jar ..//config//das_rt.xml“
   min_instances=„1“ post_startup_delay=„5“
   shutdown_command=„cmd //C
   &quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
   bat&quot; localhost DAS_RT“
   working_directory=„$(ESEC_HOME)/sentinel/bin“/>
```

f. Um diese Änderung für den DAS_Query-Prozess vorzunehmen, suchen Sie nach der Zeile mit dem Text

```
-Dsrv_name=DAS_Query
```

und fügen Sie genau danach das Argument

```
-Djava.io.tmpdir=<tmp-verzeichnis>
```

ein. Hier ein Beispiel für die Zeile aussehen sollte (die Argumennte –Xmx, -Xms, und –XX können abweichen):

```
<process component=„DAS“
   image=„&quot;$(ESEC_JAVA_HOME)/java&quot; -server -
   Dsrv_name=DAS_Query -Djava.io.tmpdir=D:\Temp2 -
   Xmx256m -Xms85m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/BaseMetaDat
   a.xml,/xml/WorkflowMetaData.xml -
   Djava.util.logging.config.file=../config/das_query_
```

```
log.prop -
Djava.security.auth.login.config=../config/auth.log
in -Djava.security.krb5.conf=../../lib/krb5.conf -
Desecurity.execution.config.file=../config/executio
n.properties -
Dcom.esecurity.configurationfile=../../configuratio
n.xml -jar ../../lib/ccsbase.jar
..//config//das_query.xml“ min_instances=„1“
post_startup_delay=„5“ shutdown_command=„cmd //C
&amp;quot;$(ESEC_HOME)/sentinel/scripts/stop_container.
bat&amp;quot; localhost DAS_Query“
working_directory=„$(ESEC_HOME)/sentinel/bin“/>
```

Maximieren der Ereignisberichterstellung für Crystal Reporting

Je nachdem, wie viele Ereignisse Crystal abfragt, erhalten Sie möglicherweise eine Fehlermeldung bezüglich der maximalen Verarbeitungszeit oder der maximalen Datensatzgrenze. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Berichten einzurichten, müssen Sie den Crystal Page Server neu konfigurieren.

Neukonfiguratin von Crystal Page Server (nur Windows Crystal Server)

1. Klicken Sie auf *Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager*.
2. Klicken Sie mit der rechten Maustaste auf *Crystal Page Server* (Crystal Reports Page Server) und wählen Sie *Stop* (Stopp).
3. Klicken Sie mit der rechten Maustaste auf *Crystal Page Server* (Crystal Reports Page Server) und wählen Sie *Properties* (Eigenschaften).
4. Fügen Sie auf der Registerkarte „Properties“ (Eigenschaften) im Feld „Command“ (Befehl) am Ende der Befehlszeile Folgendes hinzu:

   ```
   maxDBResultRecords <Wert größer als 20000 oder 0 zur
      Deaktivierung der Standardgrenze>
   ```

5. Starten Sie *Crystal Page Server* erneut.

Neukonfiguration von Crystal Page Server (Linux oder Windows Crystal Server)

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   Für Linux Crystal Servers:

   ```
   http://<DNS oder IP von Crystal
      Server>:8080/businessobjects/enterprise11/adminlaun
      ch
   ```

   Für Window Crystal Servers:

   ```
   http://<DNS-Name oder IP-Adresse des
      Webservers>/businessobjects/enterprise11/WebTools/a
      dminlaunch/default.aspx
   ```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).

3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *Log On* (Anmelden).
5. Klicken Sie auf *Servers* (Server).
6. Klicken Sie auf *<Servername>.pageserver*.
7. Klicken Sie unter *Database Records to Read When Previewing Or Refreshing a report* (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf *Unlimited records* (Unbegrenzt viele Datensätze).
8. Klicken Sie auf *Apply* (Anwenden).
9. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf *OK* (OK).
10. Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager Betriebssystems aufgefordert.

Von Sentinel bereitgestellte Berichte

1. Für v5.1.1 SP1 und höher werden durch die Abfragen für die 10 wichtigsten Berichte Tabellen zusammengestellt, und keine detaillierte Ereignistabelle. Vergewissern Sie sich, dass EventFileRedirectService und die Aggregationsdienste (Zusammenfassungen) aktiviert sind.

   EventFileRedirectService befindet sich auf Ihrem DAS-Computer und kann durch Bearbeiten der Datei das_binary.xml aktiviert werden.

   Folgende drei Zusammenfassungen müssen aktiviert werden:

   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   HINWEIS: Informationen zu EventFileRedirectService und den drei Aggregationszusammenfassungen finden Sie im SDM-Kapitel im *Sentinel-Benutzerhandbuch* oder im Kapitel zur Crystal-Installation im *Sentinel-Installationshandbuch.*

2. Berichte, die einen großen Datenbereich abfragen, werden möglicherweise nur langsam ausgeführt. Sie sollten geplant und nicht interaktiv ausgeführt werden.

   HINWEIS: Informationen zur Planung von Crystal Reports finden Sie in der Dokumentation zu *Crystal BusinessObjects Enterprise™ 11*.

Tipps für die Entwicklung benutzerdefinierter Crystal-Berichte

Für benutzerdefinierte Berichte wird folgende Vorgehensweise empfohlen:

1. Nutzen Sie nach Möglichkeit aggregierte Tabellen.
2. Wenn die Berichte vordefinierte aggregierte Tabellen verwenden können, wählen Sie diejenige aggregierte Tabelle aus, bei der die wenigsten Daten verarbeitet werden.
3. Versuchen Sie, einen möglichst großen Teil der Verarbeitung auf die Datenbank-Engine zu verlagern.
4. Um den Verarbeitungs-Overhead in Crystal Server zu verringern, sollten Sie die in Crystal Server zu ladende Datenmenge so gering wie möglich halten.

Optimale Verfahren für die Wartung

Datenbankanalyse für Oracle

Da laufend Ereignisse in die Sentinel-Datenbank eingefügt werden, sollte die Datenbankstatistik regelmäßig aktualisiert werden, um eine gute Abfrageleistung zu gewährleisten. Mit dem Dienstprogramm für die Datenbankanalyse werden die Datenbankstatistiken für Ereignisdaten in Oracle aktualisiert. Um eine optimale Leistung zu erzielen, sollte die regelmäßige Ausführung dieses Dienstprogramms geplant werden.

HINWEIS: Dieses Dienstprogramm enthält ein erforderliches SQL-Skript, das regelmäßig aktualisiert werden kann. Sie sollten regelmäßig das Novell-Kundenportal aufsuchen, um zu überprüfen, ob Aktualisierungen vorliegen.

Das folgende Shell-Skript sollte regelmäßig über Cron oder einen anderen Planer ausgeführt werden:

- AnalyzePartitions.sh

Analyze Partitions

Das Skript AnalyzePartitions.sh analysiert Partitionen, die vor Kurzem mit Daten gefüllt wurden. Dieses Skript sollte für die tägliche Ausführung geplant werden, um Datenbankstatistiken in Partitionen zu aktualisieren, die am Vortag gefüllt wurden. Das Skript sollte zwei Stunden nach Mitternacht ausgeführt werden, nachdem die Ereignisse für die vorangegangenen Tage in die Datenbank eingefügt wurden.

Dieses Skript befindet sich in $ESEC_HOME/utilities/db. Es sollte lokal auf dem Server ausgeführt werden, auf dem die Sentinel-Datenbank installiert ist. Das UNIX-Benutzerkonto, das das Skript ausführt, muss in der Lage sein, eine Verbindung als sysdba herzustellen (z. B. – oracle).

HINWEIS: Wenn Sie eine neuere Version dieses Dienstprogramms heruntergeladen haben, als zurzeit auf Ihrem Computer installiert ist, müssen Sie sp_esec_dba_utl.sql installieren.

Installation von sp_esec_dba_utl.sql

1. Melden Sie sich als Eigentümer der Oracle-Software an.
2. Stellen Sie mithilfe von SQL*Plus als ESECDBA eine Verbindung mit der Datenbank her.
3. Installieren Sie das Paket ESEC_DBA_UTL. Geben Sie an der SQL-Eingabeaufforderung (SQL>) Folgendes ein:

   ```
   @sp_esec_dba_utl.sql
   ```

4. Beenden Sie SQL*Plus.

Ausführung von AnalyzePartitions.sh

1. Wechseln Sie auf dem Computer mit dem Oracle-Datenbankserver in das Verzeichnis:

   ```
   $ESEC_HOME/utilities/db/
   ```

   bzw. in das Verzeichnis, in das Sie die letzte Datei heruntergeladen haben.

2. Geben Sie an der Befehlseingabeaufforderung Folgendes ein:

   Für Solaris:

   ```
   ./AnalyzePartitions.sh <ORACLE-SID> >>
      <Name_der_Protokolldatei>
   ```

   Für Linux:

   ```
   ksh ./AnalyzePartitions.sh <ORACLE-SID> >>
      <Name_der_Protokolldatei>
   ```

   - ORACLE-SID – Der Name der Oracle-Instanz für Ihre Datenbank.
   - Name_der_Protokolldatei – Der vollständige Pfadname der Datei, in die die Protokollmeldungen geschrieben werden sollen.

   Wenn das Skript erfolgreich ausgeführt wird, wird es mit dem Rückgabecode 0 beendet. Anderenfalls wird es mit dem Rückgabecode 1 beendet. Planen Sie Ihre Aufträge entsprechend, um den Rückgabecode zu überprüfen. Wenn der Analyseauftrag nicht erfolgreich ausgeführt werden kann, sollten Sie die detaillierten Fehlermeldungen in der Protokolldatei nachschlagen.

Database Health Check für Oracle

dbHealthCheck.sh ist ein Skript, das Informationen zur Sentinel Oracle-Datenbank sammelt. Dieses Skript führt folgende Prüfungen durch:

- Überprüft, ob die Datenbankinstanz aktiv ist.
- Überprüft, ob Oracle Listener aktiv ist
- Zeigt die Speicherplatzauslastung an.
- Prüft auf nicht verwendbare Indizes.
- Prüft auf ungültige Datenbankobjekte.
- Prüft auf Datenbankanalyse.

Dieses Skript sollte regelmäßig über Cron oder einen anderen Planer ausgeführt werden.

HINWEIS: Dieses Dienstprogramm mit einem erforderlichen SQL-Skript kann regelmäßig aktualisiert werden. Sie sollten regelmäßig das Novell-Kundenportal aufsuchen, um zu überprüfen, ob Aktualisierungen vorliegen.

Installation und Ausführung von dbHealthCheck.sh

HINWEIS: Wenn Sie eine neuere Version dieses Dienstprogramms heruntergeladen haben, als zurzeit auf Ihrem Computer installiert ist, müssen Sie sp_esec_dba_utl.sql installieren.

Installation von sp_esec_dba_utl.sql

1. Melden Sie sich als Eigentümer der Oracle-Software an.
2. Stellen Sie auf Ihrem Datenbankserver sicher, dass $ORACLE_HOME und $ORACLE_SID in Ihrer Umgebung festgelegt sind.
3. Stellen Sie mithilfe von SQL*Plus als ESECDBA eine Verbindung mit der Datenbank her.
4. Installieren Sie das Paket ESEC_DBA_UTL. Geben Sie an der SQL-Eingabeaufforderung (SQL>) Folgendes ein:

   ```
   @sp_esec_dba_utl.sql
   ```

5. Beenden Sie SQL*Plus.

Ausführen von dbHealthCheck.sh

HINWEIS: Das Skript muss über das Kontos des Eigentümers der Oracle-Software ausgeführt werden bzw. über ein anderes Konto, das eine Verbindung mit "AS SYSDBA" herstellen kann.

HINWEIS: dbHealthCheck.sh muss lokal auf dem Datenbankserver ausgeführt werden.

1. Stellen Sie auf Ihrem Datenbankserver sicher, dass $ORACLE_HOME und $ORACLE_SID in Ihrer Umgebung festgelegt sind.
2. Wechseln Sie auf dem Computer mit dem Oracle-Datenbankserver in das Verzeichnis:

   ```
   $ESEC_HOME/utilities/db/
   ```

   bzw. in das Verzeichnis, in das Sie die letzte Datei heruntergeladen haben.
3. Geben Sie an der Befehlseingabeaufforderung Folgendes ein:

   Für Solaris:

   ```
   ./dbHealthCheck.sh
   ```

   Informationen zur Sentinel-Datenbank werden auf dem Bildschirm angezeigt. Alternativ können Sie die Ergebnisse in eine Datei schreiben lassen.

   ```
   ./dbHealthCheck.sh >> <Dateiname>
   ```

   Für Linux:

   ```
   ksh ./dbHealthCheck.sh
   ```

   Informationen zur Sentinel-Datenbank werden auf dem Bildschirm angezeigt. Alternativ können Sie die Ergebnisse in eine Datei schreiben lassen.

   ```
   ksh ./dbHealthCheck.sh >> <Dateiname>
   ```

Automatisches Archivieren von Daten und Hinzufügen von Partitionen (nur Windows)

HINWEIS: Wenn Ihr Computer keinen Zugriff auf DAS_Binary und DAS_Query hat, kann anstatt der SDM-GUI die SDM-Befehlszeilenoption verwendet werden.

Dieses Verfahren gilt nur für Windows. Vergewissern Sie sich, dass während der Ausführung von Vorkonfiguration und Konfiguration folgende Aufgaben ausgeführt werden:

- Vergewissern Sie sich, dass „sdm.connect“ entweder über die SDM-GUI oder über die Befehlszeile initialisiert wird.
- Vergewissern Sie sich, dass das Archivverzeichnis existiert.
- Vergewissern Sie sich, dass die Tage für „achiveConfig“ und „dropPartitions“ gleich sind.
- Vergewissern Sie sich, dass die Stapeldatei mindestens einmal ordnungsgemäß über die Befehlszeilenaufforderung ausgeführt wird, bevor Sie die automatische Ausführung der Datei planen.

HINWEIS: Wenn das geplante Task nicht erfolgreich ausgeführt werden kann, wird eine Benachrichtigung ausgegeben. Diese wird in SDM_*.log protokolliert.

Vorkonfiguration

Vor der automatischen Einstellung von „Archive Data“ (Daten archivieren) und „Add Partitions“ (Partitionen hinzufügen) müssen Sie folgende Aufgaben ausführen:

- Speichern von Verbindungseigenschaften
- Festlegen von Archivierungsparametern

Speichern von Verbindungseigenschaften in Sentinel Data Manager

Dies muss vor der Verwendung der Befehlszeilenoptionen von Sentinel Data Manager durchgeführt werden. Um Ihre Verbindung zu Sentinel Data Manager (saveConnection) zu speichern, müssen Sie die SDM-Befehlszeile mit der Aktion saveConnection ausführen.

Wenn Sie die SDM-GUI ausgeführt haben, können Sie die Datei sdm.connect verwenden, die aus der GUI erstellt wurde. Sie befindet sich unter %ESEC_HOME%\sdm.

Mit der Aktion „saveConnection“ werden die Verbindungsdetails in connectFile gespeichert. Der in der Datei configuration.xml referenzierte Keystore wird verwendet, um das Passwort vor dem Speichern in connectFile zu verschlüsseln.

Folgende Befehlszeilenoptionen für die Aktion „saveConnection“ sind für die Festlegung der Verbindungsdetails verfügbar:

-action	saveConnection
-server	Mssql
-host	<IP-Adresse des Datenbank-Host oder Hostname für Verbindung>
-port	<Datenbank-Portnummer für Verbindung [Standard bei SQL Server: 1433]>
-database	<Datenbankname/SID für Verbindung>
-user	<Datenbank-Benutzername>
-password	<Datenbankpasswort>
-winAuth	Für Windows-Authentifizierung verwendet. Bei Verwendung dieser Option, dürfen Sie -user und –password nicht verwenden.
-connectFile	<Dateiname zum Speichern der Verbindungsdetails [frei wählbarer Dateiname]>

Die Anwendung speichert alle oben genannten Verbindungsdetails sowie das verschlüsselte Passwort in der angegebenen Datei. Diese Anwendung führt mithilfe der gespeicherten Verbindungsdetails die anderen SDM-Befehlszeilenaktionen aus. Dieser Schritt sollte durchgeführt werden, wenn Sie die Anwendung zum ersten Mal starten, und jedes Mal, wenn Sie die Verbindungsdetails ändern möchten.

Ausführung von saveConnection

1. Führen Sie den Befehl wie folgt aus:

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps
   <Eigenschaftendatei>] {-user <dbUser> -password
   <dbPass>} -connectFile
   <Dateiname_zum_Speichern_der_Verbindung>
```

Im folgenden Beispiel werden in der Datei file sdm.connect Verbindungsdetails für eine Datenbank mit der Bezeichnung „esec“ auf einem Host mit IP-Adresse 172.16.0.36 und Port 1433 gespeichert, bei einer Authentifizierung als esecdba-Benutzer.

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user esecdba
   -password XXXXXX -connectFile  sdm.connect
```

Im folgenden Beispiel für die Windows-Authentifizierung werden in der Datei file sdm.connect Verbindungsdetails für eine Datenbank mit der Bezeichnung „esec_51“ auf einem Host mit IP-Adresse 172.16.1.3 und Port 1433 gespeichert. Dabei wird Windows-Authentifizierung verwendet.

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth -
   connectFile  sdm.connect
```

Dadurch werden die Verbindungsdetails in der Datei sdm.connect gespeichert. Die Restlichen Befehlszeilenaktionen verwenden diesen Dateinamen als Eingabe, um die Verbindung zu der designierten Datenbank herzustellen und Ihre Aktionen auszuführen.

HINWEIS: Wenn Sie eine Verbindungsdatei mit einem anderen Speicherort oder einem anderen Namen erstellt haben, als im Beispiel angegeben, müssen Sie die Datei manage_data.bat bearbeiten.

Erstellen von Archivierungsparametern

Dies ist über die SDM-Befehlszeile möglich.

Diese Aktion (archiveConfig) wird zum Konfigurieren der Archivierung verwendet. Diese Konfiguration steuert, wie die Daten aus den Sentinel-Datenbanktabellen archiviert werden.

Bei diser Aktion werden folgende Flaggen verwendet :

-action	archiveConfig
-dirPath	<gültiger Verzeichnispfad, in den die archivierten Dateien geschrieben werden sollen>
-keepDays	<Beibehaltungsdauer in Tagen>
-connectFile	<Pfad zu dem durch „saveConnection“> gespeicherten Dateinamen>

Erstellen von Archivierungsparametern über die Befehlszeile

1. Erstellen Sie im Stammverzeichnis ein Ausgabeverzeichnis für das Archiv mit der Bezeichung „SDM_archive“ („c:\SDM_archive“).

   HINWEIS: Wenn Sie einen anderen Namen oder einen anderen Speicherort für das Ausgabeverzeichnis wählen, müssen Sie die Datei „manage_data.bat“ bearbeiten.

2. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action archiveConfig  -dirPath <Verzeichnispfad,
   in den die archivierten Dateien geschrieben werden
   sollen> -keepDays <Beibehaltungsdauer in Tage> -
   connectFile <Pfad zu dem durch “saveConnection”
   gespeicherten Dateinamen>
```

Im folgenden Beispiel werden alle Daten, die älter sind als 30 Tage im Verzeichnis c:\SDM_archive archiviert.

```
sdm -action archiveConfig –dirpath c:\SDM_archive -
   keepDays 30 -connectFile sdm.connect
```

Erstellen von Archivierungsparametern über die GUI

1. Erstellen Sie im Stammverzeichnis ein Ausgabeverzeichnis für das Archiv mit der Bezeichung „SDM_archive“ („c:\SDM_archive“).

   HINWEIS: Wenn Sie einen anderen Namen oder einen anderen Speicherort für das Ausgabeverzeichnis wählen, müssen Sie die Datei „manage_data.bat“ bearbeiten.

2. Für die SDM-GUI sind keine Archivierungsparameter erforderlich. Die GUI kann direkt Daten archivieren, ohne dass Archivparameter erstellt werden müssen.

Löschen von Daten (Verwerfen von Partitionen)

Diese Aktion (deleteData) löscht die Daten, die älter als „keepDays“ sind, aus folgenden Tabellen:

- EVENTS
- CORRELATED_EVENTS

Standardmäßig werden bei dieser Aktion keine Partitionen abgelegt, die nicht archiviert wurden. Wenn Sie nicht archivierte Partitionen löschen möchten, muss das optionale Flag „forceDelete“ mit dem Wert „wahr“ angegeben sein. Bei Verwendung von forceDelete gilt Folgendes:

„false“ (falsch) oder nicht angegeben	Es werden nur archivierte Partitionen verworfen, die älter sind als keepDays. Es werden keine nicht archivierten Partitionen verworfen, selbst wenn sie älter sind als keepDays.
„true“ (wahr)	Es werden alle Partitionen verworfen, die älter sind als „keepDays“, auch wenn sie nicht archiviert wurden.

Für diesen Befehl werden folgende Flags verwendet:

-action	deleteData
-keepDays	<Beibehaltungsdauer in Tagen>
[-forceDelete]	<entweder „wahr“ oder „falsch“>
-connectFile	<Pfad zu dem durch „saveConnection“> gespeicherten Dateinamen>

Ausführen von deleteData

1. Führen Sie diesen Befehl wie folgt aus:

   ```
   sdm -action deleteData -keepDays <Beibehaltungsdauer
      in Tagen> -connectFile <Pfad zu dem durch
      “saveConnection” gespeicherten Dateinamen>
   ```

   Im folgenden Beispiel werden die Partitionen aus der Tabelle EVENTS und CORRELATED_EVENTS verworfen, die älter als 30 Tage sind und archiviert wurden. Nach Abschluss des Vorgangs werden alle Partitionen aufgelistet, die nicht gelöscht wurden, weil sie nicht zuvor archiviert wurden.

   ```
   sdm -action deleteData -keepDays 30 -connectFile
      sdm.connect
   ```

Planen der Datenarchivierung und des Hinzufügens von Partitionen

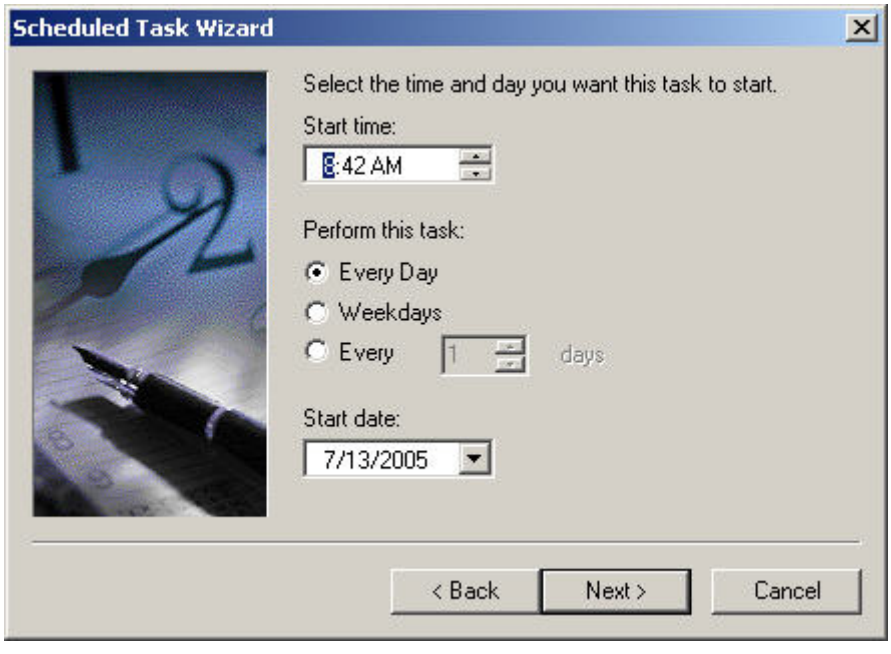
HINWEIS: Bei der Datei manage_data.bat ist der keepDay-Wert auf 30, die Archivausgabe auf c:\SDM_archive und die Verbindungsdatei auf %ESEC_HOME%\SDM\sdm.connect gesetzt. Wenn Ihre Werte abweichen, müssen Sie die Datei manage_data.bat bearbeiten.

Wenn Sie Ihre Verbindungseigenschaften und Archivparameter festgelegt haben, führen Sie die Datei „manage_data.bat“ über die Befehlseingabeaufforderung aus, um die ordnungsgemäße Ausführung sicherzustellen.

So können Sie automatisch Daten archivieren und Partitionen hinzufügen

HINWEIS: Folgende Schritte gelten für Windows 2000 Professional. Die Schritte für Windows 2000 Server, XP und 2003 Server können abweichen, sind jedoch ähnlich.

1. Klicken Sie unter Windows auf *Start* > *Einstellungen*> *Systemsteuerung.*
2. Doppelklicken Sie auf *Geplante Tasks.*
3. Doppelklicken Sie auf *Geplanten Task hinzufügen.* Klicken Sie auf *Weiter*.
4. Klicken Sie auf *Durchsuchen* und wechseln Sie zu der Datei manage_data.bat (%ESEC_HOME%\sdm).
5. Geben Sie einen Namen für den geplanten Task ein, beispielsweise „SDM_Archive“. Wählen Sie unter *Task ausführen:* die Option „Täglich“. Klicken Sie auf *Weiter*.
6. Wählen Sie eine Uhrzeit für die Ausführung des Tasks aus. Klicken Sie auf *Weiter*.
7. Geben Sie das gewünschte Datum und die gewünschte Uhrzeit ein. Klicken Sie auf *Weiter*.



8. Geben Sie einen Benutzer ein, für den der Task ausgeführt werden soll. Bei dem Benutzer kann es sich nicht um ein lokales Systemkonto handeln. Er muss als bestimmter Benutzer ausgeführt werden. Bei Verwendung von Windows-Authentifizierung für die Verbindung mit der Datenbank müssen Sie den Windows-Benutzer den Sentinel-Datenbankadministrator verwenden. Klicken Sie auf *Weiter*.
9. Klicken Sie auf *Fertig stellen* um den Vorgang als geplanten Task fertig zu stellen.

Correlation Engine

HINWEIS: Damit Sentinel Correlation Engine ordnungsgemäß arbeitet, muss das Computersystem mit einer Genauigkeit von 30 gegenüber allen Collector Manager-Computern synchronisiert werden. Alle Correlation Engine- und Collector Manager-Computer sollten mit einem NTP (Network Time Protocol)-Server verbunden sein, der einen anderen Typ aufweist als der Zeitserver.

Erweiterte Korrelationsregeln

Mithilfe der erweiterte Korrelationsregel können Beziehungen zwischen Ereignissen erkannt werden, beispielsweise, wenn ein bestimmtes Ereignis (Ereignis B) nach Ereignis A eintritt und eine Beziehung zwischen den beiden Ereignissen besteht. In diesem Fall ist Ereignis B das aktuelle Ereignis und sollte mit einem im Fenster des Assitenten für Ereignisfilterkriterien eingegebenen Filter erkannt werden. Ereignis A ist das Vergangene Ereignis und sollte mit einem im Assistentenfenster „Filterkriterien für frühere Ereignisse“ eingegebenen Filter erkannt werden. Die Beziehung zwischen den beiden Ereignissen (z. B. dieselbe IP-Adresse für Quelle bzw. Ziel) sollte im Assistentenfenster „Kriterien für Vergleich von Ereignissen mit früheren Ereignissen“ eingegeben werden. In diesem Fenster geben Sie auch den maximalen Zeitraum ein, der zwischen den beiden zu ermittelnden Ereignissen liegen darf (Zeitfenster). Wenn ein Ereignis alle diese Kriterien erfüllt, kann es gruppiert und bis zu dem im Assistentenfenster „Schwellenwert und Gruppierungskriterien“ angegebenen Schwellenwert gezählt werden.

Zeitsteuerung

Mit Fenster- und Auslösevorgängen ist jeweils ein Zeitfenster verknüpft. Je größer das Zeitfenster, desto mehr Ereignisse (eigentlich einzelne Ereignisinformationen) können für das betreffende Zeitfenster im Arbeitsspeicher abgelegt werden. Für den Fenstervorgang hängen die gespeicherten Elemente von dem Filter ab, der für die vergangenen Ereignisse angegeben wurde. Je spezifischer dieser Filter ist, desto weniger Ereignisse werden im Zeitfenster gespeichert, sodass (sofern erforderlich) ein längerer Zeitraum verwendet werden kann. Beim Auslöservorgang hängt der maximale Gesamtspeicherplatz, der verwendet werden kann, von der Mächtigkeit des Diskriminators ab (d. h., je mehr Gruppierungen möglich sind, desto mehr Ereignisse können in einem bestimmten Zeitraum gespeichert werden) – bis zu dem für die einzelnen Gruppen geltenden Schwellenwert. Häufig führt das Senken von Schwellenwert und Zeitraum für die Auslöseroperation zu gleichwertigen Ergebnissen.

Auslöseraktualisierung

Angenommen, sie haben ein korreliertes Ereignis für eine Regel erhalten, erwarten jedoch weitere korrelierte Ereignisse. Dies kann am Aktualisierungsverhalten der Triggeroperation liegen. In der Auslöseroperation können Sie festlegen, dass beim Auftreten einer Menge von n Ereignissen im Zeitraum t ein korreliertes Ereignis ausgelöst werden soll. Jedesmal, wenn Correlation Engine diese Menge von n Ereignissen im Zeitraum t findet, wird er ausgelöst. Wenn beim Auslösen festgestell wird, dass Correlation Engine bereits zuvor (für dieselbe Gruppe) ausgelöst wurde und wenn mindestens ein Mitglied in beiden Mengen vorkommt, werden die betreffenden Mitglieder zum ursprünglichen korrelierten Ereignis hinzugefügt und es wird kein neues korreliertes Ereignis erstellt.

Boolesche Ausdrücke unterstützen Kurzschlussanalyse

Zahlenvergleiche sind schneller als Zeichenkettenvergleiche und Zeichenkettenvergleiche sind schneller als Vergleiche regulärer Ausdrücke. Die Filteroperation führt eine Kurzschlussanalyse für die booleschen Ausdrücke durch. Durch eine sorgfältige Anordnung des Ausdrucks können Sie eventuell die Evaluierungsgeschwindigkeit erhöhen.

Keine Angst vor Freiform

Wenn eine Korrelationsregel nicht mithilfe der drei vordefinierten Schablonen des Assistenten („Beobachtungsliste“, „Grundlegend“ oder „Erweitert“) ausgedrückt werden kann, sollten Sie sich nicht scheuen, eine Freiformregel zu erstellen. Alle Schablonen bilden letztlich eine Freiformregel für den Benutzer. Sie können die Freiformdarstellung anzeigen, indem Sie eine Regel bearbeiten und ihren Typ auf „Freiform“ setzen. So können Sie schnell und einfach eine Regel erweitern, die sich mit einer der drei anderen Optionen nicht ohne weiteres ausdrücken ließ.

Transaktionsprotokoll

Für SQL Server werden standardmäßig Sentinel-Datenbanken gemäß dem Modell für vollständige Wiederherstellung erstellt. Bei dem Modell für vollständige Wiederherstellung wird der für das Transaktionsprotokoll verwendete Speicherplatz erst dann freigegeben, wenn eine Sicherung des Transaktionsprotokolls ausgeführt wurde. Um zu Verhindern, dass der Speicherplatz des Transaktionsprotokolls völlig aufgebraucht wird, sollten über den Tag verteilt (3- bis 4mal täglich, je nach Ereignisrate) Protokollsicherungen in SQL Server geplant werden. Wenn es in Ihrer Organisation nicht erforderlich ist, eine Wiederherstellung ab dem Ausfallzeitpunkt durchzuführen, können Sie auch das einfache Modell für die Datenbankwiederherstellung verwenden. Beim einfachen Modell für die Datenbankwiederherstellung gibt SQL Server automatisch Speicherplatz für das Transaktionsprotokoll frei, ohne Protokollsicherungen zu erstellen.

Speicherorte der Sentinel-Protokolldateien

Es gibt bestimmte Protokolle in Sentinel, die Ihnen bei der Fehlersuche in Ihrem System behilflich sein können. Diese Protokolle können bei der Zusammenarbeit mit dem technischen Support von Novell zur Lösung von Problemen extrem nützlich sein.

Sentinel Data Manager

Protokolliert mithilfe von Sentinel Data Manager ausgeführte Aktivitäten für den speziellen Cliente, der auf diesem Computer ausgeführt wird.

Für Windows:

```
%ESEC_HOME%\sdm\SDM_*.0.log
```

Für UNIX:

```
$ESEC_HOME/sdm/SDM_*.0.log
```

iTRAC

Protokolliert iTRAC-bezogene Aktivitäten.

Für Windows:

```
%ESEC_HOME%\sentinel\log\das_itrac_0.*.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
```

„Advisor“

Protokolliert Aktivitäten in Bezug auf das Herunterladen und Verarbeiten von Advisor-Daten.

Für Windows:

```
%ESEC_HOME%\sentinel\log\advisor.log
%ESEC_HOME%\sentinel\log\Advisor_0.*.log
```

Für UNIX:

```
%ESEC_HOME%\sentinel\log\advisor.log
$ESEC_HOME/sentinel/log/Advisor_0.*.log
```

Einfügen von Ereignissen

Protokolliert Aktivitäten in Bezug auf das Einfügen von Ereignissen in die Datenbank.

Für Windows:

```
%ESEC_HOME%\sentinel\log\das_binary0.*.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/das_binary0.*.log
```

Datenbankabfragen

Protokolliert Aktivitäten in Bezug auf Datenbankabfragen, Collector, Collector Manager-Zustand und alle anderen DAS-Aktivitäten, die nicht von anderen DAS-Komponenten ausgeführt werden.

Für Windows:

```
%ESEC_HOME%\sentinel\log\das_query0.*.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/das_query0.*.log
```

Active Views

Protokolliert Active Views-bezogene Aktivitäten.

Für Windows:

```
%ESEC_HOME%\sentinel\log\das_rt0.*.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/das_rt0.*.log
```

Aggregation

Protokolliert aggregationsbezogene Aktivitäten.

Für Windows:

```
%ESEC_HOME%\sentinel\log\das_aggregation0.*.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

Sentinel Watchdog

Protokolliert Aktivitäten in Bezug auf Sentinel Watchdog.

HINWEIS: sentinel_wrapper.log ist für Service Wrapper.

Für Windows:

```
%ESEC_HOME%\sentinel\log\sentinel0.*.log
%ESEC_HOME%\sentinel\log\sentinel_wrapper.log
```

Für UNIX:

```
$ESEC_HOME/sentinel/log/sentinel0.*.log
$ESEC_HOME/sentinel/log/sentinel_wrapper.log
```

Collector Manager

Protokolliert Aktivitäten in Bezug auf Collector Manager.

HINWEIS: agent-manager.log ist für Service Wrapper.

Für Windows:

```
%ESEC_HOME%\wizard\logs\agent-manager.log
%ESEC_HOME%\wizard\logs\am0.*.log
```

Für UNIX:

```
$ESEC_HOME/wizard/logs/agent-manager.log
$ESEC_HOME/wizard/logs/am0.*.log
```

3 Installation von Sentinel 5 für Oracle unter Solaris

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

In diesem Kapitel erfahren Sie, wie Sie Sentinel Enterprise Security Management Sentinel 5 für Oracle unter Solaris installieren.

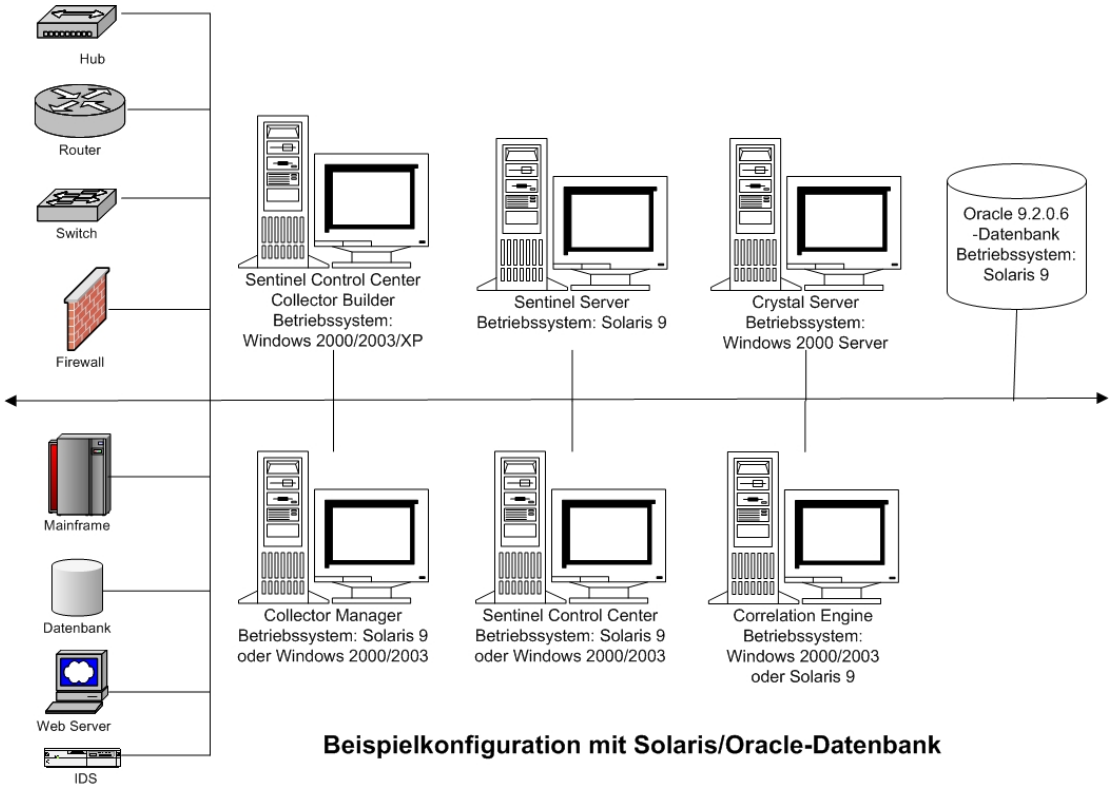
Vor der Installation von Sentinel 5 für Oracle unter Solaris

HINWEIS: Vergewissern Sie sich vor der Installation, dass Ihre Maschinen den Mindestsystemanforderungen entsprechen und dass das Betriebssystem mithilfe der besten Sicherheitsvorkehrungen geschützt ist.

HINWEIS: Installieren Sie Oracle Enterprise mit Partitionierung. Der Sentinel Data Manager benötigt diese Funktion zur Verwaltung der Sentinel-Datenbank.

HINWEIS: Wenn Sie eine Neuinstallation von Sentinel durchführen möchten, nachdem bereits eine frühere Version installiert wurde, müssen Sie bestimmte Dateien und Systemeinstellungen entfernen, die eventuell noch von einer früheren Installation übrig geblieben sind. Wenn Sie diese Dateien bzw. Einstellungen nicht entfernen, kann die Neuinstallation scheitern. Dieser Vorgang sollte auf jedem Computer durchgeführt werden, auf dem eine Neuinstallation erfolgen soll. Weitere Informationen finden Sie in *Anhang E*.

Im Folgenden sehen Sie typische Konfigurationen für Solaris und Sentinel. Je nach der von Ihnen verwendeten Umgebung kann die Konfiguration abweichen. Unabhängig von der gewählten Konfiguration müssen Sie zuerst die Datenbank installieren.



HINWEIS: Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in Kapitel 1 – *Einführung, Unterstützte Plattformen für Sentinel Server unter Solaris.*

Abrufen eines Lizenzschlüssels

Für die Installation und Ausführung von Sentinel Server Database Access Service (DAS) ist ein gültiger Lizenzschlüssel erforderlich. Dieser Lizenzschlüssel ist an den Computer gebunden, auf dem DAS installiert werden soll. Ein für einen bestimmten Computer ausgegebener Lizenzschlüssel funktioniert nicht auf anderen Computern.

Zum Abrufen des Lizenzschlüssels müssen Sie Ihre Host-ID-Nummer ermitteln und diese Informationen an Novell weiterleiten. Dort erhalten Sie einen Lizenzschlüssel.

So ermitteln Sie Ihre Host-ID (Solaris)

1. Geben Sie den folgenden Befehl ein:

   ```
   hostid
   ```

2. Übermitteln Sie die betreffende Host-ID-Nummer an Novell Technical Support. Von dort erhalten Sie einen Lizenzschlüssel.

Sentinel-Datenbank

Vor der Installation der Sentinel-Datenbank brauchen Sie:

- Die Hardware-Anforderungen finden Sie in den *Kapiteln 1* und *2*.
- Sun SPARC Solaris Server mit Solaris 9 und dem Recommended Patch Cluster DATUM: 03. Mai 2005
- Oracle 9i Enterprise Edition 9.2.0.6 bzw. 9.2.0.7 mit Partitionierung

- Für Solaris eine Kopie von Oracle Note: 148673.1 SOLARIS: Quick Start Guide
- Oracle-Betriebssystembenutzer (Standard: oracle)
- Vergewissern Sie sich, dass die folgenden Umgebungsvariablen für den Oracle-Betriebssystembenutzer festgelegt wurden:
  - ORACLE_HOME
  - ORACLE_BASE
  - PATH (muss enthalten $ORACLE_HOME/bin)
  - Obwohl es nicht empfohlen wird, können Sie die Oracle-Datenbankinstanz auch manuell erstellen. Unter Erstellen einer Oracle-Instanz für die Sentinel-Datenbank finden Sie eine Anleitung zum Erstellen Ihrer Oracle-Instanz. Wenn Sie diese Option wählen, müssen Sie dennoch das Installationsprogramm verwenden, um die Datenbankobjekte der manuell erstellen Oracle-Datenbankinstanz hinzuzufügen. (Unter Benutzerdefinierte Installation erfahren Sie, wie Sie dabei vorgehen.)

HINWEIS: Wenn Sie eine vorhandene oder manuell erstellte Oracle-Datenbankinstanz verwenden, muss diese bis auf die Präsenz des esecdba-Benutzers leer sein.

- Wird die Oracle-Datenbank mithilfe des Installationsprogramms erstellt (empfohlen), benötigen Sie die Verzeichnispfade für die Datenbankdateien. Diese Verzeichnisse müssen bereits vorhanden sein, bevor das Installationsprogramm ausgeführt wird, da sie nicht vom Installationsprogramm erstellt werden können. Außerdem muss der Oracle-Betriebssystembenutzer (z. B. oracle) über eine Schreibberechtigung für diese Verzeichnisse verfügen.

HINWEIS: Um eine möglichst hohe Leistung zu erreichen, sollte, sofern die Installation in RAID vorgenommen wird und sofern es die RAID-Umgebung zulässt, das Redo-Protokoll auf die Festplatte mit der höchsten Schreibgeschwindigkeit verweisen, die verfügbar ist.

HINWEIS: Standardmäßig legt das Installationsprogramm fest, dass folgende Tabellenbereiche NICHT automatisch wachsen: ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX. Für alle anderen Tabellenbereiche wird automatisches Wachstum festgelegt. Der Grund, warum automatisches Wachstum für ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX nicht zugelassen wird, ist, dass sie Daten über Ereignisse und Zusammenfassungsereignisse enthalten. Die Speicherplatzauslastung für Ereignisse und Zusammenfassungen kann höchst dynamisch sein. Diese Ereignistabellenbereiche sollten überwacht und auf gesteuerte Weise in Ihrer Dateisystemkonfiguration erweitert werden. Dabei sind E/A-Lastenausgleich und Datenbanksicherung und -wiederherstellung zu berücksichtigen.

Die SDM-Partitionsverwaltung (Archivieren, Verwerfen und Hinzufügen von Partitionen) sollte zeitlich geplant sein, um die Größe der Ereignisdaten überschaubar zu halten.

Sentinel Server

HINWEIS: Wenn Sie die Sentinel-Datenbank nicht zusammen mit Sentinel Server installieren, muss die Sentinel-Datenbank zuerst installiert werden.

Vor der Installation von Sentinel Server benötigen Sie folgende Elemente:

- Die Hardware-Anforderungen finden Sie in den *Kapiteln 1* und *2*.
- Sun SPARC Solaris Server mit Solaris 9 und dem Recommended Patch Cluster DATUM: 03. Mai 2005
- Seriennummer und Lizenzschlüssel von Sentinel 5 (für DAS). Weitere Informationen finden Sie unter Abrufen eines Lizenzschlüssels.
- SMTP-Server – Wird benötigt, um Emails über Sentinel zu versenden.

Sentinel Control Center und Wizard

Vor der Installation von Sentinel Server benötigen Sie Folgendes:

- Die Hardware-Anforderungen finden Sie in *Kapitel 1 und 2*.
- Eines der folgenden Betriebssysteme:
  - Sun SPARC Solaris Server mit Solaris 9 und dem empfohlenen Solaris 9 Recommended Patch Cluster DATUM: 3. Mai 2005 Patches
  - (nur Collector Builder) – Windows 2000 oder 2003

„Advisor“

Zur Installation von Advisor müssen Sie eine Advisor-ID und ein Passwort von Sentinel anfordern. Beim direkten Herunterladen aus dem Internet wird Port 443 verwendet.

HINWEIS: Wenn Sie Advisor nur für Exploit-Erkennung verwenden, brauchen Sie die Crystal Enterprise-Software nicht zu installieren. Dies ist nur erforderlich, wenn Sie vorhaben, Crystal Reports für Sentinel auszuführen. Weitere Informationen finden Sie in *Kapitel 8, Advisor-Konfiguration*.

Überprüfen des Solaris-Layouts (Anforderungen für den Betriebssystem-Patch)

Überprüfen des Solaris-Layouts

1. Gehen Sie zur Sun-Website und laden Sie den empfohlenen Patch-Satz für Solaris 9 herunter:
   - Patch Cluster DATUM: 03. Mai 2005

   HINWEIS: Sehen Sie in der README-Datei und in der anderen im Lieferumfang enthaltenen Dokumentation nach. Es wird UNBEDINGT empfohlen, dass Sie vor der Installation von Patches eine komplette Systemsicherung vornehmen.
2. Melden Sie sich als Benutzer „root“ an und installieren Sie den entsprechenden Patch Cluster und die Kernel-Patches.
3. Sobald die Patches installiert wurden, löschen Sie die Datei *_Recommended.zip und die dekomprimierten Dateien in den Verzeichnissen, die durch den Patch erstellt wurden und booten Sie Ihren Server neu.

Vor der Installation von Oracle unter Solaris

Vor der Installation von Oracle unter Solaris für Sentinel sind folgende Aktionen erforderlich:

- Einstellen der Kernel-Werte
- Erstellen eines Gruppen und Benutzerkontos für Oracle
- Festlegen der Umgebungsvariablen
- Installieren von Oracle 9.2.0.6 oder 9.2.0.7
- Installieren der Patches für Oracle 9.2.0.6 oder 9.2.0.7

Festlegen der Kernel-Werte für Oracle unter Solaris

Für Oracle unter Solaris müssen die folgenden Kernel-Werte in /etc/system eingestellt werden.

ACHTUNG: Im Folgenden finden Sie die vorgeschlagenen Mindestwerte. Von Ihrem Systemadministrator und in der Oracle-Dokumentation erhalten Sie genauere Informationen.

- shmmax=4294967295
- shmmin=1
- shmseg=50
- shmmni=400
- semmns=14000
- semmni=1024
- semmsl=1024
- shmopm=100
- shmvmx=32767

HINWEIS: Wenn Ihre Kernel-Werte den Anforderungen entsprechen oder darüber liegen, müssen Sie die Einstellungen nicht ändern.

1. Melden Sie sich als „root“ an.
2. Erstellen Sie eine Sicherungskopie von /etc/system
3. Verwenden Sie einen Texteditor und ändern Sie die Kernel-Parametereinstellungen in der Datei /etc/system entsprechend der obigen Tabelle.
4. Booten Sie den Computer neu.

Vor der Installation von Oracle unter Solaris

HAFTUNGSAUSSCHLUSS: Die folgende Anleitung ersetzt nicht die Dokumentation von Oracle. Es handelt sich hierbei nur um ein Beispiel eines Einrichtungsszenarios. Diese Dokumentation setzt voraus, dass das Basisverzeichnis des Oracle-Benutzers /export/home/oracle lautet und dass Oracle im Verzeichnis /opt/oracle installiert wird. Ihre genaue Konfiguration ist eventuell anders. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem und zu Oracle.

HINWEIS: Bei der Installation der Oracle-Software wird eine „typische“ Installation empfohlen. Anderenfalls müssen Sie bei einer benutzerdefinierten Installation sicherstellen, dass Sie Oracle JDBC/OCI Interface zur Installation auswählen. Weitere Informationen finden Sie in der Dokumentation zu Oracle.

1. Melden Sie sich als „root“ an.
2. Erstellen Sie eine UNIX-Gruppe und UNIX-Benutzerkonten für den Oracle-Datenbankeigentümer.

   Fügen Sie eine dba-Gruppe hinzu (als „root“):

   ```
   groupadd –g 400 dba
   ```

   Fügen Sie den Benutzer „oracle“ hinzu (als „root“):

   ```
   useradd –g dba –d /export/home/oracle –m –s /bin/csh
      oracle
   ```

3. Beim Festlegen der erforderlichen Umgebungsvariablen für Oracle sollten der Datei local.cshrc die folgenden Informationen hinzugefügt werden:

   ```
   umask 022

   setenv ORACLE_HOME /opt/oracle

   setenv ORACLE_SID ESEC

   setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib

   setenv DISPLAY :0.0

   set path=(/bin /bin/java /usr/bin /usr/sbin
      ${ORACLE_HOME}/bin /usr/ucb/etc.)

   if ( $?prompt ) then

   set history=32

   endif
   ```

4. Befolgen Sie die Schritte in Oracle Note: 148673.1 SOLARIS: Quick Start Guide.
5. Installieren Sie Oracle 9i Release 2 als Benutzer „oracle“. Sie werden aufgefordert, zwei zusätzliche CD-ROMs einzulegen. Sie müssen für jede der zusätzlichen CD-ROMs in verschiedene Verzeichnisse wechseln.
6. Wenden Sie den Patch für Ihr System auf Release 9.2.0.6.0 oder 9.2.0.7.0 an. In der Oracle-Dokumentation finden Sie Genaueres zum Installieren von Patches.
7. Wenn Sie die Patch-Stufe als Oracle UNIX-Benutzer überprüfen möchten, geben Sie Folgendes ein:

   ```
   sqlplus ‘/as sysdba’
   ```

   Als Ergebnis erhalten Sie eine Release 9.2.0.6.0 oder 9.2.0.7.0. Beenden Sie das Programm, indem Sie „quit“ eingeben.
8. Löschen Sie das Verzeichnis, das Sie für den Patch erstellt haben.
9. Nach der Installation der Patches löschen Sie die Patch-Verzeichnisse und -Dateien.
10. Booten Sie den Computer neu.

Installation von Sentinel 5 für Oracle unter Solaris

Sentinel 5 unterstützt zwei Installationstypen. Hierbei handelt es sich um:

- Einfach – Die Option zur All-in-One-Installation. Sentinel-Services, Collector-Service und Anwendungen mit Oracle auf demselben Computer. Dieser Installationstyp dient lediglich zu Demonstrationszwecken.
- Benutzerdefiniert – Ermöglicht eine vollständig verteilte Installation.

Einfache Installation unter Solaris

Bei dieser Installation werden die allgemeinen Komponenten auf einem einzigen Computer installiert (kein Collector Builder und keine Drittanbieter-Integrationsfunktionen). Dies dient vorrangig zu Demonstrationszwecken. Für Test- bzw. Produktionszwecke nicht empfohlen.

HINWEIS: Bei der einfachen Installation wird die Collector Manager-Passwortauthentifizierung nicht unterstützt.

So führen Sie eine einfache Installation durch

1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für Oracle die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Überprüfen Sie die Solaris Oracle-Einrichtung.
3. Melden Sie sich als Benutzer „root“ an.
4. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
5. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   Für GUI-Modus:

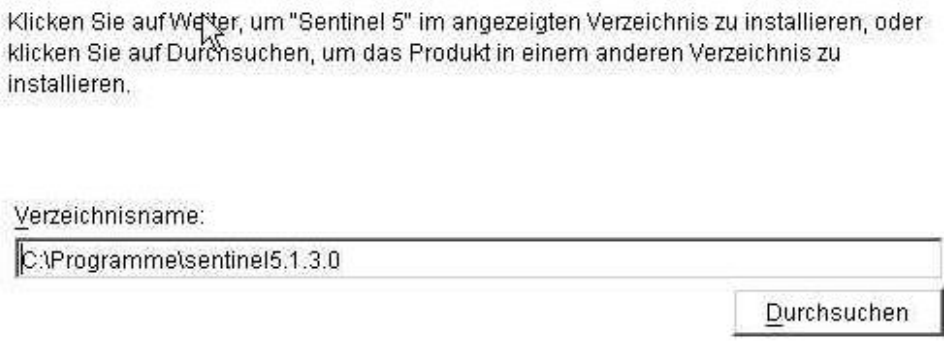
   ```
   ./setup.sh
   ```

   oder

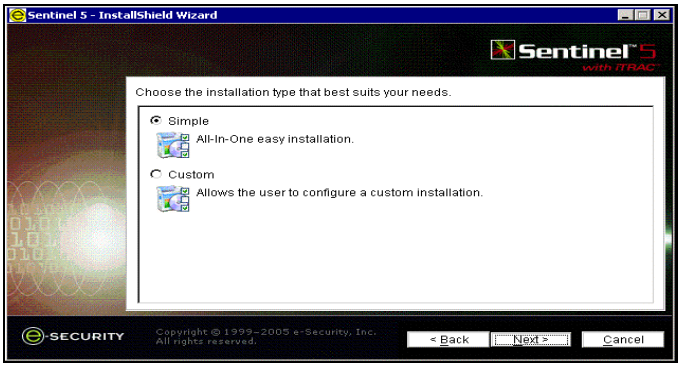
   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```

6. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
7. Folgen Sie den Eingabeaufforderungen des Installationsprogramms.
8. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
9. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
10. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



11. Wählen Sie *Einfach* aus. Klicken Sie auf *Weiter*.



12. Geben Sie Ihre Konfigurationsinformationen ein.
    - Seriennummer und Lizenzschlüssel
    - SMTP-Server (entweder DNS-Name oder IP-Adresse) – sofern Sentinel in der Lage sein soll, Emails zu versenden
    - Email – Geben Sie eine gültige Email-Adresse ein, über die Advisor-Benachrichtigungs-Emails gesendet werden sollen (z. B. Sent_Server@myserver.com).
    - Globales Systempasswort – Geben Sie ein Passwort und dasselbe Passwort nochmal zur Bestätigung ein. Dieses Passwort wird für alle Standardbenutzer verwendet. Dazu gehören sowohl der Benutzer des esecadm-Betriebssystems als auch die Datenbankbenutzer. Eine Liste der Standard-Datenbankbenutzer, die während der Installation erstellt werden, finden Sie unter Sentinel-Datenbank im Abschnitt Vor der Installation von Sentinel 5 für Oracle.

- Datenverzeichnis – der Speicherort für alle Datendateien der Datenbank und des Advisors zum Herunterladen (falls Sie Advisor installieren). Um den Standard-Speicherort zu ändern, klicken Sie auf die Schaltfläche „...“ und wählen Sie den gewünschten Speicherort aus. Der Standard-Speicherort ist $ESEC_HOME/data.

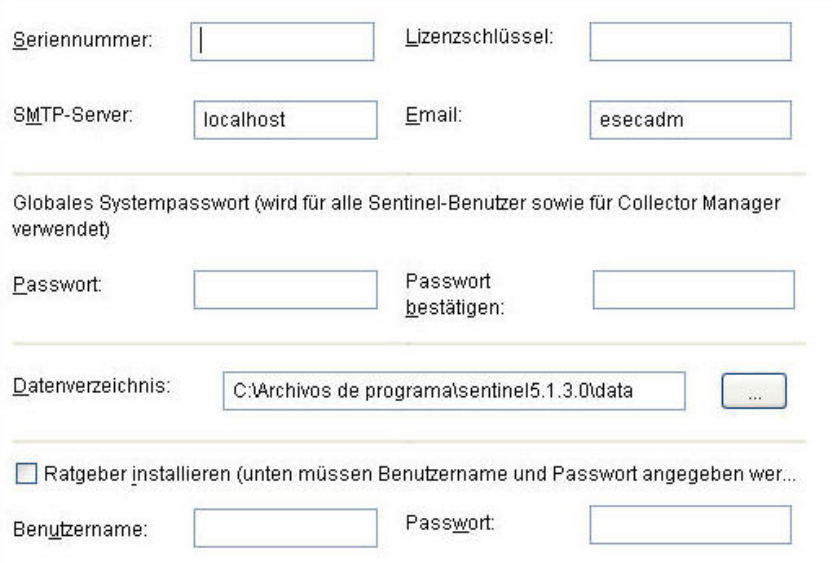
HINWEIS: Das Datenverzeichnis muss sowohl für den Benutzer „oracle“ als auch für den Benutzer „esecadm“ verfügbar sein (zum Lesen, Schreiben und Ausführen). Da diese Installation nur zu Demonstrationszwecken dient, wird empfohlen, dass Sie diesen Zugriff ermöglichen, indem Sie allen Benutzern für das Datenverzeichnis Lese-, Schreib- und Ausführberechtigungen erteilen. Das erzielen Sie, indem Sie den folgenden Befehl ausführen:

chmod 777 <directory_path>

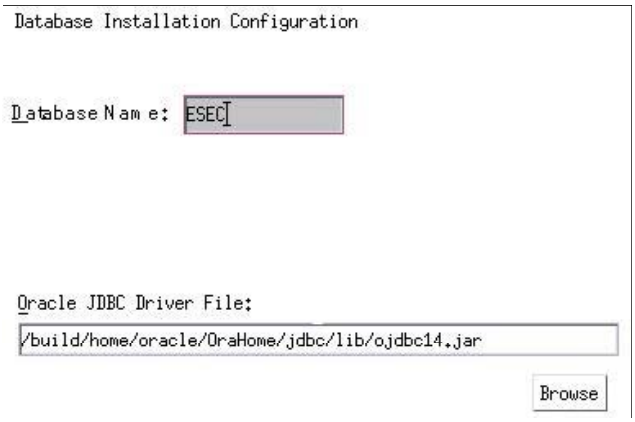
HINWEIS: Sofern Advisor installiert wird, konfiguriert die einfache Installation Advisor für die Verwendung von „Direktes Herunterladen vom Internet“ mit einem Aktualisierungsintervall von 12 Stunden und unter Aktivierung aller Email-Benachrichtigungen.

- Wählen Sie zur Installation von Advisor die Option *Advisor installieren*. Geben Sie einen Benutzernamen und ein Passwort ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.

Klicken Sie auf *Weiter*.



13. Geben Sie Ihre Datenbank-Konfigurationsinformationen ein.
    - Datenbankname – Der Name der Oracle-Datenbankinstanz zum Erstellen und Installieren von Sentinel-Datenbankobjekten. Es darf keine Datenbank mit diesem Namen existieren.
    - Oracle JDBC-Treiberdatei. Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).



14. Bestätigen Sie den Oracle-Standardbenutzernamen, indem Sie auf *OK* klicken.

15. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation müssen Sie das System neu starten.

HINWEIS: Wenn Sie Drittanbieter-Integrationssoftware (HP Service Desk oder Remedy Integration) installieren möchten, führen Sie nach dem erneuten Booten Ihres Computers das Installationsprogramm erneut aus und wählen Sie die gewünschte Drittanbieter-Integrationssoftware aus. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration*.

16. Das Sentinel-Installationsprogramm deaktiviert standardmäßig die Archivprotokollierung. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank keine Ereignisse mehr entgegen.

Benutzerdefinierte Installation unter Solaris

Durchführen einer benutzerdefinierten Installation

1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für Oracle die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Überprüfen Sie die Solaris Oracle-Einrichtung.
3. Melden Sie sich als Benutzer „root“ an.
4. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.

5. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   Für GUI-Modus:

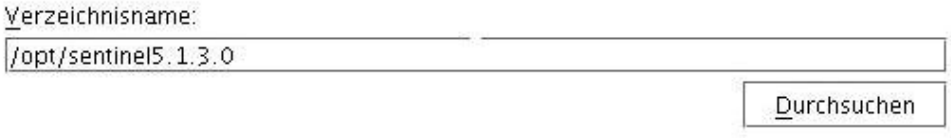
   ```
   ./setup.sh
   ```

   oder

   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```

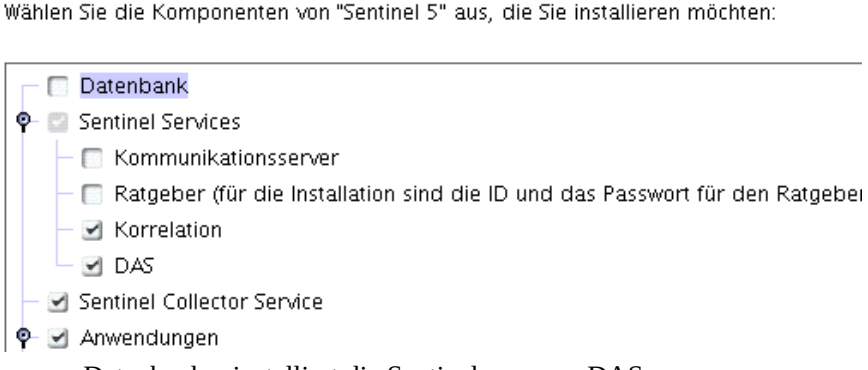
6. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
7. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter.*
8. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
9. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



10. Wählen Sie *Benutzerdefiniert* (Standard). Klicken Sie auf *Weiter*.
11. Wählen Sie die zu installierenden Funktionen aus.

HINWEIS: Weitere Informationen darüber, welche Komponenten bei verschiedenen Konfigurationen an welchem Ort installiert werden können, finden Sie in *Kapitel 1, Systemanforderungen*.

Folgende Optionen stehen zur Verfügung:



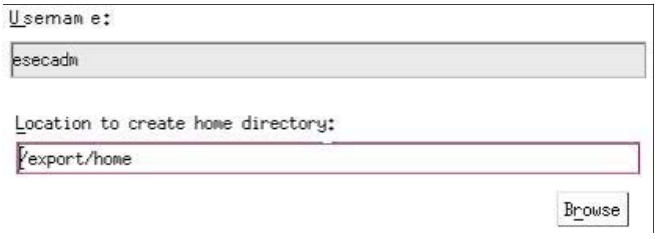
- Datenbank – installiert die Sentinel-Datenbank
- Kommunikationsserver – installiert den Nachrichtenbus (iSCALE)
- Advisor
- Correlation Engine
- DAS
- Collector-Service
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk*
- Remedy Integration*

HINWEIS: *Informationen zur Installation von HP OpenView Service Desk bzw. von Remedy Integration finden Sie im *Handbuch für Drittanbieter-Integration*.

HINWEIS: Wenn keine der untergeordneten Funktionen von „Sentinel Services“ ausgewählt wurde, müssen Sie auch die Funktion *Sentinel Services* selbst deaktivieren. Sie wird abgeblendet mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.

HINWEIS: Als Teil der Installation der Sentinel-Datenbank legt das Installationsprogramm Dateien im Ordner $ESEC_HOME/utilities/db ab.

12. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, werden Sie zur Eingabe folgender Informationen aufgefordert:
    - Seriennummer
    - Lizenzschlüssel
13. Wenn Sie ausgewählt haben, dass Drittanbieter-Integrationskomponenten installiert werden sollen, werden Sie aufgefordert, ein Passwort einzugeben, um die ausgewählten Drittanbieter-Integrationskomponenten zu entsperren. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration.*
14. Geben Sie den Benutzernamen des Betriebssystem-Sentinel-Administrators ein und den Standort seines Basisverzeichnisses. Das ist der Name des Benutzers, dem das installierte Sentinel-Produkt gehört. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem Basisverzeichnis im angegebenen Verzeichnis erstellt.
    - Benutzername des Betriebssystem-Administrators – Standardmäßig „esecadm“
    - Basisverzeichnis des Betriebssystem-Administrators – Standardmäßig /export/home. Wenn der Benutzername „esecadm“ lautet, ist das dazugehörige Basisverzeichnis /export/home/esecadm.



HINWEIS: Wird ein neuer Benutzer erstellt, muss sein Passwort manuell eingerichtet werden und nicht innerhalb dieses Installationsprogramms. Es wird dringend empfohlen, dass Sie das sofort durch Anmelden beim System nach der Installation des Produkts vornehmen.

Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (#$_) und eine Zahl (0-9) enthalten. Verwenden Sie keine Leerzeichen.

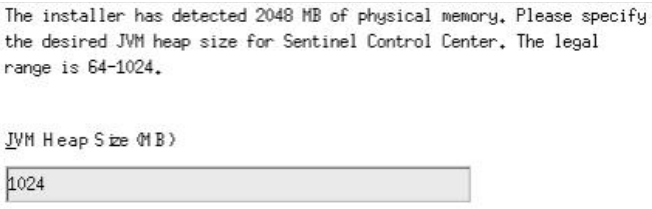
2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zu Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Beispiel: MSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).

15. Wenn Sie ausgewählt haben, dass Sentinel Control Center installiert werden soll, wird eine JVM-(Java Virtual Machine)-Heap-Größe angezeigt:
    - JVM-Heap-Größe (MB) – Standardmäßig ist dieser Wert auf die Hälfte der Größe des auf dem Computer gefundenen physischen Arbeitsspeichers eingestellt (maximal 1.024 MB). Dies ist die maximal von Sentinel Control Center verwendete JVM-Heap-Größe.



16. Wenn Sie ausgewählt haben, dass *Collector Service* installiert werden soll, müssen Sie festlegen, ob Collector Manager durch ein Passwort geschützt werden soll oder nicht. Wenn Sie festgelegt haben, dass Collector Manager geschützt werden soll, werden Sie aufgefordert, ein Collector Manager-Passwort zu erstellen.

HINWEIS: Um eine Collector-Instanz durch ein Passwort zu schützen, müssen Sie dieses Passwort beim Herauf- und Herunterladen sowie bei der Fehlersuche für Collectors im betreffenden Collector Manager angeben. Dieses Passwort und der Sentinel-Benutzername und das Passwort werden für die Anmeldung bei Collector Builder benötigt.

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

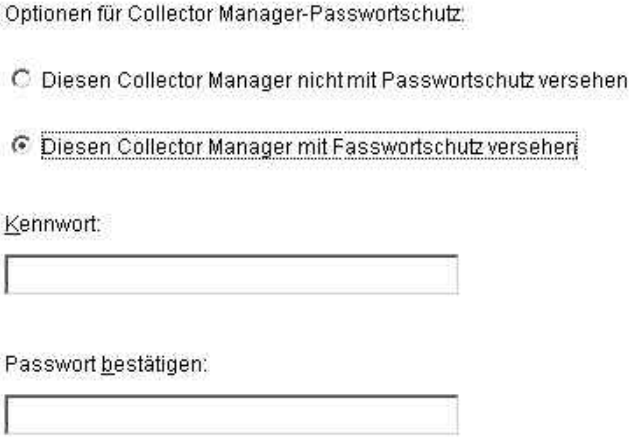
1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (!@#$%^&*()_+) und eine Zahl (0-9) enthalten.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

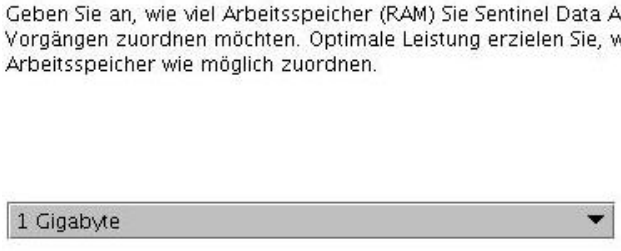
3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zu Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Beispiel: mSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).



17. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, legen Sie fest, wie viel RAM in Ihrem System für Data Access Service zur Verfügung gestellt werden soll. Für verteilte Umgebungen sollten Sie die Höchstmenge an Arbeitsspeicher (4 GB) auswählen. Für Einzelplatzumgebungen wird die Hälfte des RAM-Speichers empfohlen.



18. Bei der Datenbankinstallation werden folgende Eingabeaufforderungen angezeigt:
    a. Wählen Sie die Serverplattform der Zieldatenbank, Oracle 9i, und eines der folgenden Elemente aus:
        - Neue Datenbank mit Datenbankobjekten erstellen – erstellt eine neue Oracle-Datenbankinstanz und füllt die neue Instanz mit Datenbankobjekten
        - Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen – fügt nur Datenbankobjekte zu einer bestehenden Oracle-Datenbankinstanz hinzu. Wenn Sie eine vorhandene Oracle-Datenbankinstanz verwenden, muss diese bis auf die Präsenz des esecdba-Benutzers leer sein.
    b. Geben Sie das Verzeichnis für das Datenbankinstallationsprotokoll ein (Standard: $ESEC_HOME/logs/db). Übernehmen Sie den Standardwert für „Verzeichnis für das Protokoll der Datenbankinstallation“ oder klicken Sie auf *Durchsuchen*, um einen anderen Speicherort anzugeben.

    c. Bestätigen Sie den Oracle-Standardbenutzernamen, indem Sie auf *OK* klicken.

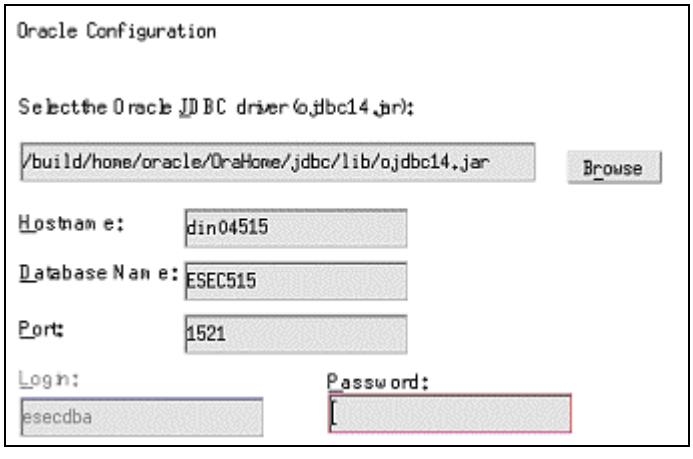
    d. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Folgendes ein:
        - Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
        - Hostname – Der Hostname des Computers für die Installation der Datenbank. Dieses Feld lässt sich nicht konfigurieren, wenn Sie eine neue Datenbankinstanz erstellen.
        - Datenbankname – Der Name der zu installierenden Datenbankinstanz.

e. Wenn Sie einer vorhandenen leeren Oracle-Datenbank Datenbankobjekte hinzufügen, werden Sie um die folgenden Informationen gebeten.

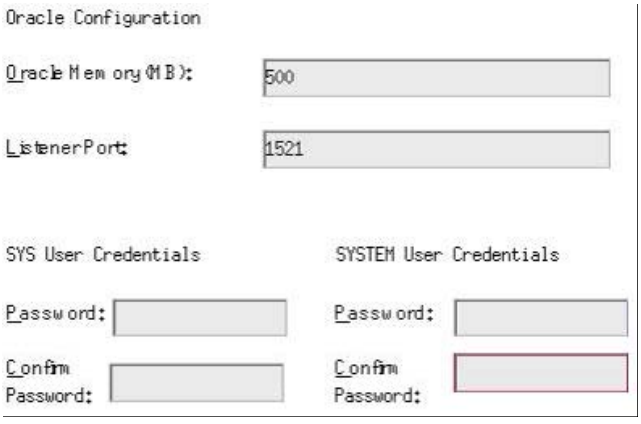
- Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
- Datenbank-Hostname oder IP-Adresse – Der Name oder die IP-Adresse des Host mit der Oracle-Datenbank, der Sie Datenbankobjekte hinzufügen möchten. Das kann der lokale Hostname oder ein Remote-Hostname sein.
- Datenbankname – Der Name der bestehenden leeren Oracle-Datenbankinstanz, zu der Datenbankobjekte hinzugefügt werden sollen (standardmäßig ESEC). Dieser Datenbankname muss als Servicename in der Datei tnsnames.ora (im Verzeichnis $ORACLE_HOME/network/admin/) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, enthalten sein.

HINWEIS: Wenn der Datenbankname nicht in der Datei tnsnames.ora enthalten ist, gibt das Installationsprogramm zu diesem Zeitpunkt in der Installation keinen Fehler aus (weil es die Verbindung über eine direkte JDBC-Verbindung überprüft). Die Datenbankinstallation scheitert erst dann, wenn das Datenbankinstallationsprogramm versucht, die Verbindung mit der Datenbank über sqlplus herzustellen. Wenn die Datenbankinstallation zu diesem Zeitpunkt nicht erfolgt, können Sie zurück zu dieser Eingabeaufforderung gehen und das Problem mit dem Datenbanknamen beheben.

- Datenbank-Port (Standard: 1521)
- Geben Sie für Sentinel-Datenbankadministratoren (DBA) das Passwort für den Benutzer „esecdba“ ein. Das Benutzernamenfeld in dieser Eingabeaufforderung lässt sich nicht bearbeiten.



f. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, sehen Sie die folgende Eingabeaufforderung:
   - Oracle-Speicher (MB) – Die Menge RAM, die dieser Oracle-Datenbankinstanz zugeordnet wird.
   - Listener Port – Der Port, an dem der Oracle-Listener erstellt werden soll (standardmäßig 1521).
   - SYS-Benutzerpasswort und Passwortbestätigung – SYS ist ein Oracle-Standardbenutzer. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.
   - SYSTEM-Benutzerpasswort und Passwortbestätigung – SYSTEM ist ein Oracle-Standardbenutzer. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.



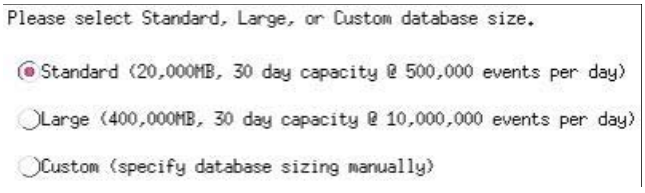
g. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, die Größe der Datenbank einzugeben. Es stehen folgende Optionen zur Auswahl:
   - Standard (20 GB)
   - Groß (400 GB)
   - Benutzerdefiniert (manuelle Größenfestlegung). Wenn Sie diese Option ausgewählt haben, werden Sie zur Eingabe folgender Informationen aufgefordert:

     Ursprüngliche Größe der einzelnen Datenbankdateien in MB (100-10.000)

     Maximale Größe der einzelnen Datenbankdateien in MB (2.000–100.000)

     Größe aller Datenbankdateien in MB (7.000–2.000.000)

     Größe der einzelnen Protokolldateien in MB (100–100.000)



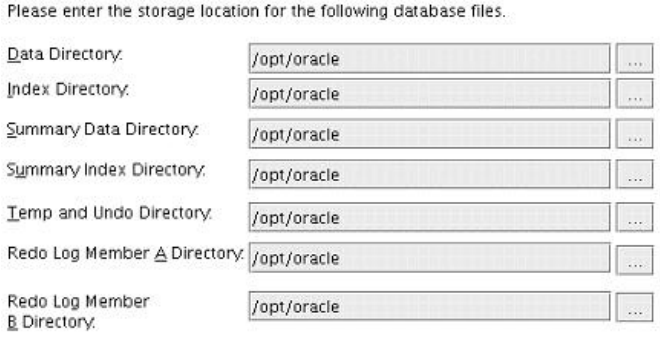
h. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, den Speicherort für folgende Datenbankdateien einzugeben:

HINWEIS: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung sollten diese Speicherorte auf unterschiedlichen E/A-Geräten liegen.

Diese Verzeichnisse werden nicht vom Installationsprogramm erstellt. Sie müssen also extern erstellt werden, um mit dem nächsten Schritt fortfahren zu können.

Der Oracle-Benutzer muss über eine Schreibberechtigung für diese Verzeichnisse verfügen.

- Datenverzeichnis
- Indexverzeichnis
- Zusammenfassungsdatenverzeichnis
- Zusammenfassungsindexverzeichnis
- Temporäres Verzeichnis und Tabellenbereichsverzeichnis zum Rückgängigmachen
- Verzeichnis für Redo-Protokollmitglied A
- Verzeichnis für Redo-Protokollmitglied B



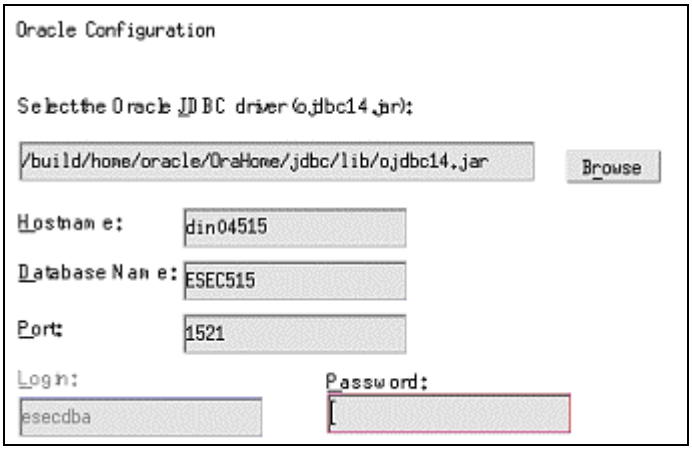
i. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Authentifizierungsinformationen für den Sentinel Database Administrator (DBA) ein. Hierbei handelt es sich um „esecdba“, den Eigentümer der Datenbankobjekte.

j. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Anwendungsdatenbank ein. Hierbei handelt es sich um „esecapp“, den Benutzernamen für die Sentinel-Anwendung, den die Sentinel-Prozesse verwenden, um eine Verbindung zu der Datenbank herzustellen.

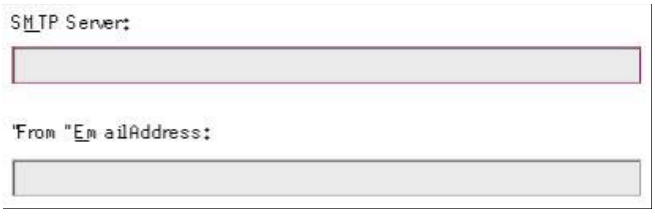
k. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Administratordatenbank ein. Hierbei handelt es sich um „esecadm“, den Sentinel-Administratorbenutzer.

l. Klicken Sie im Zusammenfassungsfenster für die Datenbankinstallation auf *Weiter*.

19. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, nicht jedoch, dass die Sentinel-Datenbank installiert werden soll, werden Sie aufgefordert, folgende Informationen für die Oracle Sentinel-Datenbank einzugeben. Diese Informationen werden verwendet, um DAS so zu konfigurieren, dass es auf die Sentinel-Datenbank verweist.
    - Datenbank-Hostname oder IP-Adresse – Der Name oder die IP-Adresse der bestehenden Oracle Sentinel-Datenbank, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten.
    - Datenbankname – Der Name der bestehenden leeren Oracle-Datenbankinstanz, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten (standardmäßig ESEC).
    - Datenbank-Port (Standard: 1521)
    - Geben Sie für den Sentinel-Anwendungsdatenbankbenutzer den Anmeldenamen „esecapp“ an und geben Sie das Passwort ein, das während der Installation der Sentinel-Datenbank für den Benutzer festgelegt wurde.

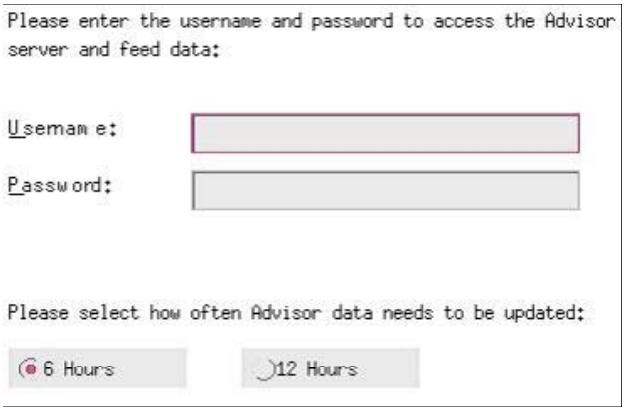


20. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, müssen Sie Email-Unterstützung für Sentinel konfigurieren. Geben Sie den SMTP-Server und die Email-Absenderadresse ein, die Execution Service beim Versenden von Nachrichten verwenden soll (optional – dieser Wert kann nach der Installation manuell geändert werden [$ESEC_HOME\sentinel\config\execution.properties]):

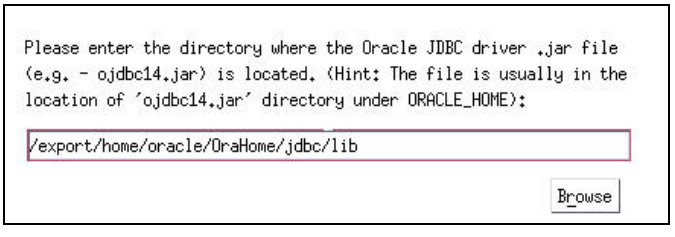


21. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, müssen Sie den Installationstyp auswählen (falls die Advisor-Option gewählt wurde, einen Benutzernamen und ein Passwort eingeben)
    - Direktes Herunterladen vom Internet – Der Advisor-Computer ist direkt mit dem Internet verbunden. In dieser Konfiguration werden regelmäßig automatisch Aktualisierungen von Sentinel über das Internet heruntergeladen.
    - Einzelplatz – Advisor ist als isoliertes System konfiguriert, in das manuell eingegriffen werden muss, um eine Aktualisierung von Sentinel zu empfangen.

22. Wenn Sie ausgewählt haben, dass Advisor installiert werden und „Direktes Herunterladen vom Internet“ verwendet werden soll, geben Sie Ihren Advisor-Benutzernamen, Ihr Passwort und die gewünschte Aktualisierungshäufigkeit für die Advisor-Daten ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.



23. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, geben Sie den Pfad zum Verzeichnis mit dem Oracle JDBC-Treiber ein (typischer Name der Treiberdatei: ojdbc14.jar). Das ist der vollständige Pfad zum Verzeichnis mit der jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).



24. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, geben Sie Folgendes ein:
    - Das Verzeichnis, in dem Advisor-Datenfeed-Dateien gespeichert werden. Dies ist der Speicherort, an dem die Angriffs- und Warnmeldungs-Feed-Dateien beim Herunterladen gespeichert werden.

HINWEIS: Die Advisor-Datenfeed-Dateien müssen über folgende Eigentümereinstellungen verfügen:

Benutzer – esecadm

Gruppe – esec

Wenn das Verzeichnis nicht über diese Einstellungen verfügt, führen Sie als Benutzer „root“ folgenden Befehl aus, um die Eigentümereinstellungen festzulegen:

```
chown esecadm:esec <directory_path>
```

    - Der Absender, der in Email-Benachrichtigungen angezeigt wird
    - Die Empfängeradresse zum Senden von Email-Benachrichtigungen

HINWEIS: Nach der Installation können Sie die Advisor-Email-Adressen ändern, indem Sie die Dateien attackcontainer.xml und alertcontainer.xml im Verzeichnis $ESEC_HOME/sentinel/config directory bearbeiten. Weitere Informationen finden Sie in *Kapitel 7 – Registerkarte „Advisor“ – im Sentinel-Benutzerhandbuch.*

- Wählen Sie aus, ob Sie per Email über erfolgreiche Advisor-Aktualisierungen benachrichtigt werden möchten. Fehlerbenachrichtigungen werden immer gesendet.

25. Wenn Sie ausgewählt haben, dass HP Service Desk oder Remedy Integration installiert werden soll, werden Sie zur Eingabe weiterer Informationen aufgefordert. Weitere Informationen finden Sie im *Sentinel-Handbuch für Drittanbieter-Integration*.
26. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten. Klicken Sie auf *Fertig stellen*, um das System neu zu booten.
27. Das Sentinel-Installationsprogramm deaktiviert standardmäßig die Archivprotokollierung. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank keine Ereignisse mehr entgegen.
28. Wenn Sie eine hohe Ereignisrate (mehr als 500 Ereignisse pro Sekunde) erwarten, müssen Sie die zusätzlichen Konfigurationsanweisungen in Abschnitt Einrichten der OCI-Strategie (Oracle Call Interface) zum Einfügen von Ereignissen befolgen.

Nach der Installation von Sentinel 5 für Oracle

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter $ESEC_HOME/sentinel/config. Um diese Datei zu konfigurieren, führen Sie mailconfig.sh aus, um die Datei zu ändern, und mailconfigtest.sh, um Ihre Änderungen zu testen.

So konfigurieren Sie Ihre execution.properties-Datei

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

   ```
   ./mailconfig.sh -host <SMTP-Server> -from <Quell-Email-
      Adresse> -user <Mail-Authentifizierungsbenutzer> –
      password
   ```

   Beispiel:

   ```
   ./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com
      -user my_user_name –password
   ```

   Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

   ```
   Enter your password:*********
   Confirm your password:*********
   ```

   HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfigtest“ wie folgt aus:

   ```
   ./mailconfigtest.sh -to <Ziel-Email-Adresse>
   ```

   Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

   ```
   Email has been sent successfully!
   ```

Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

```
Subject: Testing Sentinel mail property

This is a test for Sentinel mail property set up. If you
   see this message, your Sentinel mail property has been
   configured correctly to send emails
```

Sentinel-Datenbank

Nach der Installation der Sentinel-Databank enthält die Datenbank folgende Standardbenutzer:

- esecdba - Eigentümer des Datenbankschemas. Aufgrund von Sicherheitsbeschränkungen wird „esecdba“ keine DBA-Berechtigung gewährt. Erstellen Sie zur Verwendung von Enterprise Manager einen Benutzer mit DBA-Berechtigungen.
- esecapp – Datenbankanwendungsbenutzer. Das ist der Anwendungsbenutzer für die Verbindung mit der Datenbank.
- esecadm – Hierbei handelt es sich um den Datenbankbenutzer, der der Sentinel-Administrator ist. Das ist nicht dasselbe Benutzerkonto, wie der Betriebssystembenutzer „esecadm“.
- esecrpt - Datenbankreport-Benutzer
- SYS – SYS-Datenbankbenutzer
- SYSTEM – SYSTEM-Datenbankbenutzer

Collector-Service

Während der Installation des Collector-Service werden folgende Collectors installiert und für jeden wird ein Collector-Port eingerichtet, um ihn auszuführen.

Produkt **Demo-Collectors**	**Collector-Name**
Führt Tests für das Heraufladen von Beständen durch, arbeitet mit dem DemoEvents-Collector	DemoAssetUpload
Führt Tests für Demo-Ereignisse durch, arbeitet mit DemoAssetUpload- und DemoVulnerabilityUpload-Collector	DemoEvents
Führt Tests für das Heraufladen von Anfälligkeiten durch, arbeitet mit dem DemoEvents-Collector	DemoVulnerabilityUpload
Test für das Senden eines Ereignisses	SendOneEvent
Test für das Senden mehrerer Ereignisse	SendMultipleEvents

HINWEIS: Weitere Informationen zur Konfiguration der Demo-Collectors finden Sie in *Kapitel 12, Testen der Installation.*

HINWEIS: Weitere Collectors finden Sie im Sentinel-Kundenportal. Weitere Informationen (auch zur Konfiguration) finden Sie in der Dokumentation zu den einzelnen Collectors in:

$WORKBENCH_HOME/Elements/<Collector-Name>/Docs/

Zur Installation weiterer Collectors führen Sie das Service Pack-Skript auf der Service Pack-CD aus. Das Skript installiert die Collectors lokal.

Unter Windows:

```
.\service_pack.bat
```

Unter UNIX:

```
./service_pack.sh
```

Installationsanweisungen für das Service Pack und eine Liste der Collectors finden Sie in den *Service Pack-Versionshinweisen.*

Aktualisieren des Lizenzschlüssels

Aktualisieren Ihres Lizenzschlüssels (Solaris)

1. Melden Sie sich als Benutzer „esecadm“ an.
2. Wechseln Sie in das Verzeichnis „$ESEC_HOME/utilities“.
3. Geben Sie den folgenden Befehl ein:

   ```
   ./softwarekey
   ```

4. Geben Sie die Ziffer 1 ein, um den Primärschlüssel anzugeben. Drücken Sie die EINGABETASTE.

Erstellen einer Oracle-Instanz für die Sentinel-Datenbank

HINWEIS: Dieses Verfahren dient als Beispiel, wenn Sie, statt die Funktion zur Tabellenbereichserstellung auf der Installations-CD zu nutzen, Ihre eigenen Tabellenbereiche erstellen möchten. Die Größenwerte können je nach Systemkonfiguration und Anforderungen variieren. Die Tabellenbereiche müssen genau wie unten angegeben benannt werden.

In der Oracle-Instanz müssen Sie folgende Elemente konfigurieren:

- Parameter
- „Tablespaces“ (Tabellenbereiche)

Erstellen einer Oracle-Instanz

1. Melden Sie sich als Oracle-Benutzer an.
2. Verwenden Sie den Oracle-Datenbankassistenten und erstellen Sie Folgendes:

HINWEIS: Die Werte können je nach Systemkonfiguration und Anforderungen variieren.

Empfohlene Mindestwerte für die Solaris-Konfigurationsparameter	
Parameter	**Größe (in Byte, wenn nicht anders angegeben)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Empfohlene Mindestgröße für den Solaris-Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
REDO	3 x 100 M	Dies ist ein Mindestwert. Bei einem hohen EPS-Wert sollten größere Redo-Protokolle erstellt werden.
SYSTEM	500 M	Mindestwert
TEMP	1 G	Mindestwert
UNDO	1 G	Mindestwert
ESENTD	5 G	Mindestwert Für Ereignisdaten
ESENTD2	500 M	Mindestwert Daten für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
ESENTWFD	250 M	Für iTrac-Daten (autoextend aktiviert)
ESENTWFX	250 M	Für iTrac-Index (autoextend aktiviert)
ESENTX	3 G	Mindestwert Für Ereignisindex
ESENTX2	500 M	Mindestwert Index für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
SENT_ADVISORD	200 M	Mindestwert Für Advisor-Daten (autoextend aktiviert)
SENT_ADVISORX	100 M	Mindestwert Für Advisor-Index (autoextend aktiviert)
SENT_LOBS	100 M	Mindestwert Für große Datenbankobjekte (autoextend aktiviert)
SENT_SMRYD	3 G	Mindestwert Für die Aggregation, Zusammenfassungsdaten
SENT_SMRYX	2 G	Mindestwert Für die Aggregation, Zusammenfassungsindex

3. Führen Sie das Skript createEsecdba.sh aus dem Verzeichnis „sentinel\dbsetup\bin“ auf der Sentinel-Installations-CD aus. Dieses Skript erstellt den Benutzer „esecdba“, der für das Hinzufügen von Datenbankobjekten mit dem Sentinel-Installationsprogramm erforderlich ist.
4. Sichern Sie die Datenbank.

Einrichten der OCI-Strategie (Oracle Call Interface) zum Einfügen von Ereignissen

Sentinel 5.1 bietet einen Rahmen zur Integration verschiedener Strategien zum Einfügen von Ereignissen in die Datenbank. Sentinel 5.1 bietet zwei Strategien zum Einfügen von Ereignissen in die Oracle-Datenbank:

- JDBCLoadStrategy
- OCILoadStrategy

Die zum Einfügen von Ereignissen zu verwendende Strategie richtet sich nach der Eigenschaft insert.strategy der Komponente EventStoreService in das_binary.xml.

Die JDBC-Strategie ist die Standardstrategie, die bereits vorkonfiguriert ist.

Die OCI-Strategie ist eine native Einfügestrategie für das schnellere Einfügen von Ereignissen. Bei dieser Strategie ist es erforderlich, dass die Oracle OCI-Bibliotheken auf dem Computer installiert werden, auf dem die DAS-Komponente ausgeführt wird. Die OCI-Strategie muss bei Konfigurationen verwendet werden, bei denen eine hohe Ereignisrate erwartet wird.

Die Anzahl der zum Einfügen in einer Gruppe zusammenzufassenden Ereignisse wird durch die Eigenschaft insert.batchsize festgelegt. Die Eigenschaft insert.batchsize wird von allen Strategien zum Einfügen von Ereignissen verwendet.

Um die von Sentinel verwendete Strategie zum Einfügen von Ereignissen von der standardmäßig verwendeten JDBC-Einfügestrategie zur OCI-Einfügestrategie zu ändern, müssen einige Schritte durchgeführt werden.

Wechsel von der JDBC-Einfügestrategie zur OCI-Einfügestrategie

1. Stellen Sie sicher, dass die Oracle OCI-Bibliotheken auf dem Computer installiert werden, auf dem die Sentinel-DAS-Komponente ausgeführt wird. Sie müssen für die folgenden Schritte den Pfad zu ORACLE_HOME kennen.
2. Melden Sie sich beim Computer ab Schritt 1 als Benutzer „esecadm“ an.
3. Erstellen Sie im Basisverzeichnis von „esecadm“ die Datei „.profile“. Fügen Sie in diese Datei den folgenden Text ein (passen Sie den Pfad für ORACLE_HOME an Ihre Installation an):

   ```
   ORACLE_HOME=/build/home/oracle/OraHome
   export ORACLE_HOME
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   export LD_LIBRARY_PATH
   ```

4. Öffnen Sie die Datei $ESEC_HOME/sentinel/config/das_binary.xml in einem beliebigen Texteditor.
5. Führen Sie eine Suche nach folgendem Text durch:

   ```
   JDBCLoadStrategy
   ```

6. Ändern Sie diesen Text in:

   ```
   OCILoadStrategy
   ```

7. Speichern Sie diese Änderung in der Datei das_binary.xml.
8. Starten Sie die DAS-Binäranwendung neu. (Der Neustart der DAS-Binäranwendung wird am einfachsten durchgeführt, indem Sie „ps –ef | grep DAS_Binary“ ausführen, um die Prozess-ID zu erhalten, diesen Prozess anschließend mit „kill“ zu beenden und ihn dann automatisch von Sentinel Watchdog neu starten zu lassen.)

   Sobald die DAS-Binäranwendung neu gestartet wurde, wird die Bibliothek $ESEC_HOME/sentinel/lib/libocievent.so geladen und zum Einfügen der Ereignisse in die Datenbank über OCI verwendet.

Zusätzliche Optionen zum Einfügen von Ereignissen mit OCI

Zusätzlich zur Angabe von „OCILoadStrategy“ in der Datei das_binary.xml gibt es einige andere OCI-Optionen, die ebenfalls konfiguriert werden können.

- insert.batchsize – Mit dieser Einstellung können Sie die maximale Anzahl der Ereignisse festlegen, die gleichzeitig in die Datenbank aufgenommen werden.
- insert.oci.workerCount – Diese Einstellung legt die Anzahl der Threads fest, die verwendet werden, um Ereignisdaten in die Datenbank einzufügen.
- insert.oci.queueWaitTime – Diese Einstellung legt die maximale Zeitspanne in Sekunden fest, die gewartet wird, bevor die Daten aus der eingehenden Warteschlange in die Datenbank aufgenommen werden. Sobald eine vollständige Stapelanzahl („batchsize“) von Ereignissen empfangen wird, wird der gesamte Stapel eingefügt. Aber wenn der eingehende Ereignisfluss langsam ist, bestimmt die Zeit in der Warteschlange, wann sie in die Datenbank eingefügt werden (auch wenn die Stapelanzahl noch nicht erreicht wurde).
- insert.oci.highWatermark – Die obere Grenze der eingehenden Ereignisse.
- insert.oci.lowWatermark – Die untere Grenze der eingehenden Ereignisse.
- insert.oci.optimizationFlag – Optimierungsflagge. „Ein“ oder „Aus“.

Tipps für die OCI-Fehlersuche

Die OCI-Schnittstelle protokolliert Fehlermeldungen ausschließlich in der Datei $ESEC_HOME/sentinel/log/ocievent.log. Anfängliche Meldungen, die in die Protokolldatei geschrieben werden, sollten erfolgreiche (oder fehlgeschlagene) Datenbankverbindungsmeldungen enthalten... Damit können Sie überprüfen, ob die OCI-Bibliothek geladen und korrekt konfiguriert wurde.

Die OCI-Schnittstelle protokolliert auch Fehler in der Protokolldatei das_binary im Verzeichnis $ESEC_HOME/sentinel/log. Zu den in der Protokolldatei das_binary protokollierten Fehlern gehören Fehler beim Auffinden/Laden der Bibliothek libocievent.so, Fehler bei der Herstellung einer Verbindung mit der Datenbank und Fehler beim Einfügen von Ereignissen/Ereignisverknüpfungen.

Wenn die Fehlermeldungen angeben, dass die Datei libocievent.so nicht auffindbar oder geladen ist, müssen Sie drei Dinge überprüfen:

1. Vergewissern Sie sich, dass die Oracle-OCI-Bibliotheken installiert sind.
2. Vergewissern Sie sich, dass sich die Datei libocievent.so im Verzeichnis $ESEC_HOME/sentinel/lib befindet.

3. Vergewissern Sie sich, dass sich das Verzeichnis $ESEC_HOME/sentinel/lib in LD_LIBRARY_PATH des Benutzers „esecadm“ befindet. Falls nicht, können Sie LD_LIBRARY_PATH im Benutzerprofil von „esecadm“ aktualisieren.
4. Vergewissern Sie sich, dass die Umgebungsvariablen ORACLE_HOME und LD_LIBRARY_PATH in den Umgebungsvariablen des Benutzers „esecadm“ entsprechend aktualisiert wurden, wie im Abschnitt „Wechsel von der JDBC-Einfügestrategie zur OCI-Einfügestrategie“ beschrieben.

4 Installation von Sentinel 5 für Oracle unter Linux

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

In diesem Kapitel erfahren Sie, wie Sie Sentinel Enterprise Security Management Sentinel 5 für Oracle unter SuSE Linux Enterprise Server und Red Hat Enterprise Linux installieren.

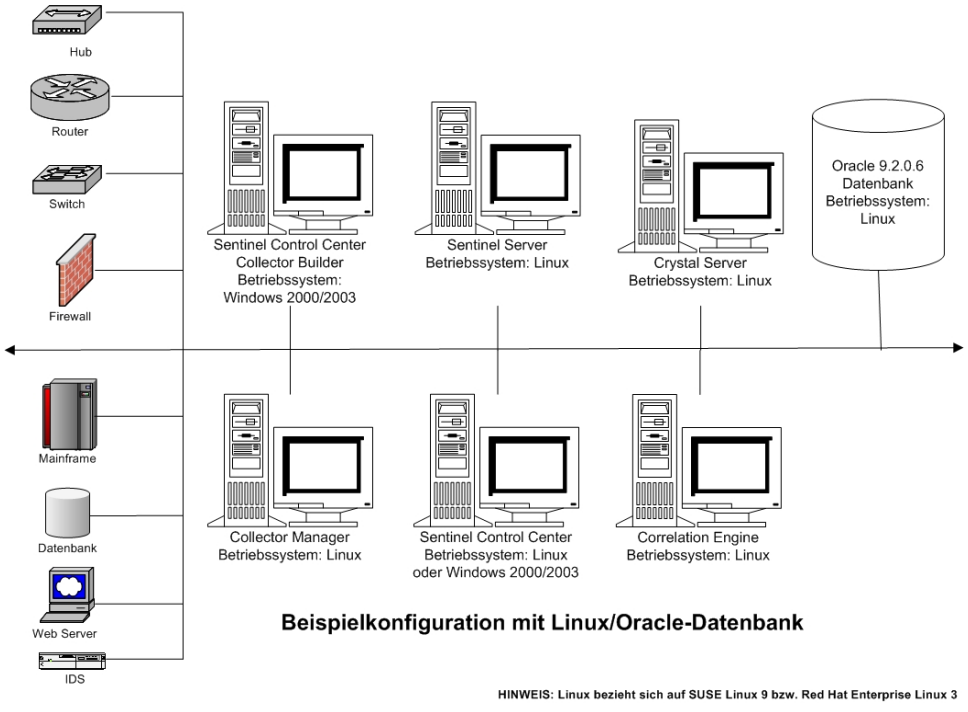
Vor der Installation von Sentinel 5 für Oracle unter Linux

HINWEIS: Vergewissern Sie sich vor der Installation, dass Ihre Maschinen den Mindestsystemanforderungen entsprechen und dass das Betriebssystem mithilfe der besten Sicherheitsvorkehrungen geschützt ist.

HINWEIS: Installieren Sie Oracle Enterprise mit Partitionierung. Der Sentinel Data Manager benötigt diese Funktion zur Verwaltung der Sentinel-Datenbank.

HINWEIS: Wenn Sie eine Neuinstallation von Sentinel durchführen möchten, nachdem bereits eine frühere Version installiert wurde, müssen Sie bestimmte Dateien und Systemeinstellungen entfernen, die eventuell noch von einer früheren Installation übrig geblieben sind. Wenn Sie diese Dateien bzw. Einstellungen nicht entfernen, kann die Neuinstallation scheitern. Dieser Vorgang sollte auf jedem Computer durchgeführt werden, auf dem eine Neuinstallation erfolgen soll. Weitere Informationen finden Sie in *Anhang E*.

Im Folgenden sehen Sie typische Konfigurationen für Linux und Sentinel. Je nach der von Ihnen verwendeten Umgebung kann die Konfiguration abweichen. Unabhängig von der gewählten Konfiguration müssen Sie zuerst die Datenbank installieren.



HINWEIS: Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in Kapitel 1 – *Einführung, Unterstützte Plattformen für Sentinel Server unter Linux.*

Abrufen eines Lizenzschlüssels

Für die Installation und Ausführung von Sentinel Server Database Access Service (DAS) ist ein gültiger Lizenzschlüssel erforderlich. Dieser Lizenzschlüssel ist an den Computer gebunden, auf dem DAS installiert werden soll. Ein für einen bestimmten Computer ausgegebener Lizenzschlüssel funktioniert nicht auf anderen Computern.

Zum Abrufen des Lizenzschlüssels müssen Sie Ihre Host-ID-Nummer ermitteln und diese Informationen an Novell weitergeben. Anschließend wird ihnen ein Lizenzschlüssel zugewiesen.

So ermitteln Sie Ihre Host-ID (Linux)

1. Melden Sie sich als Benutzer „root“ an.
2. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
3. Wechseln Sie zum Verzeichnis utilities/linux und geben Sie Folgendes ein:

   ```
   ./esechostid
   ```

4. Übermitteln Sie die betreffende Host-ID-Nummer an Novell Technical Support. Von dort erhalten Sie einen Lizenzschlüssel.

Sentinel-Datenbank

Vor der Installation der Sentinel-Datenbank brauchen Sie:

- Die Hardware-Anforderungen finden Sie in den *Kapiteln 1* und *2*.
- SuSE Linux Enterprise Server 9 mit SP2 oder Red Hat Enterprise Linux 3 Update 5 ES (x86) oder
- Oracle 9i Enterprise Edition 9.2.0.6 (nur SuSE Linux) bzw. 9.2.0.7 mit Partitionierung
- Oracle-Betriebssystembenutzer (Standard: oracle)
- Vergewissern Sie sich, dass die folgenden Umgebungsvariablen für den Oracle-Betriebssystembenutzer festgelegt wurden:
  `ORACLE_HOME`

  `ORACLE_BASE`

  `PATH (muss enthalten $ORACLE_HOME/bin)`

  - Obwohl es nicht empfohlen wird, können Sie die Oracle-Datenbankinstanz auch manuell erstellen. Unter Erstellen einer Oracle-Instanz für die Sentinel-Datenbank finden Sie eine Anleitung zum Erstellen Ihrer Oracle-Instanz. Wenn Sie diese Option wählen, müssen Sie dennoch das Installationsprogramm verwenden, um die Datenbankobjekte der manuell erstellen Oracle-Datenbankinstanz hinzuzufügen. (Unter Benutzerdefinierte Installation erfahren Sie, wie Sie dabei vorgehen.)

HINWEIS: Wenn Sie eine vorhandene oder manuell erstellte Oracle-Datenbankinstanz verwenden, muss diese bis auf die Präsenz des esecdba-Benutzers leer sein. Im Abschnitt Erstellen einer Oracle-Instanz für die Sentinel-Datenbank finden Sie eine Anleitung zum Erstellen dieses Benutzers, wenn er noch nicht vorhanden ist.

- Wird die Oracle-Datenbank mithilfe des Installationsprogramms erstellt (empfohlen), benötigen Sie die Verzeichnispfade für die Datenbankdateien. Diese Verzeichnisse müssen bereits vorhanden sein, bevor das Installationsprogramm ausgeführt wird, da sie nicht vom Installationsprogramm erstellt werden können. Außerdem muss der Oracle-Betriebssystembenutzer (z. B. oracle) über eine Schreibberechtigung für diese Verzeichnisse verfügen.

HINWEIS: Um eine möglichst hohe Leistung zu erreichen, sollte, sofern die Installation in RAID vorgenommen wird und sofern es die RAID-Umgebung zulässt, das Redo-Protokoll auf die Festplatte mit der höchsten Schreibgeschwindigkeit verweisen, die verfügbar ist.

HINWEIS: Standardmäßig legt das Installationsprogramm fest, dass folgende Tabellenbereiche NICHT automatisch wachsen: ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX. Für alle anderen Tabellenbereiche wird automatisches Wachstum festgelegt. Der Grund, warum automatisches Wachstum für ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX nicht zugelassen wird, ist, dass sie Daten über Ereignisse und Zusammenfassungsereignisse enthalten. Die Speicherplatzauslastung für Ereignisse und Zusammenfassungen kann höchst dynamisch sein. Diese Tabellenbereiche sollten überwacht und auf gesteuerte Weise in Ihrer Dateisystemkonfiguration erweitert werden. Dabei sind EA-Lastenausgleich und Datenbanksicherung und -wiederherstellung zu berücksichtigen.

Die SDM-Partitionsverwaltung (Archivieren, Verwerfen und Hinzufügen von Partitionen) sollte zeitlich geplant sein, um die Größe der Ereignisdaten überschaubar zu halten.

Sentinel Server

HINWEIS: Wenn Sie die Sentinel-Datenbank nicht zusammen mit Sentinel Server installieren, muss die Sentinel-Datenbank zuerst installiert werden.

Vor der Installation von Sentinel Server benötigen Sie folgende Elemente:

- Die Hardware-Anforderungen finden Sie in den *Kapiteln 1* und *2*.
- SuSE Linux Enterprise Server 9 mit SP2 oder Red Hat Enterprise Linux 3 Update 5 ES (x86) oder
- Seriennummer und Lizenzschlüssel von Sentinel 5 (für DAS). Weitere Informationen finden Sie unter Abrufen eines Lizenzschlüssels.
- SMTP-Server – Wird benötigt, um Emails über Sentinel zu versenden.

Sentinel Control Center und Wizard

Vor der Installation von Sentinel Server benötigen Sie Folgendes:

- Die Hardware-Anforderungen finden Sie in *Kapitel 1 und 2*.
- SuSE Linux Enterprise Server 9 mit SP2 oder Red Hat Enterprise Linux 3 Update 5 ES (x86)
- (Collector Builder und Sentinel Control Center) – Windows 2000 oder 2003

Advisor

Zur Installation von Advisor müssen Sie eine Advisor-ID und ein Passwort von Sentinel anfordern. Beim direkten Herunterladen aus dem Internet wird Port 443 verwendet.

HINWEIS: Wenn Sie Advisor nur für Exploit-Erkennung verwenden, brauchen Sie die Crystal Enterprise-Software nicht zu installieren. Dies ist nur erforderlich, wenn Sie vorhaben, Crystal Reports für Sentinel auszuführen. Weitere Informationen finden Sie in *Kapitel 10, Advisor-Konfiguration*.

Vor der Installation von Oracle unter Linux

Vor der Installation von Oracle unter Linux für Sentinel sind folgende Aktionen erforderlich:

- Einstellen der Kernel-Werte
- Erstellen eines Gruppen und Benutzerkontos für Oracle
- Festlegen der Umgebungsvariablen für Oracle-Benutzer
- Verknüpfen von gcc
- Installieren des Patch für Linux für Oracle 9.2.0.4 (Patch p3006854_9204_LINUX direkt erhältlich von Oracle)
- Installation von Oracle 9.2.0.4 (Software direkt erhältlich von Oracle)
- Installieren des Patch für Oracle 9.2.0.4 auf Oracle 9.2.0.6 (nur SuSE Linux) oder 9.2.0.7 (Patch Oracle 9.2.0.6 oder 9.2.0.7 direkt erhältlich von Oracle)

Festlegen der Kernel-Werte für Oracle unter Linux (SuSE und Red Hat)

Für Oracle unter Linux müssen die folgenden Kernel-Werte eingestellt werden.

HAFTUNGSAUSSCHLUSS: Im Folgenden finden Sie die vorgeschlagenen Mindestwerte. Sind Ihre Systemwerte größer als diese Zahlen, müssen Sie sie nicht ändern. Von Ihrem Systemadministrator und in der Oracle-Dokumentation erhalten Sie genauere Informationen.

- shmmax=2147483648 (Mindestwert)
- shmmni=4096
- semmns=32000
- semmni=1024
- semmsl=1024
- semopm=100

1. Melden Sie sich als „root“ an.
2. Legen Sie die Kernel-Parameter fest, indem Sie den folgenden Text an das Ende der Datei /etc/sysctl.conf anfügen:

HINWEIS: Im Folgenden finden Sie die vorgeschlagenen Mindestwerte. Sind Ihre aktuellen Werte größer als diese Zahlen, müssen Sie sie nicht ändern. Zum Festlegen der aktuellen Einstellung für einen bestimmten Kernel-Parameter führen Sie folgenden Befehl aus:

```
sysctl <kernel_parameter>
```

Zum Überprüfen des aktuellen Wertes für den Kernel-Parameter „kernel.sem“ führen Sie folgenden Befehl aus:

```
sysctl kernel.sem
```

```
# Kernel settings for Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM> <SEMMNI>
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

3. Führen Sie den folgenden Befehl aus, damit die Änderungen in der Datei /etc/sysctl.conf geladen werden:

```
sysctl -p
```

4. Legen Sie die Datei-Handles und Prozesslimits fest, indem Sie den folgenden Text an das Ende der Datei /etc/security/limits.conf anhängen. „nproc“ ist die maximale Grenze der Anzahl an Prozessen und „nofile“ ist die maximale Grenze der Anzahl geöffneter Dateien. Das sind die empfohlenen Werte, aber sie können bei Bedarf geändert werden. Im folgenden Text wird angenommen, dass Ihre Oracle-Benutzer-ID „oracle“ lautet. Wenn Ihre Oracle-Benutzer-ID anders lautet, ersetzen Sie „oracle“ im folgenden Text durch Ihre entsprechende Oracle-Benutzer-ID.

```
# Settings added for Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

Vor der Installation von Oracle unter SuSE Linux

Vor der Installation von Oracle unter SuSE Linux

HAFTUNGSAUSSCHLUSS: Die folgende Anleitung ersetzt nicht die Dokumentation von Oracle. Es handelt sich hierbei nur um ein Beispiel eines Einrichtungsszenarios. Folgende Anweisungen sollten unbedingt ausgeführt werden. Ihre genaue Konfiguration ist eventuell anders. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem und zu Oracle.

1. Befolgen Sie die im SLES 9-Installationshandbuch bereitgestellten Installationsanweisungen. Installieren Sie SLES 9 mit den Standardpaketen sowie die *C/C++-Compiler und -Tools.*

   HINWEIS: Falls Sie SuSE Linux bereits intalliert haben, können Sie YaST (Yet Another Setup Tool) in der SuSE Linux-GUI zur Installation der *C/C++-Compiler und -Tools* verwenden.

2. Melden Sie sich als „root“ an.
3. Überprüfen Sie den Kernel-Wert indem Sie Folgendes eingeben:

   ```
   uname –r
   ```

   Ein Kernel-Wert von 2.6* ist erforderlich. Ein Kernel-Wert von beispielsweise 2.6.5 bis 7.97 erfüllt die Anforderungen.
4. Installieren Sie die Datei gcc_old-2.95.3-175.2.i586.rpm, die sich auf der ersten CD von SLES 9 SP2 befindet.

   ```
   rpm -i <Pfad>/ gcc_old-2.95.3-175.2.i586.rpm
   ```

5. Überprüfen Sie, ob SP2 ausgeführt wird, indem sie Folgendes eingeben:

   ```
   SPident
   ```

   oder

   ```
   cat /etc/SuSE-release
   ```

   Folgendes sollte angezeigt werden:

   ```
   CONCLUSION: System is up-to-date!
      Found     SLES-9-i386-SP2
   ```

   oder

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 2
   ```

6. Installieren Sie die Datei orarun-1.8-109.15.i586.rpm, um den Großteil der Aufgaben vor der Installation von Oracle zu automatisieren und um den Oracle-Benutzer zu erstellen.

   HINWEIS: Eine vollständige Auflistung der Voraussetzungen finden Sie in der Oracle-Dokumentation zur Installation.

   ```
   rpm -i <Pfad>/orarun-1.8-109.15.i586.rpm
   ```

   HINWEIS: orarun steht auch unter http://www.novell.com zur Verfügung. Weitere Funktionen von orarun:

   ```
   export LD_ASSUME_KERNEL=2.4.21
   export LD_PRELOAD=/usr/lib/libInternalSymbols.so
   ```

7. Das Konto für den Oracle-Benutzer ist deaktiviert. Aktivieren Sie es, indem Sie die Shell für den Oracle-Benutzer mit der YaST-Benutzerverwaltung von /bin/false in /bin/bash ändern bzw. indem Sie /etc/passwd bearbeiten.
8. Legen Sie ein neues Passwort für den Oracle-Benutzer fest, indem Sie YaST verwenden oder Folgendes eingeben:

   ```
   /usr/bin/passwd oracle
   ```

9. Führen Sie zum Festlegen der Kernel-Parameter Folgendes aus:

   ```
   /usr/sbin/rcoracle start
   ```

   Ignorieren Sie dabei möglicherweise auftretende Fehler.
10. Wenn Sie Oracle 9.2.0.4 von der Disk1 installieren möchten, führen Sie folgendes Skript aus:

    ```
    ./runinstaller
    ```

11. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Bei der Aufforderung zum UNIX-Gruppennamen geben Sie Folgendes ein: dba
    - Für den Installationstyp wählen Sie „Benutzerdefiniert“.

    Wählen Sie folgende Komponenten für die Installation aus:
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
      - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
      - Oracle Net Listener 9.2.0.4.0
    - Oracle Enterprise Manager Products 9.2.0.1.0 (Alle)
    - Oracle 9i Development Kit 9.2.0.1.0 (Alle)
    - Oracle 9i für UNIX Dokumentation 9.2.0.1.0
    - Oracle HTTP Server 9.2.0.1.0 (Alle)
    - iSQL*Plus 9.2.0.4.0 (Alle)
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
12. Wenn Sie aufgefordert werden, eine Datenbank zu erstellen, wählen Sie „Nein“.
13. Optional können Sie alle Konfigurationsassistenten, die vom Installationsprogramm gestartet werden, abbrechen.

14. Ändern Sie die Datei /opt/oracle/network/admin/sqlnet.ora (oder erstellen Sie die Datei, wenn sie noch nicht vorhanden ist), damit Sie Folgendes enthält (entfernen Sie alle unkommentierten Informationen aus der Datei):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

15. Zum Anwenden des Oracle 9.2.0.6 Patch für das Oracle-Installationsprogramm auf der Disk1 der Oracle 9.2.0.6 Patch-Distribution führen Sie das Skript aus:

    HINWEIS: Der Oracle 9.2.0.6 Patch wird NICHT angewendet, wenn nicht zuerst das Oracle-Installationsprogramm gepatcht wird.

    ```
    ./runInstaller
    ```

16. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
    - Auf dem Bildschirm „Dateistandorte angeben“. Als Zielname wählen Sie *OUIHome* aus der Dropdown-Liste (oder den von Ihnen während der Installation von Oracle 9.2.0.4 angegebenen Zielnamen). Klicken Sie dann auf *Weiter*.
    - Wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option *Oracle Universal Installer 10.1.0.3.0*. Klicken Sie dann auf *Weiter*.
    - Überprüfen Sie auf dem Bildschirm „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf *Installieren*.
    - Am Ende des Installationsbildschirms klicken Sie auf *Beenden*.
17. Zum Anwenden des Oracle 9.2.0.6 Patch für Oracle auf der Disk1 der Oracle 9.2.0.6 Patch-Distribution führen Sie das Skript aus:

    ```
    ./runInstaller
    ```

18. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
    - Auf dem Bildschirm „Dateistandorte angeben“. Als Zielname wählen Sie „OUIHome“ aus der Dropdown-Liste (oder den von Ihnen während der Installation von Oracle 9.2.0.4 angegebenen Zielnamen). Klicken Sie dann auf *Weiter*.
    - Je nach Ihrer Version wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option *Oracle 9iR2 Patchset 9.2.0.6.0*. Klicken Sie dann auf *Weiter*.
    - Überprüfen Sie auf dem Bildschirm „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf *Installieren*.
    - Am Ende des Installationsbildschirms klicken Sie auf *Beenden*.

Vor der Installation von Oracle unter Red Hat Linux

Vor der Installation von Oracle unter Red Hat Linux

HAFTUNGSAUSSCHLUSS: Die folgende Anleitung ersetzt nicht die Dokumentation von Oracle. Es handelt sich hierbei nur um ein Beispiel eines Einrichtungsszenarios. Diese Dokumentation setzt voraus, dass das Basisverzeichnis des Oracle-Benutzers **/export/home/oracle** lautet und dass Oracle im Verzeichnis **/opt/oracle** installiert wird. Ihre genaue Konfiguration ist eventuell anders. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem und zu Oracle.

1. Melden Sie sich als „root“ an.
2. Erstellen Sie eine UNIX-Gruppe und ein UNIX-Benutzerkonto für den Oracle-Datenbankeigentümer.

   Fügen Sie eine dba-Gruppe hinzu (als „root“):

   ```
   groupadd dba
   ```

3. Fügen Sie den Oracle-Benutzer hinzu (als „root“):

   ```
   useradd –g dba –s /bin/bash –d /export/home/oracle –m
      oracle
   ```

4. Erstellen Sie ein Verzeichnis für ORACLE_HOME und ORACLE_BASE:

   ```
   mkdir –p /opt/oracle/
   ```

5. Ändern Sie die Eigentümereinstellungen des Verzeichnisses ORACLE_BASE und darunter bis oracle/dba:

   ```
   chown -R oracle:dba /opt/oracle
   ```

6. Wechseln Sie zum Benutzer „oracle“

   ```
   su - oracle
   ```

7. Öffnen Sie die Datei „.bash_profile“ (im Basisverzeichnis des Benutzers „oracle“) und fügen Sie Folgendes an das Dateiende an:

   HINWEIS: Diese Umgebungsvariablen dürfen nur für den Benutzer „oracle“ verwendet werden. Sie sollten keinesfalls in der Systemumgebung oder in der Umgebung des Benutzers „esecadm“ festgelegt werden.

   ```
   # Set the LD_ASSUME_KERNEL environment variable only for
      Red Hat 9,
   # RHEL AS 3, and RHEL AS 4 !!
   # Use the "Linuxthreads with floating stacks"
      implementation instead of NPTL:
   # for RH 9 and RHEL AS 3
   export LD_ASSUME_KERNEL=2.4.1
   # for RHEL AS 4
   # export LD_ASSUME_KERNEL=2.4.19
   # Oracle Environment
   ```

```
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# export TNS_ADMIN= Set if sqlnet.ora, tnsnames.ora, etc.
   are not in $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Set shell search paths
export PATH=$PATH:$ORACLE_HOME/bin
```

8. Melden Sie sich erneut als Benutzer „oracle“ an, um die Änderungen der Umgebungsvariablen im letzten Schritt zu laden:

```
exit
su - oracle
```

9. Verknüpfen Sie gcc mit Version 2.9.6

HINWEIS: Falls /usr/bin/gcc296 oder /usr/bin/g++296 nicht vorhanden ist, wurden gcc oder g++ nicht installiert. In diesem Fall installieren Sie diese Komponenten und kehren anschließend zu diesem Schritt zurück.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Beenden Sie das Programm, um zur Eingabeaufforderung für den Benutzer „oracle“ zurückzukehren.

```
exit
```

11. Führen Sie den Oracle-Patch p3006854_9204_LINUX.zip aus, der das Linux-Betriebssystem auf die Oracle-Installation vorbereitet. Diesen Patch erhalten Sie direkt von Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Beenden Sie das Programm, um zur Eingabeaufforderung für den Benutzer „oracle“ zurückzukehren.

```
exit
```

13. Wenn Sie Oracle 9.2.0.4 von der Disk1 installieren möchten, führen Sie folgendes Skript aus:

    ```
    ./runInstaller
    ```

14. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Bei der Aufforderung zum UNIX-Gruppennamen geben Sie Folgendes ein: dba
    - Für den Installationstyp wählen Sie „Benutzerdefiniert“.

    Wählen Sie folgende Komponenten für die Installation aus:
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
      - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
      - Oracle Net Listener 9.2.0.4.0
    - Oracle Enterprise Manager Products 9.2.0.1.0 (Alle)
    - Oracle 9i Development Kit 9.2.0.1.0 (Alle)
    - Oracle 9i für UNIX Dokumentation 9.2.0.1.0
    - Oracle HTTP Server 9.2.0.1.0 (Alle)
    - iSQL*Plus 9.2.0.4.0 (Alle)
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
15. Wenn Sie aufgefordert werden, eine Datenbank zu erstellen, wählen Sie „Nein“.
16. Optional können Sie alle Konfigurationsassistenten, die vom Installationsprogramm gestartet werden, abbrechen.
17. Ändern Sie die Datei /opt/oracle/network/admin/sqlnet.ora (oder erstellen Sie die Datei, wenn sie noch nicht vorhanden ist) damit Sie Folgendes enthält (entfernen Sie alle unkommentierten Informationen aus der Datei):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

18. Zum Anwenden des Oracle 9.2.0.6 oder 9.2.0.7 Patches für das Oracle-Installationsprogramm auf der Disk1 der Oracle 9.2.0.6 oder 9.2.0.7 Patch-Distribution führen Sie das Skript aus:

    HINWEIS: Der Oracle 9.2.0.6 Patch wird NICHT angewendet, wenn nicht zuerst das Oracle-Installationsprogramm gepatcht wird.

    ```
    ./runInstaller
    ```

19. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
    - Auf dem Bildschirm „Dateistandorte angeben“. Als Zielname wählen Sie *OUIHome* aus der Dropdown-Liste (oder den von Ihnen während der Installation von Oracle 9.2.0.4 angegebenen Zielnamen). Klicken Sie dann auf *Weiter*.
    - Wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option *Oracle Universal Installer 10.1.0.3.0*. Klicken Sie dann auf *Weiter*.

- Überprüfen Sie auf dem Bildschirm „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf *Installieren*.
- Am Ende des Installationsbildschirms klicken Sie auf *Beenden*.

20. Zum Anwenden des Oracle 9.2.0.6 oder 9.2.0.7 Patch für Oracle auf der Disk1 der Oracle 9.2.0.6 oder 9.2.0.7 Patch-Distribution führen Sie das Skript aus:

    ```
    ./runInstaller
    ```

21. Während des Fortschritts des Installationsprogramms lassen Sie alle Eingabeaufforderungen auf den Standardwerten, außer es ist im Folgenden anderweitig angegeben.
    - Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
    - Auf dem Bildschirm „Dateistandorte angeben“. Als Zielname wählen Sie „OUIHome“ aus der Dropdown-Liste (oder den von Ihnen während der Installation von Oracle 9.2.0.4 angegebenen Zielnamen). Klicken Sie dann auf *Weiter*.
    - Je nach Ihrer Version wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option *Oracle 9iR2 Patchset 9.2.0.6.0* oder *Oracle 9iR2 Patchset 9.2.0.7.0*. Klicken Sie dann auf *Weiter*.
    - Überprüfen Sie auf dem Bildschirm „Zusammenfassung“ die Installationszusammenfassung und klicken Sie dann auf *Installieren*.
    - Am Ende des Installationsbildschirms klicken Sie auf *Beenden*.
22. Unlink gcc:

    ```
    su - root
    rm /usr/bin/gcc
    rm /usr/bin/gcc
    ```

23. Beenden Sie das Programm, um zur Eingabeaufforderung für den Benutzer „oracle“ zurückzukehren.

    ```
    exit
    ```

Installation von Sentinel 5 für Oracle unter Linux

Sentinel 5 unterstützt zwei Installationstypen. Hierbei handelt es sich um:

- Einfach – Die Option zur All-in-One-Installation. Sentinel-Services, Collector-Service und Anwendungen mit Oracle auf demselben Computer. Dieser Installationstyp dient lediglich zu Demonstrationszwecken.
- Benutzerdefiniert – Ermöglicht eine vollständig verteilte Installation.

Einfache Installation unter Linux

Bei dieser Installation werden die allgemeinen Komponenten auf einem einzigen Computer installiert (kein Collector Builder und keine Drittanbieter-Integrationsfunktionen). Dies dient vorrangig zu Demonstrationszwecken. Für Test- bzw. Produktionszwecke nicht empfohlen.

HINWEIS: Bei der einfachen Installation wird die Collector Manager-Passwortauthentifizierung nicht unterstützt.

So führen Sie eine einfache Installation durch

1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für Oracle die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Überprüfen Sie die Solaris Oracle-Einrichtung.
3. Melden Sie sich als Benutzer „root“ an.
4. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
5. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   Für GUI-Modus:

   ```
   ./setup.sh
   ```

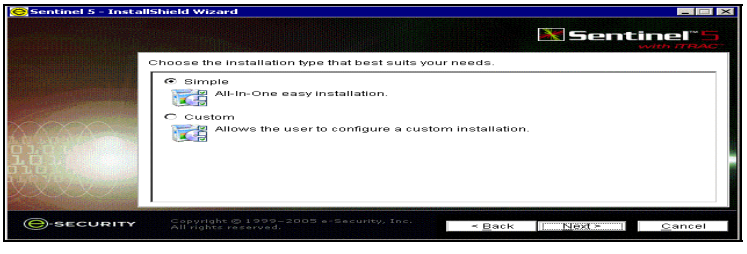
   oder

   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```

6. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
7. Folgen Sie den Eingabeaufforderungen des Installationsprogramms.
8. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
9. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
10. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.

11. Wählen Sie *Einfach* aus. Klicken Sie auf *Weiter*.



12. Geben Sie Ihre Konfigurationsinformationen ein.
    - Seriennummer und Lizenzschlüssel
    - SMTP-Server (entweder DNS-Name oder IP-Adresse) – sofern Sentinel in der Lage sein soll, Emails zu versenden
    - Email – Geben Sie eine gültige Email-Adresse ein, über die Advisor-Benachrichtigungs-Emails gesendet werden sollen (z. B. Sent_Server@myserver.com).
    - Globales Systempasswort – Geben Sie ein Passwort und dasselbe Passwort nochmal zur Bestätigung ein. Dieses Passwort wird für alle Standardbenutzer verwendet. Dazu gehören sowohl der Benutzer des esecadm-Betriebssystems als auch die Datenbankbenutzer. Eine Liste der Standard-Datenbankbenutzer, die während der Installation erstellt werden, finden Sie unter Sentinel-Datenbank im Abschnitt Vor der Installation von Sentinel 5 für Oracle.
    - Datenverzeichnis – der Speicherort für Ihre Datenbankdateien. Um den Standard-Speicherort zu ändern, klicken Sie auf die Schaltfläche „...“ und wählen Sie den gewünschten Speicherort aus. Standardmäßig ist das $ESEC_HOME/data.

    HINWEIS: Der Benutzer „oracle“ muss über eine Schreibberechtigung für das Datenverzeichnis verfügen. Das erzielen Sie, indem Sie den folgenden Befehl als Benutzer „root“ ausführen:

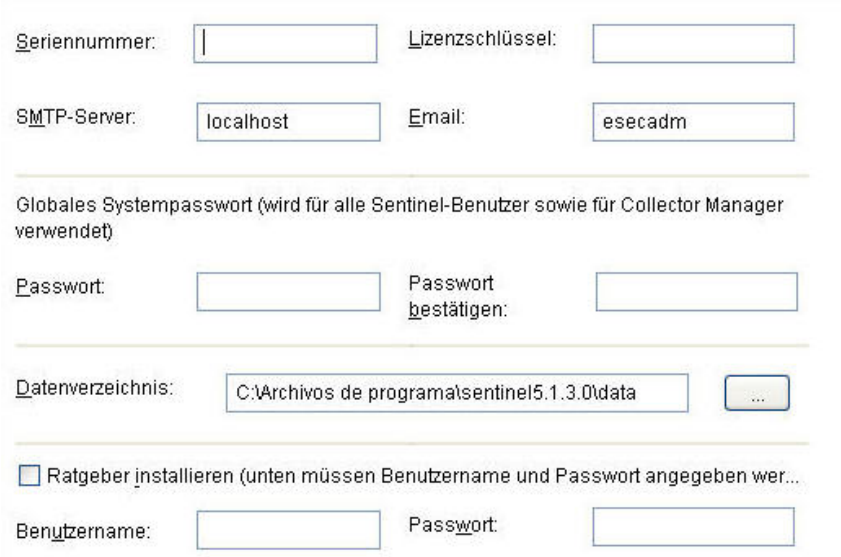
    ```
    chown –R oracle:dba <Verzeichnispfad>
    chmod –R 770 <Verzeichnispfad>
    ```

    Dabei wird davon ausgegangen, dass „oracle“ Ihr Oracle-Benutzername und „dba“ Ihr Oracle-Gruppenname ist.

    HINWEIS: Sofern Advisor installiert wird, konfiguriert die einfache Installation Advisor für die Verwendung von „Direktes Herunterladen vom Internet“ mit einem Aktualisierungsintervall von 12 Stunden und unter Aktivierung aller Email-Benachrichtigungen.

    - Wählen Sie zur Installation von Advisor die Option *Advisor installieren*. Geben Sie einen Benutzernamen und ein Passwort ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.

    Klicken Sie auf *Weiter*.



13. Geben Sie Ihre Datenbank-Konfigurationsinformationen ein.
    - Datenbankname – Der Name der Oracle-Datenbankinstanz zum Erstellen und Installieren von Sentinel-Datenbankobjekten. Es darf keine Datenbank mit diesem Namen existieren.
    - Oracle JDBC-Treiberdatei. Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).

14. Bestätigen Sie den Oracle-Standardbenutzernamen, indem Sie auf *OK* klicken.

15. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation müssen Sie das System neu starten.

HINWEIS: Wenn Sie Drittanbieter-Integrationssoftware (HP Service Desk oder Remedy Integration) installieren möchten, führen Sie nach dem erneuten Booten Ihres Computers das Installationsprogramm erneut aus und wählen Sie die gewünschte Drittanbieter-Integrationssoftware aus. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration*.

---

16. Das Sentinel-Installationsprogramm deaktiviert standardmäßig die Archivprotokollierung. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank keine Ereignisse mehr entgegen.

Benutzerdefinierte Installation unter Linux

So führen Sie eine benutzerdefinierte Installation durch

1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für Oracle die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Überprüfen Sie die Solaris Oracle-Einrichtung.
3. Melden Sie sich als Benutzer „root“ an.
4. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
5. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   Für GUI-Modus:

   ```
   ./setup.sh
   ```

   oder

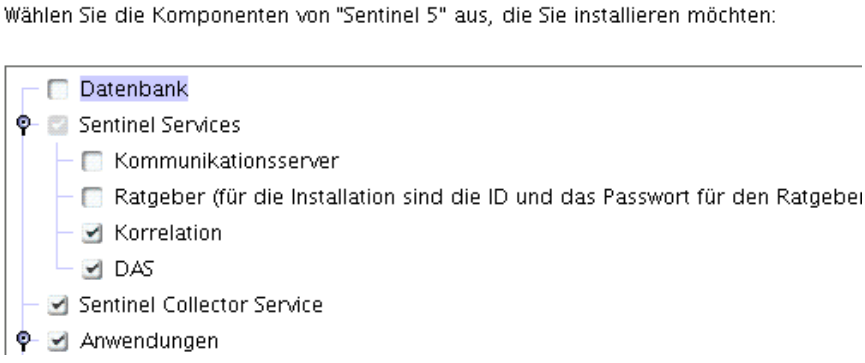
   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```

6. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
7. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
8. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
9. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.

10. Wählen Sie *Benutzerdefiniert* (Standard). Klicken Sie auf *Weiter*.
11. Wählen Sie die zu installierenden Funktionen aus.

HINWEIS: Weitere Informationen darüber, welche Komponenten bei verschiedenen Konfigurationen an welchem Ort installiert werden können, finden Sie in *Kapitel 1, Systemanforderungen*.



Folgende Optionen stehen zur Verfügung:

- Datenbank – installiert die Sentinel-Datenbank
- Kommunikationsserver – installiert den Nachrichtenbus (iSCALE)
- Advisor
- Correlation Engine
- DAS
- Collector-Service
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk**
- Remedy Integration**

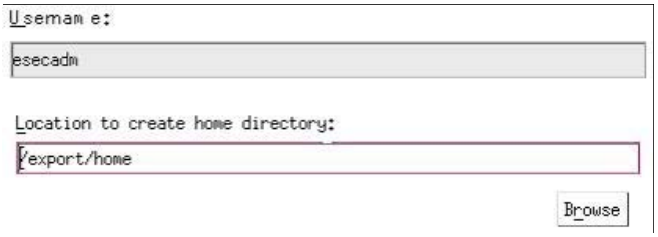
HINWEIS: **Informationen zur Installation von HP OpenView Service Desk bzw. von Remedy Integration finden Sie im *Handbuch für Drittanbieter-Integration*.

HINWEIS: Wenn keines der untergeordneten Funktionen von „Sentinel Services“ ausgewählt wurde, müssen Sie auch die Funktion „Sentinel Services“ selbst deaktivieren. Sie wird abgeblendet mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.

HINWEIS: Als Teil der Installation der Sentinel-Datenbank legt das Installationsprogramm Dateien im Ordner $ESEC_HOME/utilities/db ab.

---

12. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, werden Sie zur Eingabe folgender Informationen aufgefordert:
    - Seriennummer
    - Lizenzschlüssel
13. Wenn Sie ausgewählt haben, dass Drittanbieter-Integrationskomponenten installiert werden sollen, werden Sie aufgefordert, ein Passwort einzugeben, um die ausgewählten Drittanbieter-Integrationskomponenten zu entsperren. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration.*
14. Geben Sie den Benutzernamen des Betriebssystem-Sentinel-Administrators ein und den Standort seines Basisverzeichnisses. Das ist der Name des Benutzers, dem das installierte Sentinel-Produkt gehört. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem Basisverzeichnis im angegebenen Verzeichnis erstellt.
    - Benutzername des Betriebssystem-Administrators – Standardmäßig „esecadm“
    - Basisverzeichnis des Betriebssystem-Administrators – Standardmäßig /export/home. Wenn der Benutzername „esecadm“ lautet, ist das dazugehörige Basisverzeichnis /export/home/esecadm.



HINWEIS: Wird ein neuer Benutzer erstellt, muss sein Passwort manuell eingerichtet werden und nicht innerhalb dieses Installationsprogramms. Sentinel empfiehlt, dass Sie dies sofort durch Anmelden beim System nach der Installation des Produkts vornehmen.

Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (#$_) und eine Zahl (0-9) enthalten. Verwenden Sie keine Leerzeichen.

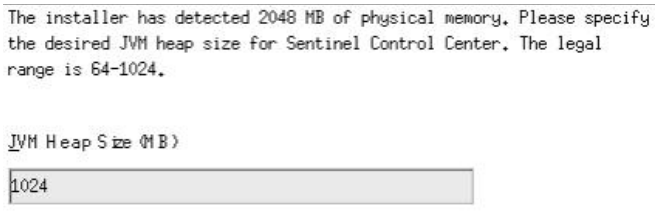
2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches, umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zum Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können, und das dennoch komplex ist. Beispiel: MSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).

15. Wenn Sie ausgewählt haben, dass Sentinel Control Center installiert werden soll, wird eine JVM-(Java Virtual Machine)-Heap-Größe angezeigt:
    - JVM-Heap-Größe (MB) – Standardmäßig ist dieser Wert auf die Hälfte der Größe des auf dem Computer gefundenen physischen Arbeitsspeichers eingestellt (maximal 1.024 MB). Dies ist die maximal von Sentinel Control Center verwendete JVM-Heap-Größe.



16. Wenn Sie ausgewählt haben, dass der Collector-Service installiert werden soll, müssen Sie festlegen, ob Wizard Collector Manager durch ein Passwort geschützt werden soll oder nicht. Wenn Sie festgelegt haben, dass der Wizard Collector Manager geschützt werden soll, werden Sie aufgefordert, ein Wizard Collector Manager-Passwort zu erstellen.

HINWEIS: Um eine Wizard Collector-Instanz durch ein Passwort zu schützen, müssen Sie dieses Passwort beim Herauf- und Herunterladen sowie bei der Fehlersuche für Collectors im betreffenden Wizard Collector Manager angeben. Dieses Passwort und der Sentinel-Benutzername und das Passwort werden für die Anmeldung bei Wizard Collector Builder benötigt.

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

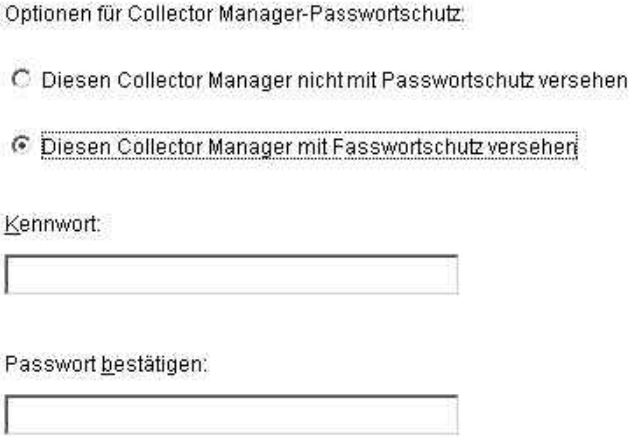
1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (!@#$%^&*()_+) und eine Zahl (0-9) enthalten.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

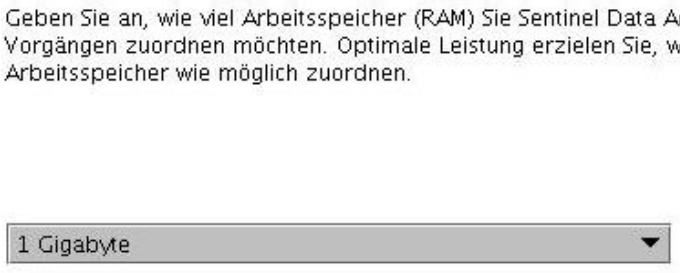
3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches, umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zum Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können, und das dennoch komplex ist. Beispiel: mSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe sei 5 Jahren in Köln).



17. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, legen Sie fest, wie viel RAM in Ihrem System für Data Access Service zur Verfügung gestellt werden soll. Für verteilte Umgebungen sollten Sie die Höchstmenge an Arbeitsspeicher (4 GB) auswählen. Für Einzelplatzumgebungen wird die Hälfte des RAM-Speichers empfohlen.



18. Bei der Datenbankinstallation werden folgende Eingabeaufforderungen angezeigt:
    a. Wählen Sie die Serverplattform der Zieldatenbank, Oracle 9i, und eines der folgenden Elemente aus:
        - Neue Datenbank mit Datenbankobjekten erstellen – erstellt eine neue Oracle-Datenbankinstanz und füllt die neue Instanz mit Datenbankobjekten
        - Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen – fügt nur Datenbankobjekte zu einer bestehenden Oracle-Datenbankinstanz hinzu. Wenn Sie eine vorhandene Oracle-Datenbankinstanz verwenden, muss diese bis auf die Präsenz des esecdba-Benutzers leer sein.
    b. Geben Sie das Verzeichnis für das Datenbankinstallationsprotokoll ein (Standard: $ESEC_HOME/logs/db). Übernehmen Sie den Standardwert für „Verzeichnis für das Protokoll der Datenbankinstallation“ oder klicken Sie auf *Durchsuchen*, um einen anderen Speicherort anzugeben.

    c. Bestätigen Sie den Oracle-Standardbenutzernamen, indem Sie auf *OK* klicken.

d. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Folgendes ein:

- Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
- Hostname – Der Hostname des Computers für die Installation der Datenbank. Dieses Feld lässt sich nicht konfigurieren, wenn Sie eine neue Datenbankinstanz erstellen.
- Datenbankname – Der Name der zu installierenden Datenbankinstanz.

e. Wenn Sie einer vorhandenen leeren Oracle-Datenbank Datenbankobjekte hinzufügen, werden Sie um die folgenden Informationen gebeten.

- Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
- Datenbank-Hostname oder IP-Adresse – Der Name oder die IP-Adresse des Host mit der Oracle-Datenbank, der Sie Datenbankobjekte hinzufügen möchten. Das kann der lokale Hostname oder ein Remote-Hostname sein.
- Datenbankname – Der Name der bestehenden leeren Oracle-Datenbankinstanz, zu der Datenbankobjekte hinzugefügt werden sollen (standardmäßig ESEC). Dieser Datenbankname muss als Servicename in der Datei tnsnames.ora (im Verzeichnis $ORACLE_HOME/network/admin/) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, enthalten sein.

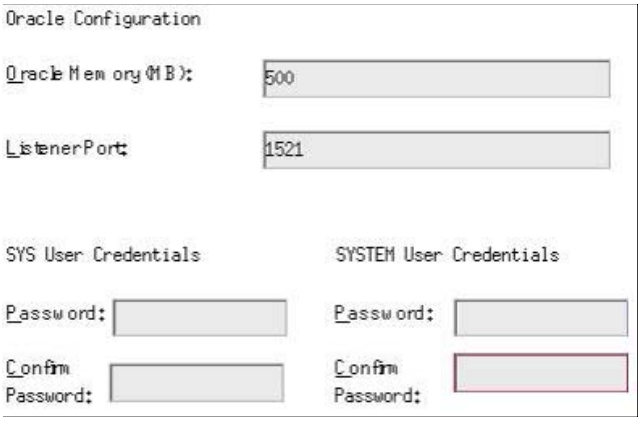
HINWEIS: Wenn der Datenbankname nicht in der Datei tnsnames.ora enthalten ist, gibt das Installationsprogramm zu diesem Zeitpunkt in der Installation keinen Fehler aus (weil es die Verbindung über eine direkte JDBC-Verbindung überprüft). Die Datenbankinstallation scheitert erst dann, wenn das Datenbankinstallationsprogramm versucht, die Verbindung mit der Datenbank über sqlplus herzustellen. Wenn die Datenbankinstallation zu diesem Zeitpunkt scheitert, sollten Sie –ohne das Installationsprogramm zu beenden– den Service-Namen für die Datenbank in der Datei tnsnames.ora auf dem betreffenden Computer ändern, im Installationsprogramm zum ersten Bildschirm zurückblättern und dann den Vorgang erneut durchführen. Dadurch wird versucht, die Datenbankinstallation mit den neuen Werten in der Datei tnsnames.ora durchzuführen.

- Datenbank-Port (Standard: 1521)

- Geben Sie für Sentinel-Datenbankadministratoren (DBA) das Passwort für den Benutzer „esecdba“ ein. Das Benutzernamenfeld in dieser Eingabeaufforderung lässt sich nicht bearbeiten.

f. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, sehen Sie die folgende Eingabeaufforderung:

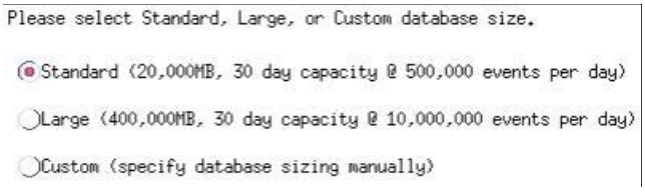
- Oracle-Speicher (MB) – Die Menge RAM, die dieser Oracle-Datenbankinstanz zugeordnet wird.
- Listener Port – Der Port, an dem der Oracle-Listener erstellt werden soll (standardmäßig 1521).
- SYS-Benutzerpasswort und Passwortbestätigung – SYS ist ein Oracle-Standardbenutzer, der in der neuen Datenbankinstanz erstellt wird. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.
- SYSTEM-Benutzerpasswort und Passwortbestätigung – SYSTEM ist ein Oracle-Standardbenutzer, der in der neuen Datenbankinstanz erstellt wird. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.



g. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, die Größe der Datenbank einzugeben. Es stehen folgende Optionen zur Auswahl:

- Standard (20 GB)
- Groß (400 GB)

- Benutzerdefiniert (manuelle Größenfestlegung). Wenn Sie diese Option ausgewählt haben, werden Sie zur Eingabe folgender Informationen aufgefordert:
  - Ursprüngliche Größe der einzelnen Datenbankdateien in MB (100–10.000)
  - Maximale Größe der einzelnen Datenbankdateien in MB (2.000–100.000)
  - Größe aller Datenbankdateien in MB (7.000–2.000.000)
  - Größe der einzelnen Protokolldateien in MB (100–100.000)



h. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, den Speicherort für folgende Datenbankdateien einzugeben:

HINWEIS: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung sollten diese Speicherorte auf unterschiedlichen E/A-Geräten liegen.

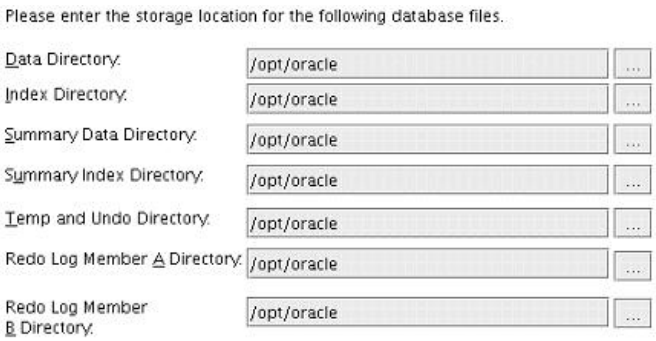
Diese Verzeichnisse werden nicht vom Installationsprogramm erstellt. Sie müssen also extern erstellt werden, um mit dem nächsten Schritt fortfahren zu können.

Der Oracle-Benutzer muss über eine Schreibberechtigung für diese Verzeichnisse verfügen. Um dem Oracle-Benutzer eine Schreibberechtigung für diese Verzeichnisse zu gewähren, führen Sie als Benutzer „root“ folgende Befehle für die einzelnen Verzeichnisse aus:

```
chown –R oracle:dba <Verzeichnispfad>
chmod –R 770 <Verzeichnispfad>
```

Dabei wird davon ausgegangen, dass „oracle“ Ihr Oracle-Benutzername und „dba“ Ihr Oracle-Gruppenname ist.

- Datenverzeichnis
- Indexverzeichnis
- Zusammenfassungsdatenverzeichnis
- Zusammenfassungsindexverzeichnis
- Temporäres Verzeichnis und Tabellenbereichsverzeichnis zum Rückgängigmachen
- Verzeichnis für Redo-Protokollmitglied A
- Verzeichnis für Redo-Protokollmitglied B



i. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Authentifizierungsinformationen für den Sentinel Database Administrator (DBA) ein. Hierbei handelt es sich um „esecdba“, den Eigentümer der Datenbankobjekte.

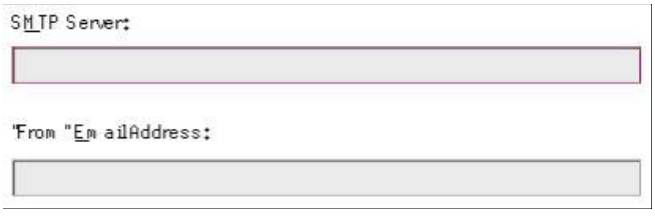
j. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Anwendungsdatenbank ein. Hierbei handelt es sich um „esecapp“, den Benutzernamen für die Sentinel-Anwendung, den die Sentinel-Prozesse verwenden, um eine Verbindung zu der Datenbank herzustellen.

k. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Administratordatenbank ein. Hierbei handelt es sich um „esecadm“, den Sentinel-Administratorbenutzer.

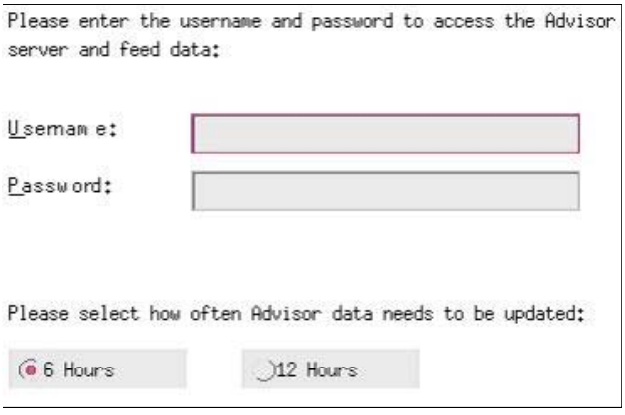
l. Klicken Sie im Zusammenfassungsfenster für die Datenbankinstallation auf *Weiter*.

19. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, nicht jedoch, dass die Sentinel-Datenbank installiert werden soll, werden Sie aufgefordert, folgende Informationen für die Oracle Sentinel-Datenbank einzugeben. Diese Informationen werden verwendet, um DAS so zu konfigurieren, dass es auf die Sentinel-Datenbank verweist.
    - Datenbank-Hostname oder IP-Adresse – Der Name oder die IP-Adresse der bestehenden Oracle Sentinel-Datenbank, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten.
    - Datenbankname – Der Name der bestehenden leeren Oracle-Datenbankinstanz, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten (standardmäßig ESEC).
    - Datenbank-Port (Standard: 1521)
    - Geben Sie für den Sentinel-Anwendungsdatenbankbenutzer den Anmeldenamen „esecapp“ an und geben Sie das Passwort ein, das während der Installation der Sentinel-Datenbank für den Benutzer festgelegt wurde.

20. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, müssen Sie Email-Unterstützung für Sentinel konfigurieren. Geben Sie den SMTP-Server und die Email-Absenderadresse ein, die Execution Service beim Versenden von Nachrichten verwenden soll (optional – dieser Wert kann nach der Installation manuell geändert werden [$ESEC_HOME\sentinel\config\execution.properties]):



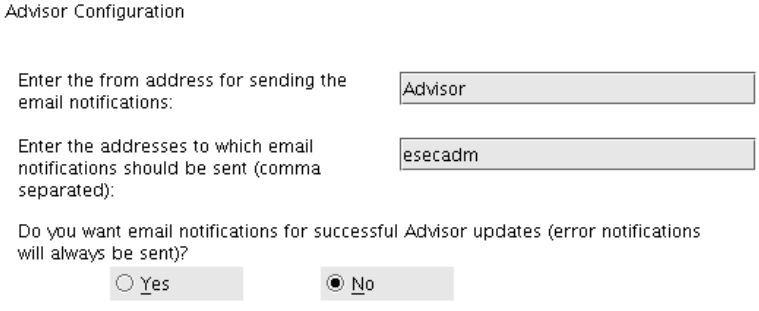
21. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, müssen Sie den Installationstyp auswählen (falls die Advisor-Option gewählt wurde, einen Benutzernamen und ein Passwort eingeben)
    - Direktes Herunterladen vom Internet – Der Advisor-Computer ist direkt mit dem Internet verbunden. In dieser Konfiguration werden regelmäßig automatisch Aktualisierungen von Sentinel über das Internet heruntergeladen.
    - Einzelplatz – Advisor ist als isoliertes System konfiguriert, in das manuell eingegriffen werden muss, um eine Aktualisierung von Sentinel zu empfangen.
22. Wenn Sie ausgewählt haben, dass Advisor installiert werden und „Direktes Herunterladen vom Internet“ verwendet werden soll, geben Sie Ihren Advisor-Benutzernamen, Ihr Passwort und die gewünschte Aktualisierungshäufigkeit für die Advisor-Daten ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.



23. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, geben Sie Folgendes ein:
    - Der Absender, der in Email-Benachrichtigungen angezeigt wird
    - Die Empfängeradresse zum Senden von Email-Benachrichtigungen

    HINWEIS: Nach der Installation können Sie die Advisor-Email-Adressen ändern, indem Sie die Dateien attackcontainer.xml und alertcontainer.xml im Verzeichnis $ESEC_HOME/sentinel/config directory bearbeiten. Weitere Informationen finden Sie in *Kapitel 7 – Registerkarte „Advisor“ – im Sentinel-Benutzerhandbuch.*

    - Wählen Sie aus, ob Sie per Email über erfolgreiche Advisor-Akutalisierungen benachrichtigt werden möchten. Fehlerbenachrichtigungen werden immer gesendet.



24. Wenn Sie ausgewählt haben, dass HP Service Desk oder Remedy Integration installiert werden soll, werden Sie zur Eingabe weiterer Informationen aufgefordert. Weitere Informationen finden Sie im *Sentinel-Handbuch für Drittanbieter-Integration*.
25. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten. Klicken Sie auf *Fertig stellen*, um das System neu zu booten.
26. Das Sentinel-Installationsprogramm deaktiviert standardmäßig die Archivprotokollierung. Zum Zwecke der Datenbankwiederherstellung sollten Sie unbedingt nach der Installation und vor dem Eingang der Ereignisdaten für die Produktion die Archivprotokollierung aktivieren. Außerdem sollten Sie die Sicherung der Archivprotokolle regelmäßig einplanen, um Speicher am Zielort Ihres Archivprotokolls freizugeben. Anderenfalls nimmt die Datenbank keine Ereignisse mehr entgegen.

27. Wenn Sie eine hohe Ereignisrate (mehr als 500 Ereignisse pro Sekunde) erwarten, müssen Sie die zusätzlichen Konfigurationsanweisungen in Abschnitt Einrichten der OCI-Strategie (Oracle Call Interface) zum Einfügen von Ereignissen befolgen.

Installation von Sentinel Control Center und Collector Builder unter Windows:

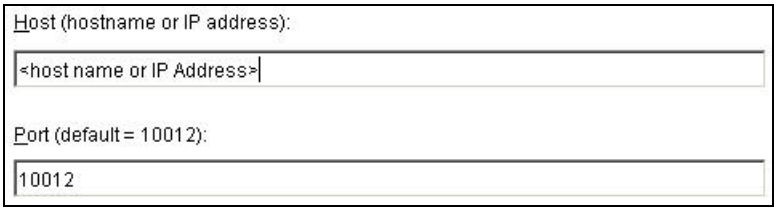
Installation von Sentinel Control Center und Collector Builder unter Windows:

1. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
2. Wechseln Sie zu der CD und doppelklicken Sie auf *setup.bat*.

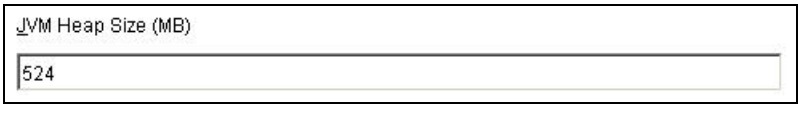
HINWEIS: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.

3. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
4. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
5. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Next* (Weiter).

6. Wählen Sie die zu installierenden Funktionen aus.
7. Geben Sie die Host-Adresse und den Port an, an dem der Kommunikationsserver installiert ist.



8. Wenn Sie ausgewählt haben, dass Sentinel Control Center installiert werden soll, wird eine JVM-(Java Virtual Machine)-Eingabeaufforderung angezeigt:
   - JVM-Heap-Größe (MB) – Standardmäßig ist dieser Wert auf die Hälfte der Größe des auf dem Computer gefundenen physischen Arbeitsspeichers eingestellt (maximal 1.024 MB). Dies ist die maximal von Sentinel Control Center verwendete JVM-Heap-Größe.



   Klicken Sie auf *Weiter*.
9. Klicken Sie auf *Installieren*.
10. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Klicken Sie auf *Fertig stellen*.

Nach der Installation von Sentinel 5 für Oracle

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter $ESEC_HOME/sentinel/config. Um diese Datei zu konfigurieren, führen Sie mailconfig.sh aus, um die Datei zu ändern, und mailconfigtest.sh, um Ihre Änderungen zu testen.

So konfigurieren Sie Ihre execution.properties-Datei

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

   ```
   ./mailconfig.sh -host <SMTP Server> -from <source email
      address> -user <mail authentication user> –password
   ```

   Beispiel:

   ```
   ./mailconfig.sh -host 10.0.1.14 -from my_name@domain.com
      -user my_user_name –password
   ```

   Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

   ```
   Enter your password:*********
   Confirm your password:*********
   ```

   HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfigtest“ wie folgt aus:

   ```
   ./mailconfigtest.sh -to <Ziel-E-Mail-Adresse>
   ```

   Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

   ```
   Email has been sent successfully!
   ```

   Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

   ```
   Subject: Testing Sentinel mail property
   This is a test for Sentinel mail property set up. If you
      see this message, your Sentinel mail property has been
      configured correctly to send emails
   ```

Sentinel-Datenbank

Nach der Installation der Sentinel-Databank enthält die Datenbank folgende Standardbenutzer:

- esecdba – Eigentümer des Datenbankschemas. Aufgrund von Sicherheitsbeschränkungen wird „esecdba“ keine DBA-Berechtigung gewährt. Erstellen Sie zur Verwendung von Enterprise Manager einen Benutzer mit DBA-Berechtigungen.
- esecapp – Datenbankanwendungsbenutzer. Das ist der Anwendungsbenutzer für die Verbindung mit der Datenbank.
- esecadm – Hierbei handelt es sich um den Datenbankbenutzer, der der Sentinel-Administrator ist. Das ist nicht dasselbe Benutzerkonto, wie der Betriebssystembenutzer „esecadm“.
- esecrpt - Datenbankreport-Benutzer
- SYS – SYS-Datenbankbenutzer
- SYSTEM – SYSTEM-Datenbankbenutzer

Collector-Service

Während der Installation des Collector-Service werden folgende Collectors installiert und für jeden wird ein Collector-Port eingerichtet, um ihn auszuführen.

Produkt	**Collector-Name**
Demo-Collectors	
Führt Tests für das Hochladen von Beständen durch, arbeitet mit dem DemoEvents-Collector	DemoAssetUpload
Führt Tests für Demo-Ereignisse durch, arbeitet mit DemoAssetUpload- und DemoVulnerabilityUpload-Collector	DemoEvents
Führt Tests für das Heraufladen von Anfälligkeiten durch, arbeitet mit dem DemoEvents-Collector	DemoVulnerabilityUpload
Test für das Senden eines Ereignisses	SendOneEvent
Test für das Senden mehrerer Ereignisse	SendMultipleEvents

HINWEIS: Weitere Informationen zur Konfiguration der Demo-Collectors finden Sie in *Kapitel 12, Testen der Installation.*

HINWEIS: Weitere Collectors erhalten Sie vom Sentinel-Kundenportal im neusten Service Pack für die von Ihnen installierte Version. Der neuste Service Pack für Ihre Release enthält einen vollständigen Satz der neusten Collectors für die von Ihnen verwendete Sentinel-Version.

Weitere Informationen (auch zur Konfiguration) finden Sie in der Dokumentation zu den einzelnen Collectors in:

$WORKBENCH_HOME/Elements/<Collector-Name>/Docs/

Zur Installation weiterer Collectors führen Sie das Service Pack-Skript auf der Service Pack-CD aus. Das Skript installiert die Collectors lokal.

Unter Windows:

.\service_pack.bat

Unter UNIX:

./service_pack.sh

Installationsanweisungen für das Service Pack und eine Liste der Collectors finden Sie in den *Service Pack-Versionshinweisen.*

Aktualisieren des Lizenzschlüssels

Aktualisieren Ihres Lizenzschlüssels (Linux)

1. Melden Sie sich als Benutzer „esecadm“ an.
2. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
3. Wechseln Sie zum Verzeichnis disk1/utilities/linux.
4. Geben Sie den folgenden Befehl ein:

   ```
   ./softwarekey
   ```

5. Geben Sie die Ziffer 1 ein, um den Primärschlüssel anzugeben. Drücken Sie die EINGABETASTE.

Erstellen einer Oracle-Instanz für die Sentinel-Datenbank

HINWEIS: Dieses Verfahren dient als Beispiel, wenn Sie, statt die Funktion zur Tabellenbereichserstellung auf der Installations-CD zu nutzen, Ihre eigenen Tabellenbereiche erstellen möchten. Die Größenwerte können je nach Systemkonfiguration und Anforderungen variieren. Die Tabellenbereiche müssen genau wie unten angegeben benannt werden.

In der Oracle-Instanz müssen Sie folgende Elemente konfigurieren:

- Parameter
- „Tablespaces“ (Tabellenbereiche)

Erstellen einer Oracle-Instanz

1. Melden Sie sich als Oracle-Benutzer an.
2. Verwenden Sie den Oracle-Datenbankassistenten und erstellen Sie Folgendes:

HINWEIS: Die Werte können je nach Systemkonfiguration und Anforderungen variieren.

Empfohlene Mindestwerte für die Linux-Konfigurationsparameter	
Parameter	**Größe (in Byte, wenn nicht anders angegeben)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500

Empfohlene Mindestwerte für die Linux-Konfigurationsparameter	
Parameter	**Größe (in Byte, wenn nicht anders angegeben)**
cursor_sharing	SIMILAR
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Empfohlene Mindestgröße für den Linux-Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
REDO	3 x 100 M	Dies ist ein Mindestwert. Bei einem hohen EPS-Wert sollten größere Redo-Protokolle erstellt werden.
SYSTEM	500 M	Mindestwert
TEMP	1 G	Mindestwert
UNDO	1 G	Mindestwert
ESENTD	5 G	Mindestwert Für Ereignisdaten
ESENTD2	500 M	Mindestwert Daten für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
ESENTWFD	250 M	Für iTrac-Daten (autoextend aktiviert)
ESENTWFX	250 M	Für iTrac-Index (autoextend aktiviert)
ESENTX	3 G	Mindestwert Für Ereignisindex
ESENTX2	500 M	Mindestwert Index für Konfiguration, Bestände, Anfälligkeit und Verknüpfungen (autoextend aktiviert)
SENT_ADVISORD	200 M	Mindestwert Für Advisor-Daten (autoextend aktiviert)
SENT_ADVISORX	100 M	Mindestwert Für Advisor-Index (autoextend aktiviert)
SENT_LOBS	100 M	Mindestwert Für große Datenbankobjekte (autoextend aktiviert)
SENT_SMRYD	3 G	Mindestwert Für die Aggregation, Zusammenfassungsdaten
SENT_SMRYX	2 G	Mindestwert Für die Aggregation, Zusammenfassungsindex

3. Führen Sie das Skript createEsecdba.sh aus dem Verzeichnis „sentinel\dbsetup\bin“ auf der Sentinel-Installations-CD aus. Dieses Skript erstellt den Benutzer „esecdba“, der für das Hinzufügen von Datenbankobjekten mit dem Sentinel-Installationsprogramm erforderlich ist.
4. Sichern Sie die Datenbank.

Einrichten der OCI-Strategie (Oracle Call Interface) zum Einfügen von Ereignissen

Sentinel 5.1 bietet einen Rahmen zur Integration verschiedener Strategien zum Einfügen von Ereignissen in die Datenbank. Sentinel 5.1 bietet zwei Strategien zum Einfügen von Ereignissen in die Oracle-Datenbank:

- JDBCLoadStrategy
- OCILoadStrategy

Die zum Einfügen von Ereignissen zu verwendende Strategie richtet sich nach der Eigenschaft insert.strategy der Komponente EventStoreService in das_binary.xml.

Die JDBC-Strategie ist die Standardstrategie, die bereits vorkonfiguriert ist.

Die OCI-Strategie ist eine native Einfügestrategie für das schnellere Einfügen von Ereignissen. Bei dieser Strategie ist es erforderlich, dass die Oracle OCI-Bibliotheken auf dem Computer installiert werden, auf dem die DAS-Komponente ausgeführt wird. Die OCI-Strategie muss bei Konfigurationen verwendet werden, bei denen eine hohe Ereignisrate erwartet wird.

Die Anzahl der zum Einfügen in einer Gruppe zusammenzufassenden Ereignisse wird durch die Eigenschaft insert.batchsize festgelegt. Die Eigenschaft insert.batchsize wird von allen Strategien zum Einfügen von Ereignissen verwendet.

Um die von Sentinel verwendete Strategie zum Einfügen von Ereignissen von der standardmäßig verwendeten JDBC-Einfügestrategie zur OCI-Einfügestrategie zu ändern, müssen einige Schritte durchgeführt werden.

Wechsel von der JDBC-Einfügestrategie zur OCI-Einfügestrategie

1. Stellen Sie sicher, dass die Oracle OCI-Bibliotheken auf dem Computer installiert werden, auf dem die Sentinel-DAS-Komponente ausgeführt wird. Sie müssen für die folgenden Schritte den Pfad zu ORACLE_HOME kennen.
2. Melden Sie sich beim Computer ab Schritt 1 als Benutzer „esecadm“ an.
3. Erstellen Sie im Basisverzeichnis von „esecadm“ die Datei „.bash_profile“. Fügen Sie in diese Datei den folgenden Text ein (passen Sie den Pfad für ORACLE_HOME an Ihre Installation an):

   ```
   ORACLE_HOME=/build/home/oracle/OraHome
   export ORACLE_HOME
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   export LD_LIBRARY_PATH
   ```

4. Öffnen Sie die Datei $ESEC_HOME/sentinel/config/das_binary.xml in einem beliebigen Texteditor.
5. Führen Sie eine Suche nach folgendem Text durch:

   ```
   JDBCLoadStrategy
   ```

6. Ändern Sie diesen Text in:

   ```
   OCILoadStrategy
   ```

7. Speichern Sie diese Änderung in der Datei das_binary.xml.

8. Starten Sie die DAS-Binäranwendung neu. (Der Neustart der DAS-Binäranwendung wird am einfachsten durchgeführt, indem Sie „ps –ef | grep DAS_Binary“ ausführen, um die Prozess-ID zu erhalten, diesen Prozess anschließend mit „kill“ zu beenden und ihn dann automatisch von Sentinel Watchdog neu starten zu lassen.)

   Sobald die DAS-Binäranwendung neu gestartet wurde, wird die Bibliothek $ESEC_HOME/sentinel/lib/libocievent.so geladen und zum Einfügen der Ereignisse in die Datenbank über OCI verwendet.

Zusätzliche Optionen zum Einfügen von Ereignissen mit OCI

Zusätzlich zur Angabe von „OCILoadStrategy“ in der Datei das_binary.xml gibt es einige andere OCI-Optionen, die ebenfalls konfiguriert werden können.

- insert.batchsize – Mit dieser Einstellung können Sie die maximale Anzahl der Ereignisse festlegen, die gleichzeitig in die Datenbank aufgenommen werden.
- insert.oci.workerCount – Diese Einstellung legt die Anzahl der Threads fest, die verwendet werden, um Ereignisdaten in die Datenbank einzufügen.
- insert.oci.queueWaitTime – Diese Einstellung legt die maximale Zeitspanne in Sekunden fest, die gewartet wird, bevor die Daten aus der eingehenden Warteschlange in die Datenbank aufgenommen werden. Sobald eine vollständige Stapelanzahl („batchsize“) von Ereignissen empfangen wird, wird der gesamte Stapel eingefügt. Aber wenn der eingehende Ereignisfluss langsam ist, bestimmt die Zeit in der Warteschlange, wann sie in die Datenbank eingefügt werden (auch wenn die Stapelanzahl noch nicht erreicht wurde).
- insert.oci.highWatermark – Die obere Grenze der eingehenden Ereignisse.
- insert.oci.lowWatermark – Die untere Grenze der eingehenden Ereignisse.
- insert.oci.optimizationFlag – Optimierungsflagge. „Ein“ oder „Aus“.

Tipps für die OCI-Fehlersuche

Die OCI-Schnittstelle protokolliert Fehlermeldungen ausschließlich in der Datei $ESEC_HOME/sentinel/log/ocievent.log. Anfängliche Meldungen, die in die Protokolldatei geschrieben werden, sollten erfolgreiche (oder fehlgeschlagene) Datenbankverbindungsmeldungen enthalten... Damit können Sie überprüfen, ob die OCI-Bibliothek geladen und korrekt konfiguriert wurde.

Die OCI-Schnittstelle protokolliert auch Fehler in der Protokolldatei das_binary im Verzeichnis $ESEC_HOME/sentinel/log. Zu den in der Protokolldatei das_binary protokollierten Fehlern gehören Fehler beim Auffinden/Laden der Bibliothek libocievent.so, Fehler bei der Herstellung einer Verbindung mit der Datenbank und Fehler beim Einfügen von Ereignissen/Ereignisverknüpfungen.

Wenn die Fehlermeldungen angeben, dass die Datei libocievent.so nicht auffindbar oder geladen ist, müssen Sie drei Dinge überprüfen:

1. Vergewissern Sie sich, dass die Oracle-OCI-Bibliotheken installiert sind.
2. Vergewissern Sie sich, dass sich die Datei libocievent.so im Verzeichnis $ESEC_HOME/sentinel/lib befindet.
3. Vergewissern Sie sich, dass sich das Verzeichnis $ESEC_HOME/sentinel/lib in LD_LIBRARY_PATH des Benutzers „esecadm“ befindet. Falls nicht, können Sie LD_LIBRARY_PATH im Benutzerprofil von „esecadm“ aktualisieren.
4. Vergewissern Sie sich, dass die Umgebungsvariablen ORACLE_HOME und LD_LIBRARY_PATH in den Umgebungsvariablen des Benutzers „esecadm“ entsprechend aktualisiert wurden, wie im Abschnitt „Wechsel von der JDBC-Einfügestrategie zur OCI-Einfügestrategie“ beschrieben.

5 Installation von Sentinel für MS SQL

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

In diesem Kapitel erfahren Sie, wie Sie Sentinel Enterprise Security Management Sentinel 5 für MS SQL installieren.

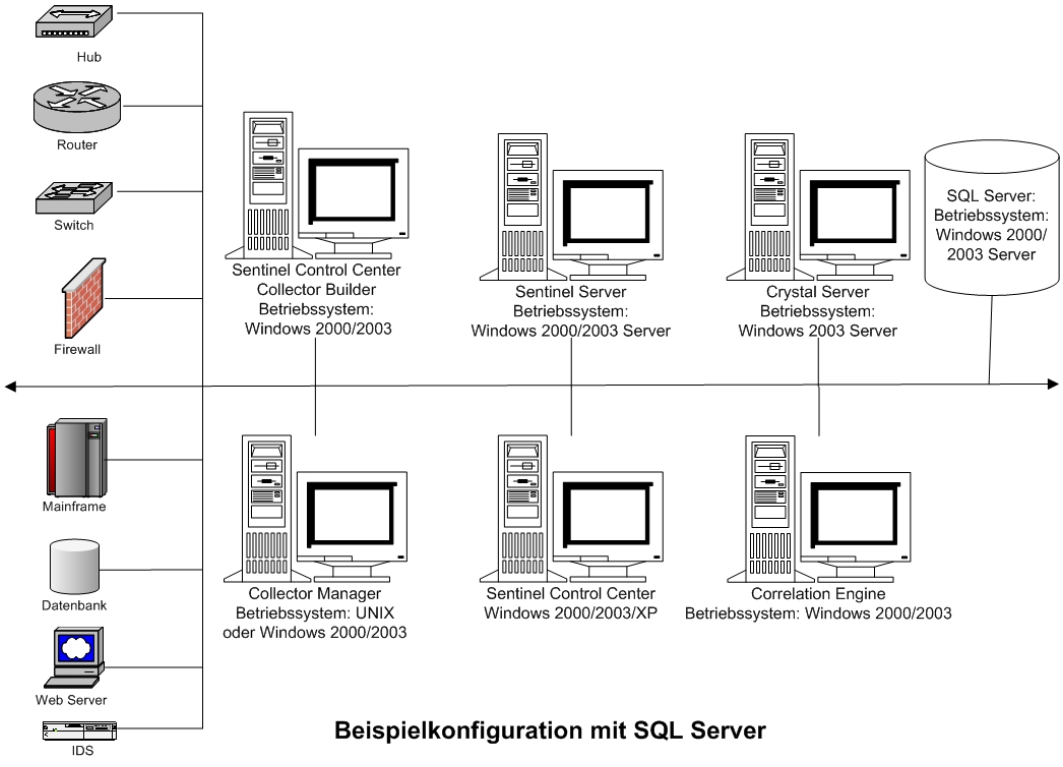
Vor der Installation von Sentinel 5 für MSSQL

HINWEIS: Vergewissern Sie sich vor der Installation, dass Ihre Maschinen den Mindestsystemanforderungen entsprechen und dass das Betriebssystem mithilfe der besten Sicherheitsvorkehrungen geschützt ist.

HINWEIS: Sentinel unterstützt nicht MS Clustering oder High Availability für Windows.

HINWEIS: Wenn Sie eine Neuinstallation von Sentinel durchführen möchten, nachdem bereits eine frühere Version installiert wurde, müssen Sie bestimmte Dateien und Systemeinstellungen entfernen, die eventuell noch von einer früheren Installation übrig geblieben sind. Wenn Sie diese Dateien bzw. Einstellungen nicht entfernen, kann die Neuinstallation scheitern. Dieser Vorgang sollte auf jedem Computer durchgeführt werden, auf dem eine Neuinstallation erfolgen soll. Weitere Informationen finden Sie in *Anhang E*.

Im Folgenden sehen Sie eine typische Konfiguration für Sentinel. Je nach der von Ihnen verwendeten Umgebung kann die Konfiguration abweichen. Unabhängig von der gewählten Konfiguration müssen Sie zuerst die Datenbank installieren.



Beispielkonfiguration mit SQL Server

HINWEIS: Weitere Informationen zu den unterstützten Betriebssystemen finden Sie in Kapitel 1 – *Einführung, Unterstützte Plattformen für Sentinel Server unter Windows*.

Abrufen eines Lizenzschlüssels

Für die Installation und Ausführung von Sentinel Server Database Access Service (DAS) ist ein gültiger Lizenzschlüssel erforderlich. Dieser Lizenzschlüssel ist an den Computer gebunden, auf dem DAS installiert werden soll. Ein für einen bestimmten Computer ausgegebener Lizenzschlüssel funktioniert nicht auf anderen Computern.

Zum Abrufen des Lizenschlüssels müssen Sie Ihre Host-ID-Nummer ermitteln und diese Informationen an Novell weitergeben. Anschließend wird ihnen ein Lizenzschlüssel zugewiesen.

So ermitteln Sie Ihre Host-ID

1. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
2. Wechseln Sie zum Verzeichnis für die Dienstprogramme auf der CD.
3. Führen Sie folgende ausführbare Datei aus:

   ```
   hostid.exe
   ```

4. Übermitteln Sie die betreffende Host-ID-Nummer an Novell Technical Support. Von dort erhalten Sie einen Lizenzschlüssel.

Sentinel-Datenbank

Vor der Installation von Sentinel Server benötigen Sie folgende Elemente:

- Die Hardware-Anforderungen finden Sie in *Kapitel 1 und 2*.
- Windows 2000 Server mit Service Patch 4 oder Windows 2003 Server mit Service Patch 1.
- SQL Server 2000 Enterprise Edition Service Pack 3a oder SQL Server 2005 Enterprise Addition (Sentinel v5.1.1 SP1 und höher) (installiert und ausgeführt).

  HINWEIS: Wenn Sie die Installation in RAID vornehmen und Ihre RAID-Umgebung es zulässt, sollte das Transaktionsprotokoll zugunsten einer möglichst hohen Leistung UNBEDINGT auf die Festplatte mit der höchsten Schreibgeschwindigkeit verweisen, die verfügbar ist.

  HINWEIS: Wenn Sie SQL Server mit einer Authentifizierung mit gemischtem Modus installiert haben, können Sie sich über Ihre Windows-Anmeldung oder über die SQL Server-Authentifizierung anmelden. Wenn der Modus nicht gemischt ist, müssen Sie sich über die Windows-Authentifizierung anmelden.

  Um die Einstellungen für den Authentifizierungsmodus zu bearbeiten, klicken Sie in SQL Enterprise Manager mit der rechten Maustaste auf den Server, dessen Einstellungen Sie bearbeiten möchten (Standard: (lokal) (Windows NT)), wählen Sie *Eigenschaften*, klicken Sie auf die Registerkarte *Sicherheit* und wählen Sie unter „Authentifizierung“ die Option *SQL Server und Windows* bzw. *Nur Windows*. „Dienststartkonto“ sollte auf *Systemkonto* gesetzt sein.
- Name der als Ziel fungierenden SQL Server-Instanz – (Standard wird empfohlen).

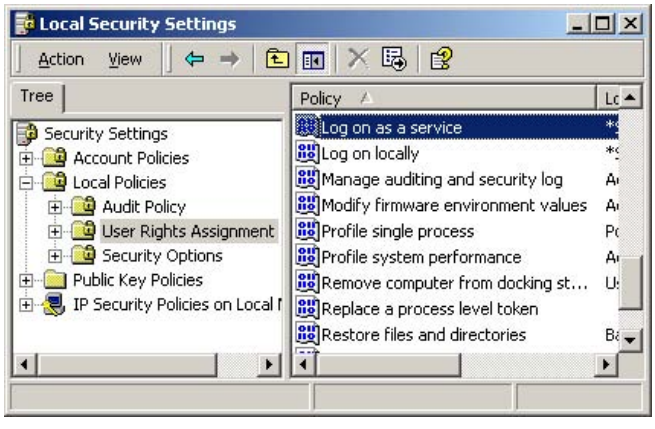
  HINWEIS: Sofern Sie Ihre Instanz während der Installation von SQL Server benannt haben, verwenden Sie diesen Namen, wenn Sie während der Installation der Datenbank und/oder der DAS-Komponenten zur Eingabe des Namens der SQL Server-Instanz aufgefordert werden. Wenn Sie Ihre Instanz nicht während der SQL Server-Installation benannt haben, lassen Sie den Instanzennamen während der Installation leer (d. h.: wenn Sie den Hostnamen eingeben, fügen Sie nicht“\<Instanzennamen>„ zum Datenbank-Hostnamen hinzu).
- Portnummer der als Ziel fungierenden SQL Server-Instanz (Standard: 1433).
- Wenn Sie vorhaben, für einen oder mehrere Sentinel-Benutzer Windows-Authentifizierung zu verwenden, muss der zugehörige Windows-Domänenbenutzer bereits vor der Installation der Sentinel-Datenbank vorhanden sein. Folgende Sentinel-Benutzer können einem Windows-Domänenbenutzer zugewiesen werden:
  - Sentinel-Datenbankadministrator – Eigentümer des Datenbankschemas (z. B. – esecdba)
  - Sentinel-Anwendungsbenutzer – Von Sentinel-Anwendungen für die Verbindung mit der Datenbank verwendet (z. B. – esecapp)
  - Sentinel-Administrator – Administrator für die Anmeldung beim Sentinel Control Center (z. B. – esecadm)
  - Sentinel Report-Benutzer – Zum Erstellen von Berichten verwendet (z. B. – esecrpt)

Sentinel Server

HINWEIS: Wenn Sie die Sentinel-Datenbank nicht zusammen mit Sentinel Server installieren, muss die Sentinel-Datenbank zuerst installiert werden.

Vor der Installation von Sentinel Server benötigen Sie folgende Elemente:

- Die Hardware-Anforderungen finden Sie in *Kapitel 1 und 2*.
- Windows 2000 Server mit Service Patch 4 oder Windows 2003 Server mit Service Patch 1.
- Seriennummer und Lizenzschlüssel von Sentinel 5 (für DAS). Weitere Informationen finden Sie unter Abrufen eines Lizenzschlüssels.
- Wenn Sie DAS installieren und das Konto eines Windows-Domänenbenutzers für den Sentinel-Anwendungsbenutzer verwenden, müssen Sie diesem Benutzer die Berechtigung zur Anmeldung als Dienst gewähren. Öffnen Sie dazu das Systemsteuerungselement „Lokale Sicherheitsrichtlinie“ auf dem Computer, auf dem DAS installiert werden soll (*Start > Einstellungen> Systemsteuerung > Verwaltung > Lokale Sicherheitsrichtlinie*). Wechseln Sie im Fenster Lokale Sicherheitsrichtlinie zu *Lokale Richtlinien > Zuweisen von Benutzerrechten*. Öffnen Sie die Richtlinie *Als Dienst anmelden* und fügen Sie den Benutzer hinzu.



- SMTP-Server – Wird benötigt, um Emails über Sentinel zu versenden.

Sentinel Control Center und Wizard

Vor der Installation von Sentinel Server benötigen Sie folgende Elemente:

- Die Hardware-Anforderungen finden Sie in *Kapitel 1 und 2*.
- Windows 2000 Server mit Service Patch 4 oder Windows 2003 Server mit Service Patch 1.

Advisor

Zur Installation von Advisor müssen Sie eine Advisor-ID und ein Passwort von Novell anfordern. Beim direkten Herunterladen aus dem Internet wird Port 443 verwendet.

HINWEIS: Wenn Sie Advisor nur für Exploit-Erkennung verwenden, brauchen Sie die Crystal Enterprise-Software nicht zu installieren. Dies ist nur erforderlich, wenn Sie vorhaben, Crystal Reports für Sentinel auszuführen. Weitere Informationen finden Sie in *Kapitel 8, Advisor-Konfiguration*.

Installation von Sentinel 5 für MS SQL

Sentinel 5 unterstützt zwei Installationstypen. Hierbei handelt es sich um:

- Einfach – Die Option zur All-in-One-Installation. Windows Sentinel-Services, Collector-Service und Anwendungen mit MS SQL Server auf demselben Computer. Unterstützt nur SQL Server-Authentifizierung. Dieser Installationstyp dient lediglich zu Demonstrationszwecken.
- Benutzerdefiniert – Ermöglicht eine vollständig Verteilte Installation.

HINWEIS: Standardmäßig legt das Installationsprogramm fest, dass folgende Dateigruppen NICHT automatisch wachsen: ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX. Für alle anderen Dateigruppen wird automatisches Wachstum festgelegt. Der Grund, warum automatisches Wachstum für ESENTD, ESENTX, SENT_SMRYD und SENT_SMRYX nicht zugelassen wird, ist, dass sie Daten über Ereignisse und Zusammenfassungsereignisse enthalten. Die Speicherplatzauslastung für Eregnisse und Zusammenfassungen kann höchst dynamisch sein. Diese Ereignisdateigruppen sollten überwacht und auf gesteuerte Weise in Ihrer Dateisystemkonfiguration erweitert werden. Dabei sind EA-Lastenausgleich und Datenbanksicherung und -wiederherstellung zu berücksichtigen.

Die SDM-Partitionsverwaltung (Archivieren, Verwerfen und Hinzufügen von Partitionen) sollte zeitlich geplant sein, um die Größe der Ereignisdaten überschaubar zu halten.

Einfache Installation

Bei dieser Installationsweise werden alle Komponenten (einschließlich der Datenbank) auf einer einzelnen Plattform installiert und SQL Server-Authentifizierung wird unterstützt. Dies dient vorrangig zu Demonstrationszwecken. Für Test- bzw. Produktionszwecke nicht emfpohlen.

HINWEIS: Bei der einfachen Installation wird die Collector Manager-Passwortauthentifizierung nicht unterstützt.

Einfache Sentinel-Installation

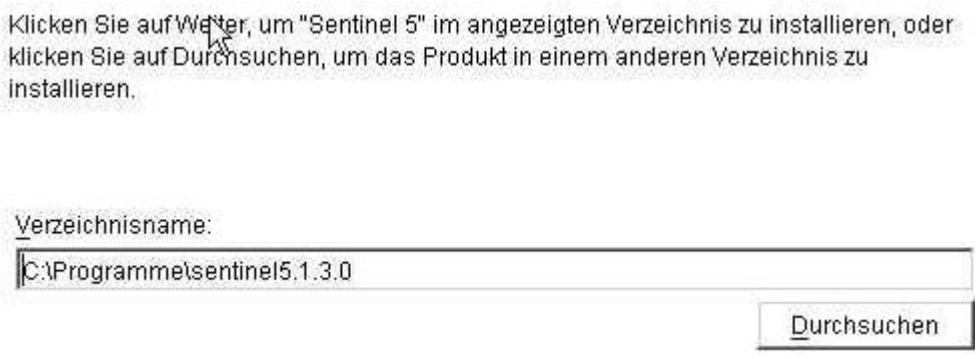
1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für MSSQL die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
3. Wechseln Sie zu der CD und doppelklicken Sie auf *setup.bat*.

HINWEIS: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.

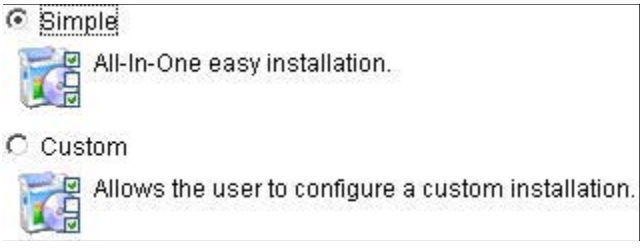
---

4. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
5. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
6. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.

7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



8. Wählen Sie *Einfach* aus. Klicken Sie auf *Weiter*.



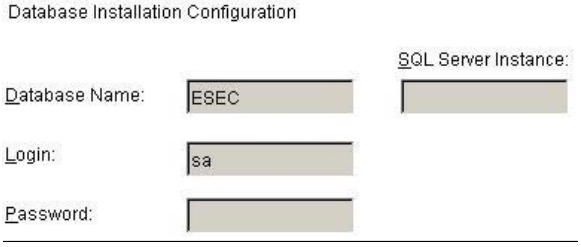
9. Geben Sie Ihre Konfigurationsinformationen ein.
   - Seriennummer und Lizenzschlüssel
   - SMTP-Server (entweder DNS-Name oder IP-Adresse) – sofern Sentinel in der Lage sein soll, Emails zu versenden
   - Email – Geben Sie eine gültige Email-Adresse ein, über die Advisor-Benachrichtigungs-Emails gesendet werden sollen (z. B. Sent_Server@myserver.com).
   - Globales Systempasswort – Geben Sie ein Passwort und dasselbe Passwort nochmals zur Bestätigung ein. Dieses Passwort wird für alle Standardbenutzer verwendet. Dazu gehören Sowohl der Benutzer des esecadm-Betriebssystems als auch die Datenbankbenutzer. Eine Liste der Standard-Datenbankbenutzer, die während der Installation erstellt werden, finden Sie unter Sentinel-Datenbank im Abschnitt Vor der Installation von Sentinel 5 für MSSQL.
   - Datenverzeichnis – der Speicherort für alle Datendateien der Datenbank und der Advisor-Datenbank. Um den Standard-Speicherort zu ändern, klicken Sie auf die Schaltfläche „...“ und wählen sie den gewünschten Speicherort aus. Standard: %ESEC_HOME%\data.

HINWEIS: Sofern Advisor installiert wird, konfiguriert die einfache Installation Advisor für die Verwendung von „Direktes Herunterladen vom Internet“ mit einem Aktualisierungsintervall von 12 Stunden und unter Aktivierung aller Email-Benachrichtigungen.

- Wählen Sie zur Installation von Advisor die Option *Advisor installieren*. Geben Sie einen Benutzernamen und ein Passwort ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.

Klicken Sie auf *Weiter*.

10. Geben Sie zur Konfiguration der Datenbankinstallation Folgendes ein:
    - sa-Benutzernamen und Passwort.
    - Wenn Sie die SQL Server-Instanz benannt haben, geben Sie den betreffenden Namen ein.



11. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation müssen Sie das System neu starten.

HINWEIS: Wenn Sie Drittanbieter-Integrationssoftware (HP Service Desk oder Remedy Integration) installieren möchten, führen Sie nach dem erneuten Booten Ihres Computers das Installationsprogramm erneut aus und wählen Sie die gewünschte Drittanbieter-Integrationssoftware aus. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration*.

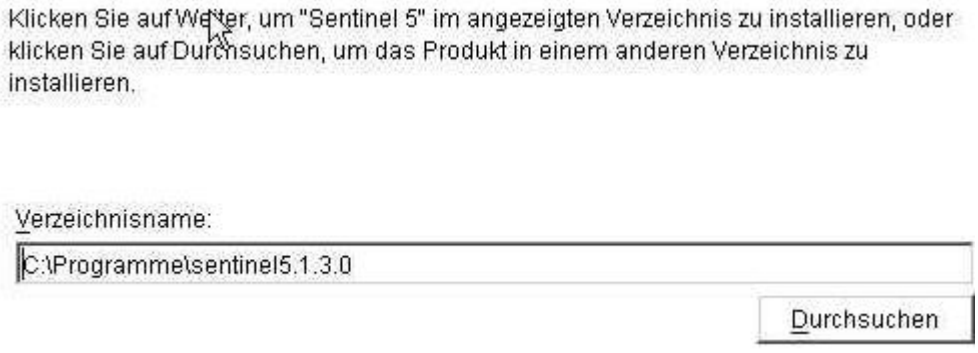
Benutzerdefinierte Installation

Benutzerdefinierte Sentinel-Installation

1. Vergewissern Sie sich, dass Sie für die zu installierenden Komponenten gemäß den Angaben in Abschnitt Vor der Installation von Sentinel 5 für MSSQL die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben.
2. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
3. Wechseln Sie zu der CD und doppelklicken Sie auf *setup.bat*.

HINWEIS: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.

4. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
5. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
6. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



8. Wählen Sie *Benutzerdefiniert* (Standard). Klicken Sie auf *Weiter*.
9. Wählen Sie die zu installierenden Funktionen aus.

HINWEIS: Weitere Informationen darüber, welche Komponenten bei verschiedenen Konfigurationen an welchem Ort installiert werden können, finden Sie in *Kapitel 1, Systemanforderungen*.

Die Installation folgender Komponenten ist möglich:

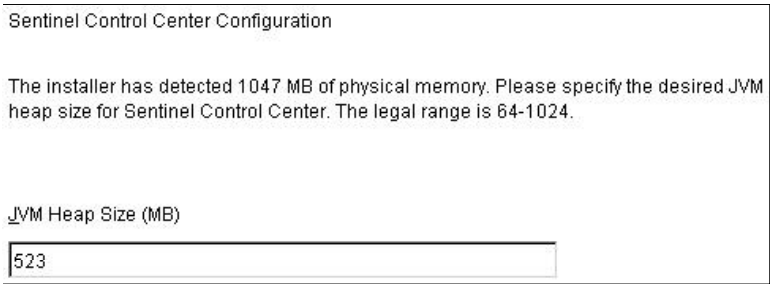
- Datenbank – Installiert die Sentinel-Datenbank
- Kommunikationsserver – installiert den Nachrichtenbus (iSCALE)
- Advisor
- Correlation Engine
- DAS
- Collector-Service
- Collector Builder
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk
- Remedy Integration

HINWEIS: Informationen zur Installation von HP OpenView Service Desk bzw. von Remedy Integration finden Sie im *Handbuch für Drittanbieter-Integration.*

HINWEIS: Wenn keine der untergeordneten Funktionen von *Sentinel Services* ausgewählt wurde, müssen Sie auch die Funktion *Sentinel Services* selbst deaktivieren. Sie wird abgeblendet mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.

HINWEIS: Als Teil der Installation der Sentinel-Datenbank legt das Installationsprogramm Dateien im Ordner %ESEC_HOME%\utilities\db ab.

10. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, werden Sie zur Eingabe folgender Informationen aufgefordert:
    - Seriennummer
    - Lizenzschlüssel
11. Wenn Sie ausgewählt haben, dass Drittanbieter-Integrationskomponenten installiert werden sollen, werden Sie aufgefordert, ein Passwort einzugeben, um die ausgewählten Drittanbieter-Integrationskomponenten zu entsperren. Weitere Informationen finden Sie im *Handbuch für Drittanbieter-Integration.*
12. Wenn ausgewählt haben, dass Sentinel Control Center installiert werden soll, wird eine JVM-(Java Virtual Machine)-Eingabeaufforderung angezeigt:
    - JVM-Heap-Größe (MB) – Standardmäßig ist dieser Wert auf die Hälfte der Größe des auf dem Computer gefundenen physischen Arbeitsspeicher eingestellt (maximal 1024 MB). Dies ist die maximal von Sentinel Control Center verwendete JVM-Heap-Größe.



13. Wenn Sie ausgewählt haben, dass der Collector-Service, installiert werden soll, müssen Sie festlegen, ob Wizard Collector Manager durch ein Passwort geschützt werden soll oder nicht. Wenn Sie festgelegt haben, dass der Wizard Collector Manager geschützt werden soll, werden Sie aufgefordert, ein Wizard Collector Manager-Passwort zu erstellen.

HINWEIS: Um eine Collector-Instanz durch ein Passwort zu schützen, müssen Sie dieses Passwort beim Herauf- und Herunterladen sowie bei der Fehlersuche für Collectors im betreffenden Collector Manager angeben. Dieses Passwort und der Sentinel-Benutzername und das Passwort werden für die Anmeldung bei Collector Builder benötigt.

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

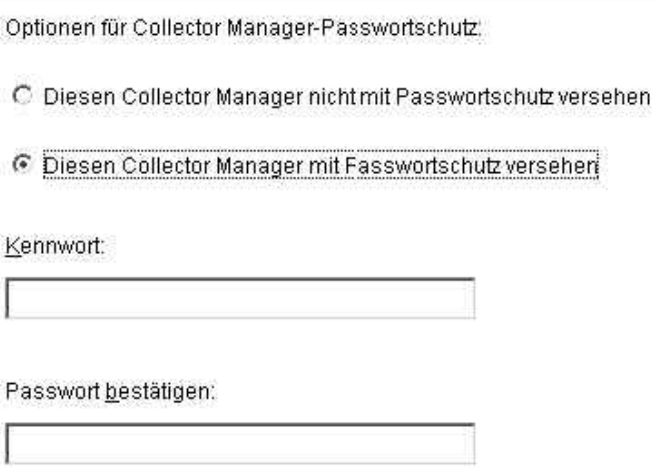
1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (!@#$%^&*()_+) und eine Zahl (0-9) enthalten.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

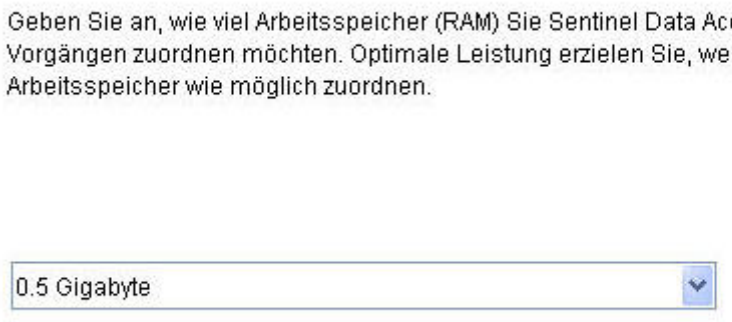
3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zum Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

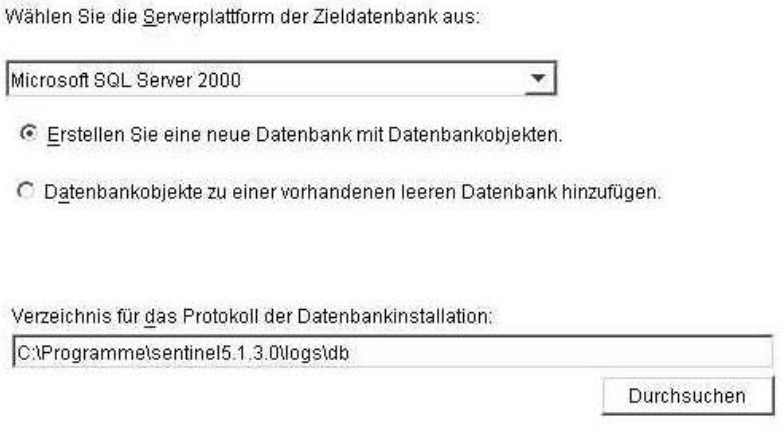
5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Z.B. mSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).



14. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, legen Sie fest, wie viel RAM in Ihrem System für Data Access Service zur Verfügung gestellt werden sollen. Für verteilte Umgebungen sollten Sie die Höchstmenge an Arbeitsspeicher (4 GB) auswählen. Für Einzelplatzumgebungen wird die Hälfte des RAM-Speichers empfohlen.



15. Bei der Datenbankinstallation werden folgende Eingabeaufforderungen angezeigt:
    a. Wählen Sie die Serverplattform der Zieldatenbank – Microsoft SQL Server 2000 oder 2005 – und eines der folgenden Elemente aus:
        - Erstellen Sie eine neue Datenbank mit Datenbankobjekten – erstellt eine neue MS SQL-Datenbank und füllt die neue Datenbank mit Datenbankobjekten
        - Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen – fügt nur Datenbankobjekte zu einer bestehenden MS SQL-Datenbank hinzu. Die bestehende Datenbank muss leer sein.
    b. Geben Sie das Verzeichnis für das Datenbankinstallationsprotokoll ein (Standard: %ESEC_HOME%\logs\db). Übernehmen Sie den Standardwert für „Verzeichnis für das Protokoll der Datenbankinstallation“ oder klicken Sie auf *Durchsuchen*, um einen anderen Speicherort anzugeben.

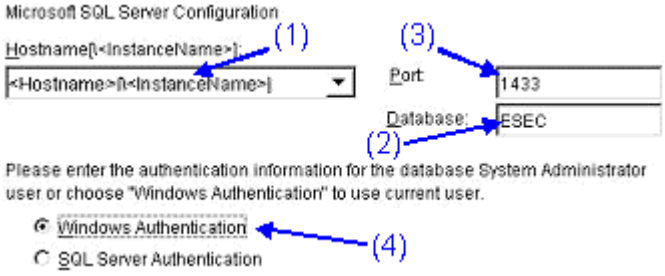


    c. Geben Sie die Informationen für die SQL Server-Konfiguration wie folgt ein:
        - (1) Hostname oder IP-Adresse der Datenbasnk – standardmäßig wird ihr lokaler Host-Computer angezeigt, sofern SQL Server lokal installiert ist. Wenn der gewünschte SQL Server nicht in der Dropdown-Liste angezeigt wird, wählen Sie die Option *Sonstiges* in der Liste aus. Es wird ein Textfeld angezeigt, in dem Sie den Hostnamen eingeben können. Sie müssen den vollständigen Hostnamen eingeben (z. B. – „sqlserver.sentinel.net“ und nicht nur „sqlserver“). Wenn Sie während der SQL Server-Installation einen Instanzennamen angegeben haben, müssen Sie am Ende des Hostnamens „\<Instanzenname>“ hinzufügen, wobei <Instanzenname> der Name ist, den Sie der Instanz während der SQL Server-Installation zugewiesen haben.
        - (2) Datenbankname (Neue Datenbank) – Der Name für die neue SQL Server-Datenbank. Neben der hier benannten Datenbank wird außerdem eine Datenbank mit dem Namen <Ihr_DB-Name>_WF für die Verwendung durch iTRAC erstellt.
        - (2) Datenbankname (bestehende Datenbank) – Der Name der bestehenden leeren SQL Server-Datenbank, zu der Datenbankobjekte hinzugefügt werden sollen. Verwenden Sie den Datenbankamen ohne das Suffix „_WF“.
        - (3) Datenbank-Port (Standard: 1433)

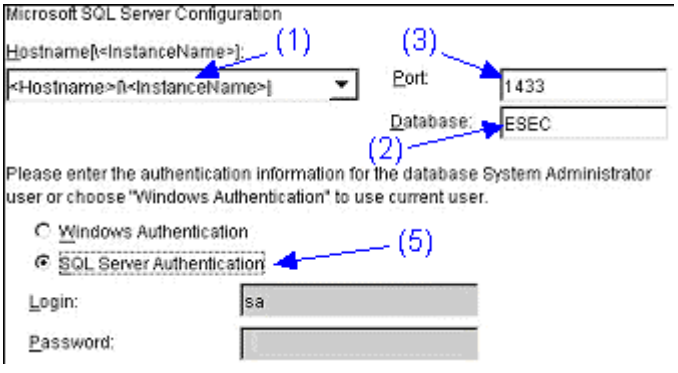
- Wählen Sie für den Systemdatenbankadministrator eines der folgenden Elemente:

  (4) Windows-Authentifizierung –der Benutzername, unter dem Sie das Installationsprogramm ausführen, wird verwendet.

  (5) SQL Server-Authentifizierung – Geben Sie das Passwort des sa-Benutzers ein.



Windows-Authentifizierung

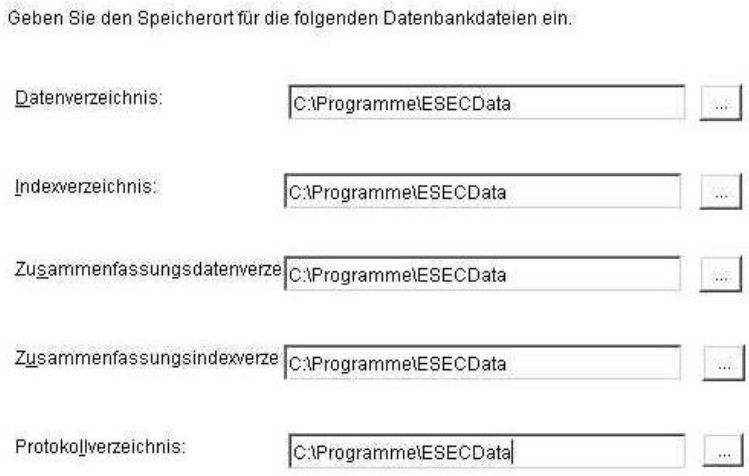


SQL Server-Authentifizierung

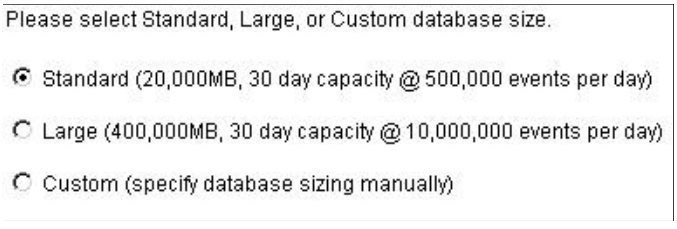
d. Wenn Sie ausgewählt haben, dass eine neue Datenbank installiert werden soll, müssen Sie den Speicherort für folgende Datenbankdateien angeben:

HINWEIS: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung sollten diese Speicherorte auf unterschiedlichen E/A-Geräten liegen.

- Datendateien
- Indexdateien
- Zusammenfassung Datendateien
- Zusammenfassung Indexdateien
- Protokolldateien

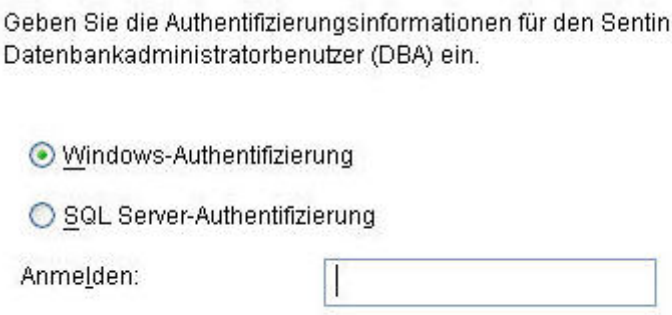


e. Wenn Sie ausgewählt haben, dass eine neue Datenbank installiert werden soll, geben Sie die gewünschte Größe der Datenbank ein:
   - Standard (20.000 MB) – 30 Tage Kapazität bei 500.000 Ereignissen pro Tag
   - Groß (400.000 MB) – 30 Tage Kapazität bei 10.000.000 Ereignissen pro Tag
   - Benutzerdefiniert (manuelle Größenfestlegung). Wenn Sie diese Option wählen, werden Sie außerdem aufgefordert, folgende Informationen einzugeben:
     (1) Größe Ihrer Datenbank in MB (10.000 – 2.000.000)
     (2) Größe der einzelnen Protkolldateien in MB (100 – 100.000)
     (3) Maximale Größe der einzelnen Datenbankdateien in MB (2.000 – 100.000)

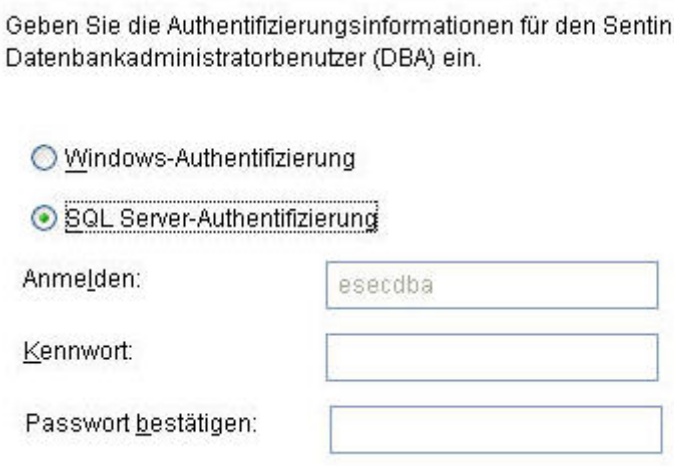


f. Wählen Sie für den Sentinel-Datenbankadministrator (DBA) eines der folgenden Elemente aus:
   - Windows -Authentifizierung, geben Sie ein: <Domänenname>\<Benutzername>
   - SQL Server-Authentifizierung (esecdba), Passwort und Passwortbestätigung

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



Windows-Authentifizierung



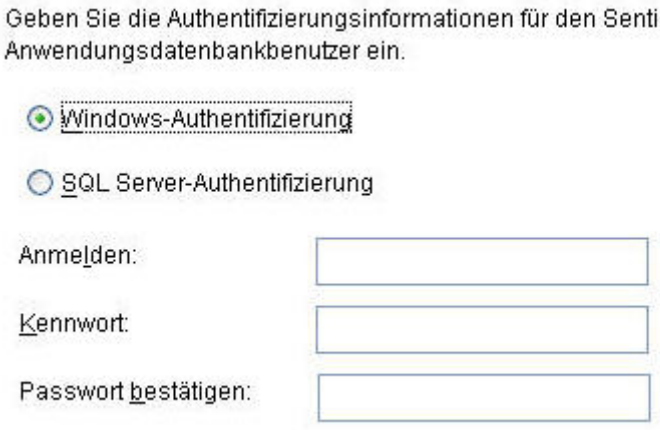
SQL Server-Authentifizierung

g. Wählen Sie für den Benutzer der Sentinel-Anwendungsdatenbank eine der folgenden Optionen:

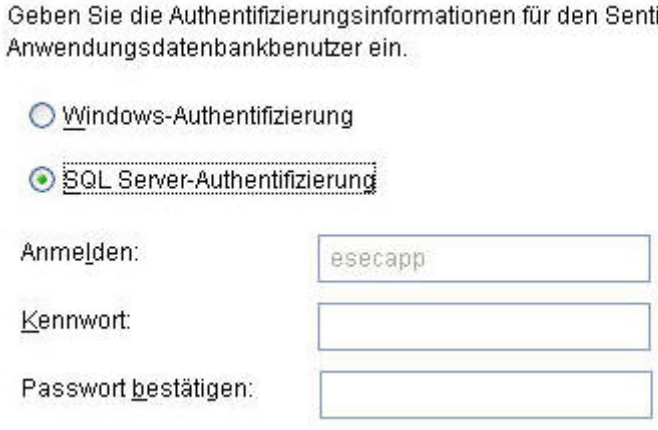
HINWEIS: Wenn Sie eine Windows-Domänenanmeldung für den Benutzer der Sentinel-Anwendungsdatenbank verwenden, müssen Sie dem betreffenden Benutzer die Berechtigung zum Anmelden als Dienst auf diesem Computer gewähren, wie im Unterabschnitt Sentinel Server von Abschnitt Vor der Installation von Sentinel 5 für MSSQL beschrieben.

- Windows-Authentifizierung, geben Sie <Domänenname>\<Benutzername>, Passwort und Passwortbestätigung ein
- SQL Server-Authentifizierung (esecapp), geben Sie Passwort und Passwortbestätigung ein

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



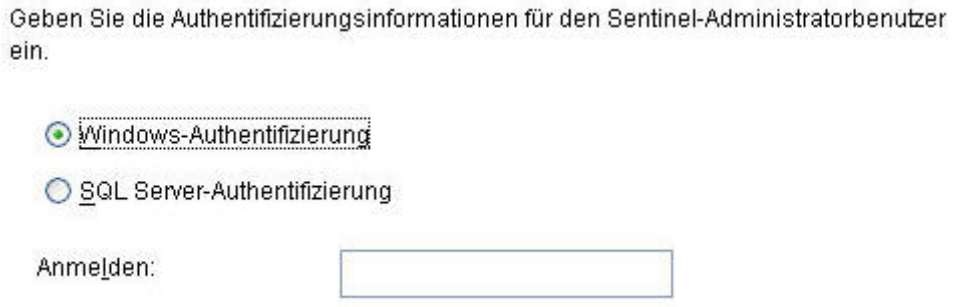
Windows-Authentifizierung



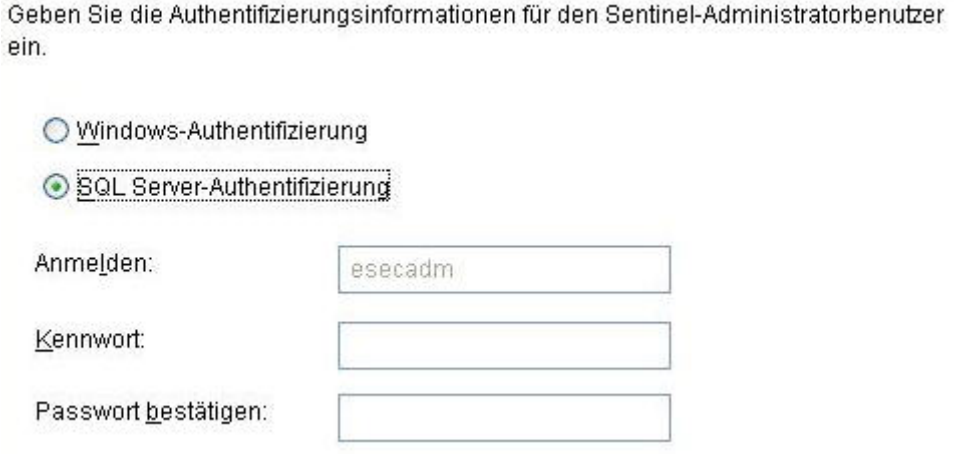
SQL Server-Authentifizierung

h. Wählen Sie für den Sentinel-Administrator eine der folgenden Optionen aus:
   - Windows-Authentifizierung, geben Sie ein: <Domänenname>\<Benutzername>
   - SQL-Authentifizierung, Geben Sie den Benutzernamen für den Sentinel-Administrator ein (Standard: esecadm), Passwort und Passwortbestätigung ein

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



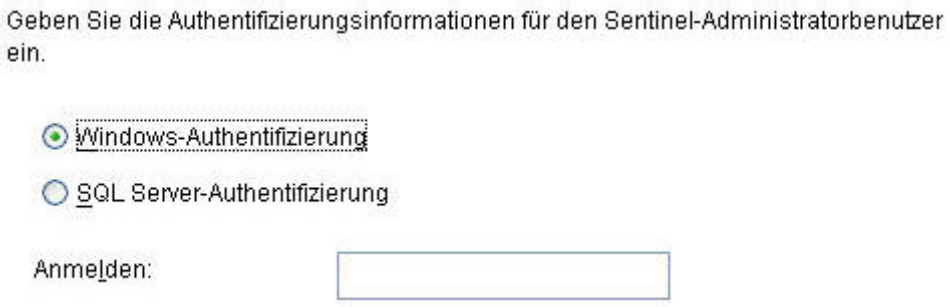
Windows-Authentifizierung



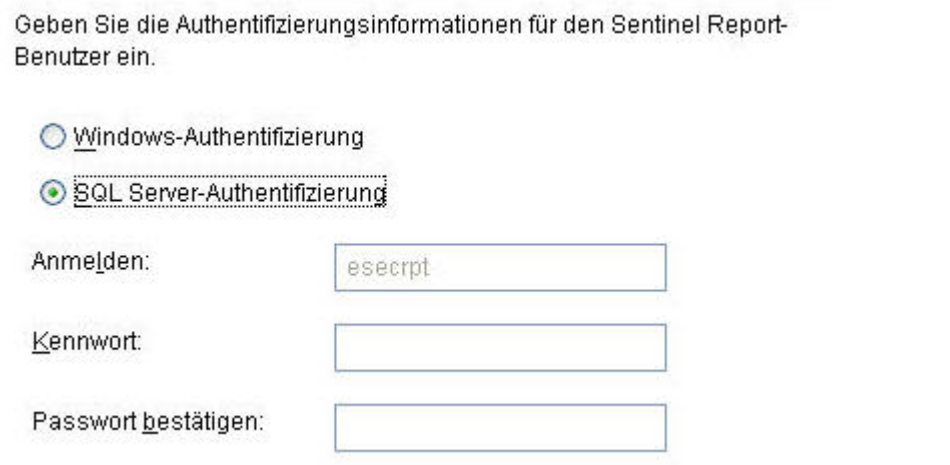
SQL Server-Authentifizierung

i. Wählen Sie für den Benutzer der Sentinel-Berichterstellung eine der folgenden Optionen:
   - Windows -Authentifizierung, geben Sie ein: <Domänenname>\<Benutzername>
   - SQL-Authentifizierung (esecrpt), geben Sie Passwort und Passwortbestätigung ein

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



Windows-Authentifizierung



SQL Server-Authentifizierung

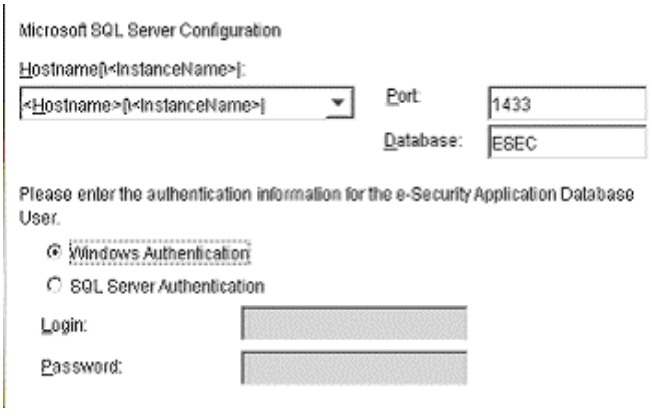
j. Klicken Sie im Zusammenfassungsfenster für die Datenbankinstallation auf *Weiter*.

16. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, nicht jedoch, dass die Sentinel-Datenbank installiert werden soll, werden Sie aufgefordert, folgende Informationen für die SQL Server Sentinel-Datenbank einzugeben. Diese Informationen werden verwendet, um DAS so zu konfigurieren, dass es auf die Sentinel-Datenbank verweist.
    - Hostname oder IP-Adresse der Datenbank – standardmäßig wird ihr lokaler Host-Computer angezeigt, sofern die SQL Server Sentinel-Datenbank lokal installiert ist. Wenn die SQL Server Sentinel-Datenbank, mit der DAS eine Verbindung herstellen soll, nicht in der Dropdown-Liste angezeigt wird, wählen Sie die Option *Sonstiges* in der Liste aus. Es wird ein Textfeld angezeigt, in dem Sie den Hostnamen eingeben können. Sie müssen den vollständigen Hostnamen eingeben (z. B. – „sqlserver.sentinel.net“ und nicht nur „sqlserver“). Wenn Sie während der SQL Server-Installation einen Instanzennamen angegeben haben, müssen Sie am Ende des Hostnamens „\<Instanzenname>“ hinzufügen, wobei <Instanzenname> der Name ist, den Sie der Instanz während der SQL Server-Installation zugewiesen haben.

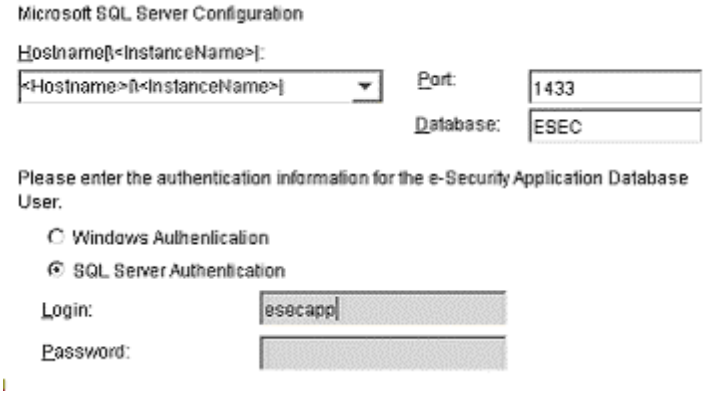
- Datenbankname – Der Name der bestehenden SQL Server Sentinel-Datenbank, mit der DAS eine Verbindung herstellen soll. Verwenden Sie den Datenbankamen ohne das Suffix „_WF“.
- Datenbank-Port (Standard: 1433)
- Wählen Sie für den Benutzer der Sentinel-Anwendungsdatenbank eine der folgenden Optionen:

HINWEIS: Wenn Sie eine Windows-Domänenanmeldung für den Benutzer der Sentinel-Anwendungsdatenbank verwenden, müssen Sie dem betreffenden Benutzer die Berechtigung zum Anmelden als Dienst auf diesem Computer gewähren, wie im Unterabschnitt Sentinel Server von Abschnitt Vor der Installation von Sentinel 5 für MSSQL beschrieben.

  - Windows-Authentifizierung – Geben Sie die Windows-Domänenanmeldung an, die während der Installation der Sentinel-Datenbank für diesen Benutzer festgelegt wurde, und geben Sie das Passwort für den Benutzer ein. Das Passwort ist hier erforderlich, um den Sentinel Windows-Service für die Anmeldung als Dienst bei dieser Windows-Domänenanmeldung zu konfigurieren.
  - SQL Server-Authentifizierung – Geben Sie die Anmeldung „esecapp“ an und geben Sie das Passwort ein, das während der Installation der Sentinel-Datenbank für den Benutzer festgelegt wurde.

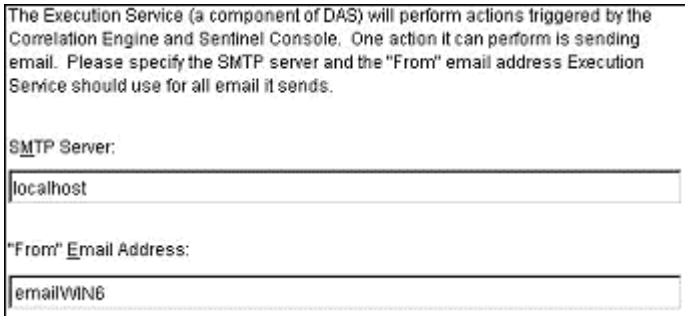


Windows-Authentifizierung

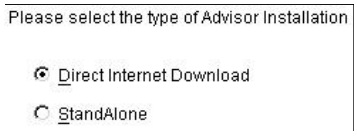


SQL-Authentifizierung

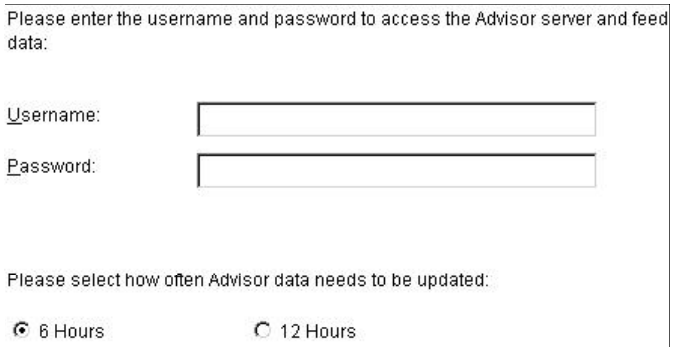
17. Wenn Sie ausgewählt haben, dass DAS installiert werden soll, müssen Sie Email-Unterstützung für Sentinel konfigurieren. Geben Sie den SMTP-Server und die Email-Absenderadresse ein, die Execution Service beim Versenden von Nachrichten verwenden soll (optional – dieser Wert kann nach der Installation manuell geändert werden [%ESEC_HOME%\sentinel\config\execution.properties]):



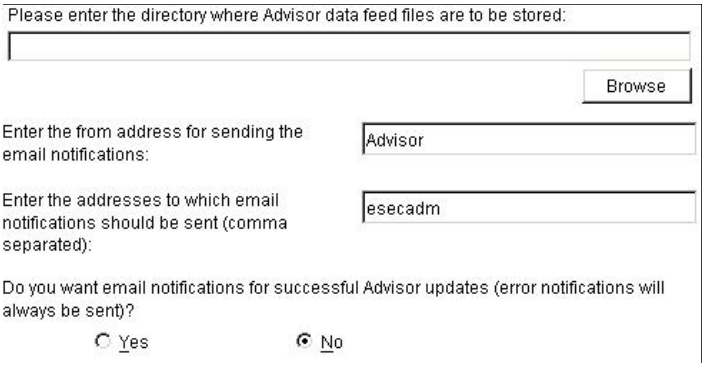
18. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, wird folgende Eingabeaufforderung angezeigt, in der Sie nach dem Installationstyp gefragt werden:
    - Direktes Herunterladen vom Internet – Der Advisor-Computer ist direkt mit dem Internet verbunden. In dieser Konfiguration werden regelmäßig automatisch Aktualisierungen von Novell über das Internet heruntergeladen.
    - Einzelplatz – Advisor ist als isoliertes System konfiguriert, in das manuell eingegriffen werden muss, um eine Aktualisierung von Sentinel zu empfangen.



19. Wenn Sie ausgewählt haben, dass Advisor installiert werden und „Direktes Herunterladen vom Internet“ verwendet werden soll, geben Sie Ihren Advisor-Benutzernamen, Ihr Passwort und die gewünschte Aktualisierungshäufigkeit für die Advisor-Daten ein. Wenn Ihr Benutzername bzw. Ihr Passwort nicht überprüft werden kann, werden Sie nach dem Klicken auf *Weiter* gefragt, ob Sie fortfahren möchten (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.



20. Wenn Sie ausgewählt haben, dass Advisor installiert werden soll, geben Sie Folgendes ein:
    - Das Verzeichnis, in dem Advisor-Datenfeed-Dateien gespeichert werden. Dies ist der Speicherort, an dem die Angriffs- und Warnmeldungs-Feed-Dateien beim Herunterladen gespeichert werden.
    - Die Empfängeradresse zum Senden von Email-Benachrichtigungen
    - Wählen Sie aus, ob Sie per Email über erfolgreiche Advisor-Akutalisierungen benachrichtigt werden möchten. Fehlerbenachrichtigungen werden immer gesendet.



HINWEIS: Nach der Installation können Sie die Advisor-Email-Adressen ändern, indem Sie die Dateien attackcontainer.xml und alertcontainer.xml bearbeiten. Weitere Informationen finden Sie in *Kapitel 9 – Registerkarte „Advsisor“* im Sentinel-Benutzerhandbuch.

21. Wenn Sie ausgewählt haben, dass HP Service Desk oder Remedy Integration installiert werden soll, werden Sie zur Eingabe weiterer Informationen aufgefordert. Weitere Informationen finden Sie im *Sentinel-Handbuch für Drittanbieter-Integration*.
22. Lesen Sie die Informationen auf den darauf folgenden Bildschirmen und klicken Sie abschließend auf *Weiter*. Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten.
23. Klicken Sie auf *Fertig stellen*, um das System neu zu booten.
24. Wenn Sie eine hohe Ereignisrate (mehr als 800 Ereignisse pro Sekunde) erwarten, müssen Sie die zusätzlichen Konfigurationsanweisungen in Abschnitt Einrichten der Strategie zum Einfügen von Ereignissen von Active Data Objects (ADO) befolgen.

Nach der Installation von Sentinel 5 für MS SQL

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter %ESEC_HOME%\sentinel\config. Um diese Datei zu konfigurieren, führen Sie mailconfig.bat aus, um die Datei zu ändern, und mailconfigtest.bat, um Ihre Änderungen zu testen.

So konfigurieren Sie die Datei execution.properties

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

   ```
   mailconfig.bat -host <SMTP Server> -from <Quellen-Email-
      Adresse> -user <Mailauthentifizierungsbenutzer> –
      password
   ```

   Beispiel:

   ```
   mailconfig.bat -host 10.0.1.14 -from my_name@domain.com -
      user my_user_name –password
   ```

   Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

   ```
   Enter your password:*********
   Confirm your password:*********
   ```

   HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Wechseln Sie auf dem Computer, auf dem DAS installiert ist, in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Führen Sie „mailconfigtest“ wie folgt aus:

   ```
   mailconfigtest.bat -to <destination email address>
   ```

   Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

   ```
   Email has been sent successfully!
   ```

   Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

   ```
   Subject: Testing Sentinel mail property
   This is a test for Sentinel mail property set up. If you
      see this message, your Sentinel mail property has been
      configured correctly to send emails
   ```

Sentinel-Datenbank

Nach der Installatoin der Sentinel-Databank enthält die Datenbank folgende Standardbenutzer:

- esecdba – Schemaeigentümer (bie Verwendung des Windows-Domänenbenutzers, zum Zeitpunkt der Installation zu konfigurieren)
- esecapp – Der von Sentinel-Anwendungen zur Herstellung einer Verbindung mit der Datenbank verwendete Benutzername (bei Verwendung des Windows-Domänenbenutzers, zum Zeitpunkt der Installation zu konfigurieren)
- esecadm – Sentinel-Administrator (bei Verwendung des Windows-Domänenbenutzers, zum Zeitpunkt der Installation zu konfigurieren)
- esecrpt – Reporter-Benutzer (bei Verwendung des Windows-Domänenbenutzers, zum Zeitpunkt der Installation zu konfigurieren)

Collector-Service

Während der Installation des Collector-Service werden folgende Collectors installiert und für jeden wird ein Collector-Port eingerichtet, um ihn auszuführen.

Produkt	Collector-Name
Demo-Collectors	
Führt Tests für das Hochladen von Beständen durch, arbeitet mit dem DemoEvents-Collector	DemoAssetUpload
Führt Tests für Demo-Ereignisse durch, arbeitet mit DemoAssetUpload- und DemoVulnerabilityUpload-Collector	DemoEvents
Führt Tests für das Heraufladen von Anfälligkeiten durch, arbeitet mit dem DemoEvents-Collector	DemoVulnerabilityUpload
Test für das Senden eines Ereignisses	SendOneEvent
Test für das Senden mehrerer Ereignisse	SendMultipleEvents

HINWEIS: Weitere Informationen zur Konfiguration der Demo-Collectors finden Sie in *Kapitel 12, Testen der Installation.*

HINWEIS: Weitere Collectors finden Sie im Sentinel-Kundenportal. Weitere Informationen (auch zur Konfiguration) finden Sie in der Dokumentation zu den einzelnen Collectors in:

%WORKBENCH_HOME%\Elements\<Collector-Name>\Docs\

Zur Installatoin weiterer Collectors führen Sie das Service Pack-Skript auf der Service Pack-CD aus. Das Skript installiert die Collectors lokal.

Unter Windows:

```
.\service_pack.bat
```

Unter UNIX:

```
./service_pack.sh
```

Installationsanweisungen für das Service Pack und eine Liste der Collectors finden Sie in den *Service Pack-Versionshinweisen*.

Aktualisieren des Lizenzschlüssels

Wenn Ihr Sentinel-Lizenzschlüssel abgelaufen ist und Novell einen neuen Lizenzschlüssel ausgestellt hat, führen Sie das softwarekey-Programm aus, um Ihren Lizenzschlüssel zu aktualisieren.

So aktualisieren Sie Ihren Lizenzschlüssel

1. Melden Sie sich als Benutzer mit Administratorrechten an.
2. Wechseln Sie in das Verzeichnis „%ESEC_HOME%\utilities“.
3. Geben Sie den folgenden Befehl ein:

   ```
   softwarekey.exe
   ```

4. Geben Sie die Ziffer 1 ein, um den Primärschlüssel anzugeben. Drücken Sie die EINGABETASTE.

Konfigurationsanweisungen für die Verwendung von SQL Server Windows-Authentifizierung mit DataDirect JDBC-Treiber

HINWEIS: Die folgenden Informationen stammen aus dem Installationshandbuch für DataDirect Connect© für JDBC© . Folgende Vorgänge sollten unbedingt von Ihrem Systemadministrator ausgeführt werden.

Nach der Installation von Connect für JDBC sind einige Konfigurationsarbeiten für die folgenden Komponenten erforderlich, um Windows-Authentifizierung bei SQL Server zu verwenden:

- SQL Server-Datenbankserver
- Domänencontroller
- Client-Arbeitsstation

Weitere Informationen zur Windows-Authentifizierung und zum SQL Server-Treiber von Connect für JDBC finden Sie im *Benutzerhandbuch und der Referenz von DataDirect Connect für JDBC*.

SQL Server-Datenbankserver

In diesem Abschnitt wird die Konfiguration beschrieben, die auf dem Datenbankserver von SQL-Server durchgeführt werden muss, um Windows-Authentifizierung mit dem SQL Server-Treiber von Connect füor JDBC zu verwenden.

Service Principle Name

Zur Verwendung des Kerberos-Authentifizierungsprotokolls, muss genau ein Service Principle Name (SPN) für jede SQL Server-Instanz registriert werden. Ein SPN ist ein eindeutiger Name, der den SQL Server-Service für einen bestimmten Computer und Port einem Kontonamen zuordnet, der zum Starten des Service verwendet wird (Dienststartkonto). Ein SPN besteht aus fogendenden Elementen:

- Als Serviceklassenname wird stets MSSQLSvc für SQL Server verwendet
- Der Hostname ist der vollständige DNS-Name des Computers, auf dem SQL Server ausgeführt wird.
- Port ist die Portnummer, die die SQL Server-Instanz überwacht.

Beispiel: MSSQLSvc/DBServer.test:1433 ist ein SPN für eine SQL Server-Instanz, die auf einem Computer mit der Bezeichnung DBServer in der Testdomäne ausgeführt wird und Port 1433 überwacht.

Auflisten von SPNs

Vergewissern Sie sich bei Ihrem Datenbank- bzw. Domänenadministrator, dass die entsprechenden SPNs für jede SQL Server-Instanz registriert wurden. Ihr Datenbank- bzw. Domänenadministrator kann mithilfe des Windows-Befehls „ldifde“ die registrierten SPNs auflisten.

Registrieren von SPNs

Falls erforderlich, kann der Datenbank- bzw. Domänenadministrator SPNs mithilfe des Tools „Setspn“ registrieren, das im Windows Resource Kit enthalten ist. Beispiel:

```
setspn -A MSSQLSvc/DBServer.test:1433 sqlsvc
```

registriert eine SPN, der das Dienststartkonto „sqlsvc“ einer SQL Server-Instanz zuordnet, die auf dem Computer DBServer in der Testdomäne ausgeführt wird und Port 1433 überwacht.

Das Setspn-Tool finden Sie auf der folgenden Website:
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp.

Informationen zur Verwendung des Setspn-Tools finden Sie in der begleitenden Microsoft-Dokumentation.

HINWEIS: Wenn das Startkonto für SQL Server geändert wird, müssen die SPNs für SQL Server gelöscht und neu registriert werden.

Authentifizierungsmodus

Zur Verwendung der Windows-Authentifizierung kann der Authentifizierungsmodus von SQL Server auf einen der folgenden Modi gesetzt werden:

- Nur Windows
- Gemischte Authentifizierung

Wenn SQL Server-Authentifizierung zusätzlich zur Windows-Authentifizierung verwendet wird, muss der Authentifizierungsmodus auf „Gemischte Authentifizierung“ gesetzt sein.

Domänencontroller

Der SQL Server-Treiber unterstützt Windows-Authentifizierung, wenn Kerberos Key Distribution Center (KDC) auf einem Windows 2000-Domänen-Controller ausgeführt wird. Bei der Kommunikation mit KDC werden die zwischen KCD und SQL Server ausgetauschten Nachrichten verschlüsselt.

Da SQL Server nur den Verschlüsselungsalgorithmus DES-CBC-MD5 verwenden kann, muss das Dienststartkonto von SQL Server auf dem Domänencontroller die Active Directory-Eigenschaft „DES-Verschlüsselungstypen für dieses Konto verwenden“ enthalten. Vergewissern Sie sich bei Ihrem Domänenadministrator, dass diese Eigenschaft für das Dienststartkonto von SQL Server festgelegt ist. Das Dienststartkonto von SQL Server kann nicht als Client-Anmeldekonto verwendet werden.

Client-Computer

In diesem Abschnitt wird die Konfiguration beschrieben, die auf dem Client-Computer durchgeführt werden muss, um Windows-Authentifizierung mit dem SQL Server-Treiber von Connect füor JDBC zu verwenden.

Kerberos-Konfigurationsdatei

Für das Kerberos-Anmeldemodul ist der Kerberos-Bereichsname (Windows-Domänenname) und der KDC-Name (Windows-Domänencontrollername) für den betreffenden Kerberos-Bereich. Bei der Installation von Connect für JDBC wird eine Konfigurationsdatei installiert, die einen generischen Kerberos-Bereich und einen KDC-Namen angibt. Diese Datei heißt krb5.conf und ist im Verzeichnis /lib des Installationsverzeichnisses von Connect für JDBC installiert.

Sie müssen die Datei krb5.conf bearbeiten, um den Kerberos-Bereichsnamen und den KDC-Namen für Ihre Umgebung anzugeben. Wenn diese Datei nicht so bearbeitet wurde, dass sie einen gültigen Kerberos-Bereich und einen KDC-Namen enthält, wird folgender Fehler generiert:

```
Message:[DataDirect][SQLServer JDBC Driver]Could not
      establish a connection using integrated security:
      No valid credentials provided
```

Der SQL Server von Connect für JDBC konfiguriert automatisch das Kerberos-Anmeldemodul so, dass die Kerberos-Konfigurationsdatei krb5.conf geladen wird, es sei denn die Systemeigenschaft java.security.krb5.conf wurde bereit so eingestellt, dass Sie auf eine andere Konfigurationsdatei verweist. Sie können den Kerberos-Bereichsnamen und den KDC-Namen, die in der Datei krb5.conf angegeben wurden, durch Festlegen der folgenden Systemeigenschaften überschreiben: java.security.krb5.realm und java.security.krb5.kdc.

Einrichten der Strategie zum Einfügen von Ereignissen von Active Data Objects (ADO)

Sentinel 5.1 bietet einen Rahmen zur Integration verschiedener Strategien zum Einfügen von Ereignissen in die Datenbank. Sentinel 5.1 bietet zwei Strategien zum Einfügen von Ereignissen in die MS SQL-Datenbank:

- JDBCLoadStrategy
- ADOLoadStrategy

Die zum Einfügen von Ereignissen zu verwendende Strategie richtet sich nach der Eigenschaft insert.strategy der Komponente EventStoreService in das_binary.xml.

Die JDBC-Strategie ist die Standardstrategie, die bereits vorkonfiguriert ist.

Die ADO-Strategie ist eine native Einfügestrategie für das schnellere Einfügen von Ereignissen. Bei dieser Strategie ist es erforderlich, dass die zusätzlichen Windows-Pakete auf dem Computer installiert werden, auf dem die DAS-Komponente ausgeführt wird. Im nächsten Abschnitt finden Sie Informationen über die Pakete, die installiert werden müssen. Die ADO-Strategie muss bei Konfigurationen verwendet werden, bei denen eine hohe Ereignisrate erwartet wird.

Die Anzahl der zum Einfügen in einer Gruppe zusammenzufassenden Ereignisse wird durch die Eigenschaft insert.batchsize festgelegt. Die Eigenschaft insert.batchsize wird von allen Strategien zum Einfügen von Ereignissen verwendet.

In den folgenden Abschnitten wird beschrieben, wie Sie zu den ADO-Lastenstrategien wechseln können.

Voraussetzungen für ADOLoadStrategy

Für den native ADO-Connector müssen .net-Framework und J# Redistributable Package auf demselben Computer ausgeführt werden wie die DAS-Binärdaten.

HINWEIS: Sie müssen ggf. ältere Versionen von .nnet-Framework und J# Redistributable Package deinstallieren und die aufgeführten Versionen in folgender Reihenfolge installieren.

- net framework 2.0 Beta 2, verfügbar unter http://www.microsoft.com/downloads/details.aspx?FamilyID=7ABD8C8F-287E-4C7E-9A4A-A4ECFF40FC8E&displaylang=en
- visual J# version 2.0 Beta 2, verfügbar unter http://www.microsoft.com/downloads/details.aspx?FamilyId=A2788A92-76AB-4BF4-893A-FA9FD5031F14&displaylang=en

Einrichten der ADO-Strategie zum Einfügen von Lastereignissen

Um die von Sentinel verwendete Strategie zum Einfügen von Ereignissen von der standardmäßig verwendeten JDBC-Einfügestrategie zur ADO-Einfügestrategie zu ändern, müssen einige Schritte durchgeführt werden.

Wechsel von der JDB-Einfügestrategie zur ADO-Einfügestrategie

1. Öffnen Sie die Datei %ESEC_HOME%\sentinel\config\das_binary.xml in einem Texteditor.
2. Führen Sie eine Suche nach folgendem Text durch:

   ```
   JDBCLoadStrategy
   ```

3. Ändern Sie diesen Text in:

   ```
   ADOLoadStrategy
   ```

4. Speichern Sie diese Änderung in der Datei das_binary.xml.
5. Starten Sie die DAS-Binäranwendung neu.

Sobald die DAS-Binäranwendung neu gestartet wurde, werden die Dateien%ESEC_HOME%\Sun-1.4.2\bin\ EventInsert.dll und EventJNICLIBridge.dll geladen und zum Einfügen der Ereignisse in die Datenbank über ADO verwendet.

Tipps für die ADO-Fehlersuche

Die ADO-Schnittstelle protokolliert Fehlermeldungen ausschließlich in der Datei%ESEC_HOME%\sentinel\log\ADOEventStoreError.log. Zu den ursprünglichen Fehlermeldungen, die in die Protokolldatei geschrieben werdne, können auch Meldungen über Datenbankverbindungsfehler gehören. In dieser Datei werden auch Ausnahmen protokolliert, die beim Einfügen von Ereignissen in die Datenbank auftreten. Beachten Sie: In dieser Datei werden ausschließlich Fehler protkolliert.

Um sicherzustellen, dass ADO ordnungsgemäß verbunden und geladen ist, müssen Sie die Protokolldatei das_binary überprüfen, die sich im Verzeichnis %ESEC_HOME%\sentinel\log befindet.

Die ADO-Schnittstelle protokolliert auch Fehler in der Protokolldatei das_binary im Verzeichnis %ESEC_HOME%\sentinel\log. Zu den in der Protokolldatei das_binary protokollierten Fehler gehören Fehler beim Auffinden/Laden der Datei EventJNICLIBridge.dll, Fehler bei der Herstellung einer Verbindung mit der Datenbank und Fehler beim Einfügen von Ereignissen/Ereignisverknüpfungen.

Wenn Fehlermeldungen darauf hinweisen, dass die nativen Connectors nicht ordnungsgemäß geladen wurden, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass auf dem Computer die richtige Version von .net Framework und J# Redistributable Package installiert ist.
- Stellen Sie sicher, dass sich die Dateien „EventJNICLIBridge.dll“ und „EventInsert.dll“ im Verzeichnis %ESEC_HOME%\Sun-1.4.2\bin\ befinden.

6 Datenmigration und Patch für Oracle unter Solaris

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

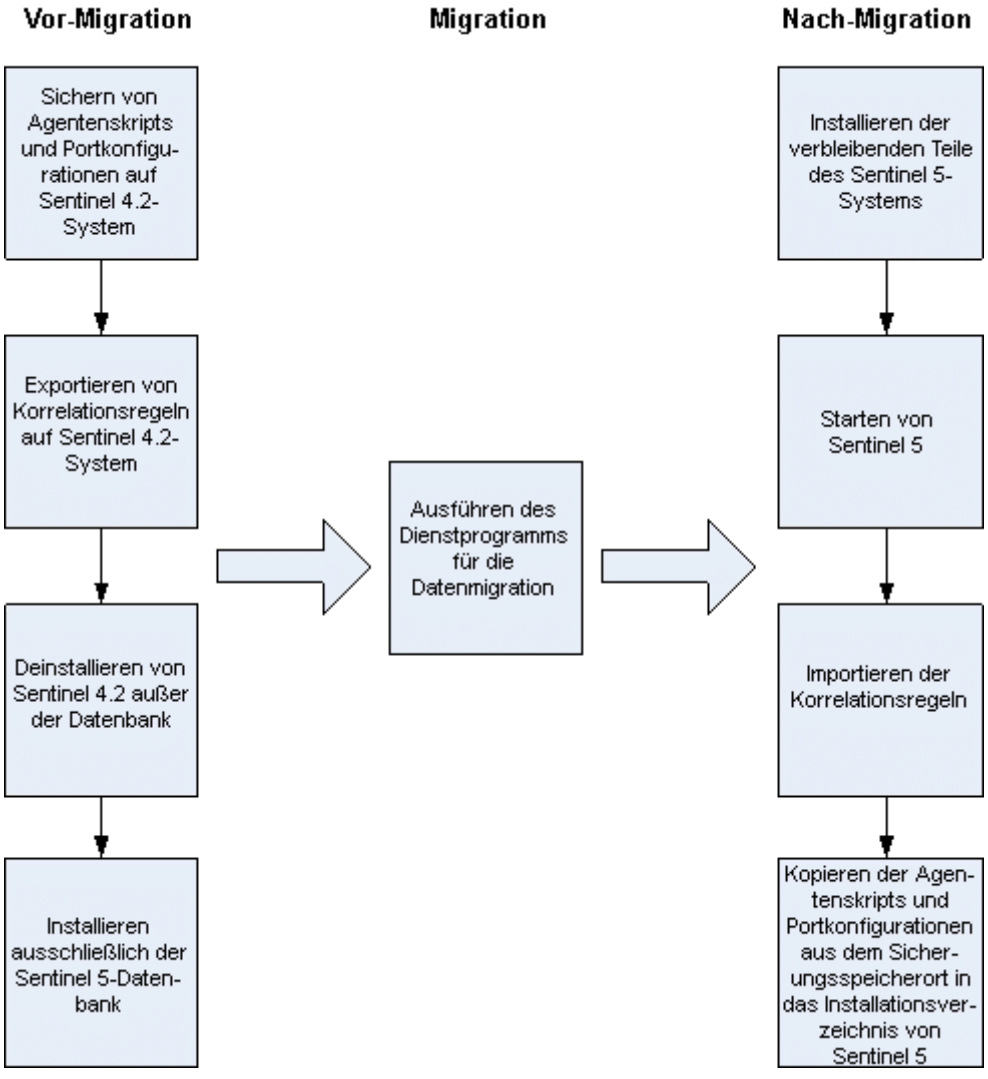
In diesem Kapitel werden folgende Themen behandelt:

Datenmigration und Aufrüstung von v4.2 auf v5.1.3

Die Aufrüstung auf Sentinel 5 mit Datenmigration ausgehend von v4.2.0 besteht aus folgenden Schritten:

- Vor-Migration
  - Sichern Sie die Sentinel-Datenbankinstanz: Dadurch können Sie die Datenbank von v4.2 wiederherstellen, falls unerwartete Fehler auftreten.
  - Sichern Sie alle über die rechte Maustaste aufzurufenden Systembefehle oder Skripts, die sich ggf. im Verzeichnis $ESEC_HOME befinden.
  - Exportieren Sie die Korrelationsregeln von Sentinel v4.2 (sofern vorhanden). Anweisungen finden Sie unter Vor-Migration – Export von Korrelationsregeln.
  - Sichern Sie Collector-Skripts und Portkonfigurationen. Anweisungen finden Sie unter Vor-Migration – Sichern von Collector-Skripts und Portkonfiguration.
  - Deinstallieren Sie Sentinel v4.2. mit Ausnahme der Datenbankkomponente. Anweisungen finden Sie unter Vor-Migration – Deinstallation von v4.2.
  - Installieren Sie ausschließlich die Sentinel 5-Datenbank. Anweisungen finden Sie unter Vor-Migration – Installation der Sentinel 5-Datenbank.
- Migration
  - Führen Sie das Dienstprogramm für die Datenmigration aus. Anweisungen finden Sie unter Migration.
- Nach-Migration
  - Installieren Sie die restlichen Komponenten von Sentinel 5. Anweisungen finden Sie unter Nach-Migration – Installation von Sentinel 5.
  - Installieren Sie das aktuellste Sentinel Service Pack.
  - Starten Sie Sentinel 5.
  - Importieren Sie die Korrelationsregeln (sofern vorhanden). Anweisungen finden Sie unter Post-Migration – Installing Sentinel 5.
  - Kopieren Sie Collector-Skripts und Portkonfigurationen aus dem Sicherungsspeicherort in das Installationsverzeichnis von Sentinel 5. Anweisungen finden Sie unter Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen.

- Konfigurieren Sie die Crystal Reporting-bezogenen Oracle 9i Client-Einstellungen so, dass sie auf die Sentinel 5-Datenbank verweisen und importieren Sie die Crystal Reports-Schablonen für Sentinel 5. Anweisungen finden Sie unter Nach-Migration – Konfigurieren von Sentinel 5 für Crystal Reporting.



Sentinel Server

Für Sentinel 5 muss die frühere Version der Software deinstalliert werden, bevor die Komponenten von Server-Komponenten von Sentinel 5 hinzugefügt werden. Deinstallieren Sie nicht die frühere Version (v4.2) der Datenbank, da diese für die Migration von Daten von v4.2 zu Sentinel 5 erforderlich ist. Sichern Sie vor der Deinstallation den Sentinel Server-Computer (Installationsverzeichnis $ESEC_HOME und Stammlaufwerk). Dadurch können Sie v4.2 wiederherstellen, falls unerwartete Fehler auftreten.

Detaillierte Anweisungen für die Datenmigration und die Aufgaben vor und nach der Installation finden Sie weiter unten.

Collector Manager

Für Sentinel 5 müssen alle Collector Manager-Instanzen von v4.2 deinstalliert werden, bevor die Sentinel 5 Collector Manager-Software installiert wird. Sichern Sie den v4.2 Collector Manager-Computer (Installationsverzeichnis $ESEC_HOME und Stammlaufwerk), bevor Sie die Deinstallation vornehmen.

Speichern Sie für jeden Computer, auf dem v4.2 Collector Manager ausgeführt wird und bei dem wenigstens ein Port konfiguriert ist, eine Kopie des Inhalts der folgenden Verzeichnisse an einem leicht zugänglichen Speicherort. Die Inhalte dieser Verzeichnisse werden während der Nach-Migration verwendet, um die Port-Einrichtung in der v4.2-Installation schnell neu konfigurieren zu können:

- $WORKBENCH_HOME/Agents – Enthält die Portkonfigurationsdateien.
- $WORKBENCH_HOME/Elements – Enthält die Collector-Skripts.
- Wenn Sie keine Kopie der Inhalte der oben angegebenen Verzeichnisse erstellen, müssen Sie alle Collector-Skripts und Ports völlig neu konfigurieren.

HINWEIS: Collector Manager und Collector Builder von Version 4.2 sind nicht mit v5-Komponenten kompatibel.

Detaillierte Anweisungen für die Datenmigration und die Aufgaben vor und nach der Installation finden Sie weiter unten.

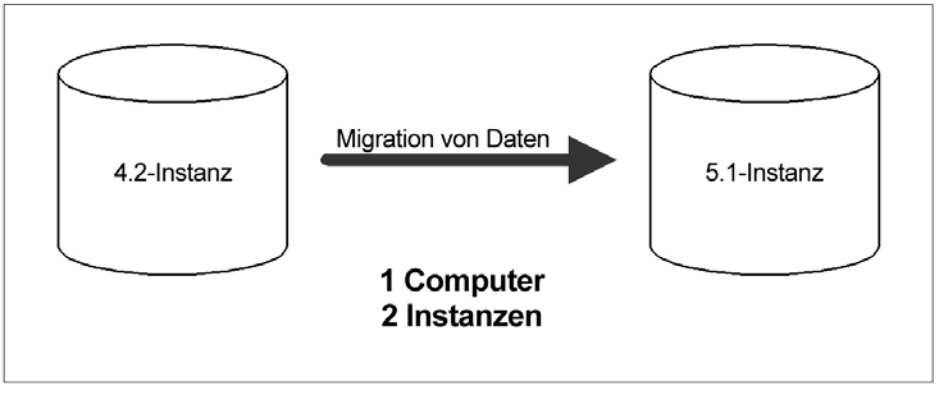
Crystal Reporting-Server

Nach dem Aufrüsten auf Sentinel 5 müssen die aktuellsten Berichte aus dem aktuellsten Service Pack verwendet werden. Die neuen Berichte entsprechen dem neuen Datenbankschema. Das aktuelle Service Pack können Sie beim technischen Support von Novell anfordern.

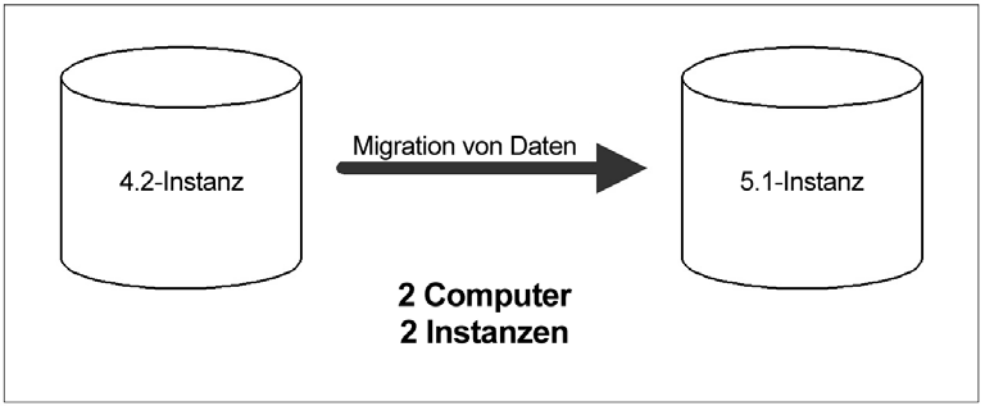
Datenbankserver

Es wird ein Dienstprogramm für die Sentinel 5-Datenmigration bereitgestellt, mit dem Daten von einer Sentinel 4.2.0-Datenbank unter Solaris 8/9 auf eine Sentinel 5.1.3-Datenbank unter Solaris 9 kopiert werden können. Das Dienstprogramm für die Datenmigration unterstützt die Migration für:

- 1 Computer mit 2 Datenbankinstanzen



- 2 Computer mit jeweils 1 Datenbankinstanz



Folgende Daten werden vom Dienstprogramm migriert:

- Benutzer und zugewiesene Berechtigungen
- Filter
- Konfigurationsoptionen für das Kontextmenü
- Umbenannte CV-Tags
- Partitions- und Archivkonfigurationen
- Fälle aus v4.2 werden als Vorfälle in v5 kopiert.
- Vorfälle und vorfallsbezogene Ereignisse

HINWEIS: Das Dienstprogramm zur Datenmigration migriert KEINE Ereignisdaten, ausgenommen Ereignisdaten, die mit Vorfällen verknüpft sind. Nur Ereignisdaten, die mit Vorfällen verknüpft sind, werden migriert.

HINWEIS: Vorfallsereignisdaten können nicht in Sentinel Control Center angezeigt werden. Vorfallsereignisdaten können entweder über Crystal Reporting oder über SQL-Abfragen eingesehen werden.

Detaillierte Anweisungen für die Datenmigration und die Aufgaben vor und nach der Installation finden Sie weiter unten.

Vor-Migration – Export von Korrelationsregeln

Exportieren von Korrelationsregelsätzen

1. Öffnen Sie in v4.2 Sentinel Console auf der Registerkarte „Admin“ das Fenster „Korrelationsregeln“.
2. Wählen Sie einen Regelsatz aus.
3. Klicken Sie auf *Exportieren*. Ein Dateibrowser wird geöffnet. Wechseln Sie zu dem Zielgerät, auf das die Regel geschrieben werden soll, und klicken Sie auf *OK*. Der Regelsatz wird als xml-Datei exportiert.

Vor-Migration – Sichern von Collector-Skripts und Portkonfiguration

Sichern von Collector-Skripts und Portkonfiguration

1. Erstellen Sie auf allen Sentinel v4.2-Computern, auf denen Collector Manager ausgeführt wird, ein Verzeichnis zum Speichern aller Collector-Skripts und Portkonfigurationen für den betreffenden Computer.

2. Erstellen Sie in dem soeben erstellten Verzeichnis eine Textdatei mit dem Namen aller Collectors, die von einer Portkonfiguration auf dieser Collector Manager-Instanz verwendet werden. Bestimmen Sie mithilfe einer Collector Builder-Instanz, welche Collectors von dieser Collector Manager-Instanz verwendet werden. Wenn die betreffende Collector Manager-Instanz unter Solaris ausgeführt wird, müssen Sie eine Collector Builder-Instanz auf einem Windows -Computer verwenden (Collector Builder wird unter Solaris nicht unterstützt).
3. Kopieren Sie folgende Verzeichnisse in das soeben erstellte Verzeichnis:
   - $WORKBENCH_HOME/Agents
   - $WORKBENCH_HOME/Elements

Vor-Migration – Deinstallation von v4.2

Deinstallation von v4.2

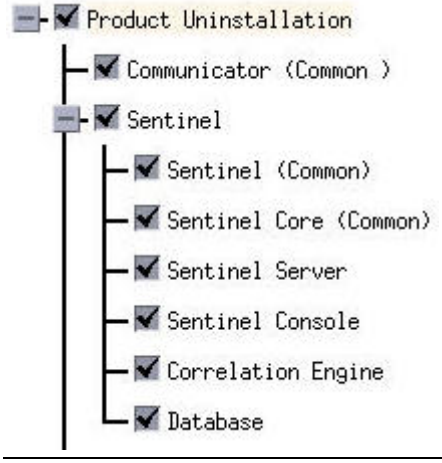
1. Schließen Sie alle Sentinel Console- und Collector Builder-Instanzen auf dem Sentinel v4.2-Computer und allen Client-Computern.
2. Melden Sie sich als Benutzer „root“ an.
3. Stoppen Sie Sentinel Server.
4. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/_uninst
   ```

5. Geben Sie Folgendes ein:

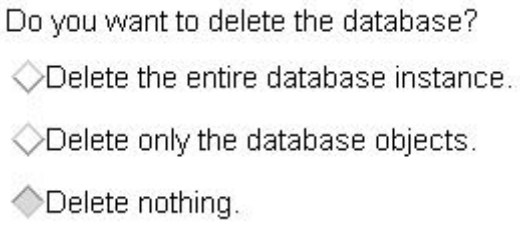
   ```
   ./uninstall.bin
   ```

6. Folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie die zu deinstallierenden Anwendungen aus. Wählen Sie alle Funktionen aus.



HINWEIS: Wenn Sie Drittanbietersoftware verwenden, wählen Sie diese für die Deinstallation aus.

7. Klicken Sie sich durch die Eingabeaufforderungen auf dem Bildschirm, bis das Fenster für die Datenbankdeinstallation geöffnet wird.
8. Klicken Sie im Fenster „Database Uninstall“ (Datenbankdeinstallation) auf *Delete nothing* (Nichts löschen).



9. Klicken Sie sich durch die restlichen Deinstallationsfenster.
10. Booten Sie das System neu.

Vor-Migration – Installation der Sentinel 5-Datenbank

Sentinel 5-Datenbankinstallation

1. Vergewissern Sie sich, dass Sie gemäß den Angaben in Abschnitt „Sentinel-Datenbank“ in Kapitel 4 die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben: *Installieren von Sentinel 5 für Oracle, Vor der Installation von Sentinel 5 für Oracle*.
2. Überprüfen Sie die Oracle-Einrichtung anhand des Abschnitts „Oracle-Einrichtung“ in *Kapitel 3*: *Installieren von Sentinel 5 für Oracle, Vor der Installation von Sentinel 5 für Oracle*.
3. Melden Sie sich als Benutzer „root“ an.
4. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
5. Wechseln Sie auf der CD zum vollständigen Verzeichnis.
6. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   Für GUI-Modus:

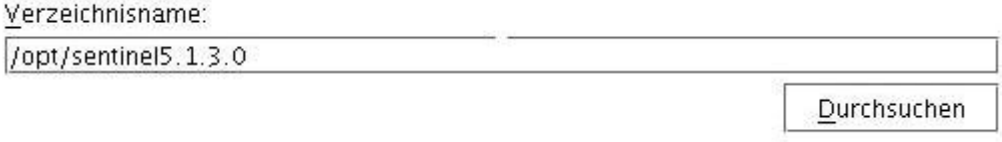
   ```
   ./setup.sh
   ```

   oder

   Für Textmodus („kopflos“):

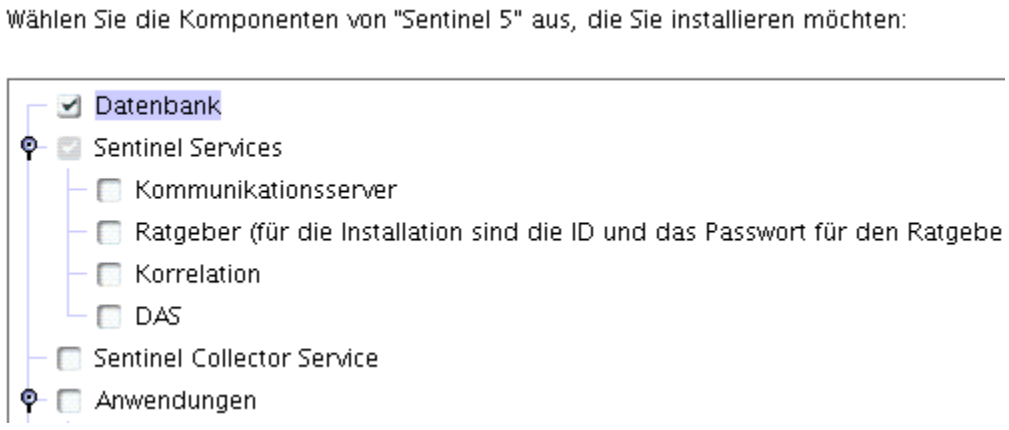
   ```
   ./setup.sh –console
   ```

7. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
8. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
9. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



10. Wählen Sie *Benutzerdefiniert* (Standard). Klicken Sie auf *Weiter*.
11. Heben Sie bei den zu installierenden Funktionen die Auswahl aller Funktionen auf und wählen Sie *Nur Datenbank* aus. Klicken Sie auf *Weiter*.

HINWEIS: Achten Sie darauf, die Auswahl der übergeordneten Funktion *Sentinel Services* aufzuheben. Sie wird abgeblendet mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.



12. Geben Sie den Benutzernamen des Betriebssystem-Sentinel-Administrators ein und den Standort seines Basisverzeichnisses. Das ist der Name des Benutzers, dem das installierte Sentinel-Produkt gehört. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem Basisverzeichnis im angegebenen Verzeichnis erstellt.
    - Benutzername des Betriebssystem-Administrators – Standardmäßig „esecadm“
    - Basisverzeichnis des Betriebssystem-Administrators – Standardmäßig /export/home. Wenn der Benutzername „esecadm“ lautet, ist das dazugehörige Basisverzeichnis /export/home/esecadm.

HINWEIS: Wird ein neuer Benutzer erstellt, muss sein Passwort manuell eingerichtet werden und nicht innerhalb dieses Installationsprogramms. Es wird dringend empfohlen, dass Sie das sofort durch Anmelden beim System nach der Installation des Produkts vornehmen.

HINWEIS: Um die strengen Sicherheitskonfigurationen zu erfüllen, die von Common Criteria Certification gefordert werden, benötigt Sentinel ein starkes Passwort mit folgenden Eigenschaften:

1. Wählen Sie Passwörter aus, die mindestens 8 Zeichen umfassen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, ein Sonderzeichen (#$_) und eine Zahl (0-9) enthalten. Verwenden Sie keine Leerzeichen.

2. Das Passwort darf nicht Ihren Email-Namen oder einen Teil Ihres vollständigen Namens enthalten.

3. Bei Ihrem Passwort sollte es sich nicht um ein „übliches“ Wort handeln (z. B. kein Wort, das im Wörterbuch steht oder ein allgemein gebräuchliches umgangssprachliches Wort).

4. Ihr Passwort sollte keine Wörter aus irgendeiner Sprache enthalten, da es zahlreiche Programme zu Knacken von Passwörtern gibt, die in wenigen Sekunden Millionen möglicher Wortkombinationen durchgehen können.

5. Sie sollten ein Passwort wählen, das Sie sich merken können und das dennoch komplex ist. Beispiel: MSi5!JalT (Mein Sohn ist 5 Jahre alt) oder iLs5#JiK (Ich lebe seit 5 Jahren in Köln).

13. Geben Sie Hostnamen (bzw. IP-Adresse) und Portnummer (Standard: 10012) für den Kommunikationsserver ein. Klicken Sie auf *Weiter*.
14. Wählen Sie die Serverplattform der Zieldatenbank als Oracle aus und wählen Sie eines der folgenden Elemente:
    - Neue Datenbank mit Datenbankobjekten erstellen – erstellt eine neue Oracle-Datenbankinstanz und füllt die neue Instanz mit Datenbankobjekten
    - Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen – fügt nur Datenbankobjekte zu einer bestehenden Oracle-Datenbankinstanz hinzu. Wenn Sie eine vorhandene Oracle-Datenbankinstanz verwenden, muss diese bis auf die Präsenz des esecdba-Benutzers leer sein.
15. Geben Sie das Verzeichnis für das Datenbankinstallationsprotokoll ein (Standard: $ESEC_HOME/logs/db). Übernehmen Sie den Standardwert für „Verzeichnis für das Protokoll der Datenbankinstallation“ oder klicken Sie auf „Durchsuchen“, um einen anderen Speicherort anzugeben.

16. Bestätigen Sie den Oracle-Standardbenutzernamen, indem Sie auf *OK* klicken.

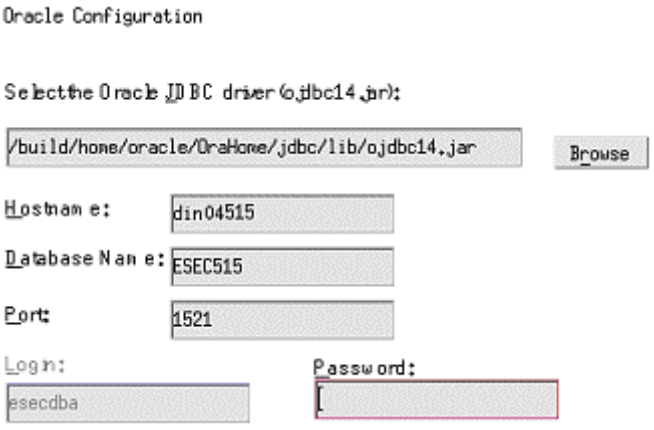
17. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Folgendes ein:
    - Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
    - Hostname – Der Hostname des Computers für die Installation der Datenbank. Dieses Feld lässt sich nicht konfigurieren, wenn Sie eine neue Datenbankinstanz erstellen.
    - Datenbankname – Der Name der zu installierenden Datenbankinstanz.

HINWEIS: Sie müssen der Datenbank einen anderen Namen zuweisen als den in der 4.2-Installation angegebenen.

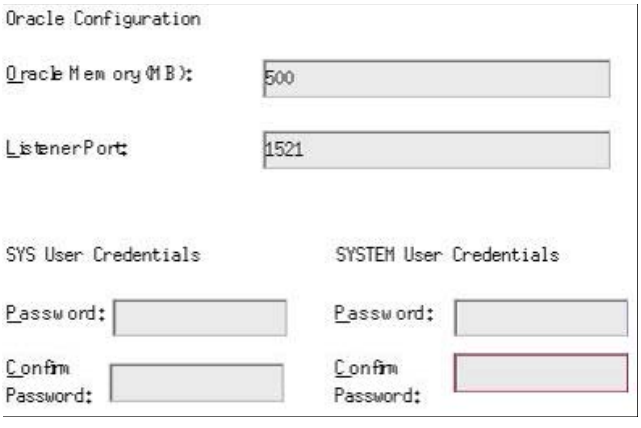
18. Wenn Sie einer vorhandenen leeren Oracle-Datenbank Datenbankobjekte hinzufügen, werden Sie aufgefordert, die folgenden Informationen einzugeben.
    - Pfad für die Oracle JDBC-Treiberdatei (typischer Name der jar-Datei lautet ojdbc14.jar). Das ist der vollständige Pfad zur jar-Datei, für gewöhnlich $ORACLE_HOME/jdbc/lib/ojdbc14.jar (Umgebungsvariablen können in diesem Feld nicht verwendet werden).
    - Datenbank-Hostname oder IP-Adresse – Der Name oder die IP-Adresse des Host mit der Oracle-Datenbank, der Sie Datenbankobjekte hinzufügen möchten. Das kann der lokale Hostname oder ein Remote-Hostname sein.
    - Datenbankname – Der Name der bestehenden leeren Oracle-Datenbankinstanz, zu der Datenbankobjekte hinzugefügt werden sollen (standardmäßig ESEC). Sie müssen der Datenbank einen anderen Namen zuweisen als den in der 4.2-Installation angegebenen. Dieser Datenbankname muss als Servicename in der Datei tnsnames.ora (im Verzeichnis $ORACLE_HOME/network/admin/) auf dem Computer, auf dem Sie das Installationsprogramm ausführen, enthalten sein.

HINWEIS: Wenn der Datenbankname nicht in der Datei tnsnames.ora enthalten ist, gibt das Installationsprogramm zu diesem Zeitpunkt in der Installation keinen Fehler aus (weil es die Verbindung über eine direkte JDBC-Verbindung überprüft). Die Datenbankinstallation scheitert erst dann, wenn das Datenbankinstallationsprogramm versucht, die Verbindung mit der Datenbank über sqlplus herzustellen. Wenn die Datenbankinstallation zu diesem Zeitpunkt scheitert, sollten Sie –ohne das Installationsprogramm zu beenden– den Service-Namen für die Datenbank in der Datei tnsnames.ora auf dem betreffenden Computer ändern, im Installationsprogramm zum ersten Bildschirm zurückblättern und dann den Vorgang erneut durchführen. Dadurch wird versucht, die Datenbankinstallation mit den neuen Werten in der Datei tnsnames.ora durchzuführen.

    - Datenbank-Port (Standard: 1521)
    - Geben Sie für Sentinel-Datenbankadministratoren (DBA) das Passwort für den Benutzer „esecdba“ ein. Das esecdba-Passwort muss dem esecdba-Passwort der v4.2-Installation entsprechen. Das Benutzernamenfeld in dieser Eingabeaufforderung lässt sich nicht bearbeiten.

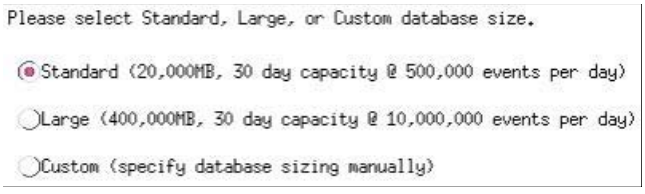


19. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, sehen Sie die folgende Eingabeaufforderung:
    - Oracle-Speicher (MB) – Die Menge RAM, die dieser Oracle-Datenbankinstanz zugeordnet wird.
    - Listener Port – Der Port, an dem der Oracle-Listener erstellt werden soll (standardmäßig 1521).
    - SYS-Benutzerpasswort und Passwortbestätigung – SYS ist ein Oracle-Standardbenutzer, der in der neuen Datenbankinstanz erstellt wird. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.
    - SYSTEM-Benutzerpasswort und Passwortbestätigung – SYSTEM ist ein Oracle-Standardbenutzer, der in der neuen Datenbankinstanz erstellt wird. Das Passwort dieses Benutzers wird auf den hier angegebenen Wert gesetzt.



20. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, die Größe der Datenbank einzugeben. Es stehen folgende Optionen zur Auswahl:
    - Standard (20 GB)
    - Groß (400 GB)
    - Benutzerdefiniert (manuelle Größenfestlegung). Wenn Sie diese Option ausgewählt haben, werden Sie zur Eingabe folgender Informationen aufgefordert:
        - Ursprüngliche Größe der einzelnen Datenbankdateien in MB (100–10.000)
        - Maximale Größe der einzelnen Datenbankdateien in MB (2.000–100.000)

- Größe aller Datenbankdateien in MB (7.000–2.000.000)
- Größe der einzelnen Protokolldateien in MB (100–100.000)



21. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, werden Sie aufgefordert, den Speicherort für folgende Datenbankdateien einzugeben:

HINWEIS: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung sollten diese Speicherorte auf unterschiedlichen E/A-Geräten liegen.

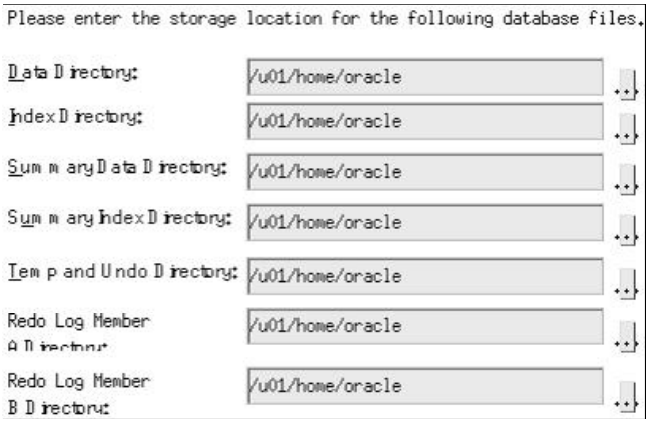
Diese Verzeichnisse werden nicht vom Installationsprogramm erstellt. Sie müssen also extern erstellt werden, um mit dem nächsten Schritt fortfahren zu können.

Der Oracle-Benutzer muss über eine Schreibberechtigung für diese Verzeichnisse verfügen. Um dem Oracle-Benutzer eine Schreibberechtigung für diese Verzeichnisse zu gewähren, führen Sie als Benutzer „root“ folgende Befehle für die einzelnen Verzeichnisse aus:

```
chown –R oracle:dba <Verzeichnispfad>
chmod –R 770 <Verzeichnispfad>
```

Dabei wird davon ausgegangen, dass „oracle“ Ihr Oracle-Benutzername und „dba“ Ihr Oracle-Gruppenname ist.

- Datenverzeichnis
- Indexverzeichnis
- Zusammenfassungsdatenverzeichnis
- Zusammenfassungsindexverzeichnis
- Temporäres Verzeichnis und Tabellenbereichsverzeichnis zum Rückgängigmachen
- Verzeichnis für Redo-Protokollmitglied A
- Verzeichnis für Redo-Protokollmitglied B



22. Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Authentifizierungsinformationen für den Sentinel Database Administrator (DBA) ein. Hierbei handelt es sich um „esecdba“, den Eigentümer der Datenbankobjekte.

23. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Anwendungsdatenbank ein. Hierbei handelt es sich um „esecapp“, den Benutzernamen für die Sentinel-Anwendung, den die Sentinel-Prozesse verwenden, um eine Verbindung zu der Datenbank herzustellen.
24. Geben Sie Authentifizierungsinformationen für den Benutzer der Sentinel-Administratordatenbank ein. Hierbei handelt es sich um „esecadm“, den Sentinel-Administratorbenutzer.
25. Klicken Sie im Zusammenfassungsfenster für die Datenbankinstallation auf *Weiter*.
26. Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten. Klicken Sie auf *Fertig stellen*, um das System neu zu booten.

Migration

Das Dienstprogramm für die Datenmigration migriert nur folgende Elemente:

- Benutzer und zugewiesene Berechtigungen
- Filter
- Konfigurationsoptionen für das Kontextmenü
- Umbenannte CV-Tags
- Partitions- und Archivkonfigurationen
- Fälle aus v4.2 werden als Vorfälle in v5 kopiert.
- Vorfälle und vorfallsbezogene Ereignisse

HINWEIS: Das Dienstprogramm zur Datenmigration migriert KEINE Ereignisdaten, ausgenommen Ereignisdaten, die mit Vorfällen verknüpft sind. Nur Ereignisdaten, die mit Vorfällen verknüpft sind, werden migriert.

HINWEIS: Vorfallsereignisdaten können nicht über Sentinel Control Center angezeigt werden. Vorfallsereignisdaten können entweder über Crystal Reporting oder über SQL-Abfragen eingesehen werden.

Für Sentinel 4.2-Datenbanken, die nicht esecdba als Eigentümer des Sentinel-Datenbankschemas verwenden

HINWEIS: Bei diesem Verfahren wird die esecdba-ID zur v4.2-Datenbank hinzugefügt, um die Datenmigration von v4.2 auf v5 zu ermöglichen.

1. Melden Sie sich unter Solaris als Eigentümer der Oracle-Software an.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/utilities/db/scripts/ddl/oracle/Migration
   ```

3. Stellen Sie mithilfe von SQL*Plus als SYSDBA eine Verbindung mit der v4.2-Datenbank her.
4. Geben Sie an der SQL-Eingabeaufforderung (SQL>) Folgendes ein:

   ```
   @import_add_esecdba.sql
   ```

5. Beenden Sie SQL*Plus.

HINWEIS: Nach der Durchführung der Datenmigration können Sie mithilfe von Oracle Enterprise Manager den esecdba-Benutzer aus der Sentinel 4.2-Datenbank löschen.

HINWEIS: Unter Solaris verwendet das Dienstprogramm für die Datenmigration Oracle*Net für die Verbindung mit der Sentinel 5-Datenbank und zwischen den Datenbanken von Sentinel 5 und 4.2. Vergewissern Sie sich, dass die Datei tnsnames.ora, über die Sie das Dienstprogramm für die Datenmigration ausführen, Einträge sowohl für die Sentinel 4.2- als auch für die Sentinel 5-Datenbank enthält, sodass Oracle*Net-Verbindungen hergestellt werden können.

1. Melden Sie sich als Benutzer „root“ an.
2. Überprüfen Sie die Umgebungsvariablen, um sicherzustellen, dass Java (Version 1.4.2) sich in PATH befindet. Diese Prüfung lässt sich durch Ausführung des folgenden Befehls in der Befehlszeile durchführen:

   ```
   java -version
   ```

   Wenn der oben angegebene Befehl nicht erfolgreich ist, müssen Sie entweder den Ort suchen, an dem Java in Ihrem System installiert ist, oder Java herunterladen und installieren. Aktualisieren Sie anschließend die Umgebungsvariable PATH, sodass sie die ausführbare Java-Datei enthält. Beispiel für den Fall, dass Java im Verzeichnis installiert ist:

   ```
   /opt/sentinel5.1.3.0/Sun-1.4.2
   ```

   Fügen Sie folgende Zeichenkette am Anfang der Umgebungsvariablen PATH ein:

   ```
   /opt/sentinel5.1.3.0/Sun-1.4.2/bin:
   ```

3. Mounten Sie die Sentinel 5-Software-Installations-CD auf dem Datenbankserver, auf dem sich die Sentinel 5-Datenbank befindet.
4. Wechseln Sie zum folgenden Verzeichnis auf der Sentinel 5-Software-Installations-CD:

   ```
   sentinel/dbsetup/bin
   ```

5. Führen Sie folgenden Befehl aus:

   ```
   ./MigrateDb.sh
   ```

6. Sie werden zur Eingabe folgender Informationen aufgefordert:
   - Hostname der Datenbank (auf der die Sentinel 5-Datenbank, zu der Sie migrieren, ausgeführt wird)
   - Zieldatenbankname (der Sentinel 5-Datenbank, zu der Sie migrieren)
   - esecdba-Passwort (das Passwort für den esecdba-Benutzer muss auf der Sentinel v4.2- und der Sentinel v5-Datenbank übereinstimmen)
   - Name der Quelldatenbank (v4.2-Datenbankname)
   - Protokollverzeichnis (Speicherort für die Migrationsprotokolldateien)
   - Migrationsoption:
     - (1) Systemeinstellungen
     - (2) Vorfälle/Fälle
     - (3) Beides
     - (4) Fertig

HINWEIS: Vorfälle und Fälle sollten erst nach der erfolgreichen Migration der Systemeinstellungen migriert werden.

HINWEIS: Wenn die Migration der Systemeinstellungen scheitert, deinstallieren Sie die Sentinel 5-Datenbank, indem Sie auswählen, dass nur die Datenbankobjekte gelöscht werden sollen. Installieren Sie anschließend die Sentinel 5-Datenbank erneut, indem Sie die Option „Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen“ auswählen. Führen Sie abschließend die Anweisungen zur Datenmigration erneut aus.

HINWEIS: Wenn die Vorfallsmigration nicht erfolgreich ist, führen Sie sie erneut aus. Das Dienstprogramm für die Migration beginnt beim Fehlerpunkt erneut. Es müssen keine zusätzlichen Bereinigungsaufgaben durchgeführt werden.

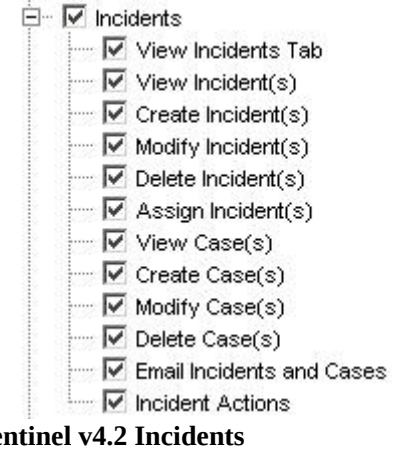
HINWEIS: Nach der Durchführung der Datenmigration können Sie mithilfe von Oracle Enterprise Manager den esecdba-Benutzer aus der Sentinel 4.2-Datenbank löschen, wenn Sie ihn wegen des Datenmigrations-Dienstprogramms hinzufügen mussten.

Nach-Migration – Installation von Sentinel 5

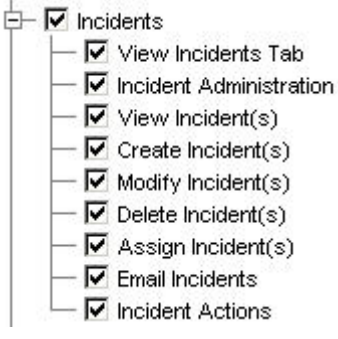
In Sentinel 5 sind folgende Funktionen neu oder wurden geändert bzw. entfernt.

- iTRAC – Dies ist eine neue Funktion. Die zugehörigen Benutzerberechtigungen sind:

- Incidents – „Vorfallsverwaltung“ wurde hinzugefügt. Alle fallbezogenen Funktionen wurden entfernt. Die zugehörigen Benutzerberechtigungen sind:



Sentinel v4.2 Incidents



Sentinel v5 Incidents

- Collector Management – in v4.2 ist dies Wizard Monitoring. „Registerkarte 'Wizards' anzeigen“ wurde geändert in „Collectors anzeigen“. „Wizards und Collector steuern“ wurde geändert in „Collectors steuern“ und „Collector-Administration“. Die zugehörigen Benutzerberechtigungen sind:

Sentinel v4.2 Wizard Monitoring

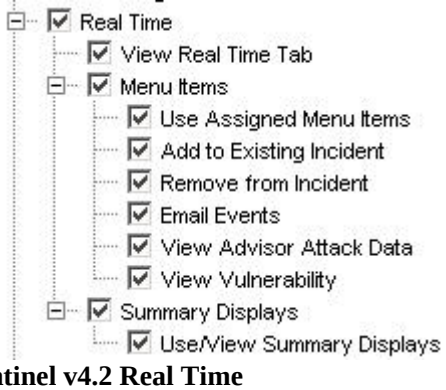
Sentinel v5 Collector Management

- Administration – DAS-Statisitk, Benutzersitzungsverwaltung und iTRAC-Rollenverwaltung hinzugefügt. „Korrelationsregeln“ wurde in „Korrelation“ umbenannt. Die Funktion „Ereigniskonfiguration“ wurde nach Sentinel Data Manager verlagert. „Benutzerkonfiguration“ wurde in „Benutzerverwaltung“ umbenannt. Die zugehörigen Benutzerberechtigungen sind:

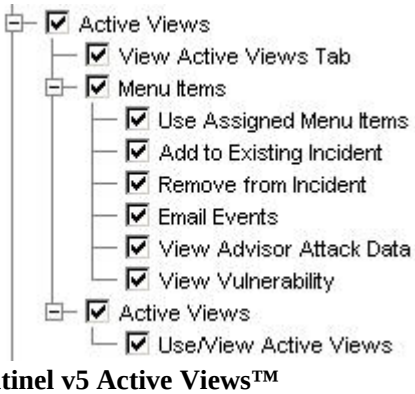
Sentinel v4.2 Administration

Sentinel v5 Administration

- ActiveViews™ – in v4.2 wurde diese Funktion „Real Time“ genannt. „Zusammenfassungsdisplays“ wurde in „Active Views“ umbenannt. Die zugehörigen Benutzerberechtigungen sind:



Sentinel v4.2 Real Time



Sentinel v5 Active Views™

- Die Funktion für die Systemübersicht ist in Sentinel 5 nicht verfügbar.

Installieren von Sentinel 5

1. Installieren Sie Sentinel 5, siehe Kapitel „Installation von Sentinel für Oracle“.
2. Installieren Sie das aktuellste Sentinel Service Pack.
3. Führen Sie folgende Schritte aus, wenn Sie eine neue Funktion für einen der bestehenden Benutzer aus v4.2 hinzufügen möchten.
   a. Vergewissern Sie sich, dass Sentinel Server ausgeführt wird.
   b. Melden Sie sich als Benutzer mit der Berechtigung zur Administration/Benutzerverwaltung (z. B. – esecadm) bei Sentinel Control Center an.
   c. Klicken Sie in Sentinel Control Center auf die Registerkarte „Admin“. Erweitern Sie im Navigationsfenster den Bereich „Benutzerkonfiguration“ oder klicken Sie in der Navigationsleiste auf *Admin > Benutzerkonfiguration.*

d. Klicken Sie mit der rechten Maustaste auf den Benutzer, für den Sie die Funktion hinzufügen möchten (z. B. – esecadm), und wählen Sie die Option *Benutzerdetails*. Klicken Sie auf die Registerkarte *Berechtigungen*.
e. Erweitern Sie iTRAC und weisen Sie die erforderlichen Berechtigungen zu.
f. Erweitern Sie Incidents und weisen Sie nach Bedarf „Incident Administration“ zu.
g. Erweitern Sie „Collector Management“ und weisen Sie nach Bedarf „Collector Administration“ zu.
h. Erweitern Sie „Administration“ und weisen Sie nach Bedarf „DAS-Statistik“, „Benutzersitzungsverwaltung“ bzw. „iTRAC-Rollenverwaltung“ zu.
i. Klicken Sie auf die Registerkarte *Funktionen* und weisen Sie nach Bedarf die Workflow-Funktion „Admin“ bzw. „Analyst“ zu.
j. Klicken Sie auf *OK*.

4. Importieren Sie gegebenenfalls etwaige Korrelationsregeln. Aus Sentinel 4.2 exportierte Regelsätze werden beim Import in Sentinel 5 als Regelordner angezeigt.
5. Kopieren Sie aus Sicherungsskripts von Collectors und Portkonfigurationen, indem Sie die Anweisungen in Abschnitt Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen befolgen.

Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen

Führen Sie auf jedem Computer, auf dem der Sentinel 5 Collector-Service (Collector Manager) installiert ist, folgende Schritte aus, um die Collector-Skripts und Portkonfigurationen, die in der Sentinel v4.2-Installation verwendet wurden, wieder zu erstellen.

So erstellen Sie die alten Collector-Skripts und Portkonfigurationen erneut

1. Stoppen Sie Collector Manager, indem Sie folgenden Befehl als esecadm-Benutzer ausführen:

   ```
   $ESEC_HOME/wizard/agent-manager.sh stop
   ```

2. Kopieren Sie aus dem Speicherort, in dem Sie eine Sicherungskopie des Verzeichnisses $WORKBENCH_HOME/Agents der Sentinel v4.2-Installation abgelegt haben, folgende Dateien in das Verzeichnis $WORKBENCH_HOME/Agents der aktuellen Sentinel 5-Installation (überschreiben Sie die Dateien, falls erforderlich):
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Lesen Sie die während der Vor-Migration erstellte Textdatei, in der alle von der Sentinel v4.2 Collector Manager-Installation auf diesem Computer verwendeten Collectors aufgelistet werden. Sie benötigen die Collector-Namen im nächsten Schritt.
4. Kopieren Sie aus dem Speicherort, in dem Sie eine Sicherungskopie des Verzeichnisses $WORKBENCH_HOME/Elements der Sentinel v4.2-Installation abgelegt haben, die Verzeichnisse, deren Namen mit den Collector-Namen in der Textdatei übereinstimmen, in das Verzeichnis $WORKBENCH_HOME/Elements der aktuellen Sentinel 5-Installation (überschreiben Sie die Verzeichnisse/Dateien, falls erforderlich).
5. Rufen Sie das Dienstprogramm UpgradePortCfgFile von der Website des technischen Support von Sentinel (hier herunterladen) ab.

6. Extrahieren Sie die ZIP-Datei UpgradePortCfgFile ZIP.
7. Öffnen Sie eine Befehlszeilenaufforderung und wechseln Sie in das Verzeichnis mit dem extrahierten Dienstprogramm UpgradePortCfgFile. Führen Sie in diesem Verzeichnis folgenden Befehl aus:

   ```
   ./UpgradePortCfgFile.sh
   ```

8. Führen Sie folgenden Befehl als Benutzer „root“ aus, um sicherzustellen, dass die Eigentümerschaft an den soeben kopierten Dateien ordnungsgemäß festgelegt wurde:

   ```
   chown –R esecadm:esec $ESEC_HOME/wizard
   ```

9. Starten Sie Collector Manager, indem Sie folgenden Befehl als esecadm-Benutzer ausführen:

   ```
   $ESEC_HOME/wizard/agent-manager.sh start
   ```

Nach-Migration – Konfigurieren von Sentinel 5 für Crystal Reporting

Gehen Sie wie folgt vor, wenn Sie Crystal Reporting für v4.2 ausgeführt haben und Crystal Reporting in Sentinel 5 ausführen möchten:

- Bearbeiten Sie die Crystal Reporting-bezogenen Oracle 9i Client-Einstellungen so, dass sie auf die Sentinel 5 -Datenbank verweisen.
- Importieren Sie die Crystal Reports-Schablonen (einschließlich der Schablonen für die Datenmigration) aus dem letzten Service Pack.

Weitere Informationen finden Sie im Installationskapitel zu „Crystal Reports“.

Patch zur Aufrüstung von v5.x.x auf v5.1.3

Führen Sie dieses Verfahren auf jedem Computer durch, auf dem Sentinel-Komponenten installiert sind.

Wenn Sie das Patch-Installationsprogramm von dem Computer ausführen, auf dem Sie ursprünglich die Datenbankkomponente installiert hatten, müssen Sie das Passwort des Sentinel-Datenbankadministrators (esecdba) kennen.

Aufrüsten von v5.x.x auf v5.1.3 für Solaris

1. Melden Sie sich als Benutzer „root“ an.
2. Erstellen Sie gegebenenfalls eine Sicherungskopie der Datei syslog.conf.

   HINWEIS: Wenn Sie v5.1.1sp1 oder höher ausführen und Änderungen an der Datei syslog.conf vornehmen, müssen Sie eine Kopie dieser Datei erstellen. Das Patch-Installationsprogramm überschreibt die Datei syslog.conf. Nach der Anwendung des Patch müssen Sie Ihre neue syslog.conf-Datei bearbeiten bzw. überschreiben, sodass sie mit ihrer ursprünglichen syslog.conf-Datei übereinstimmt.

3. Legen Sie die Sentinel-Patch-CD ein und mounten Sie sie.

4. Starten Sie das Installationsprogramm, indem Sie zum entsprechenden Patch-Verzeichnis auf der CD-ROM wechseln und folgenden Befehl ausführen:

   Für GUI-Modus:

   ```
   ./setup.sh
   ```

   oder

   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```

5. Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
6. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
7. Klicken Sie auf *Weiter*, bis das Fenster mit den Datenbankinformationen angezeigt wird.
8. Stellen Sie sicher, dass der Datenbanktyp korrekt ist. Wählen Sie den Speicherort des Protokollverzeichnisses für die Datenbankinstallation aus. Klicken Sie auf *Weiter*.
9. Vergewissern Sie sich, dass die Informationen für den Oracle-Server korrekt sind. Geben Sie das esecdba-Passwort ein. Folgen Sie den restlichen Eingabeaufforderungen des Installationsprogramms.

Aktualisieren des Syslog-Connectors

Wenn Sie die Syslog-Connector-Skripts aus einer Sentinel-Version vor 5.1.1.1 (d- h. – 5.0, 5.0.1.0, 5.1.0.0 oder 5.1.1.0) verwendet haben, müssen Sie die aktualisierten Syslog-Connector-Skripts verwenden, die im Patch enthalten sind. Um von der Verwendung des alten Syslog-Connector-Skripts zur Verwendung der neuen Syslog-Connector-Skripts überzugehen, müssen Sie das alte Skript entfernen und ein neues installieren.

Der Syslog-Connector wird mit Skripts installiert, die unter Windows und UNIX mit verbesserten Konfigurationsdateien ausgeführt werden. Außerdem wurde die Installation des Syslog-Proxyservers als Service vereinfacht.

So entfernen Sie den Syslog-Connector

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

So installieren Sie den Syslog-Connector

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Wenn Sie Änderungen an der Datei syslog.conf Ihrer ursprünglichen Installation vorgenommen haben, müssen Sie die neue syslog.conf-Datei bearbeiten oder überschreiben, sodass Sie der ursprünglichen syslog.conf-Datei entspricht. syslog.conf befindet sich an folgendem Speicherort:

   ```
   $ESEC_HOME/wizard/syslog/config
   ```

Zusätzliche Aktualisierung für v5.0.x auf v5.1.3

Nach der Patch-Aufrüstung von v5.0.x auf v5.1.3 müssen Sie die Berechtigungen für die Benutzerverwaltung und die Optionen für die Menükonfiguration aktualisieren. Optional können Sie die Berechtigungen für Serveransichten aktualisieren.

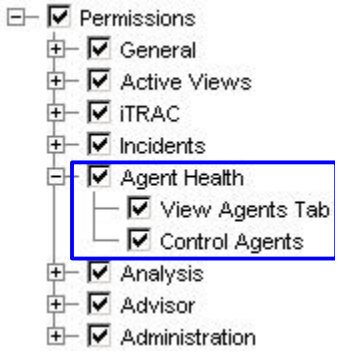
Aktualisieren der Benutzerverwaltungsberechtigungen von v5.0.x auf v5.1.3

Bei der Aufrüstung von v5.0.x auf v5.1.3 wird „Collector Health“ in „Collector Management“ geändert und eine zusätzliche Funktion, „Collector-Administration“, hinzugefügt

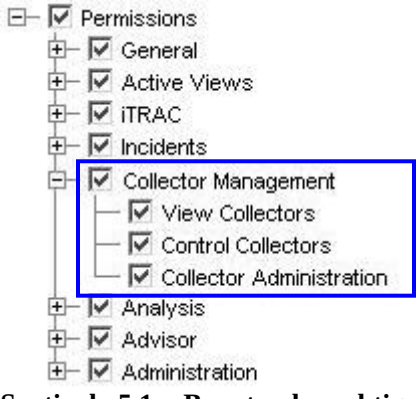
Aktualisieren der Berechtigungen für die Benutzerverwaltung

1. Melden Sie sich als Benutzer mit der Berechtigung zur Administration/Benutzerverwaltung bei Sentinel Control Center an.

   In v5.1 wurde „Collector Health“ unter „Berechtigungen“ in „Collector Management“ geändert und es wurden weitere Berechtigungen hinzugefügt.



Sentinel v5.0-Benutzerberechtigung



Sentinel v5.1.x-Benutzerberechtigung

2. Klicken Sie in Sentinel Control Center auf die Registerkarte „Admin“. Erweitern Sie im Navigationsfenster den Bereich „Benutzerkonfiguration“ oder klicken Sie in der Navigationsleiste auf *Admin > Benutzerkonfiguration.*
3. Klicken Sie mit der rechten Maustaste auf einen Admin-Benutzer (d. h. esecadm oder ein anderer Admin-Benutzer) > *Benutzerdetails.* Klicken Sie auf die Registerkarte *Berechtigungen*.
4. Erweitern Sie *Collector Management* und weisen Sie *Collector-Administration* zu. Klicken Sie auf *OK*.

Aktualisieren von Menükonfigurationsoptionen von v5.0.x auf v5.1.3

Wenn vor der Aufrüstung auf v5.1 zusätzliche Einträge in der Menükonfiguration erstellt wurden, müssen die Pfade zu den Befehlen aktualisiert werden. Ab Versopm 5.1.0.0 muss unter Solaris der in der Menükonfiguration auszuführende Befehl im Verzeichnis $ESEC_HOME/sentinel/exec vorhanden sein. Außerdem sind alle Pfade zu den in der Menükonfiguration ausgeführten Befehlen immer relativ zum Verzeichnis $ESEC_HOME/sentinel/exec. Wenn Sie einen Befehl an einem anderen Ort im Dateisystem ausführen müssen, erstellen Sie einen symbolischen Link von einem Speicherort unter $ESEC_HOME/sentinel/exec zu dem auszuführenden Befehl.

Die Menükonfiguration für „traceroute“ muss manuell von „tracert“ in „traceroute“ geändert werden, um ordnungsgemäß zu funktionieren.

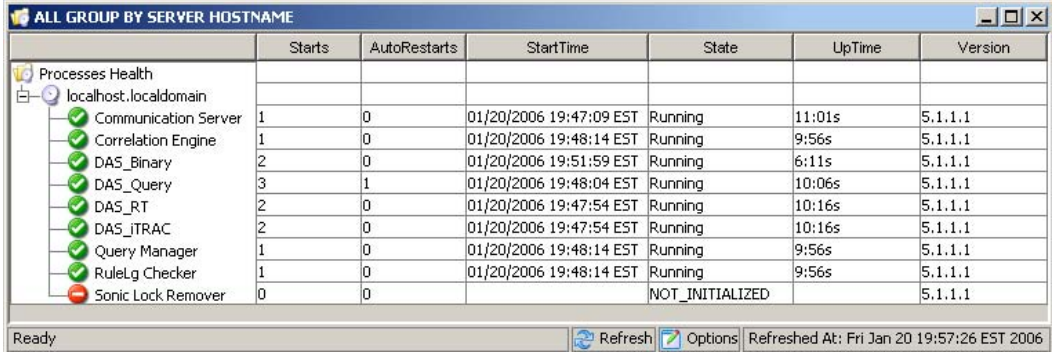
So fügen Sie eine Option zum Menü „Menükonfiguration“ hinzu

1. Melden Sie sich als Benutzer mit der Berechtigung zur Administration/Benutzerverwaltung bei Sentinel Control Center an.
2. Klicken Sie auf die Registerkarte *Admin*.
3. Klicken Sie im Admin-Navigator auf *Admin* > *Menükonfiguration*.
4. Klicken Sie im Fenster „Menükonfiguration“ auf *Bearbeiten* und markieren Sie ein Menüelement, das aktualisiert werden soll. Klicken Sie auf *Details*.
5. Nehmen Sie im Dialogfeld „Menükonfigurationen“ die notwendigen Änderungen an folgenden Elementen vor:
   - Befehlszeile/URL
   - Parameter – müssen in Prozentzeichen eingeschlossen sein (z. B. %EventName%)

   HINWEIS: Eine Liste der verfügbaren Tags, die Sie bei der Angabe von Paramtern verwenden können, erhalten Sie, wenn Sie im Dialogfeld „Menükonfiguration“ auf „Hilfe“ klicken oder im Sentinel-Referenzhandbuch für Benutzer im Kapitel „META-Tag“ nachschlagen.
6. Klicken Sie auf *OK*.
7. Klicken Sie auf *Speichern*.

Aktualisieren der Option „Serveransichten“ von v5.0.x auf v5.1.3

Um den Bildschirm „Serveransichten“ nach der Patch-Installation verwenden zu können, müssen Sie mithilfe des Benutzer-Managers dem Sentinel-Benutzer die Berechtigung „Serveransichten“ gewähren. Der Benutzer-Manager befindet sich unter der Registerkarte „Admin“ von Sentinel Control Center.



Crystal Reporting-Server

Nach der Aufrüstung auf Sentinel 5.1.3, einschließlich der Anwendung des letzten Service Pack, müssen Sie die Berichte aus dem letzten Service Pack importieren. Weitere Informationen finden Sie im Kapitel *Crystal Reports* im *Sentinel-Installationshandbuch*.

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter $ESEC_HOME/sentinel/config. Um diese Datei zu konfigurieren, führen Sie mailconfig.sh aus, um die Datei zu ändern, und mailconfigtest.sh, um Ihre Änderungen zu testen.

So konfigurieren Sie die Datei execution.properties

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

   ```
   ./mailconfig.sh -host <SMTP Server> -from <Quellen-
      Email-Adresse> -user
      <Mailauthentifizierungsbenutzer> –password
   ```

   Beispiel:

   ```
   ./mailconfig.sh -host 192.0.2.14 -from
      my_name@domain.com -user my_user_name –password
   ```

   Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

   ```
   Enter your password:*********
   Confirm your password:*********
   ```

   HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfigtest“ wie folgt aus:

   ```
   ./mailconfigtest.sh -to <Ziel-Email-Adresse>
   ```

   Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

   ```
   Email has been sent successfully!
   ```

Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

```
Subject: Testing Sentinel mail property

This is a test for Sentinel mail property set up. If
   you see this message, your Sentinel mail property
   has been configured correctly to send emails
```

7 Datenmigration und Patch für MS SQL

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

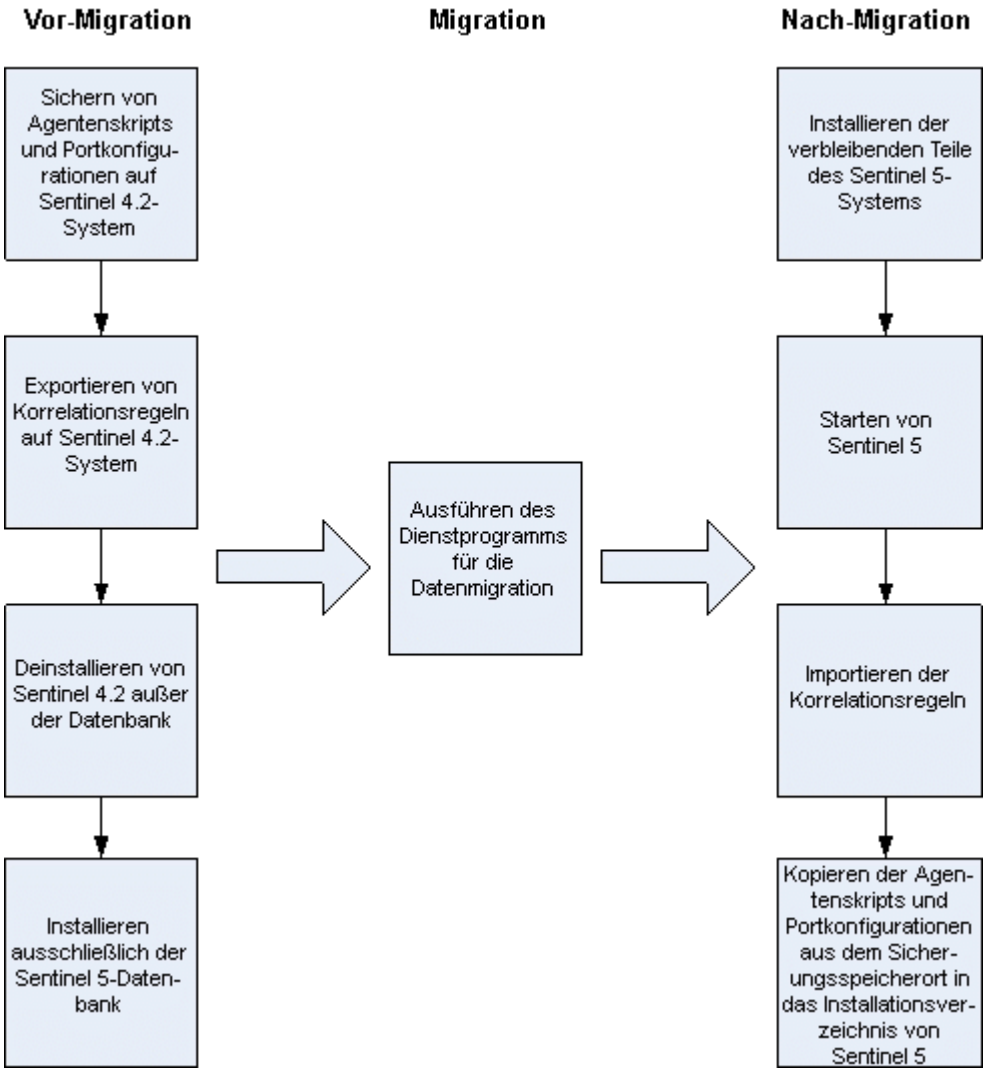
In diesem Kapitel werden Datenmigration und Aufrüstung für folgende Bereiche behandelt:

- Datenmigration und Aufrüstung von v4.2.1 auf v5.1.3.
- Patch zur Aufrüstung von v5.x.x auf v5.1.3

Datenmigration und Aufrüstung von v4.2 auf v5.1.3

Die Aufrüstung auf Sentinel 5 mit Datenmigration ausgehend von v4.2.0 besteht aus folgenden Schritten:

- Vor-Migration
  - Sichern Sie die Sentinel Server-Datenbankinstanz: Dadurch können Sie die Datenbank von v4.2 wiederherstellen, falls unerwartete Fehler auftreten.
  - Sichern Sie alle über die rechte Maustaste aufzurufenden Systembefehle oder Skripts, die sich ggf. im Verzeichnis %ESEC_HOME% befinden.
  - Exportieren Sie die Korrelationsregeln von Sentinel v4.2 (sofern vorhanden). Anweisungen finden Sie unter Vor-Migration – Export von Korrelationsregeln.
  - Sichern Sie Collector-Skripts und Portkonfigurationen. Anweisungen finden Sie unter Vor-Migration – Sichern von Collector-Skripts und Portkonfiguration.
  - Deinstallieren Sie Sentinel v4.2. mit Ausnahme der Datenbankkomponente. Anweisungen finden Sie unter Vor-Migration – Deinstallation von v4.2.
  - Installieren Sie ausschließlich die Sentinel 5-Datenbank. Anweisungen finden Sie unter Vor-Migration – Installation der Sentinel 5-Datenbank.
- Migration
  - Führen Sie das Dienstprogramm für die Datenmigration aus. Anweisungen finden Sie unter Migration.
- Nach-Migration
  - Installieren Sie die restlichen Komponenten von Sentinel 5. Anweisungen finden Sie unter Nach-Migration – Installation von Sentinel 5.
  - Installieren Sie das aktuellste Sentinel Service Pack.
  - Starten Sie Sentinel 5.
  - Importieren Sie die Korrelationsregeln (sofern vorhanden). Anweisungen finden Sie unter Nach-Migration – Installation von Sentinel 5.
  - Kopieren Sie Collector-Skripts und Portkonfigurationen aus dem Sicherungsspeicherort in das Installationsverzeichnis von Sentinel 5. Anweisungen finden Sie unter Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen.
  - Wenn Sie Crystal Server mit Sentinel ausführen, müssen Sie die Sentinel 5 Crystal Reports-Schablonen importieren. Anweisungen finden Sie unter Nach-Migration – Konfigurieren von Sentinel 5 für Crystal Reporting.



Sentinel Server

Für Sentinel 5 muss die frühere Version der Software deinstalliert werden, bevor die Komponenten von Server-Komponenten von Sentinel 5 hinzugefügt werden. Deinstallieren Sie nicht die frühere Version (v4.2) der Datenbank, da diese für die Migration von Daten von v4.2 zu Sentinel 5 erforderlich ist. Sichern Sie vor der Deinstallation den Sentinel Server-Computer (Installationsverzeichnis %ESEC_HOME% und Stammlaufwerk). Dadurch können Sie v4.2 wiederherstellen, falls unerwartete Fehler auftreten.

Detaillierte Anweisungen für die Datenmigration und die Aufgaben vor und nach der Installation finden Sie weiter unten.

Collector Manager

Für Sentinel 5 müssen alle Collector Manager-Instanzen von v4.2 deinstalliert werden, bevor die Sentinel 5 Collector Manager-Software installiert wird. Sichern Sie den v4.2 Collector Manager-Computer (Installationsverzeichnis %ESEC_HOME% und Stammlaufwerk), bevor Sie die Deinstallation vornehmen.

Speichern Sie für jeden Computer, auf dem v4.2 Collector Manager ausgeführt wird und bei dem wenigstens ein Port konfiguriert ist, eine Kopie des Inhalts der folgenden Verzeichnisse an einem leicht zugänglichen Speicherort. Die Inhalte dieser Verzeichnisse werden während der Nach-Migration verwendet, um die Port-Einrichtung in der v4.2-Installation schnell neu konfigurieren zu können:

- %WORKBENCH_HOME%/Agents – Enthält die Portkonfigurationsdateien.
- %WORKBENCH_HOME%/Elements – Enthält die Collector-Skripts.
- Wenn Sie keine Kopie der Inhalte der oben angegebenen Verzeichnisse erstellen, müssen Sie alle Collector-Skripts und Ports völlig neu konfigurieren.

HINWEIS: Collector Manager und Collector Builder von Version 4.2 sind nicht mit v5-Komponenten kompatibel.

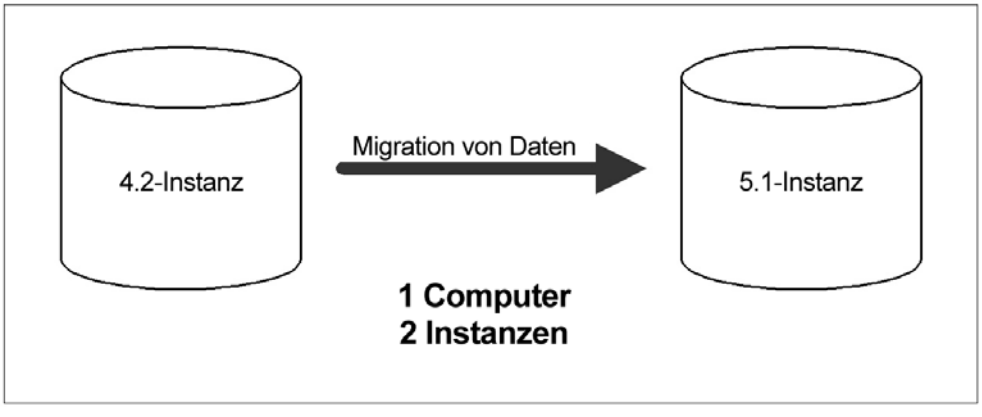
Detaillierte Anweisungen für die Datenmigration und die Aufgaben vor und nach der Installation finden Sie weiter unten.

Crystal Reporting-Server

Nach dem Aufrüsten auf Sentinel 5 müssen die aktuellsten Berichte aus dem aktuellsten Service Pack verwendet werden. Die neuen Berichte entsprechen dem neuen Datenbankschema. Das aktuelle Service Pack können Sie beim Sentinel Technical Support anfordern.

Datenbankserver

Es wird ein Dienstprogramm für die Sentinel 5-Datenmigration bereitgestellt, mit dem Daten von Sentinel 4.2.1 auf Sentinel v5.1.3 kopiert werden können. Das Dienstprogramm für die Datenmigration unterstützt die Migration nur, sofern sich die Sentinel 4.2.1-Datenbank und die 5.1.3-Datenbank auf demselben Computer und in derselben SQL Server-Instanz, jedoch in getrennten Datenbanken befinden.



Folgende Elemente werden migriert:

- Benutzer und zugewiesene Berechtigungen
- Filter
- Konfigurationsoptionen für das Kontextmenü
- Umbenannte CV-Tags
- Partitions- und Archivkonfigurationen
- Fälle aus v4.2 werden als Vorfälle in v5 kopiert.
- Vorfälle und vorfallsbezogene Ereignisse

HINWEIS: Das Dienstprogramm zur Datenmigration migriert KEINE Ereignisdaten, ausgenommen Ereignisdaten, die mit Vorfällen verknüpft sind. Nur Ereignisdaten, die mit Vorfällen verknüpft sind, werden migriert.

HINWEIS: Vorfallsereignisdaten können nicht über Sentinel Control Center angezeigt werden. Vorfallsereignisdaten können entweder über Crystal Reporting oder über SQL-Abfragen eingesehen werden.

Vor-Migration – Export von Korrelationsregeln

Importieren bzw. Exportieren von Korrelationsregelsätzen

1. Öffnen Sie in v4.2 Sentinel Console auf der Registerkarte „Admin“ das Fenster „Korrelationsregeln“.
2. Wählen Sie einen Regelsatz aus.
3. Klicken Sie auf *Exportieren*. Ein Dateibrowser wird geöffnet. Wechseln Sie zu dem Zielgerät, auf das die Regel geschrieben werden soll, und klicken Sie auf *OK*. Der Regelsatz wird als xml-Datei exportiert.

Vor-Migration – Sichern von Collector-Skripts und Portkonfiguration

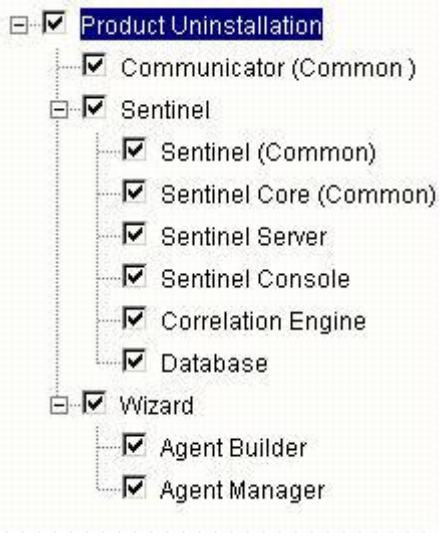
Sichern von Collector-Skripts und Portkonfiguration

1. Erstellen Sie auf allen Sentinel v4.2-Computern, auf denen Collector Manager ausgeführt wird, ein Verzeichnis zum Speichern aller Collector-Skripts und Portkonfigurationen für den betreffenden Computer.
2. Erstellen Sie in dem soeben erstellten Verzeichnis eine Textdatei mit dem Namen aller Collectors, die von einer Portkonfiguration auf dieser Collector Manager-Instanz verwendet werden. Bestimmen Sie mithilfe einer Collector Builder-Instanz, welche Collectors von dieser Collector Manager-Instanz verwendet werden. Wenn die betreffende Collector Manager-Instanz unter UNIX ausgeführt wird, müssen Sie eine Collector Builder-Instanz auf einem Windows-Computer verwenden (Collector Builder wird unter UNIX nicht unterstützt).
3. Kopieren Sie folgende Verzeichnisse in das soeben erstellte Verzeichnis:
   - %WORKBENCH_HOME%\Agents
   - %WORKBENCH_HOME%\Elements

Vor-Migration – Deinstallation von v4.2

Deinstallation von v4.2

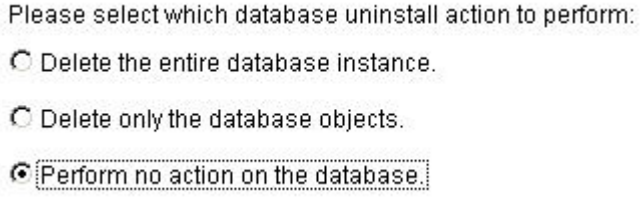
1. Gehen Sie auf Ihrem Sentinel v4.2-Computer wie folgt vor:
   - Schließen Sie alle Instanzen von Sentinel Console und Collector Builder
   - Klicken Sie auf *Start > Programme > Sentinel > Sentinel 4.2.1.x deinstallieren.*
2. Klicken Sie sich durch die Eingabeaufforderungen auf dem Bildschirm, bis das Fenster mit der Deinstallationsfunktion geöffnet wird. Wählen Sie alle Funktionen aus.



HINWEIS: Im Beispiel oben wird keine Drittanbieter-Integrationssoftware angezeigt. Wenn Sie Drittanbietersoftware verwenden, wählen Sie diese für die Deinstallation aus.

Klicken Sie sich durch die Eingabeaufforderungen auf dem Bildschirm, bis das Fenster für die Datenbankdeinstallation geöffnet wird.

3. Wählen Sie im Fenster für die Datenbankdeinstallation aus, dass keine Aktion für die Datenbank durchgeführt werden soll.



4. Klicken Sie sich durch die restlichen Deinstallationsfenster.

Vor-Migration – Installation der Sentinel 5-Datenbank

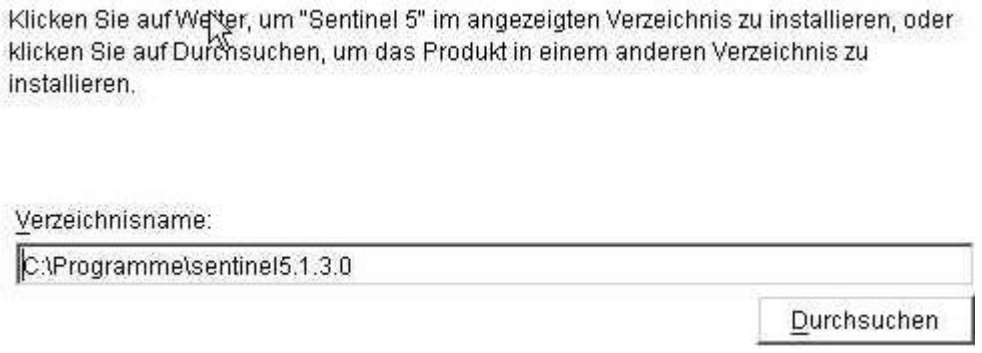
Sentinel 5-Datenbankinstallation

1. Vergewissern Sie sich, dass die Umgebungsvariablen nicht auf 4.2 verweisen. Falls doch, löschen Sie sie. Folgende Umgebungsvariablen sollten nicht vorhanden sein:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
2. Vergewissern Sie sich, dass Sie gemäß den Angaben in Abschnitt „Sentinel-Datenbank“ in *Kapitel 4* die nötigen Informationen gesammelt, die erforderlichen Aufgaben ausgeführt und die entsprechenden Anforderungen erfüllt haben: *Installieren von Sentinel 5 MS SQL, Vor der Installation von Sentinel 5 für MS SQL.*
3. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.

4. Wechseln Sie zu der CD und doppelklicken Sie auf *setup.bat*.

HINWEIS: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.

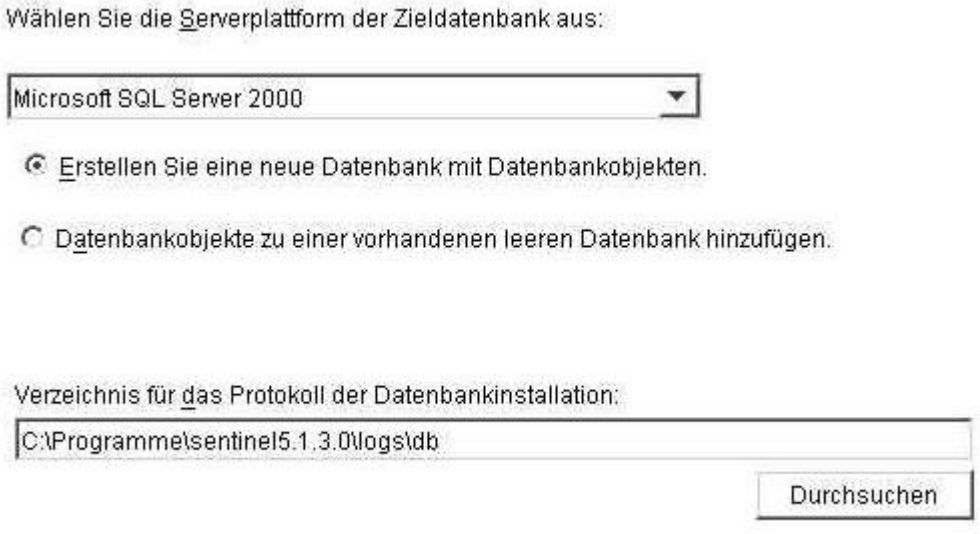
5. Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:
   - Englisch
   - Französisch
   - Deutsch
   - Italienisch
   - Portugiesisch
   - Spanisch
6. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf *Weiter*.
7. Akzeptieren Sie den Endenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
8. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um einen anderen Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.



9. Wählen Sie als Installationstyp *Benutzerdefiniert* (Standard) aus. Klicken Sie auf *Weiter*.
10. Heben Sie bei den zu installierenden Funktionen die Auswahl aller Funktionen auf und wählen Sie *Nur Datenbank* aus. Klicken Sie auf *Weiter*.

HINWEIS: Achten Sie darauf, die Auswahl der übergeordneten Funktion „Sentinel Services“ aufzuheben. Sie wird abgeblendet mit einem weißen Kontrollhäkchen angezeigt, wenn sie noch immer ausgewählt ist, jedoch die Auswahl aller untergeordneten Funktionen aufgehoben wurde.

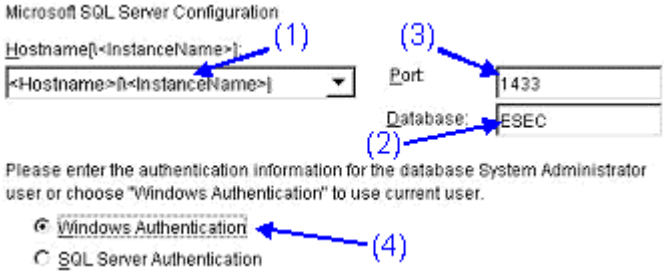
11. Geben Sie Hostnamen (bzw. IP-Adresse) und Portnummer (Standard: 10012) für den Kommunikationsserver ein. Klicken Sie auf *Weiter*.
12. Wählen Sie *Microsoft SQL Server* als Zieldatenbankplattform aus und wählen Sie *Erstellen Sie eine neue Datenbank mit Datenbankobjekten.* Geben Sie außerdem das Verzeichnis für das Datenbankinstallationsprotokoll ein (Standard: %ESEC_HOME%\logs\db). Übernehmen Sie den Standardwert für *Verzeichnis für das Protokoll der Datenbankinstallation* oder klicken Sie auf *Durchsuchen*, um einen anderen Speicherort anzugeben. Klicken Sie auf *Weiter*.



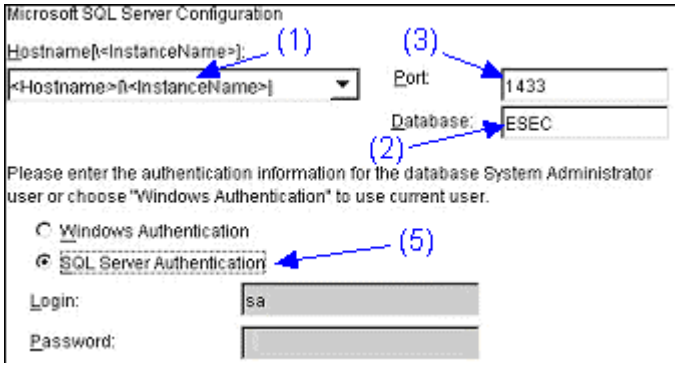
13. Geben Sie Ihre SQL Server-Konfigurationsinformationen ein:
    - (1) Hostname oder IP-Adresse der Datenbank – standardmäßig wird ihr lokaler Host-Computer angezeigt, sofern SQL Server lokal installiert ist. Wenn der gewünschte SQL Server nicht in der Dropdown-Liste angezeigt wird, wählen Sie die Option *Sonstiges* in der Liste aus. Es wird ein Textfeld angezeigt, in dem Sie den Hostnamen eingeben können. Sie müssen den vollständigen Hostnamen eingeben (z. B. – „sqlserver.sentinel.net“ und nicht nur „sqlserver“). Wenn Sie während der SQL Server-Installation einen Instanzennamen angegeben haben, müssen Sie am Ende des Hostnamens „\<Instanzenname>“ hinzufügen, wobei <Instanzenname> der Name ist, den Sie der Instanz während der SQL Server-Installation zugewiesen haben.
    - (2) Der Name für die neue SQL Server-Datenbank. Neben der hier benannten Datenbank wird außerdem eine Datenbank mit dem Namen <Ihr_DB-Name>_WF für die Verwendung durch iTRAC erstellt.

HINWEIS: Sie müssen der Datenbank einen anderen Namen zuweisen als den in der 4.2-Installation angegebenen.

    - (3) Datenbank-Port (Standard: 1433)
    - Wählen Sie für den Systemdatenbankadministrator eines der folgenden Elemente:
        - (4) Windows-Authentifizierung (der Benutzername, unter dem Sie das Installationsprogramm ausführen, wird verwendet)
        - (5) SQL Server-Authentifizierung – Geben Sie das Passwort des sa-Benutzers ein.



Windows-Authentifizierung

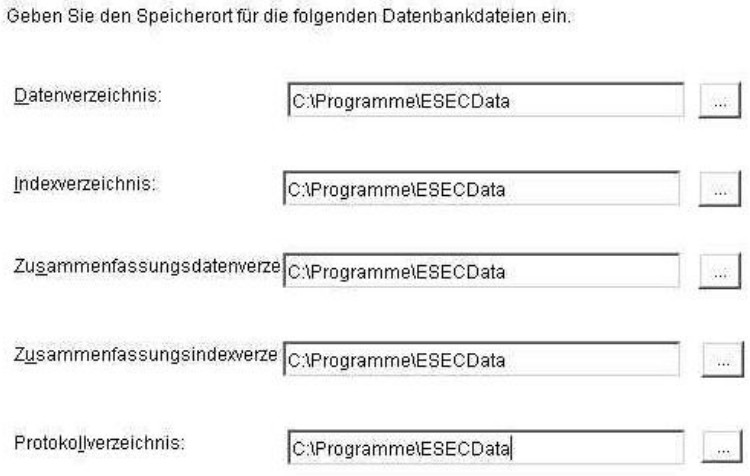


SQL Server-Authentifizierung

14. Geben Sie den Speicherort für folgende Datenbankdateien ein:

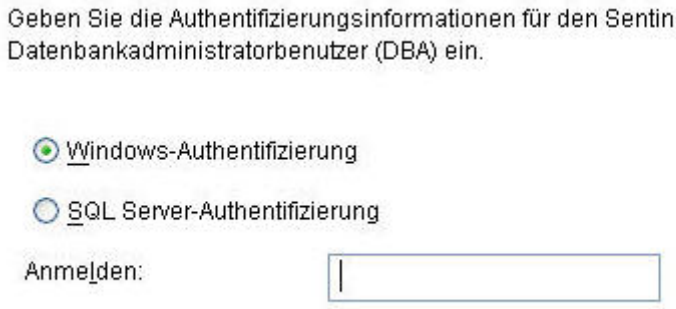
HINWEIS: Zugunsten einer möglichst effizienten Sicherung und Wiederherstellung sollten diese Speicherorte auf unterschiedlichen E/A-Geräten liegen.

- Datendateien
- Indexdateien
- Zusammenfassung Datendateien
- Zusammenfassung Indexdateien
- Protokolldateien

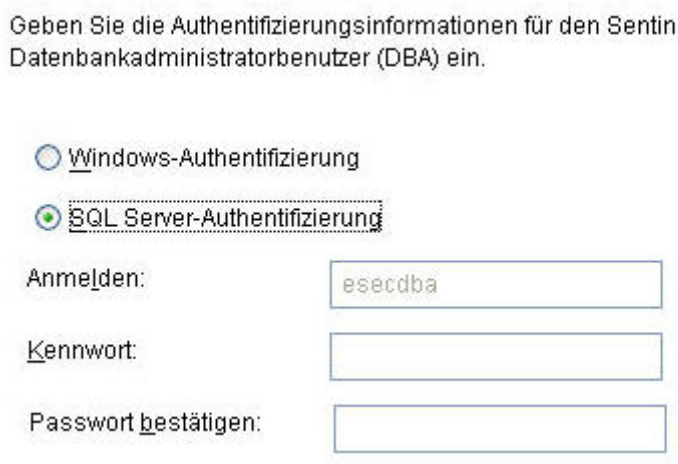


15. Geben Sie die Größe der Datenbank ein:
    - Standard (20.000 MB) – 30 Tage Kapazität bei 500.000 Ereignissen pro Tag
    - Groß (400.000 MB) – 30 Tage Kapazität bei 10.000.000 Ereignissen pro Tag
    - Benutzerdefiniert (manuelle Größenfestlegung). Wenn Sie diese Option wählen, werden Sie aufgefordert, folgende Informationen einzugeben:
      (1) Größe Ihrer Datenbank in MB (10.000 – 2.000.000)
      (2) Größe der einzelnen Protokolldateien in MB (100 – 100.000)
      (3) Maximale Größe der einzelnen Datenbankdateien in MB (2.000 – 100.000)
16. Wählen Sie für den Sentinel-Datenbankadministrator (DBA) eine der folgenden Optionen:
    - SQL Server-Authentifizierung (esecdba), Passwort und Passwortbestätigung
    - Windows-Authentifizierung, geben Sie ein: <Domänenname>\<Benutzername>

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



Windows-Authentifizierung

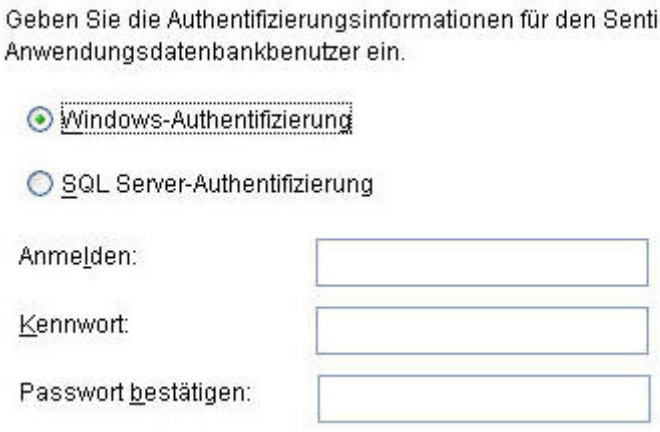


SQL Server-Authentifizierung

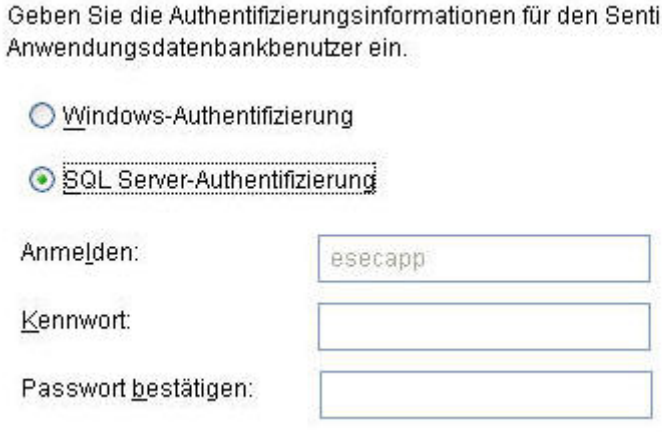
HINWEIS: Bei der SQL-Authentifizierung fährt das Installationsprogramm nur fort, wenn das esecdba-Passwort mit dem esecdba-Passwort aus v4.2 übereinstimmt.

17. Für den Benutzer der Sentinel-Anwendungsdatenbank. Wählen Sie eine der beiden folgenden Optionen:
    - *SQL Server-Authentifizierung* (esecapp), geben Sie Passwort und Passwortbestätigung ein
    - *Windows-Authentifizierung*, geben Sie <Domänenname>\<Benutzername>, Passwort und Passwortbestätigung ein

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



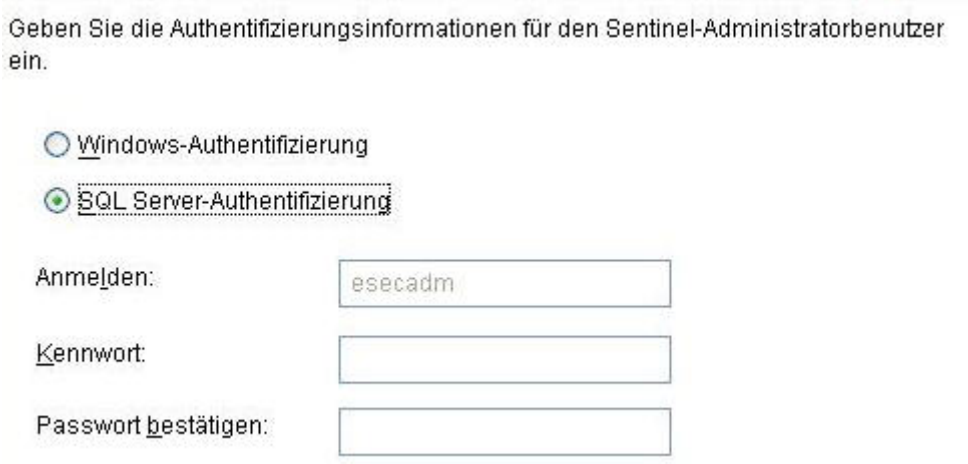
Windows-Authentifizierung



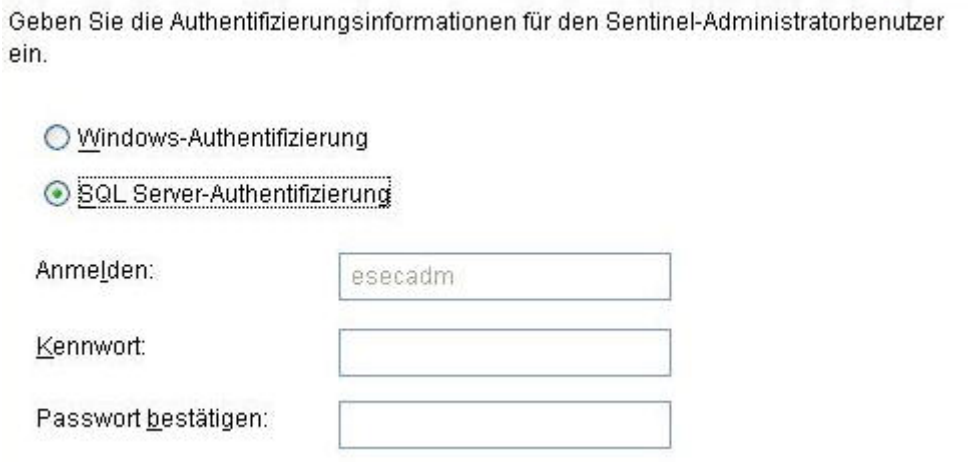
SQL Server-Authentifizierung

18. Für den Sentinel-Administratorbenutzer. Wählen Sie eine der beiden folgenden Optionen aus:
    - *SQL-Authentifizierung*, geben Sie den Benutzernamen für den Sentinel-Administrator (Standard: esecadm), Passwort und Passwortbestätigung ein
    - *Windows-Authentifizierung*, geben Sie ein: <Domänenname>\<Benutzername>

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



Windows-Authentifizierung



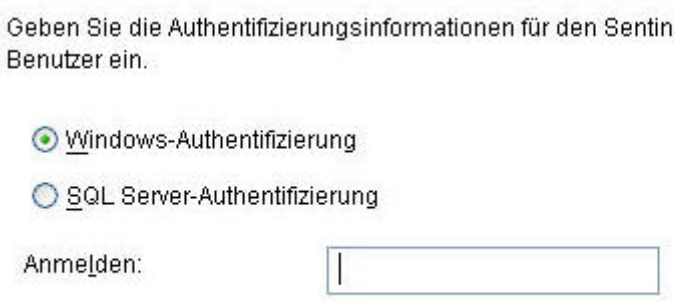
SQL Server-Authentifizierung

19. Für den Benutzer der Sentinel-Berichterstellung. Wählen Sie eine der beiden folgenden Optionen:

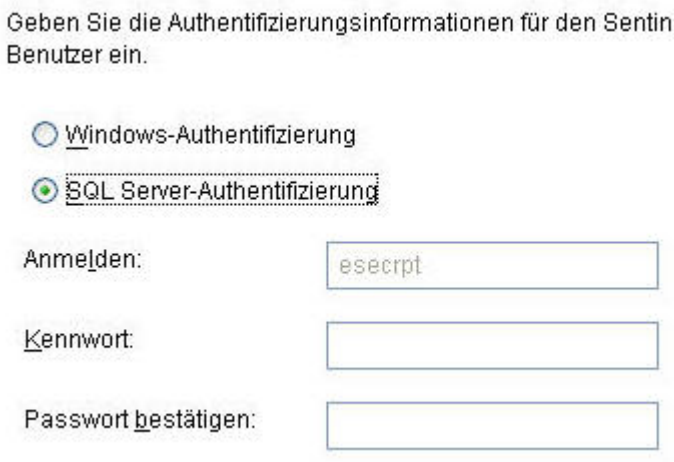
HINWEIS: Bei der Sentinel-Berichterstellung ist für die Windows-Authentifizierung die Ausführung von Crystal Enterprise Professional erforderlich. Mit der Professional-Version können Sie nach Bedarf verschiedene Konten und Zuordnungen erstellen. Wenn Sie die Standardversion verwenden, müssen Sie *SQL-Authentifizierung* auswählen.

- *SQL-Authentifizierung* (esecrpt), geben Sie Passwort und Passwortbestätigung ein
- *Windows-Authentifizierung*, geben Sie ein: <Domänenname>\<Benutzername>

HINWEIS: Wenn Sie *SQL Server-Authentifizierung* auswählen, kann der Standard-Anmeldename nicht bearbeitet werden.



Windows-Authentifizierung



SQL Server-Authentifizierung

20. Klicken Sie im Zusammenfassungsfenster für die Datenbankinstallation auf *Weiter*.
21. Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten. Klicken Sie auf *Fertig stellen*, um das System neu zu booten.

Migration

Das Dienstprogramm für die Datenmigration migriert nur folgende Elemente:

- Benutzer und zugewiesene Berechtigungen
- Filter
- Konfigurationsoptionen für das Kontextmenü
- Umbenannte CV-Tags
- Partitions- und Archivkonfigurationen
- Fälle aus v4.2 werden als Vorfälle in v5 kopiert.
- Vorfälle und vorfallsbezogene Ereignisse

HINWEIS: Das Dienstprogramm zur Datenmigration migriert KEINE Ereignisdaten, ausgenommen Ereignisdaten, die mit Vorfällen verknüpft sind. Nur Ereignisdaten, die mit Vorfällen verknüpft sind, werden migriert.

HINWEIS: Vorfallsereignisdaten können nicht über Sentinel Control Center angezeigt werden. Vorfallsereignisdaten können entweder über Crystal Reporting oder über SQL-Abfragen eingesehen werden.

Datenmigration für Sentinel 5-Datenbanken, bei denen es sich beim Sentinel-Datenbankadministrator um einen Benutzer der Windows-Authentifizierung handelt.

HINWEIS: Dieses Verfahren gilt für Sentinel 5-Datenbankinstallationen, bei denen es sich beim Sentinel-Datenbankadministrator (entspricht esecdba) um einen Benutzer der Windows-Authentifizierung handelt. Bei diesem Verfahren wird ein SQL-Authentifizierungsbenutzer zur Sentinel 5-Datenbank hinzugefügt, sodass die Daten aus v4.2 nach v5 migriert werden können.

1. Melden Sie sich als Benutzer mit Verwaltungsrechten an.
2. Starten Sie MS SQL Server Query Analyzer. Melden Sie sich als „sa“ oder als entsprechender Windows-Authentifizierungsbenutzer an.
3. Klicken Sie auf *Datei* > *Öffnen*. Navigieren Sie zu:

   ```
   %ESEC_HOME%\utilities\db\scripts\ddl\mssql\Migration
   ```

4. Wählen Sie import_add_esecdba.sql.
5. Klicken Sie auf *Öffnen*.
6. Klicken Sie auf *Abfrage* > *Ausführen*.
7. Beenden Sie Query Analyzer nach der Ausführung des Skripts.

HINWEIS: Nach der Durchführung der Datenmigration können Sie mithilfe von MS SQL Server Enterprise Manager den SQL-Authentifizierungsbenutzer esecdba aus der Sentinel 5-Datenbank löschen.

Datenmigration

1. Melden Sie sich als Benutzer mit Administratorrechten an.
2. Überprüfen Sie die Umgebungsvariablen, um sicherzustellen, dass Java (Version 1.4.2) sich in PATH befindet. Diese Prüfung lässt sich durch Ausführung des folgenden Befehls in der Befehlszeile durchführen:

   ```
   java -version
   ```

   Wenn der oben angegebene Befehl nicht erfolgreich ist, müssen Sie entweder den Ort suchen, an dem Java in Ihrem System installiert ist, oder Java herunterladen und installieren. Aktualisieren Sie anschließend die Umgebungsvariable PATH, sodass sie die ausführbare Java-Datei enthält. Beispiel für den Fall, dass Java im Verzeichnis installiert ist:

   ```
   C:\Programme\sentinel5.1.3.0\Sun-1.4.2
   ```

   Fügen Sie folgende Zeichenkette am Anfang der Umgebungsvariablen PATH ein:

   ```
   C:\Programme\sentinel5.1.3.0\Sun-1.4.2\bin;
   ```

3. Wechseln Sie an der Befehlszeilen-Eingabeaufforderung in folgendes Verzeichnis auf der Sentinel 5-Software-Installations-CD:

   ```
   sentinel\dbsetup\bin
   ```

4. Führen Sie folgenden Befehl aus:

   ```
   .\MigrateDb.bat
   ```

5. Sie werden zur Eingabe folgender Informationen aufgefordert:
   - Hostname der Datenbank (auf der die Sentinel 4.2 und die Sentinel 5-Datenbank ausgeführt werden)
   - Zieldatenbankname (der Sentinel 5-Datenbank, zu der Sie migrieren)
   - esecdba-Passwort (das Passwort für den esecdba-Benutzer muss auf der Sentinel v4.2- und der Sentinel v5-Datenbank übereinstimmen)
   - Name der Quelldatenbank (v4.2-Datenbankname)
   - Protokollverzeichnis (Speicherort für die Migrationsprotokolldateien)
   - Migrationsoption:
     - (1) Systemeinstellungen
     - (2) Vorfälle/Fälle
     - (3) Beides
     - (4) Fertig

HINWEIS: Vorfälle und Fälle sollten erst nach der erfolgreichen Migration der Systemeinstellungen migriert werden.

HINWEIS: Wenn die Migration der Systemeinstellungen scheitert, deinstallieren Sie die Sentinel 5-Datenbank, indem Sie auswählen, dass nur die Datenbankobjekte gelöscht werden sollen. Installieren Sie anschließend die Sentinel 5-Datenbank erneut, indem Sie die Option *Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen* auswählen. Führen Sie abschließend die Anweisungen zur Datenmigration erneut aus.

HINWEIS: Wenn die Vorfallsmigration nicht erfolgreich ist, führen Sie sie erneut aus. Das Dienstprogramm für die Migration beginnt beim Fehlerpunkt erneut. Es müssen keine zusätzlichen Bereinigungsaufgaben durchgeführt werden.

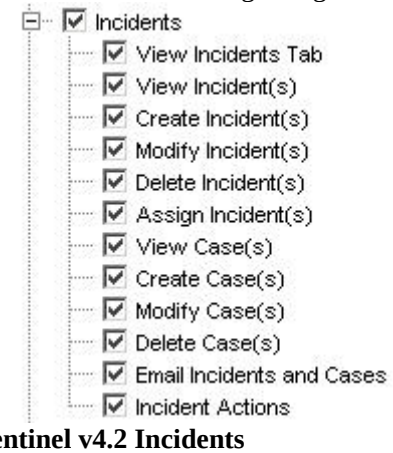
HINWEIS: Nach der Durchführung der Datenmigration können Sie mithilfe von MS SQL Server Enterprise Manager den SQL-Authentifizierungsbenutzer (esecdba) aus der Sentinel 5-Datenbank löschen, wenn Sie ihn wegen des Datenmigrations-Dienstprogramms hinzufügen mussten.

Nach-Migration – Installation von Sentinel 5

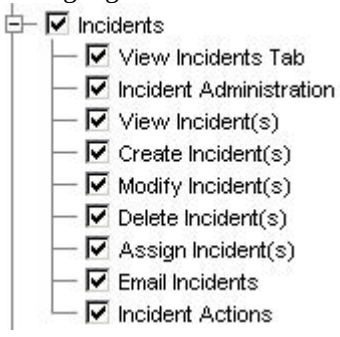
In Sentinel 5 sind folgende Funktionen neu oder wurden geändert bzw. entfernt.

- iTRAC – Dies ist eine neue Funktion. Die zugehörigen Benutzerberechtigungen sind:

- Incidents – „Vorfallsverwaltung“ wurde hinzugefügt. Alle fallbezogenen Funktionen wurden entfernt. Die zugehörigen Benutzerberechtigungen sind:



Sentinel v4.2 Incidents



Sentinel v5 Incidents

- Collector Management – in v4.2 ist dies Wizard Monitoring. *Registerkarte „Wizards“ anzeigen* wurde geändert in *Collectors anzeigen*. *Wizards und Collector steuern* wurde geändert in *Collectors steuern* und *Collector-Administration*. Die zugehörigen Benutzerberechtigungen sind:

Sentinel v4.2 Wizard Monitoring

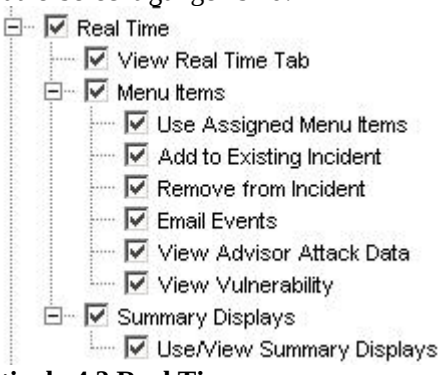
Sentinel v5 Collector Management

- Administration – DAS-Statisitk, Benutzersitzungsverwaltung und iTRAC-Rollenverwaltung hinzugefügt. *Korrelationsregeln* wurde in *Korrelation* umbenannt. Die Funktion „Ereigniskonfiguration“ wurde nach Sentinel Data Manager verlagert. *Benutzerkonfiguration* wurde in *Benutzerverwaltung* umbenannt. Die zugehörigen Benutzerberechtigungen sind:

Sentinel v4.2 Administration

Sentinel v5 Administration

- ActiveViews™ – in v4.2 wurde diese Funktion „Real Time“ genannt. *Zusammenfassungsdisplays* wurde in *Active Views* umbenannt. Die zugehörigen Benutzerberechtigungen sind:



Sentinel v4.2 Real Time

Sentinel v5 Active Views™

- Die Funktion für die Systemübersicht ist in Sentinel 5 nicht verfügbar.

Installieren von Sentinel 5

1. Installieren Sie Sentinel 5, siehe *Kapitel Installation von Sentinel für Windows.*
2. Installieren Sie das aktuellste Sentinel Service Pack.
3. Führen Sie folgende Schritte aus, wenn Sie eine neue Funktion für einen der bestehenden Benutzer aus v4.2 hinzufügen möchten.
   a. Vergewissern Sie sich, dass *Sentinel Server* ausgeführt wird.
   b. Melden Sie sich als Benutzer mit der Berechtigung zur Administration/Benutzerverwaltung (z. B. – esecadm) bei Sentinel Control Center an.
   c. Klicken Sie in Sentinel Control Center auf die Registerkarte „Admin“. Erweitern Sie im Navigationsfenster den Bereich „Benutzerkonfiguration“ oder klicken Sie in der Navigationsleiste auf *Admin* > *Benutzerkonfiguration.*
   d. Klicken Sie mit der rechten Maustaste auf den Benutzer, für den Sie die Funktion hinzufügen möchten (z. B. – esecadm) und wählen Sie die Option *Benutzerdetails.* Klicken Sie auf die Registerkarte *Berechtigungen.*
   e. Erweitern Sie iTRAC und weisen Sie die erforderlichen Berechtigungen zu.
   f. Erweitern Sie „Incidents“ und weisen Sie nach Bedarf *Incident Administration* zu.
   g. Erweitern Sie *Collector Management* und weisen Sie nach Bedarf *Collector Administration* zu.
   h. Erweitern Sie *Administration* und weisen Sie nach Bedarf *DAS-Statistik, Benutzersitzungsverwaltung* bzw. *iTRAC-Rollenverwaltung* zu.
   i. Klicken Sie auf die Registerkarte *Funktionen* und weisen Sie nach Bedarf die Workflow-Funktion *Admin* bzw. *Analyst* zu.
   j. Klicken Sie auf *OK.*
4. Importieren Sie gegebenenfalls etwaige Korrelationsregeln. Aus Sentinel 4.2 exportierte Regelsätze werden beim Import in Sentinel 5 als Regelordner angezeigt.
5. Kopieren Sie aus Sicherungsskripts von Collectors und Portkonfigurationen, indem Sie die Anweisungen in Abschnitt Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen befolgen.

Nach-Migration – Neukonfiguration von Collector-Skripts und Portkonfigurationen

Führen Sie auf jedem Computer, auf dem der Sentinel 5 Collector-Service (Collector Manager) installiert ist, folgende Schritte aus, um die Collector-Skripts und Portkonfigurationen, die in der Sentinel v4.2-Installation verwendet wurden, wieder zu erstellen.

So erstellen Sie die alten Collector-Skripts und Portkonfigurationen erneut

1. Stoppen Sie den Windows-Service für Collector Manager.
2. Kopieren Sie aus dem Speicherort, in dem Sie eine Sicherungskopie des Verzeichnisses %WORKBENCH_HOME%\Agents der Sentinel v4.2-Installation abgelegt haben, folgende Dateien in das Verzeichnis %WORKBENCH_HOME%\Agents der aktuellen Sentinel 5-Installation (überschreiben Sie die Dateien, falls erforderlich):
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Lesen Sie die während der Vor-Migration erstellte Textdatei, in der alle von der Sentinel v4.2 Collector Manager-Installation auf diesem Computer verwendeten Collectors aufgelistet werden. Sie benötigen die Collector-Namen im nächsten Schritt.
4. Kopieren Sie aus dem Speicherort, in dem Sie eine Sicherungskopie des Verzeichnisses %WORKBENCH_HOME%\Elements der Sentinel v4.2-Installation abgelegt haben, die Verzeichnisse, deren Namen mit den Collector-Namen in der Textdatei übereinstimmen, in das Verzeichnis %WORKBENCH_HOME%\Elements der aktuellen Sentinel 5-Installation (überschreiben Sie die Verzeichnisse/Dateien, falls erforderlich).
5. Rufen Sie das Dienstprogramm UpgradePortCfgFile von der Website des technischen Support von Sentinel (hier herunterladen) ab.
6. Extrahieren Sie die ZIP-Datei UpgradePortCfgFile ZIP.
7. Öffnen Sie eine Befehlszeilenaufforderung und wechseln Sie in das Verzeichnis mit dem extrahierten Dienstprogramm UpgradePortCfgFile. Führen Sie in diesem Verzeichnis folgenden Befehl aus:

   ```
   .\UpgradePortCfgFile.bat
   ```

8. Starten Sie den *Collector Manager*-Service.

Nach-Migration – Konfigurieren von Sentinel 5 für Crystal Reporting

Gehen Sie wie folgt vor, wenn Sie Crystal Reporting für Sentinel v4.2 ausgeführt haben und Crystal Reporting mit Sentinel 5 ausführen möchten:

- Bearbeiten Sie die Crystal Reporting-bezogenen ODBC-Einstellungen so, dass sie auf die Sentinel ODBC-Datenbank verweisen.
- Importieren Sie die Crystal Reports-Schablonen (einschließlich der Schablonen für die Datenmigration) aus dem letzten Service Pack.

Weitere Informationen finden Sie im Installationskapitel zu *Crystal Reports*.

Patch zur Aufrüstung von v5.x.x auf v5.1.3

Führen Sie dieses Verfahren auf jedem Computer durch, auf dem Sentinel-Komponenten installiert sind.

Patch von Sentinel v5.x.x auf v5.1.3 wenn es sich beim Sentinel-Datenbankadministrator (esecdba) um einen Anmeldenamen für die SQL Server-Authentifizierung handelt

Aufrüsten von v5.x.x auf v5.1.3 für SQL Server-Authentifizierung

HINWEIS: Wenn Sie v5.1.1sp1 oder höher ausführen und Änderungen an der Datei syslog.conf vornehmen, müssen Sie eine Kopie dieser Datei erstellen. Das Patch-Installationsprogramm überschreibt die Datei syslog.conf. Nach der Anwendung des Patch müssen Sie Ihre neue syslog.conf-Datei bearbeiten bzw. überschreiben, sodass sie mit ihrer ursprünglichen Datei syslog.conf übereinstimmt.

1. Schließen Sie alle geöffneten Instanzen von *Sentinel Control Center, Sentinel Data Manager* und *Collector Builders*.
2. Legen Sie die Sentinel-Patch-Installations-CD in das CD-ROM-Laufwerk ein.
3. Wechseln Sie zum entsprechenden Patch-Verzeichnis.
4. Doppelklicken Sie im Patch-Verzeichnis auf *setup.bat.*

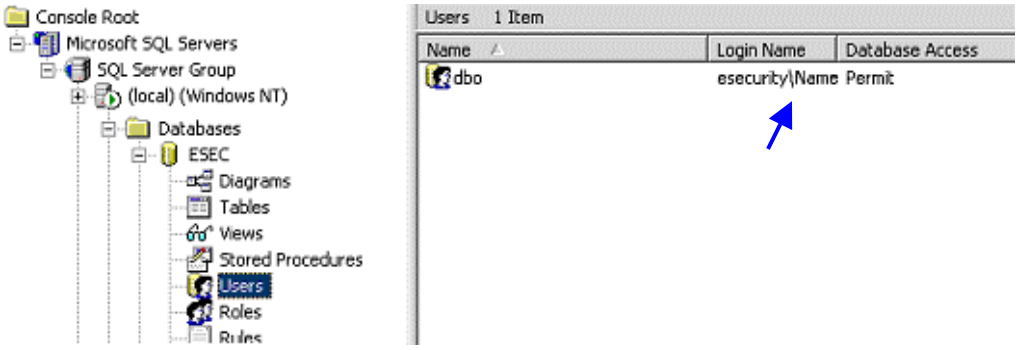
HINWEIS: Die Installation im Konsolenmodus wird zurzeit unter Windows nicht unterstützt.

5. Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
6. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
7. Klicken Sie auf *Weiter*, bis das Fenster mit den Datenbankinformationen angezeigt wird.
8. Stellen Sie sicher, dass der Datenbanktyp korrekt ist. Wählen Sie den Speicherort des Protokollverzeichnisses für die Datenbankinstallation aus. Klicken Sie auf *Weiter*.
9. Vergewissern Sie sich, dass die Informationen für den MS SQL-Server korrekt sind. Wählen Sie *SQL Server-Authentifizierung*. Geben Sie Ihren esecdba-Benutzernamen und Ihr Passwort ein. Klicken Sie auf *Weiter*.
10. Klicken Sie auf *Installieren*. Möglicherweise werden Sie aufgefordert, Ihren Computer neu zu booten. Wenn nicht, starten Sie Ihre Sentinel-Services (*Collector Manager, Sentinel und Sentinel Communications*) neu.

Patch von Sentinel v5.x.x auf v5.1.3 wenn es sich beim Sentinel-Datenbankadministrator um Windows-Authentifizierung handelt

Bei der Windows-Authentifizierung wendet das Patch-InstallShield den Datenbank-Patch nicht an. Das Installationsprogramm für den Datenbank-Patch muss als Windows-Domänenbenutzer „esecdba“ für die Sentinel-Datenbank ausgeführt werden.

Wenn Sie das Patch-Installationsprogramm auf dem Computer ausführen, auf dem Sie ursprünglich die Datenbankkomponente installiert hatten, müssen Sie den Benutzernamen und das Passwort des Sentinel-Datenbankadministrators (esecdba) kennen. Sie können die Identität des esecdba-Benutzers ermitteln, indem Sie mithilfe des SQL Server Enterprise Manager den Anmeldenamen für den dbo-Benutzer der Sentinel-Datenbank ermitteln (siehe unten).



Während des Patch-Prozesses erhalten Sie eine Popup-Meldung, die besagt, dass der Datenbank-Patch über die Befehlszeile angewendet werden muss, wie unten erläutert.

Patch von v5.x.x auf v5.1.3 für die Windows-Authentifizierung

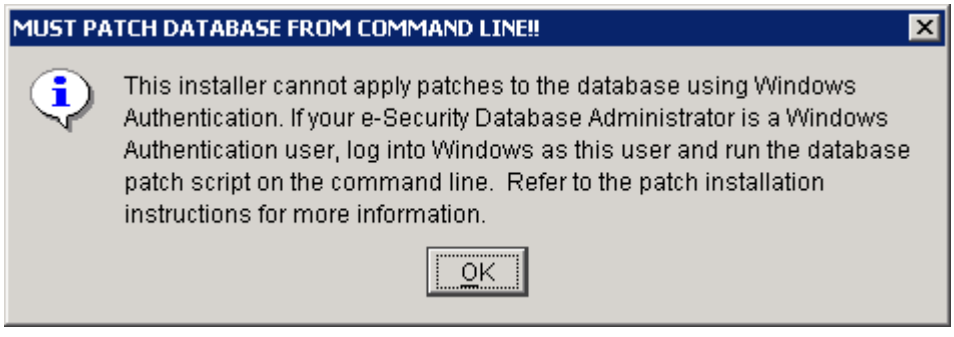
HINWEIS: Wenn Sie v5.1.1sp1 oder höher ausführen und Änderungen an der Datei syslog.conf vornehmen, müssen Sie eine Kopie dieser Datei erstellen. Das Patch-Installationsprogramm überschreibt die Datei syslog.conf. Nach der Anwendung des Patch müssen Sie Ihre neue syslog.conf-Datei bearbeiten bzw. überschreiben, sodass sie mit ihrer ursprünglichen Datei syslog.conf übereinstimmt.

1. Schließen Sie alle geöffneten Instanzen von *Sentinel Control Center*, *Sentinel Data Manager* und *Collector Builders*.
2. Legen Sie die Sentinel-Patch-Installations-CD in das CD-ROM-Laufwerk ein.
3. Wechseln Sie zum entsprechenden Patch-Verzeichnis.
4. Doppelklicken Sie im Patch-Verzeichnis auf *setup.bat.*

HINWEIS: Die Installation im Konsolenmodus wird zurzeit unter Windows nicht unterstützt.

5. Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
6. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
7. Klicken Sie auf *Weiter*, bis das Fenster mit den Datenbankinformationen angezeigt wird.
8. Stellen Sie sicher, dass Datenbanktyp und -name korrekt sind. Wählen Sie den Speicherort des Protokollverzeichnisses für die Datenbankinstallation aus. Klicken Sie auf *Weiter*.

   Die folgende Popup-Meldung wird angezeigt. Lesen Sie die Meldung und klicken Sie auf *OK*, um fortzufahren.



9. Vergewissern Sie sich, dass die Informationen für den MS SQL-Server korrekt sind. Wählen Sie *Windows-Authentifizierung*.
   Geben Sie Ihren Benutzernamen und Ihr Passwort für den Sentinel-Anwendungsbenutzer ein. Klicken Sie auf *Weiter*.

   ACHTUNG: Für den Datenbankcomputer gilt: AM ENDE DER INSTALLATION NICHT NEU BOOTEN.

10. Klicken Sie im Zusammenfassungsfenster auf *Installieren*.
11. Beenden Sie InstallShield am Datenbankcomputer, ohne neu zu booten.
12. Wenn nicht bereits geschehen, melden Sie sich am Datenbankcomputer als Windows-Domänenbenutzer „esecdba“ an.
13. Öffnen Sie eine Befehlszeilen-Eingabeaufforderung.
14. Überprüfen Sie die Umgebungsvariablen, um sicherzustellen, dass Java (Version 1.4.2) sich in PATH befindet. Diese Prüfung lässt sich durch Ausführung des folgenden Befehls in der Befehlszeile durchführen:

    ```
    java -version
    ```

    Wenn der oben angegebene Befehl nicht erfolgreich ist, müssen Sie entweder den Ort suchen, an dem Java in Ihrem System installiert ist, oder Java herunterladen und installieren. Aktualisieren Sie anschließend die Umgebungsvariable PATH, sodass sie die ausführbare Java-Datei enthält. Beispiel für den Fall, dass Java im Verzeichnis installiert ist:

    ```
    C:\Programme\sentinel5.1.3.0\Sun-1.4.2
    ```

    Fügen Sie folgende Zeichenkette am Anfang der Umgebungsvariablen PATH ein:

    ```
    C:\Programme\sentinel5.1.3.0\Sun-1.4.2\bin;
    ```

15. Wechseln Sie an der Befehlszeilen-Eingabeaufforderung in folgendes Verzeichnis auf der Sentinel-Installations-CD:

    ```
    <Patch-Verzeichnis>\sentinel\dbsetup\bin
    ```

16. Geben Sie folgenden Befehl ein:

    ```
    .\PatchDb.bat
    ```

17. Geben Sie an der Eingabeaufforderung den Hostnamen bzw. die statische IP-Adresse der SQL Server-Instanz der Sentinel Datenbank ein, auf die der Patch angewendet werden soll.
18. Geben Sie an der Eingabeaufforderung den Namen der SQL Server Sentinel-Datenbank ein, auf die der Patch angewendet werden soll.
19. Geben Sie an der Eingabeaufforderung Option 1 für die Windows-Authentifizierung ein. Das Skript überprüft die eingegebenen Informationen und beginnt mit der Anwendung des Datenbank-Patch.
20. Nachdem das Skript ausgeführt und der Patch angewendet wurde, starten Sie den Service neu.

Aktualisieren des Syslog-Connectors

Wenn Sie die Syslog-Connector-Skripts aus einer Sentinel-Version vor 5.1.1.1 (d- h. – 5.0, 5.0.1.0, 5.1.0.0 oder 5.1.1.0) verwendet haben, müssen Sie die aktualisierten Syslog-Connector-Skripts verwenden, die im Patch enthalten sind. Um von der Verwendung des alten Syslog-Connector-Skripts zur Verwendung der neuen Syslog-Connector-Skripts überzugehen, müssen Sie das alte Skript entfernen und ein neues installieren.

Der Syslog-Connector wird mit Skripts installiert, die unter Windows und UNIX mit verbesserten Konfigurationsdateien ausgeführt werden. Außerdem wurde die Installation des Syslog-Proxyservers als Service vereinfacht.

So entfernen Sie den Syslog-Connector

1. Melden Sie sich als Administrator an.
2. Wechseln Sie in das Verzeichnis d/ %ESEC_HOME%\wizard\/syslog
3. Geben Sie Folgendes ein:

```
.\syslog-server.bat remove
```

So installieren Sie den Syslog-Connector

1. Melden Sie sich als Administrator an.
2. Wechseln Sie in das Verzeichnis d/ %ESEC_HOME\wizard\syslog
3. .\syslog-server.bat install
4. Wenn Sie Änderungen an der Datei syslog.conf Ihrer ursprünglichen Installation vorgenommen haben, müssen Sie die neue syslog.conf-Datei bearbeiten oder überschreiben, sodass Sie der ursprünglichen syslog.conf-Datei entspricht. syslog.conf befindet sich an folgendem Speicherort:

```
%ESEC_HOME%\wizard\syslog\config
```

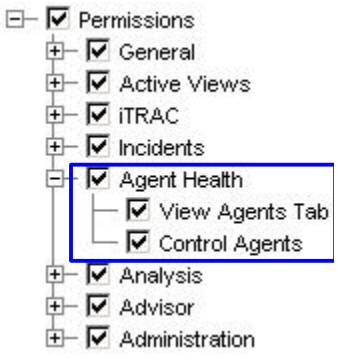
Aktualisieren der Benutzerberechtigungen von v5.0.x auf v5.1.3

Bei der Aufrüstung von v5 bzw. v5.0.1auf v5.1.3 wird „Collector Health“ in „Collector Management“ geändert und eine zusätzliche Funktion, „Collector-Administration“, hinzugefügt. Außerdem wurde die Funktion „Serveransichten“ hinzugefügt. Diese Berechtigung können Sie optional gewähren.

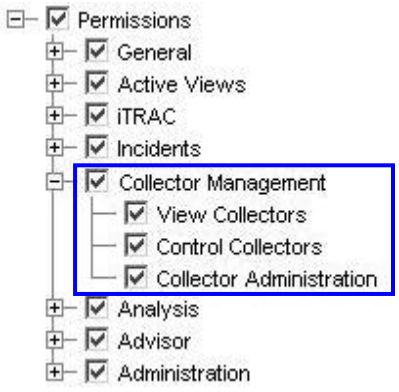
Aktualisieren der Berechtigungen für die Benutzerverwaltung

1. Melden Sie sich als Benutzer mit der Berechtigung zur Administration/Benutzerverwaltung bei Sentinel Control Center an.

   In v5.1 wurde *Collector Health* unter „Berechtigungen“ in *Collector Management* geändert und es wurden weitere Berechtigungen hinzugefügt.



Sentinel v5.0-Benutzerberechtigung

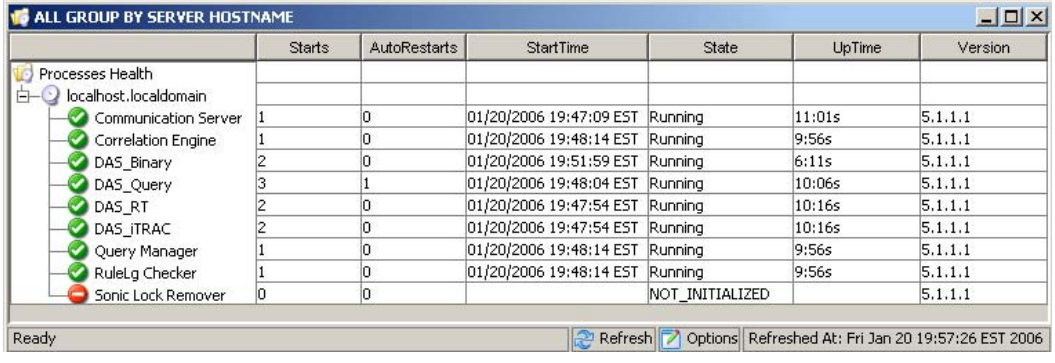


Sentinel v5.1-Benutzerberechtigung

2. Klicken Sie in Sentinel Control Center auf die Registerkarte *Admin*. Erweitern Sie im Navigationsfenster den Bereich „Benutzerkonfiguration“ oder klicken Sie in der Navigationsleiste auf *Admin > Benutzerkonfiguration.*
3. Klicken Sie mit der rechten Maustaste auf einen Admin-Benutzer (d. h. esecadm oder ein anderer Admin-Benutzer) > *Benutzerdetails.* Klicken Sie auf die Registerkarte *Berechtigungen*.
4. Erweitern Sie *Collector Management* und weisen Sie *Collector Administration* zu. Klicken Sie auf *OK*.

Aktualisieren der Berechtigungen für Serveransichten

Um den Bildschirm „Serveransichten“ nach der Patch-Installation verwenden zu können, müssen Sie mithilfe des Benutzer-Managers dem Sentinel-Benutzer die Berechtigung „Serveransichten“ gewähren. Der Benutzer-Manager befindet sich unter der Registerkarte „Admin“ von Sentinel Control Center.



Crystal Reporting-Server

Nach der Aufrüstung auf Sentinel v5.1.3, einschließlich der Anwendung des letzten Service Pack, müssen Sie die Berichte aus dem letzten Service Pack importieren. Weitere Informationen finden Sie im Kapitel zu Crystal Reports im Installationshandbuch.

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter %ESEC_HOME%\sentinel\config. Um diese Datei zu konfigurieren, führen Sie mailconfig.bat aus, um die Datei zu ändern, und mailconfigtest.bat, um Ihre Änderungen zu testen.

So konfigurieren Sie die Datei execution.properties

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

   ```
   mailconfig.bat -host <SMTP Server> -from <Quellen-Email-
      Adresse> -user <Mailauthentifizierungsbenutzer> –
      password
   ```

   Beispiel:

   ```
   mailconfig.bat -host 10.0.1.14 -from my_name@domain.com -
      user my_user_name –password
   ```

   Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

   ```
   Enter your password:*********
   Confirm your password:*********
   ```

   HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Wechseln Sie auf dem Computer, auf dem DAS installiert ist, in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Führen Sie „mailconfigtest“ wie folgt aus:

   ```
   mailconfigtest.bat -to <Ziel-Email-Adresse>
   ```

   Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

   ```
   Email has been sent successfully!
   ```

Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

```
Subject: Testing Sentinel mail property
```

```
This is a test for Sentinel mail property set up. If you
   see this message, your Sentinel mail property has been
   configured correctly to send emails
```

8 Patch für Oracle unter Linux

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

In diesem Kapitel wird die Anwendung von Patches zur Aufrüstung von v5.1.1 auf v5.1.3 erörtert.

Patch zur Aufrüstung von v5.1.1.1 auf v5.1.3

Führen Sie dieses Verfahren auf jedem Computer durch, auf dem Sentinel-Komponenten installiert sind.

Wenn Sie das Patch-Installationsprogramm von dem Computer ausführen, auf dem Sie ursprünglich die Datenbankkomponente installiert hatten, müssen Sie das Passwort des Sentinel-Datenbankadministrators (esecdba) kennen.

Aufrüsten von v5.1.1.1 auf v5.1.3 für Linux

1. Melden Sie sich als Benutzer „root“ an.

   HINWEIS: Wenn Sie Änderungen an der syslog.conf-Datei in Ihrer v5.1.1.1-Installation vorgenommen haben, müssen Sie eine Kopie der Datei syslog.conf erstellen. Das Patch-Installationsprogramm überschreibt die Datei syslog.conf. Nach der Anwendung des Patch müssen Sie Ihre neue syslog.conf-Datei bearbeiten bzw. überschreiben, sodass sie mit Ihrer ursprünglichen syslog.conf-Datei übereinstimmt.
2. Legen Sie die Sentinel-Patch-CD ein und mounten Sie sie.
3. Starten Sie das Installationsprogramm, indem Sie zum entsprechenden Patch-Verzeichnis auf der CD-ROM wechseln und folgenden Befehl ausführen:

   Für GUI-Modus:

   ```
   ./setup.sh
   ```

   oder

   Für Textmodus („kopflos“):

   ```
   ./setup.sh –console
   ```
4. Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
5. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
6. Klicken Sie auf *Weiter*, bis das Fenster mit den Datenbankinformationen angezeigt wird.
7. Stellen Sie sicher, dass der Datenbanktyp korrekt ist. Wählen Sie den Speicherort des Protokollverzeichnisses für die Datenbankinstallation aus. Klicken Sie auf *Weiter*.

8. Vergewissern Sie sich, dass die Informationen für den Oracle-Server korrekt sind. Geben Sie das esecdba-Passwort ein. Folgen Sie den restlichen Eingabeaufforderungen des Installationsprogramms.

Aktualisieren des Syslog-Connectors

Wenn Sie die Syslog-Connector-Skripts aus einer Sentinel-Version vor 5.1.1.1 (d. h. – 5.0, 5.0.1.0, 5.1.0.0 oder 5.1.1.0) verwendet haben, müssen Sie die aktualisierten Syslog-Connector-Skripts verwenden, die im Patch enthalten sind. Um von der Verwendung des alten Syslog-Connector-Skripts zur Verwendung der neuen Syslog-Connector-Skripts überzugehen, müssen Sie das alte Skript entfernen und ein neues installieren.

Der Syslog-Connector wird mit Skripts installiert, die unter Windows und UNIX mit verbesserten Konfigurationsdateien ausgeführt werden. Außerdem wurde die Installation des Syslog-Proxyservers als Service vereinfacht.

So entfernen Sie den Syslog-Connector

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh remove

So installieren Sie den Syslog-Connector

1. Melden Sie sich als „root“ an.
2. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
3. ./syslog-server.sh install
4. Wenn Sie Änderungen an der Datei syslog.conf Ihrer ursprünglichen Installation vorgenommen haben, müssen Sie die neue syslog.conf-Datei bearbeiten oder überschreiben, sodass Sie der ursprünglichen syslog.conf-Datei entspricht. syslog.conf befindet sich an folgendem Speicherort:

   ```
   $ESEC_HOME/wizard/syslog/config
   ```

Crystal Reporting-Server

Nach der Aufrüstung auf Sentinel 5.1.3, einschließlich der Anwendung des letzten Service Pack (sofern vorhanden), müssen Sie die Berichte aus dem letzten Service Pack importieren. Weitere Informationen finden Sie im Kapitel zu Crystal Reports im Installationshandbuch.

Aktualisieren der Sentinel-Email-Funktion für SMTP-Authentifizierung

Wenn für Ihr System SMTP-Authentifizierung erforderlich ist, müssen Sie die Datei execution.properties aktualisieren. Diese Datei befindet sich auf dem Computer, auf dem DAS installiert ist. Sie liegt unter $ESEC_HOME/sentinel/config. Um diese Datei zu konfigurieren, führen Sie mailconfig.sh aus, um die Datei zu ändern, und mailconfigtest.sh, um Ihre Änderungen zu testen.

So konfigurieren Sie die Datei execution.properties

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Führen Sie „mailconfig“ wie folgt aus:

```
./mailconfig.sh -host <SMTP Server> -from <Quellen-
   Email-Adresse> -user
   <Mailauthentifizierungsbenutzer> –password
```

Beispiel:

```
./mailconfig.sh -host 192.0.2.14 -from
   my_name@domain.com -user my_user_name –password
```

Nach dem Eingeben dieses Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert.

```
Enter your password:*********

Confirm your password:*********
```

HINWEIS: Wenn Sie die Passwortoption verwenden, muss es sich um das letzte Argument handeln.

So testen Sie Ihre execution.properties-Konfiguration

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als esecadm an und wechseln Sie in das folgende Verzeichnis:

```
$ESEC_HOME/sentinel/config
```

2. Führen Sie „mailconfigtest“ wie folgt aus:

```
./mailconfigtest.sh -to <destination email address>
```

Wenn die Email erfolgreich gesendet wurde, erhalten Sie die folgende Bildschirmausgabe, in der Ihnen mitgeteilt wird, dass die Email von der Zieladresse empfangen wurde.

```
Email has been sent successfully!
```

Überprüfen Sie das Postfach der Ziel-Email-Adresse, um sich zu vergewissern, dass die Email empfangen wurde. Die Betreffzeile und der Inhalt lauten wie folgt:

```
Subject: Testing Sentinel mail property

This is a test for Sentinel mail property set up. If
   you see this message, your Sentinel mail property
   has been configured correctly to send emails
```

9 Crystal Reports für Windows und Solaris

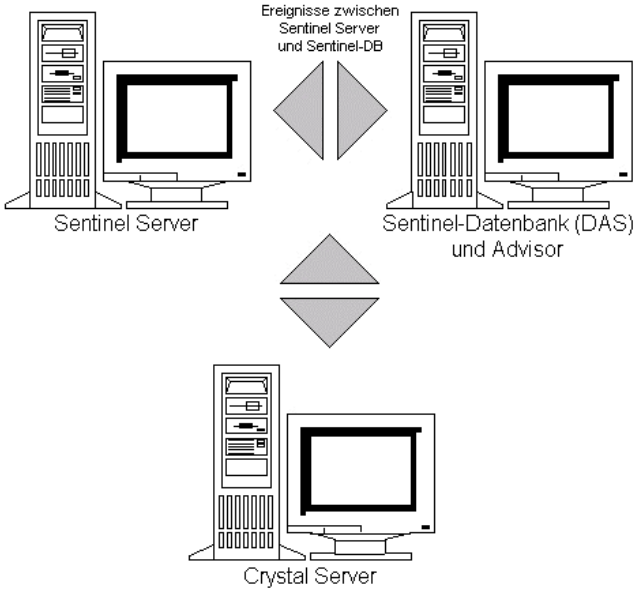
HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Crystal BusinessObjects Enterprise™ 11 ist ein Berichterstellungswerkzeug.

In diesem Kapitel wird die Installationskonfiguration von Crystal Reports Server für Sentinel erörtert. Die Installation sollte in der angegebenen Reihenfolge vorgenommen werden.

- Installation von Microsoft IIS und ASP.NET
- Installation von MS SQL (je nach Konfiguration als Windows-Authentifizierung oder SQL Server-Authentifizierung)
- Installation von Crystal Server
  - Konfiguration von Open Database Connectivity (ODBC) für SQL-Authentifizierung

  oder
  - Installation und Konfiguration der Oracle 9i-Client-Software
- Konfiguration von inetmgr
- Anwenden von Patches auf Crystal Reports-Berichte
- Veröffentlichen (Importieren) von Crystal Reports-Berichten
- Festlegen eines Kontos für einen benannten Benutzer
- Testen der Konnektivität zum Webserver
- Aktivieren der Top 10-Berichte (optional)
- Maximieren der Ereignisberichterstellung (empfohlen)
- Konfigurieren von Sentinel für den Crystal Enterprise Server



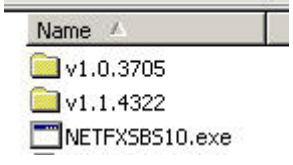
Überblick

Crystal Reports Server benötigt eine Datenbank zum Speichern von Informationen über das System und dessen Benutzer. Diese Datenbank ist als Central Management Server-(CMS-)Datenbank bekannt. Der CMS ist ein Server, der Informationen über das Crystal Reports Server-System speichert. Nach Bedarf können weitere Komponenten von Crystal Reports Server Zugriff auf diese Informationen erlangen.

Eine CMS-Datenbank muss über einer lokalen MS SQL 2000 Server-Datenbank eingerichtet werden. Mit dem Installationsprogramm von Crystal Reports Server können Sie die CMS-Datenbank über der MSDE-Datenbank einrichten, wenn kein lokaler MS SQL 2000 Server installiert ist. Sentinel 5 unterstützt keine MSDE-Konfiguration.

Systemanforderungen

- Windows® 2003 Server mit SP1 mit einer NTFS-formatierten Partition und installiertem IIS (Microsoft Internet Information Server) und NET.ASP. Sentinel 5 unterstützt Crystal XI auf Windows® 2000 Server nicht.
- .NET Framework 1.1 (Standardmäßig unter Windows 2003 installiert. BusinessObjects Enterprise™ 11 unterstützt .NET Framework 2.0 nicht). Um zu ermitteln, welche Version von .NET Framework sich auf Ihrem Computer befindet, wechseln Sie zu %SystemRoot%\Microsoft.NET\Framework. Der Ordner mit dem höchsten numerischen Wert sollte maximal die Nummer v.1.1.xxxx aufweisen. Beispiel:

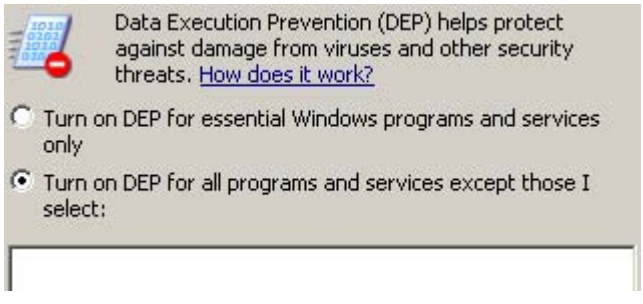


Konfigurationsanforderungen

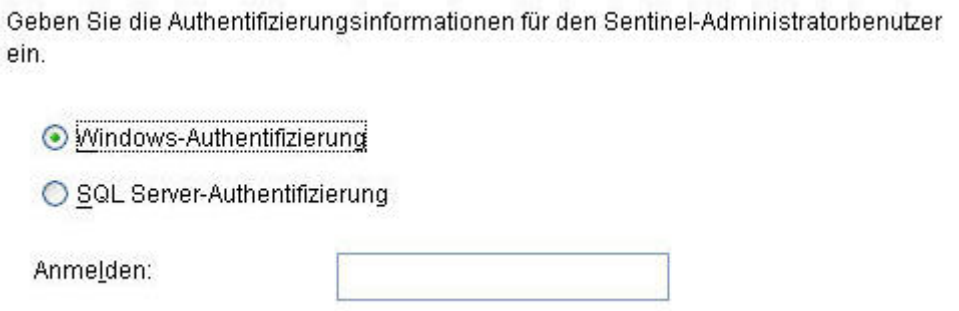
1. Vergewissern Sie sich, dass das für die Installation von Crystal Reports Server verwendete Konto über lokale Administratorrechte verfügt.
2. Stellen Sie die Datenausführungsverhinderung so ein, dass sie für die ausgewählten Programme und Services ausgeführt wird. Dies ist insbesondere hilfreich zur Vermeidung des folgenden Fehlers „Error 1920. Service ‘Crystal Report Cache Server’ on Windows 2003.“

   Der Zugriff auf die Datenausführungsverhinderung erfolgt über *Systemsteuerung* > *System* > *Registerkarte „Erweitert“* > *Leistungseinstellungen* > *Datenausführungsverhinderung*.

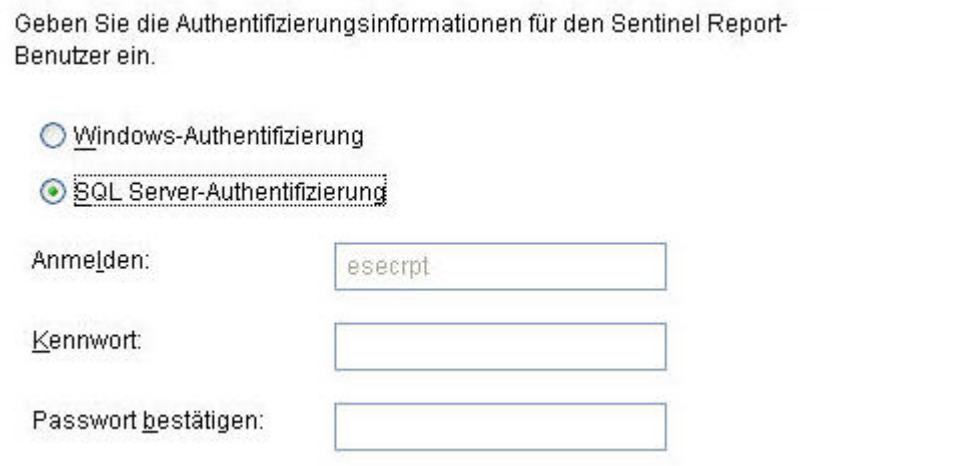
   Wählen Sie *Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten aktivieren*.



3. Wenn Sie vorhaben, Sentinel-Berichte mithilfe der Windows NT-Authentifzierung auszuführen, müssen Sie sicherstellen, dass das Windows-Domänenkonto für Sentinel Report-Benutzer bereits in der Sentinel-Datenbank vorhanden ist. Dies erfolgt während der Sentinel-Installation durch Auswahl von *Windows-Authentifizierung* bei der Einstellung von *Authentifizierungsmethode für den Sentinel Report-Benutzer*, wie in der Abbildung unten gezeigt.



4. Wenn Sie vorhaben, Sentinel-Berichte mithilfe der SQL Server-Authentifizierung auszuführen (auch für Sentinel Oracle-Installationen erforderlich), müssen Sie sicherstellen, dass die SQL Server-Anmeldung (esecrpt) bereits in der Sentinel-Datenbank vorhanden ist.
   - Bei der Sentinel MS SQL-Datenbank erfolgt dies während der Sentinel-Installation für MS SQL durch Auswahl von *SQL Server-Authentifizierung* bei der Einstellung von *Authentifizierungsmethode für den Sentinel Report-Benutzer*, wie in der Abbildung unten gezeigt.



   - Bei Sentinel Oracle-Datenbanken erfolgt dies während der Sentinel-Installation für Oracle. esecrpt nimmt dasselbe Passwort an wie esecadm.
5. Bei Oracle 9i Client Release 2 (9.2.0.1.0) müssen Sie dies vor der Installation von Crystal BusinessObjects Enterprise™ 11 installieren.
6. Bei MS SQL Server – Installieren Sie MS SQL 2000 sp3a vor der Installation von Crystal Reports Server 11.

7. Video-Auflösung von 1024 x 768 oder höher
8. Installieren Sie Microsoft Internet Information Server (IIS) und NET.ASP

HINWEIS: Sentinel 5 unterstützt MSDE nicht. Installieren Sie MS SQL 2000 sp3a vor der Installation von Crystal Reports Server 11.

Installation von Microsoft Internet Information Server (IIS) und ASP.NET

Zum Hinzufügen dieser Windows-Komponenten benötigen Sie eventuell die Installations-CD von Windows 2003 Server.

Installation von IIS und ASP.NET

1. Wechseln Sie zu Windows-Systemsteuerung > Software.
2. Klicken Sie im linken Fensterbereich auf *Windows-Komponenten hinzufügen/entfernen*.
3. Wählen Sie *Anwendungsserver* aus.

4. Klicken Sie auf *Details*.
5. Wählen Sie A*SP.NET* und *Internet Information Services (IIS)* aus.

6. Klicken Sie auf *OK* (OK).
7. Klicken Sie auf *Next* (Weiter). Möglicherweise werden Sie aufgefordert, die Windows-Installations-CD einzulegen.
8. Klicken Sie auf *Fertig stellen*.

Bekannte Probleme

1. Installation von Crystal Reports – Sie erhalten zwei Schlüssel, einen für Crystal Reports Server und den anderen für Crystal Reports Developer. Achten Sie darauf, bei der Installation von Crystal Reports Server den zugehörigen Schlüssel zu verwenden.
2. Deinstallation von Crystal Reports – Sollten Sie gezwungen sein, Crystal Reports Server zu deinstallieren, können Sie die Registrierungsschlüssel mithilfe eines manuellen Deinstallationsverfahrens bereinigen. Dies ist besonders nützlich, wenn Ihre Installation beschädigt wird. Auf der folgenden BusinessObjects-Website finden Sie Verfahren zur manuellen Deinstallation von BusinessObjects Enterprise XI, http://support.businessobjects.com/library/kbase/articles/c2017905.asp.

   HINWEIS: Die oben stehende URL war zum Veröffentlichungszeitpunkt dieses Dokuments korrekt.
3. Während der Konfiguration von .NET Administration Launchpad reagiert der Aktualisierungsprozess beim Ändern der Zugriffsebene von *(Inherited Rights)* (Vererbte Rechte) zu *View on Demand* (Auf Verlangen anzeigen) nicht mehr. Warten Sie ca. 30 Sekunden. Die Zugriffsebene wird aktualisiert.

Verwenden von Crystal Reports

Informationen zur Verwendung von Crystal Reports für die Sentinel-Berichterstellung finden Sie in der *Crystal Reports-Dokumentation* bzw. im *Sentinel-Benutzerhandbuch*.

Installationsüberblick

Installationsüberblick für MS SQL 2000 Server mit Windows-Authentifizierung

Führen Sie zur ordnungsgemäßen Installation von Crystal Reports folgendes Verfahren in der angegebenen Reihenfolge durch.

1. Installation von Crystal Reports Server 11 – Wenn Sie bei der Installation der Anwendung Sentinel 5 *Windows-Authentifizierung* für den Benutzer von Sentinel Report ausgewählt haben, folgen Sie dem Link für Installation von Crystal Server für MS SQL 2000 Server mit Windows-Authentifizierung.
2. Konfiguration von Open Database Connectivity (ODBC)
3. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
4. Patches für Crystal Reports
5. Veröffentlichen von Berichten
6. Festlegen eines Kontos für einen benannten Benutzer
7. Importieren Sie Crystal Report-Schablonen
8. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
9. Konfigurieren von Sentinel für den Crystal Enterprise Server

Installationsüberblick für MS SQL 2000 Server mit SQL Server-Authentifizierung

Führen Sie zur ordnungsgemäßen Installation von Crystal Reports folgendes Verfahren in der angegebenen Reihenfolge durch.

1. Installation von Crystal Reports Server 11 – Wenn Sie bei der Installation der Anwendung Sentinel *5 SQL Server-Authentifizierung* für den Benutzer von Sentinel Report ausgewählt haben, folgen Sie dem Link für Installation von Crystal Server für MS SQL 2000 Server mit SQL-Authentifizierung oder für Oracle.
2. Konfiguration von Open Database Connectivity (ODBC)
3. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
4. Importieren Sie Crystal Report-Schablonen
5. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
6. Konfigurieren von Sentinel für den Crystal Enterprise Server

Installationsüberblick für Oracle

Führen Sie zur ordnungsgemäßen Installation von Crystal Reports folgendes Verfahren in der angegebenen Reihenfolge durch.

1. Installation von Oracle 9i Client
2. Installation von Crystal Reports Server 11 – Folgen Sie dem Link zur Installation von Crystal Installation von Crystal Server für MS SQL 2000 Server mit SQL-Authentifizierung oder für Oracle.
3. Konfigurieren Sie den nativen Oracle-Treiber
4. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
5. Importieren Sie Crystal Report-Schablonen
6. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
7. Konfigurieren von Sentinel für den Crystal Enterprise Server

Installation

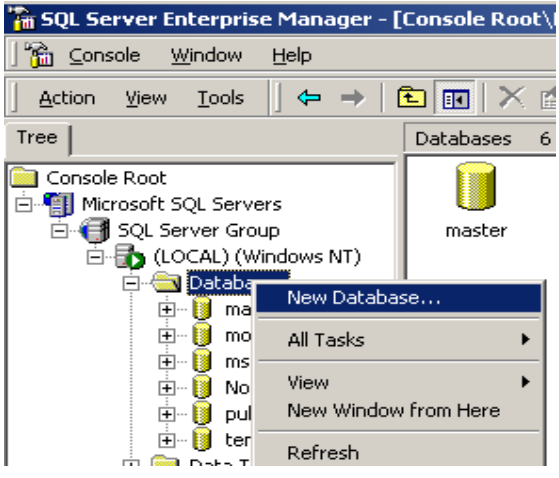
In diesem Abschnitt wird die Installation von Crystal Server für folgende Elemente beschrieben:

- MS SQL 2000 Server Sentinel-Datenbank mit Windows-Authentifizierung
- MS SQL 2000 Server Sentinel-Datenbank mit SQL Server-Authentifizierung
- Oracle Sentinel-Datenbank

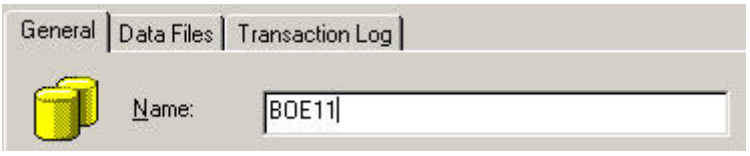
Installation von Crystal Server für MS SQL 2000 Server mit Windows-Authentifizierung

BOE XI Crystal Server – Installation für Windows-Authentifizierung

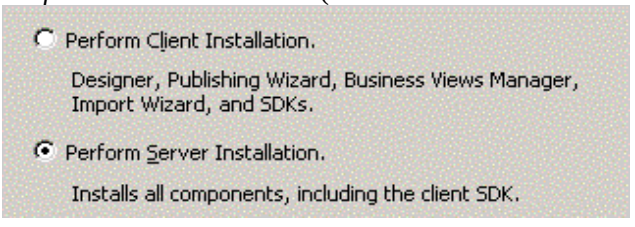
1. Installieren Sie MS SQL 2000 sp3a im gemischten Modus.
2. Starten Sie MS SQL Enterprise Manager.
3. Erweitern Sie im Navigationsfenster „(lokal)(Windows NT)“.
4. Markieren Sie *Datenbank*, klicken Sie mit der rechten Maustaste darauf und wählen Sie *Neue Datenbank…*



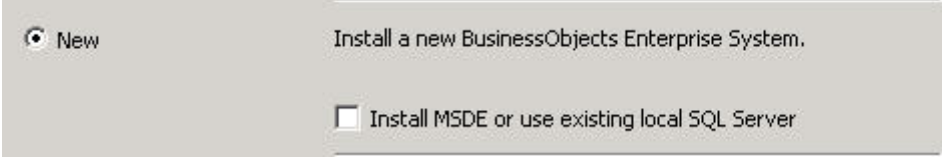
5. Geben Sie auf der Registerkarte „Allgemein“ im Feld „Name“ den Namen „BOE11“ ein und klicken Sie auf *OK*.



6. Beenden Sie MS SQL Enterprise Manager.
7. Legen Sie die CD für BOE XI Crystal Server in das CD-ROM-Laufwerk ein.
8. Wenn auf Ihrem Computer Autoplay deaktiviert ist, führen Sie die Datei *setup.exe* aus.
9. Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option *Perform Server Installation* (Serverinstallation durchführen) aus.

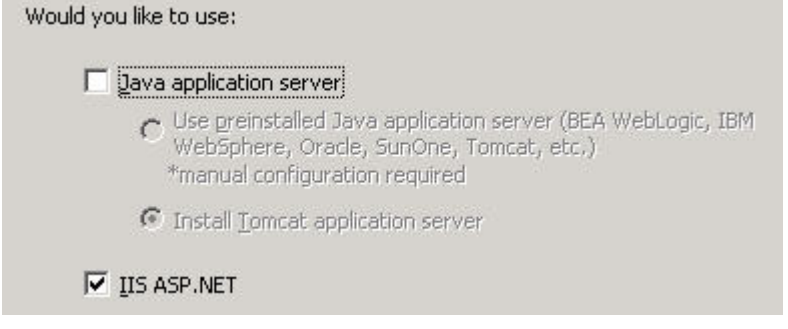


10. Wählen Sie als Installationstyp *New* (Neu) und aktivieren Sie nicht die Option *Install MSDE or use existing local SQL Server* (MSDE installieren oder lokalen SQL-Server verwenden).

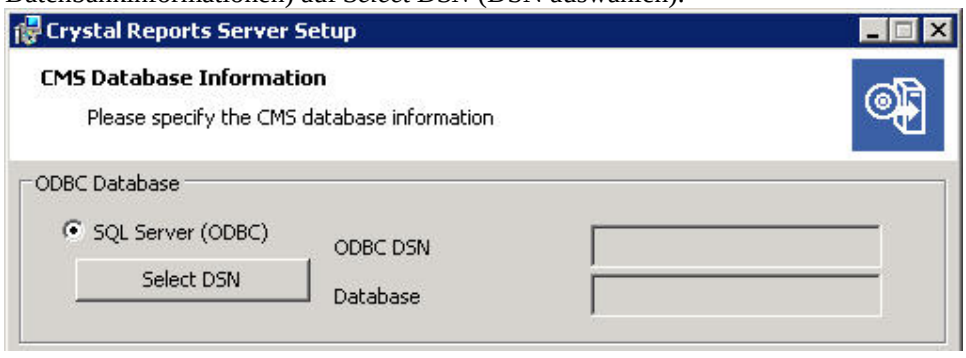


11. Wählen Sie im Fenster „Web Component Adapter Type“ (Adaptertyp der Webkomponente) die Option *IIS ASP.NET* aus.

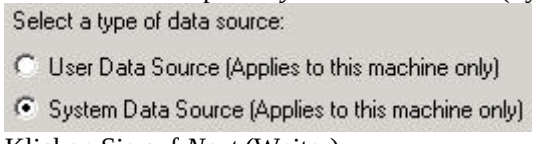
HINWEIS: Wenn Sie IIS und ASP.NET nicht über *Systemsteuerung* > *Software* > *Windows-Komponenten hinzufügen/entfernen* installiert haben, ist *IIS ASP.NET* abgeblendet.



12. Klicken Sie im Fenster „CMS Database Information“ (CMS-Datenbankinformationen) auf *Select DSN* (DSN auswählen).

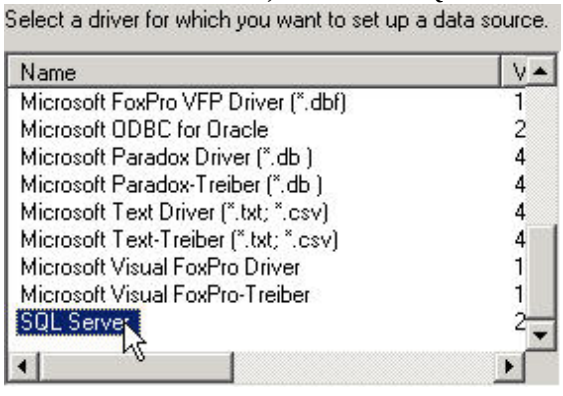


13. Klicken Sie auf die Registerkarte *Machine Data Source* (Computer-Datenquelle).
14. Klicken Sie auf *New*... (Neu...).
15. Wählen Sie die Option *System Data Source* (Systemdatenquelle)

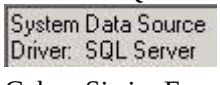


Klicken Sie auf *Next* (Weiter).

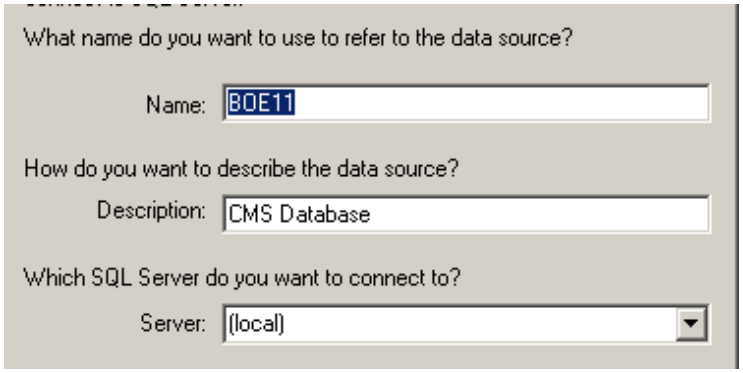
16. Blättern Sie nach unten, wählen Sie *SQL Server* und klicken Sie auf *Next* (Weiter).



17. Eine neue Quelle wird angezeigt. Klicken Sie auf *Finish* (Fertig stellen).

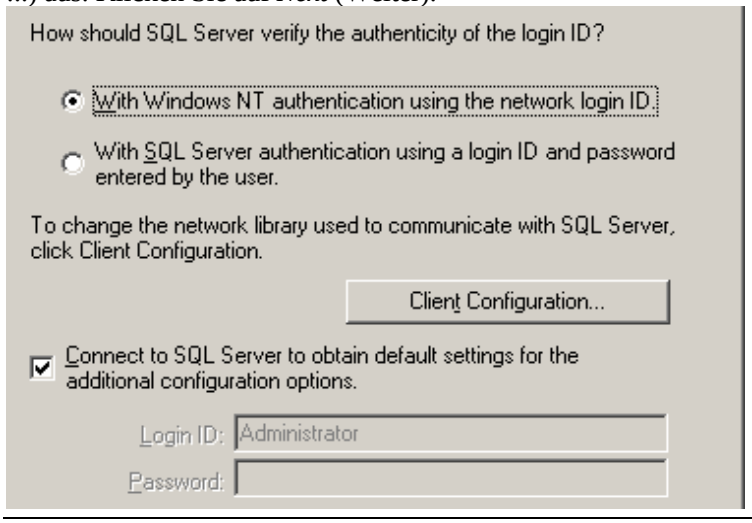


18. Geben Sie im Fenster …*New Data Source to SQL Server* (...Neue Datenquelle für SQL Server) Folgendes ein:
    - Name Ihrer Datenquelle (z. B.: BOE_XI)
    - Beschreibung (optional)
    - Klicken Sie zur Auswahl des Servers auf den nach unten weisenden Pfeil und wählen Sie *(local)* (lokal) aus.



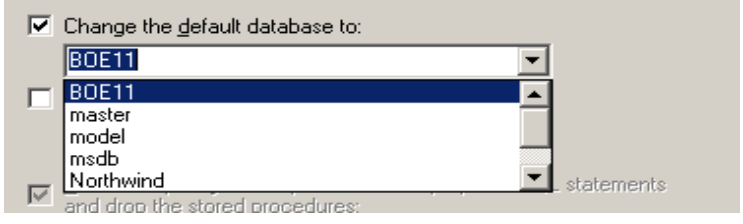
Klicken Sie auf *Next* (Weiter).

19. Wenn nicht bereits geschehen, wählen Sie *With Windows NT …* (Mit Windows NT ...) aus. Klicken Sie auf *Next* (Weiter).



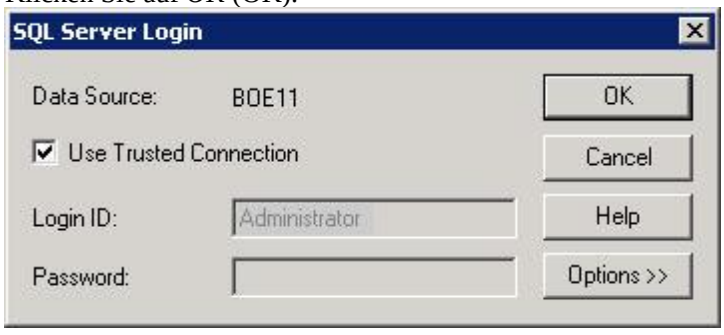
HINWEIS: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

20. Aktivieren Sie das Kontrollkästchen *Change the default database to:* (Standarddatenbank ändern in:). Ändern Sie Ihre Standarddatenbank in *BOE11*. Klicken Sie auf *Next* (Weiter).



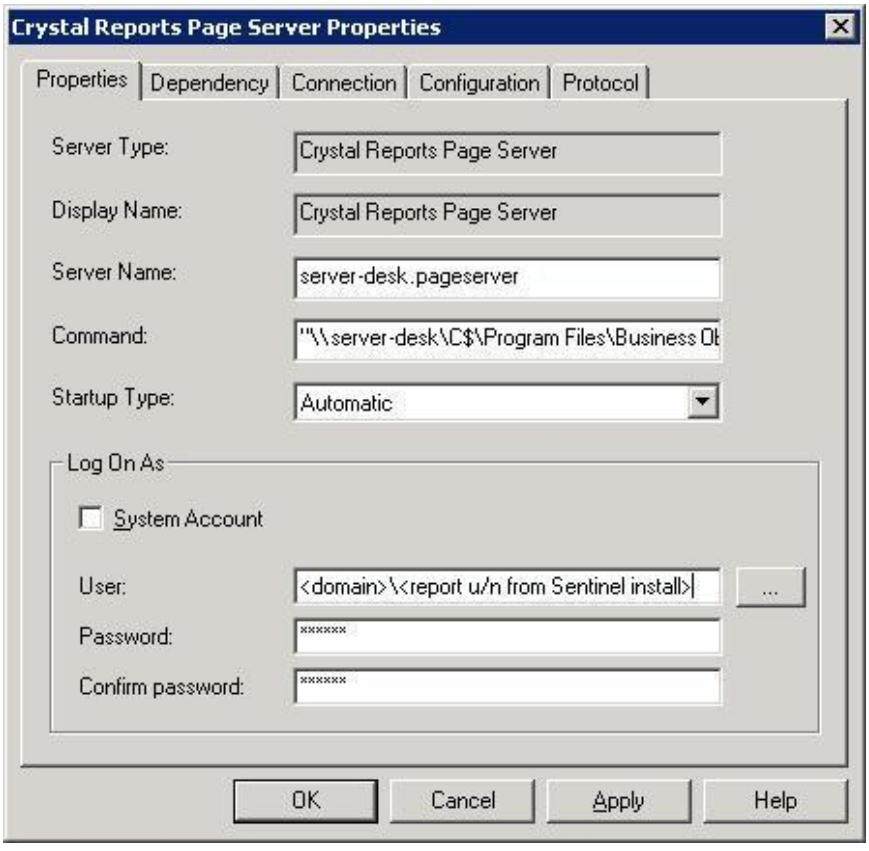
21. Klicken Sie im Fenster „Create a New Data Source to SQL Server“ (Neue Datenquelle für SQL Server erstellen) auf *Finish* (Fertig stellen).
22. Klicken Sie auf *Test Data Source…*(Datenquelle testen…). Dieser Test sollte erfolgreich verlaufen. Klicken Sie auf *OK* (OK).
23. Markieren Sie im Fenster „Select Data Source“ (Datenquelle auswählen) die Option *BOE11* und klicken Sie so lange auf „OK“ (OK), bis das Dialogfeld *SQL Server Login* (SQL Server-Anmeldung) angezeigt wird. Vergewissern Sie sich, dass *Use Trusted Connection* (Vertrauenswürdige Verbindung verwenden) ausgewählt ist.

Klicken Sie auf *OK* (OK).



HINWEIS: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

24. Klicken Sie im Warnfenster auf *OK* (OK).
25. Klicken Sie im Fenster „CMS Database Information“ (CMS-Datenbankinformationen) auf *Next* (Weiter).
26. Klicken Sie auf *Next* (Weiter), um die Installation fortzusetzen.
27. Nach der Installation müssen Sie das Anmeldekonto für Crystal Reports Page Server und Crystal Reports Job Server in das Domänenkonto des Sentinel Report-Benutzers ändern.
    a. Klicken Sie auf *Start* > *Programme* > *BusinessObjects 11* > *Crystal Reports Server* > *Central Configuration Manage*r.
    b. Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ (Crystal Reports Page Server) und wählen Sie *stop* (stopp).
    c. Klicken Sie mit der rechten Maustaste erneut auf *Crystal Reports Page Server* (Crystal Reports Page Server) und wählen Sie *Properties* (Eigenschaften).
    d. Deaktivieren Sie die Option *Log On As System Account* (Als Systemkonto anmelden) und geben Sie den Benutzernamen und das Passwort der Domäne des Sentinel Report-Benutzers ein, die während der Installation von Sentinel 5 für den Sentinel Report-Benutzer verwendet wurden. Klicken Sie auf *OK* (OK).



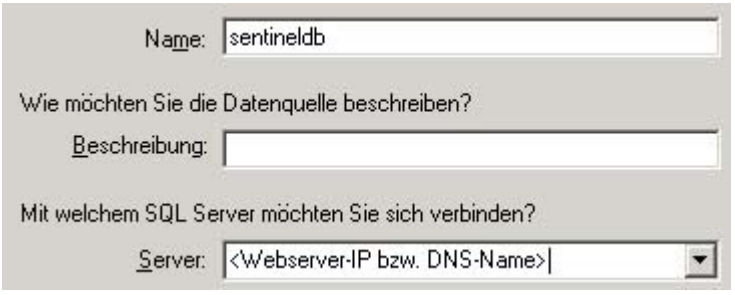
e. Markieren Sie „Crystal Reports Page Server“ und klicken Sie mit der rechten Maustaste, um „Crystal Reports Page Server“ zu starten.

Konfiguration von Open Database Connectivity (ODBC) für Windows-Authentifizierung

Bei diesem Verfahren wird eine ODBC-Datenquelle zwischen Crystal Reports unter Windows und SQL Server eingerichtet. Dies muss auf dem Crystal Server-Computer durchgeführt werden.

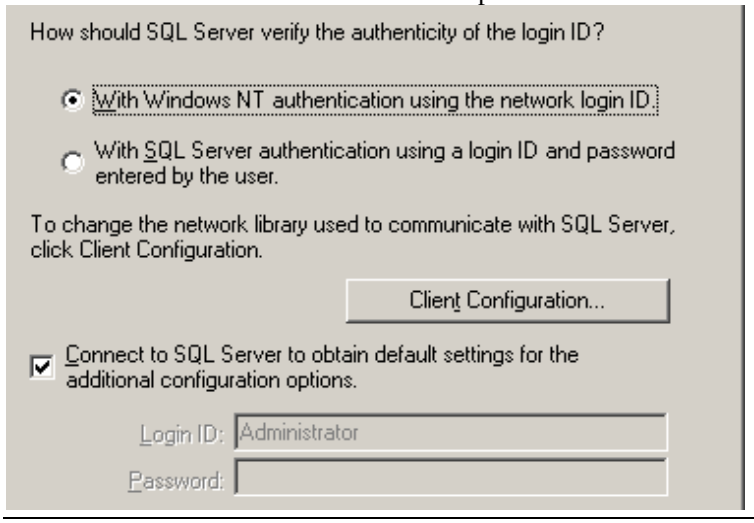
Einrichten einer ODBC-Datenquelle für die Windows-Authentifizierung

1. Wechseln Sie zu Windows-Systemsteuerung > Verwaltung > Datenquellen (ODBC).
2. Klicken Sie auf die Registerkarte *System-DSN* und dann auf *Hinzufügen*.
3. Wählen Sie *SQL Server*. Klicken Sie auf *Fertig stellen*.
4. Ein Bildschirm wird angezeigt, in dem Sie nach Informationen zur Treiberkonfiguration gefragt werden:
   - Name der Datenquelle, geben Sie „esecuritydb“ ein
   - Feld „Description“ (Beschreibung) (optional); geben Sie eine Beschreibung ein
   - Feld „Server“ (Server); geben Sie Ihren Hostnamen bzw. die IP-Adresse Ihrer Instanz von Sentinel Server ein



Klicken Sie auf *Next* (Weiter).

5. Wählen Sie im nächsten Bildschirm die Option für die Windows-Authentifizierung.



HINWEIS: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

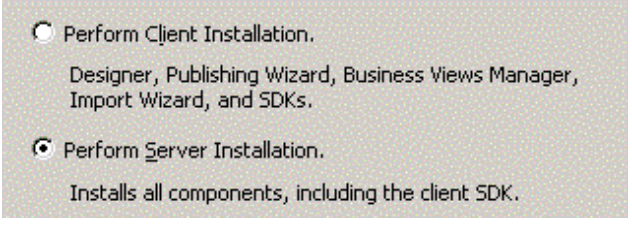
6. Gehen Sie im nächsten Bildschirm wie folgt vor:
   - Ändern Sie die Sentinel-Datenbank (Standardname: „ESEC“)
   - Behalten Sie alle Standardeinstellungen bei.

   Klicken Sie auf *Next* (Weiter).
7. Klicken Sie auf *Fertig stellen*.
8. Klicken Sie auf *Test Data Source…* (Datenquelle testen…). Die Verbindungsherstellung sollte erfolgreich sein. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

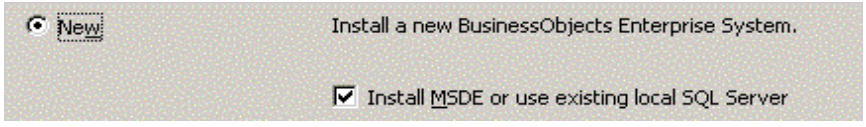
Installation von Crystal Server für MS SQL 2000 Server mit SQL-Authentifizierung

Installieren Sie Crystal Reports Server 11 mit folgenden Optionen.

- „Perform Server Installation“ (Serverinstallation durchführen)



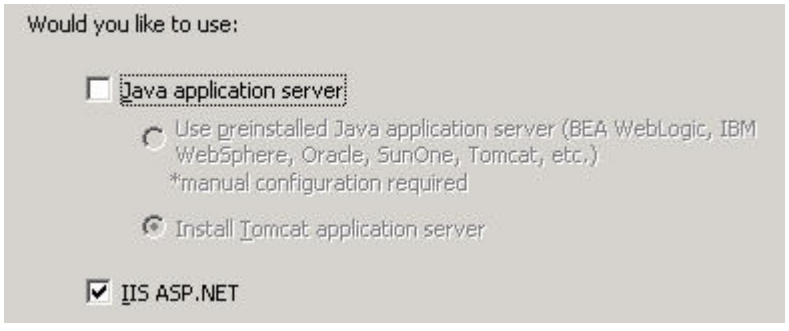
- „Install a new BusinessObjects Enterprise System“ (Neues BusinessObjects Enterprise System installieren), „Install MSDE or use existing local SQL Server“ (MSDE installieren oder lokalen SQL-Server verwenden).



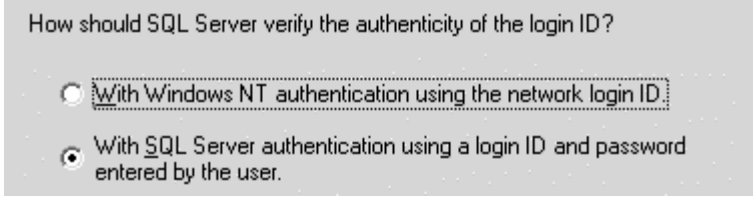
HINWEIS: Crystal Server und MS SQL Server 2000 müssen sich auf demselben Computer befinden.

- IIS ASP.NET.

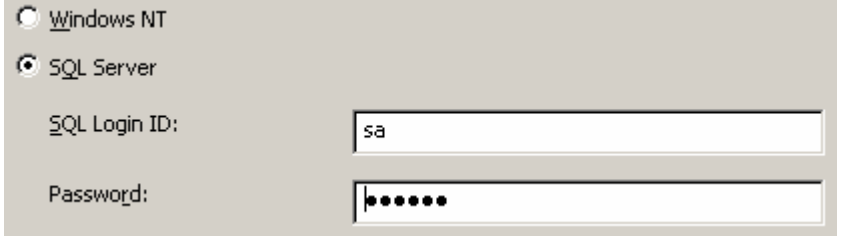
HINWEIS: Wenn Sie IIS und ASP.NET nicht über *Systemsteuerung* > *Software* > *Windows-Komponenten hinzufügen/entfernen* installiert haben, ist *IIS ASP.NET* abgeblendet.



- Sie werden zur Eingabe des Authentifizierungsmodus aufgefordert. Wählen Sie die *SQL Server-Authentifizierung* aus.



- Wählen Sie *SQL Server-Authentifizierung* aus. Geben Sie „sa“ und das Passwort für „sa“ ein.

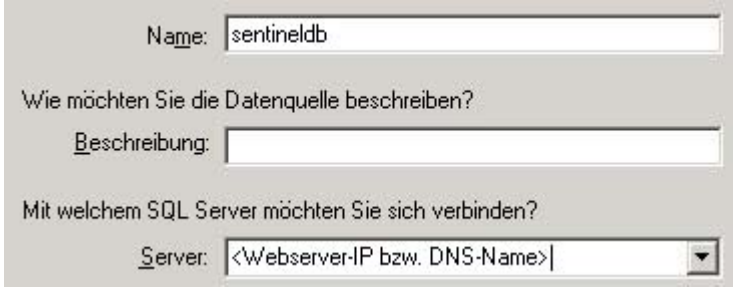


Konfiguration von Open Database Connectivity (ODBC) für SQL-Authentifizierung

Bei diesem Verfahren wird eine ODBC-Datenquelle zwischen Crystal Reports unter Windows und SQL Server eingerichtet. Dies muss auf dem Crystal Server-Computer durchgeführt werden.

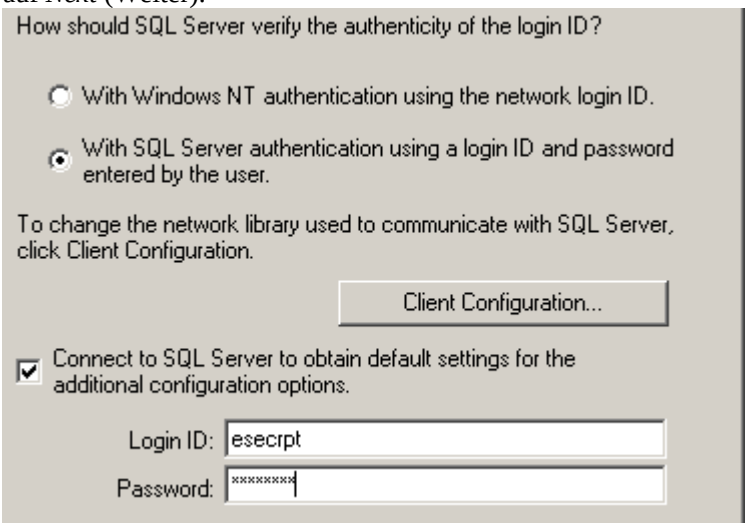
Einrichten einer ODBC-Datenquelle für Windows

1. Wechseln Sie zu Windows-Systemsteuerung > Verwaltung > Datenquellen (ODBC).
2. Klicken Sie auf die Registerkarte *System-DSN* und dann auf *Hinzufügen*.
3. Wählen Sie *SQL Server*. Klicken Sie auf *Fertig stellen*.
4. Ein Bildschirm wird angezeigt, in dem Sie nach Informationen zur Treiberkonfiguration gefragt werden:
   - Name der Datenquelle, geben Sie „esecuritydb“ einFeld „Description“ (Beschreibung) (optional); geben Sie eine Beschreibung ein
   - Feld „Server“ (Server); geben Sie Ihren Hostnamen bzw. die IP-Adresse Ihrer Instanz von Sentinel Server ein



Klicken Sie auf *Next* (Weiter).

5. Wählen Sie im nächsten Bildschirm die Option für die SQL-Authentifizierung. Geben Sie „esecrpt“ und das zugehörige Passwort als Anmelde-ID ein. Klicken Sie auf *Next* (Weiter).



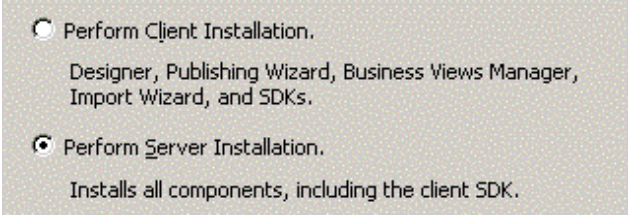
6. Gehen Sie im nächsten Bildschirm wie folgt vor:
   - Ändern Sie die Sentinel-Datenbank (Standardname: „ESEC“)
   - Behalten Sie alle Standardeinstellungen bei.

   Klicken Sie auf *Next* (Weiter).
7. Klicken Sie auf *Fertig stellen*.
8. Klicken Sie auf „Test Data Source…“ (Datenquelle testen). Die Verbindungsherstellung sollte erfolgreich sein. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

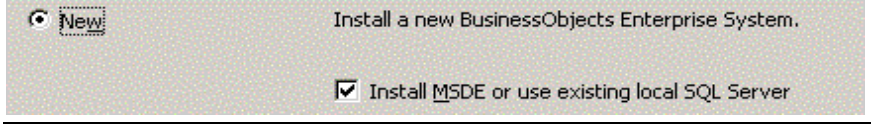
Installation von Crystal Server für Oracle

Installieren Sie Crystal Reports Server 11 mit folgenden Optionen.

- „Perform Server Installation“ (Serverinstallation durchführen)



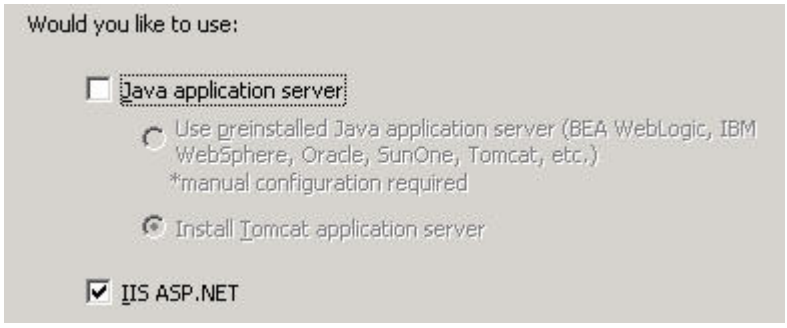
- Installieren Sie ein neues BusinessObjects Enterprise System mithilfe von *Install MSDE or use existing local SQL Server* (MSDE installieren oder lokalen SQL-Server verwenden).



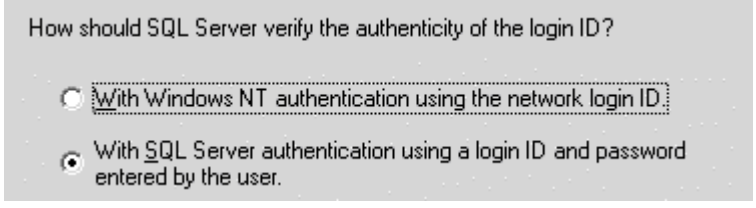
HINWEIS: Crystal Server und MS SQL Server 2000 müssen sich auf demselben Computer befinden.

- IIS ASP.NET.

HINWEIS: Wenn Sie IIS und ASP.NET nicht über *Systemsteuerung* > *Software* > *Windows-Komponenten hinzufügen/entfernen* installiert haben, ist *IIS ASP.NET* abgeblendet.



- Sie werden zur Eingabe des Authentifizierungsmodus aufgefordert. Wählen Sie die *SQL Server-Authentifizierung* aus.



Crystal Reports unterstützt direkten Zugriff auf Oracle 9-Datenbanken. Diese Zugriffsfähigkeit wird durch die crdb_oracle.dll-Übersetzungsdatei gewährleistet. Diese Datei kommuniziert mit dem Oracle 9-Datenbanktreiber, der direkt mit Oracle-Datenbanken und -Clients zusammenarbeitet und die für Ihren Bericht erforderlichen Daten abruft.

HINWEIS: Damit Crystal Reports Oracle 9-Datenbanken verwenden kann, muss die Oracle-Client-Software auf Ihrem System installiert sein und der Standort des Oracle-Client muss in der Umgebungsvariablen PATH angegeben sein.

Installation und Konfiguration der Oracle 9i-Client-Software

Bei der Installation von Oracle 9i Client:

- Übernehmen Sie das Standardinstallationsverzeichnis
- Wählen Sie „No“ (Nein) bei „Perform Typical Configuration“ (Typische Konfiguration durchführen)
- Wählen Sie „No“ (Nein) bei „Directory Service“ (Verzeichnisdienst)
- Wählen Sie *Local* (Lokal)
- „TNS Service Name“ (Name des TNS-Service): ESEC
- „User“ (Benutzer) (optional): esecrpt

Erstellen Sie nach der Installation eine lokale Net Service Name-Konfiguration.

Erstellen der Net Service Name-Konfiguration (Konfiguration des systemeigenen Oracle-Treibers)

1. Wählen Sie Oracle-OraHome92 > Configuration and Migration Tools (Konfigurations- und Migrationswerkzeuge) > Net Manager.
2. Erweitern Sie im Navigationsfenster „Local“ (Lokal) und markieren Sie „Service Naming“ (Service-Benennung).

3. Klicken Sie auf das Pluszeichen auf der linken Seite, um einen Service-Namen hinzuzufügen.
4. Geben Sie im Fenster „Service Name“ (Service-Name) einen Net Service-Namen ein.
   - Geben Sie ESECURITYDB ein.

   Klicken Sie auf *Next* (Weiter).
5. Wählen Sie im Fenster „Select Protocols“ (Protokolle auswählen) den Standardwert aus:
   - TCP/IP (Internet Protocol)

   Klicken Sie auf *Next* (Weiter).
6. Hostname und Portnummer:
   - Geben Sie den Hostnamen bzw. die IP-Adresse des Computers ein, auf dem sich die Datenbank befindet.
   - Wählen Sie „Oracle Port“ (Oracle-Port) aus (standardmäßig 1521 bei der Installation)

   Klicken Sie auf *Next* (Weiter).
7. So identifizieren Sie die Datenbank bzw. den Service:
   - Wählen Sie *(Oracle8i or later)*（Oracle8i oder höher) aus, geben Sie Ihren Service-Namen ein (dies ist der Name Ihrer Oracle-Instanz).
   - Wählen Sie als Verbindungstyp *Database Default* (Datenbankstandard) aus.

   Klicken Sie auf *Next* (Weiter).
8. Klicken Sie im Fenster *Test* (Test) auf *Test…*(Test…). Klicken Sie auf *Next* (Weiter). Möglicherweise ist der Test nicht erfolgreich, da dafür eine Datenbank-ID und ein Datenbankpasswort verwendet werden.
9. Wenn der Test nicht erfolgreich ist, gehen Sie wie folgt vor:
   - Klicken Sie im Fenster *Connecting* (Verbindungsaufbau) auf *Change Login* (Anmeldung ändern).
   - Geben Sie die Sentinel Oracle-ID (verwenden Sie „esecrpt“) und das Passwort ein. Klicken Sie auf *OK* (OK).

   Wenn der Test nicht erfolgreich ist:
   - Senden Sie ein Ping-Signal an den Sentinel Server
   - Vergewissern Sie sich, dass der Hostname des Sentinel Servers in der Hosts-Datei auf dem Crystal Reports Server vorliegt. Die Hosts-Datei finden Sie unter %SystemRoot%\system32\drivers\etc\.
10. Klicken Sie auf *Fertig stellen*.

Konfiguration für alle Authentifizierungen und Konfigurationen

Zuordnen von Crystal Reports zur Verwendung mit Sentinel

Folgende Verfahren sind erforderlich, damit Crystal Server mit Sentinel Control Center zusammenarbeiten kann.

Konfiguration von inetmgr

inetmgr

1. Kopieren Sie die Datei web.config aus:

   ```
   C:\Programme\Business Objects\BusinessObjects
      Enterprise 11\Web Content
   ```

   nach c:\Inetpub\wwwroot.
2. Starten Sie Internet Service Manager durch Klicken auf *Start* > *Ausführen*. Geben Sie *inetmgr* ein und klicken Sie auf *OK*.
3. Erweitern Sie *(lokaler Computer)* > *Websites* > *Standardwebsite* > *businessobjects.*
4. Klicken Sie bei *businessobjects* mit der rechten Maustaste > *Eigenschaften*.
5. Klicken Sie auf der Registerkarte *Virtuelles Verzeichnis* auf *Konfiguration....*
6. Folgende Zuordnungen sollten vorliegen. Wenn dies nicht der Fall ist, fügen Sie sie hinzu. Wenn Sie vorhaben, eine Zuordnung hinzuzufügen, klicken Sie nicht auf die Knoten *businessobjects* bzw. *crystalreportsviewer11*.

Erweiterung	Ausführbare Datei
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	C:\Program Files\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

   Klicken Sie auf *OK*, um das Fenster zu schließen.
7. Starten Sie IIS erneut. Gehen Sie dazu wie folgt vor: Erweitern Sie (lokaler Computer) > *Websites* > *Standardwebsite*, markieren Sie *Standardwebsite* und klicken Sie mit der rechten Maustaste > *Start*.

Patches für Crystal Reports zur Verwendung mit Sentinel

Um Crystal Reports über die Registerkarte „Analyse“ von Sentinel Control Center anzuzeigen, müssen mehrere Crystal Enterprise-Dateien aktualisiert werden, um sie mit dem in Sentinel eingebetteten Browser kompatibel zu machen.

In der folgenden Tabelle werden diese Dateien aufgelistet und es wird beschrieben, wofür die einzelnen Dateien verwendet werden.

Dateiname	*Beschreibung*

`calendar.js`
 	
`calendar.html`
	Zeigt einen Popup-Kalender an, wenn Sie ein Datum als Parameter für einen Bericht auswählen.

Dateiname	*Beschreibung*
`grouptree.html`	Zeigt die Meldung „... wird geladen“ an, während Berichte geladen werden.
`exportframe.html`	Zeigt das Fenster an, in dem Sie einen Bericht zum Speichern oder Drucken exportieren können.
`exportIce.html`	Von Sentinel beim Export eines Berichts zum Speichern oder Drucken verwendete Datei.
`GetInfoStore.asp`	Zur Abfrage des Crystal Server verwendete Datei
`GetReports.asp`	Die Datei, die Sentinel Control Center verwendet, um eine Verbindung mit Crystal Server herzustellen und die Berichtsliste anzuzeigen.
`GetReportURL.asp`	Zur Unterstützung von Hyperlinks zwischen Berichten verwendete Datei.
`helper_js.asp`	Eine von GetInfoStore.asp verwendete Aufrufdatei.

8. Wechseln Sie auf der Sentinel Service Pack-CD-ROM zu \content\reports\patch und kopieren Sie alle *.html- und *.js-Dateien zum Speicherort der Viewer-Datei; standardmäßig ist dies:

   ```
   C:\Programme\Business Objects\BusinessObjects
      Enterprise 11\Web Content\Enterprise11\viewer\en
   ```

9. Wechseln Sie auf der Sentinel Service Pack-CD-ROM zu \content\reports\patch und kopieren Sie alle *.asp- und *.js-Dateien nach:

   ```
   C:\inetpub\wwwroot
   ```

HINWEIS: Ihr Webordner kann sich auf einem anderen Laufwerk bzw. an einem anderen Speicherort befinden, als oben angegeben.

Crystal Reports-Schablonen

Crystal-Berichtsschablonen werden mithilfe von Crystal Publishing Wizard veröffentlicht.

Die aktuelle Menge der Reports-Schablonen können Sie über das Kundenportal unter http://esecurity.custhelp.com/ herunterladen.

HINWEIS: Bei „List of Attacks by CVE Report“ (Liste der Angriffe von CVE Report) handelt es sich um eine Schnittmenge aus Angriffssignaturen aus dem Advisor-Vorschub und durch Absuchen entdeckten Anfälligkeiten.

HINWEIS: Zur Ausführung von Top 10-Berichten müssen bestimmte Aggregationszusammenfassungen aktiviert werden und EventFileRedirectService (im DAS_Binary-Prozesss) muss eingeschaltet werden. Informationen zur Aktivierung von Aggregationszusammenfassungen und zum Einschalten von EventFileRedirectService finden Sie im Abschnitt Aktivieren von Sentinel Top 10-Berichten.

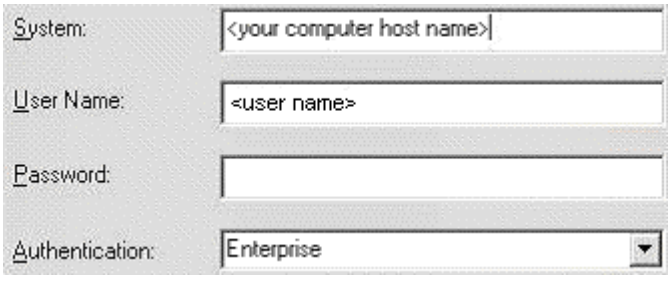
Veröffentlichen von Berichtsschablonen mithilfe von Crystal Publishing Wizard

Crystal Reports-Schablonen

HINWEIS: Wenn Sie Ihre Reports-Schablonen erneut veröffentlichen, müssen Sie den vorherigen Schablonen-Import löschen.

1. Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard.
2. Klicken Sie auf *Next* (Weiter).
3. Melden Sie sich an. Als System sollte der Name des Host-Computers verwendet werden und als Authentifizierung „Enterprise“. Der Benutzername kann „Administrator“ lauten. Aus Sicherheitsgründen sollten Sie unbedingt einen neuen Benutzer mit einem anderen Namen als „Administrator“ erstellen. Geben Sie Ihr Passwort ein und klicken Sie auf *Next* (Weiter).

HINWEIS: Auf Berichte, die als Benutzer „Verwalter“ veröffentlicht wurden, haben alle Benutzer Zugriff.



4. Klicken Sie auf *Add Folder* (Ordner hinzufügen).
5. Wählen Sie *Include Subfolder* (Unterordner einbeziehen). Rufen Sie die Sentinel Service Pack-CD-ROM auf und wechseln Sie zu:

   Für Crystal Reports (MS SQL-Benutzer):

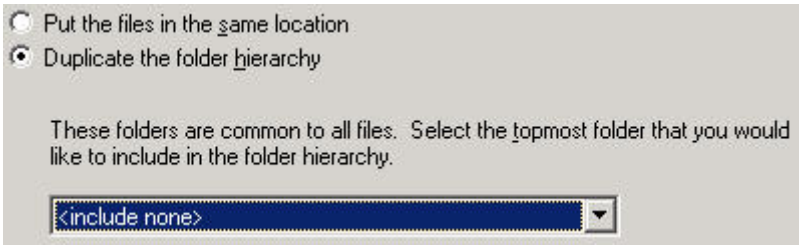
   ```
   \content\reports\Crystal_v11\SQL-Server
   ```

   Für Crystal Reports (Oracle-Benutzer):

   ```
   \content\reports\Crystal_v11\Oracle
   ```

   Klicken Sie auf *OK* (OK).
6. Klicken Sie auf *Next* (Weiter).
7. Klicken Sie im Fenster „Specify Location“ (Speicherort angeben) auf die Schaltfläche *New Folder* (Neuer Ordner) in der rechten oberen Ecke und erstellen Sie einen Ordner mit der Bezeichnung *eSecurity_Reports*. Klicken Sie auf *Next* (Weiter).

8. Wählen Sie:
   - *Duplicate the folder hierarchy* (Ordnerhierachie duplizieren).
   - Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie *<include none>* (<keine einschließen>) aus.



   Klicken Sie auf *Next* (Weiter).

9. Klicken Sie im Fenster „Confirm Location“ (Speicherort bestätigen) auf *Next* (Weiter).
10. Gehen Sie im Fenster „Specify Categories“ (Kategorien angeben) wie folgt vor:
    - Geben Sie einen beliebigen Kategorienamen an (z. B. sentinel)
    - Markieren Sie den Namen und klicken Sie auf die Schaltfläche „+“.

HINWEIS: Nur der erste Bericht wird nach dem Klicken auf „Next“ (Weiter) unter der Kategorie angezeigt.

    - Klicken Sie auf *Next* (Weiter).
11. Klicken Sie im Fenster „Specify Schedule“ (Zeitplan angeben) auf *Let users update the object* (Zulassen, dass Benutzer das Objekt aktualisieren) (sollte Standard sein). Klicken Sie auf *Next* (Weiter).
12. Klicken Sie im Fenster „Specify Repository Refresh“ (Repository-Aktualisierung angeben) auf *Enable all* (Alle aktivieren), um die Repository-Aktualisierung zu aktivieren. Klicken Sie auf *Next* (Weiter).
13. Klicken Sie im Fenster „Specify Keep Saved Data“ (Angabe für das Beibehalten gespeicherter Daten) auf *Enable all* (Alle aktivieren), um beim Veröffentlichen von Berichten die gespeicherten Daten beizubehalten. Klicken Sie auf *Next* (Weiter).
14. Klicken Sie im Fenster „Change Defaults Values“ (Standardwerte ändern) auf das Optionsfeld *Publish reports without modifying properties* (Berichte veröffentlichen, ohne Eigenschaften zu ändern) (sollte Standard sein). Klicken Sie auf *Next* (Weiter).
15. Klicken Sie auf *Next* (Weiter), um Ihre Objekte hinzuzufügen.
16. Klicken Sie auf *Next* (Weiter).
17. Eine veröffentlichte Liste wird angezeigt. Klicken Sie auf *Finish* (Fertig stellen).

Wenn die Sentinel-Schablonen für Crystal Reports auf dem Crystal Enterprise-Server veröffentlicht werden, müssen sich die Schablonen im *eSecurity_Reports*-Verzeichnis befinden.

Festlegen eines Kontos für einen benannten Benutzer

Der im Lieferumfang von Crystal Server enthaltene Schlüssel ist ein Kontoschlüssel für „Named User“ (Benannter Benutzer). Das Gastkonto muss von „Concurrent User“ (Gleichzeitiger Benutzer) in „Named User“ (Benannter Benutzer) geändert werden.

Festlegen des Gastkontos als „Named User“ (Benannter Benutzer)

1. Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad.
2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht der Fall, wählen Sie *Enterprise* aus.
4. Klicken Sie auf *Log On* (Anmelden).
5. Klicken Sie im Fenster „Organize“ (Organisieren) auf *Users* (Benutzer).
6. Klicken Sie auf *Guest* (Gast).
7. Ändern Sie den Verbindungstyp von *Concurrent User* (Gleichzeitiger Benutzer) in *Named User* (Benannter Benutzer).
8. Klicken Sie auf *Update* (Aktualisieren).
9. Melden Sie sich ab und schließen Sie das Fenster oder gehen Sie weiter zum Abschnitt *Konfigurieren von .NET Administration Launchpad*.

Konfigurieren von .NET Administration Launchpad

In diesem Verfahren wird erläutert, wie .NET Administration Launchpad so konfiguriert werden kann, dass Sie Berichte anzeigen und bearbeiten können.

Konfigurieren von .NET Administration Launchpad

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad (Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad).
2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).

   Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht der Fall, wählen Sie *Enterprise* aus.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *Log On* (Anmelden).
4. Klicken Sie im Fenster „Organize“ (Organisieren) auf *Folders* (Ordner).
5. Klicken Sie einmal (nicht doppelt) auf *eSecurity_Reports*.
6. Wählen Sie *All* (Alle).
7. Klicken Sie auf die Registerkarte *Rights* (Rechte).
8. Wählen Sie im Dropdown-Menü direkt unterhalb von „Access Level“ (Zugriffsebene) für „Everyone“ (Alle) die Option *View on Demand* (Auf Verlangen anzeigen) aus. Klicken Sie auf *Update* (Aktualisieren).

HINWEIS: Beim Ändern der Zugriffsebene von *Inherited Rights* (Vererbte Rechte) zu *View on Demand* (Auf Verlangen anzeigen) reagiert der Aktualisierungsprozess nicht mehr. Warten Sie ca. 30 Sekunden. Die Zugriffsebene wird aktualisiert.

9. Melden Sie sich ab und schließen Sie das Fenster.

Testen auf Webserver-Verbindung mit der Datenbank

Testen auf Webserver-Verbindung mit der Datenbank

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad (Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad).
2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).
3. Geben Sie als Benutzernamen „Administrator“ ein. Geben Sie Ihr Passwort ein (standardmäßig leer). Klicken Sie auf *Log On* (Anmelden).
4. Wechseln Sie zu *Public Folders (Öffentliche Ordner)* > *eSecurity_Reports* > *Internal Events (Interne Ereignisse).*
5. Wählen Sie *Column Display Details* (Spaltenanzeigedetails) aus.
6. Klicken Sie auf *Preview* (Vorschau).
7. Melden Sie sich – je nach System – als „esecrpt“ oder als Sentinel Report-Benutzer an.
8. Wählen Sie im Dropdown-Menü für das Sortierfeld *Tag* (Tag) aus.
9. Klicken Sie auf *OK* (OK). Ein Bericht sollte angezeigt werden.

Testen der Konnektivität zum Webserver

Testen der Konnektivität zum Webserver

1. Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.
2. Geben Sie Foglgendes ein:

```
http://<DNS-Name oder IP-Adresse des
   Webservers>/businessobjects/enterprise11/WebTools/a
   dminlaunch/default.aspx
```

3. Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

Aktivieren von Sentinel Top 10-Berichten

Gehen Sie wie folgt vor, um Sentinel Top 10-Berichte zu aktivieren:

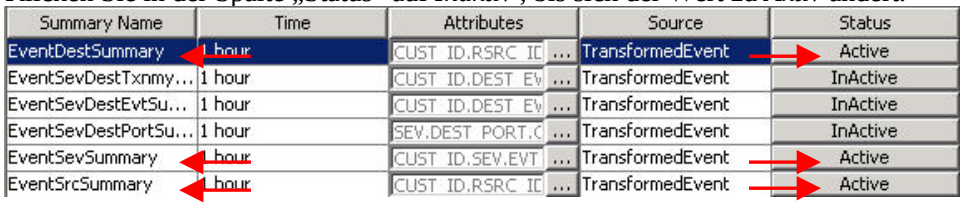
- Schalten Sie die Aggregation ein.
- Aktivieren Sie EventFileRedirectService.

Einschalten der Aggregation

1. Starten Sie Sentinel Data Manager.
2. Melden Sie sich an.
3. Klicken Sie auf die Registerkarte *Bericht für Daten.*

4. Aktivieren Sie folgende Zusammenfassungen:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Klicken Sie in der Spalte „Status“ auf *Inaktiv* , bis sich der Wert zu *Aktiv* ändert.



Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID.DEST_EV ...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID.DEST_EV ...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV.DEST_PORT.C ...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID.SEV.EVT ...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active

Aktivieren von EventFileRedirectService

1. Öffnen Sia auf Ihrem DAS-Computer mithilfe des Texteditors folgende Datei:

   Für UNIX:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

   Für Windows:

   ```
   %ESEC_HOME%\sentinel\config\das_binary.xml
   ```

2. Ändern Sie den Status von EventFileRedirectService auf „On“ (Ein).

   ```
   <property name="status">on</property>
   ```

3. Starten Sie die DAS-Komponente folgendermaßen erneut:

   Unter Windows:

   ```
   Stoppen Sie den Dienst „sentinel“ mithilfe von Service
      Manager und starten Sie ihn erneut.
   ```

   Unter Solaris:

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh stop
   ```

   ```
   Vergewissern Sie sich mithilfe des Befehls „ps –ef |
      grep $ESEC_USER“, dass alle Sentinel Server-
      Prozesse auf diesem Rechner angehalten wurden. Wenn
      einige Sentinel Server-Prozesse weiterhin
      ausgeführt werden, beenden Sie sie mit dem Befehl
      „kill“.
   ```

   ```
   $ESEC_HOME/sentinel/scripts/sentinel.sh start
   ```

Maximieren Ihrer Ereignisberichterstellung

Je nachdem, wie viele Ereignisse Crystal abfragt, erhalten Sie möglicherweise eine Fehlermeldung bezüglich der maximalen Verarbeitungszeit oder der maximalen Datensatzgrenze. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Berichten einzurichten, müssen Sie den Crystal Page Server neu konfigurieren. Hierfür gibt es zwei Methoden: mithilfe von Central Configuration Manager oder mithlife der Crystal-Webseite.

Neukonfiguration von Crystal Page Server über Central Configuration Manager

1. Klicken Sie auf Start > Alle Programme > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Klicken Sie mit der rechten Maustaste auf *Crystal Reports Page Server* (Crystal Reports Page Server) und wählen Sie *Stop* (Stopp).
3. Klicken Sie mit der rechten Maustaste auf *Crystal Reports Page Server* (Crystal Reports Page Server) und wählen Sie *Properties* (Eigenschaften).
4. Fügen Sie auf der Registerkarte „Properties“ (Eigenschaften) im Feld „Command“ (Befehl) am Ende der Befehlszeile „-maxDBResultRecords <Wert größer als 20000 oder 0 zur Deaktivierung der Standardgrenze>“ hinzu.
5. Starten Sie Crystal Page Server neu.

Neukonfiguration von Crystal Page Server über die Crystal-Webseite

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

```
http://<DNS-Name oder IP-Adresse des
   Webservers>/businessobjects/enterprise11/WebTools/a
   dminlaunch/default.aspx
```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *Log On* (Anmelden).
5. Klicken Sie auf *Servers* (Server).
6. Klicken Sie auf <*Servername*>.*pageserver*.
7. Klicken Sie unter „Database Records to Read When Previewing Or Refreshing a report“ (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf *Unlimited records* (Unbegrenzt viele Datensätze).
8. Klicken Sie auf *Apply* (Anwenden).
9. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf *OK* (OK).
10. Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager des Betriebssystems aufgefordert.

Konfigurieren von Sentinel für die Integration mit Crystal Enterprise Server

Nach der Installation von Crystal Enterprise Server kann das Sentinel Control Center für den Zugriff auf Berichte direkt über das Sentinel Control Center konfiguriert werden.

Konfigurieren von Sentinel für die Integration mit Crystal Enterprise Server

1. Melden Sie sich bei Sentinel Control Center als Benutzer mit Rechten für die Registerkarte „Admin“ an.
2. Wählen Sie auf der Registerkarte „Admin“ die Option *Berichtkonfiguration*.

3. Geben Sie in das Feld „Analyse-URL“ Folgendes ein:

```
http://<Hostname_oder_IP-
   Adresse_des_Webservers>/GetReports.asp?APS=<Hostnam
   e>&user=Guest&password=&tab=Analysis
```

HINWEIS: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse bzw. den Hostnamen des Crystal Enterprise Server ersetzt werden.

HINWEIS: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS die IP-Adresse angegeben ist. Es muss sich um den Crystal Server-Hostnamen handeln.

4. Klicken Sie neben dem Feld „Analyse-URL“ auf *Aktualisieren*.
5. Wenn Advisor auf Ihrem Computer installiert ist, geben Sie Folgendes in das Feld „Advisor-URL“ ein:

```
http://<Hostname_oder_IP-
   Adresse_des_Webservers>/GetReports.asp?APS=<Hostnam
   e>&user=Guest&password=&tab=Advisor
```

HINWEIS: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse bzw. den Hostnamen des Crystal Enterprise Server ersetzt werden.

HINWEIS: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS die IP-Adresse angegeben ist. Es muss sich um den Crystal Server-Hostnamen handeln.

6. Klicken Sie neben dem Feld „Advisor URL“ auf *Aktualisieren*.
7. Klicken Sie auf *Save* (Speichern).
8. Melden Sie sich bei Sentinel Control Center ab und erneut wieder an. Die Crystal Reports-Bäume auf den Registerkarten „Analyse“ und „Advisor“ (wenn Advisor installiert ist), sollten nun im Navigatorfenster angezeigt werden.

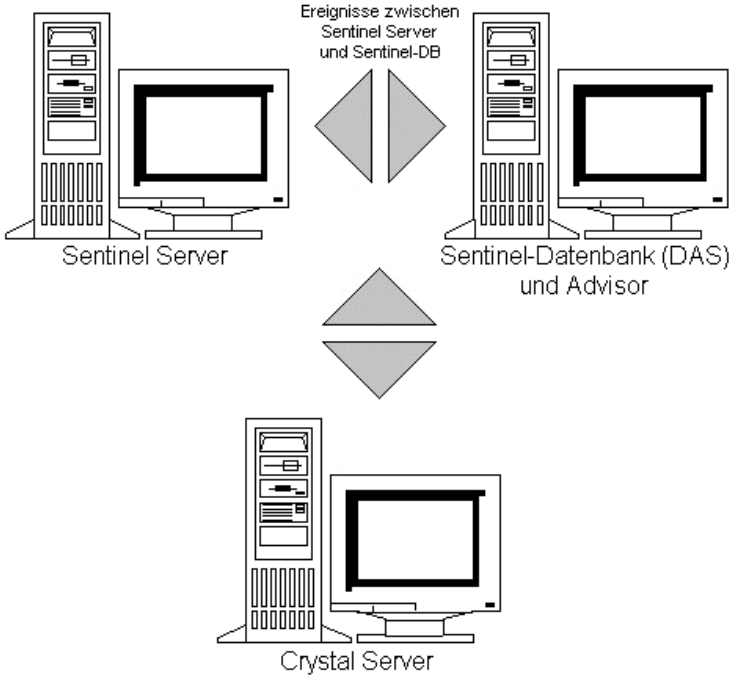
10 Crystal Reports für Linux

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Crystal BusinessObjects Enterprise™ 11 ist eines der Berichterstellungswerkzeuge für Sentinel.

In diesem Kapitel wird die Installationskonfiguration von Crystal Reports Server für Sentinel unter Linux erörtert. Die Installation sollte in der angegebenen Reihenfolge vorgenommen werden.

- Vor-Installation und Installation von Crystal BusinessObjects Enterprise™ 11
- Anwenden von Patches auf Crystal Reports-Berichte
- Veröffentlichen (Importieren) von Crystal Reports-Berichten
- Festlegen eines Kontos für einen benannten Benutzer
- Testen der Konnektivität zum Webserver
- Aktivieren der Top 10-Berichte (optional)
- Maximieren der Ereignisberichterstellung (empfohlen)
- Konfigurieren von Sentinel für den Crystal Enterprise Server



Verwenden von Crystal Reports

Informationen zur Verwendung von Crystal Reports für die Sentinel-Berichterstellung finden Sie in der *Crystal Reports-Dokumentation* bzw. im *Sentinel-Benutzerhandbuch*.

Konfiguration

- Folgende Linux-Versionen:
  - SuSE Linux Enterprise Server 9 (SLES 9)
  - Red Hat Enterprise Linux 3 Update 5 ES (x86)
- BusinessObjects Enterprise XI Server installiert
- Für Oracle – Oracle 9i Client Release 2 (9.2.0.1.0)

Installation

Vor-Installation von Crystal BusinessObjects Enterprise™ 11

Vor-Installation von Crystal BusinessObjects Enterprise

1. Wenn sich die Sentinel-Datenbank nicht auf demselben Computer befindet wie Crystal Server, müssen Sie die Oracle Client-Software auf dem Computer mit Crystal Server installieren. Dieser zusätzliche Schritt ist nicht erforderlich, wenn sich die Sentinel-Datenbank auf demselben Computer befindet wie Crystal Server, da die erforderliche Oracle-Software in diesem Fall bereits zusammen mit der von der Sentinel-Datenbank benötigten Oracle-Datenbank-Software installiert wurde.
2. Melden Sie sich als Benutzer „root“ beim Crystal Server-Computer an.
3. Erstellen Sie die Gruppe „bobje“.

   ```
   groupadd bobje
   ```

4. Erstellen Sie den Crystal-Benutzer (das Basisverzeichnis ist in diesem Fall „/export/home/crystal“, ändern Sie es, falls erforderlich; der Teil „/export/home“ des Pfads muss bereits vorhanden sein).

   ```
   useradd –g bobje –s /bin/bash –d /export/home/crystal
      –m crystal
   ```

5. Erstellen Sie ein Verzeichnis für die Crystal-Software:

   ```
   mkdir –p /opt/crystal_xi
   ```

6. Ändern Sie den Eigentümer des Verzeichnisses für die Crystal-Software (rekursiv) in crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xi
   ```

7. Wechseln Sie zum Crystal-Benutzer:

   ```
   su - crystal
   ```

8. Die Umgebungsvariable ORACLE_HOME muss in der Umgebung des Crystal-Benutzers festgelegt werden. Bearbeiten Sie dazu das Anmeldeskript des Crystal-Benutzers, um die Umgebungsvariable ORACLE_HOME auf die Basis der Oracle-Software zu setzen. Beispiel: Wenn es sich bei der Shell eines Crystal-Benutzers um eine Bash-Shell handelt und die Oracle-Software im Verzeichnis /opt/oracle/product/9.2 installiert ist, müssen Sie die Datei ~crystal/.bash_profile öffnen und folgende Zeile am Ende der Datei einfügen:

   ```
   export ORACLE_HOME=/opt/oracle/product/9.2
   ```

9. Die Umgebungsvariable LD_LIBRARY_PATH in der Umgebung des Crystal-Benutzers muss den Pfad zu den Oracle-Softwarebibliotheken enthalten. Bearbeiten Sie dazu das Anmeldeskript des Crystal-Benutzers, um die Umgebungsvariable LD_LIBRARY_PATH so festzulegen, dass sie die Oracle-Softwarebibliotheken enthält. Beispiel: Wenn es sich bei der Shell eines Crystal-Benutzers um eine Bash-Shell handelt, müssen Sie die Datei ~crystal/.bash_profile öffnen und folgende Zeile am Ende der Datei (unterhalb der Stelle, an der die Umgebungsvariable ORACLE_HOME festgelegt wurde) einfügen:

   ```
   export
      LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
   ```

10. Es muss ein Eintrag mit dem Servicenamen „esecuritydb“ zur Oracle-Datei tnsnames.ora hinzugefügt werden, der auf die Sentinel-Datenbank verweist. Gehen Sie dazu auf dem Crystal Server-Computer wie folgt vor:
    a. Melden Sie sich als Oracle-Benutzer an.
    b. Wechseln Sie in das Verzeichnis $ORACLE_HOME/network/admin
    c. Erstellen Sie eine Sicherungskopie der Datei tnsnames.ora.
    d. Öffnen Sie die Datei tnsnames.ora zur Bearbeitung.
    e. Wenn sich die Sentinel-Datenbank auf dem Crystal Server-Computer befindet, sollte bereits ein Eintrag in der Datei tnsnames.ora vorhanden sein, der auf die Sentinel-Datenbank verweist. Wenn die Sentinel-Datenbank beispielsweise den Namen ESEC trägt, ist ein Eintrag wie der folgende vorhanden:

       ```
       ESEC =
       (DESCRIPTION =
        (ADDRESS_LIST =
         (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
          = 1521))
         )
         (CONNECT_DATA =
         (SID = ESEC)
         )
       )
       ```

    f. Wenn sich die Sentinel-Datenbank nicht auf dem Crystal Server-Computer befindet, öffnen Sie die Datei tnsnames.ora auf dem Computer mit der Sentinel-Datenbank, um den oben beschriebenen Eintrag zu finden.

g. Erstellen Sie eine Kopie des gesamten Eintrags und fügen Sie ihn am Ende der Datei tnsnames.ora auf dem Crystal Server-Computer ein. Der Teil des Eintrags für den Service-Namen muss in „esecuritydb“ umbenannt werden. Wenn beispielsweise der obige Eintrag kopiert und ordnungsgemäß umbenannt wurde, sieht er folgendermaßen aus:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT
   = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

h. Achten Sie darauf, dass der HOST-Teil des Eintrags korrekt ist (d. h. stellen Sie sicher, dass er nicht auf „localhost“ gesetzt ist, wenn sich Crystal Server und die Sentinel-Datenbank auf verschiedenen Computern befinden).

i. Speichern Sie die Änderungen an der Datei tnsnames.ora.

j. Führen Sie folgenden Befehl aus, um zu überprüfen, dass der Service-Name esecuritydb ordnungsgemäß konfiguriert wurde:

```
tnsping esecuritydb
```

k. Wenn der Befehl erfolgreich ausgeführt wurde, sollten Sie eine Meldung erhalten, die besagt, dass die Verbindung in Ordnung ist.

Installation von Crystal BusinessObjects Enterprise™ 11

Installation von Crystal BusinessObjects Enterprise

1. Melden Sie sich als Crystal-Benutzer an.
2. Wechseln Sie in das Verzeichnis DISK_1des Crystal-Installationsprogramms.
3. Führen Sie folgenden Befehl aus:

```
./install
```

4. Wählen Sie folgende Sprache aus: *English* (Englisch)
5. Wählen Sie *New Installation* (Neue Installation).
6. Akzeptieren Sie die Lizenzvereinbarung.
7. Geben Sie den Produkt-Keycode ein.
8. Geben Sie das Installationsverzeichnis ein:

```
/opt/crystal_xi
```

9. Wählen Sie: *„User install“ (Benutzerinstallation)*
10. Wählen Sie: *„New Install“ (Neue Installation)*
11. Wählen Sie: *„Install MySQL“ (MySQL installieren)*

12. Geben Sie Konfigurationsinformationen für MySQL ein:
    a. „Use default port 3306“ (Standardport 3306 verwenden)
    b. „Admin password“ (Administrator-Passwort)
13. Geben Sie weitere Konfigurationsinformationen für MySQL ein:
    a. „Default DB Name“ (DB-Standardname): BOE11
    b. „User id“ (Benutzer-ID): mysqladm
    c. „Password“ (Passwort)
14. Geben Sie weitere Konfigurationsinformationen für MySQL ein:
    a. „Local Name Server“ (Lokaler Namensserver): <Hostname des lokalen Computers>
    b. „Default CMS Port Number“ (CMS-Standard-Portnummer): 6400
15. Wählen Sie: *„Install Tomcat“ (Tomcat installieren)*
16. Geben Sie Tomcat-Konfigurationsinformationen ein:
    a. „Default Receive HTTP requests port“ (Standardport zum Empfangen von HTTP-Anforderungen): 8080
    b. „Default Redirect jsp requests port“ (Standardport für die Umleitung von jsp-Anforderungen): 8443
    c. „Default Shutdown Hook port“ (Standardport für Herunterfahren des Hook): 8005
17. Drücken Sie die Eingabetaste, um den Installationsvorgang zu starten.

Patches für Crystal Reports zur Verwendung mit Sentinel

Um Crystal Reports über die Registerkarte „Analyse“ von Sentinel Control Center anzuzeigen, müssen mehrere Crystal Enterprise-Dateien aktualisiert werden, um sie mit dem in Sentinel eingebetteten Browser kompatibel zu machen.

In der folgenden Tabelle werden diese Dateien aufgelistet und es wird beschrieben, wofür die einzelnen Dateien verwendet werden.

Dateiname	***Beschreibung***

`calendar.js`
 	
`calendar.html`
	Zeigt einen Popup-Kalender an, wenn Sie ein Datum als Parameter für einen Bericht auswählen.

`grouptree.html`	Zeigt die Meldung „... wird geladen“ an, während Berichte geladen werden.
`exportframe.html`	Zeigt das Fenster an, in dem Sie einen Bericht zum Speichern oder Drucken exportieren können.
`exportIce.html`	Von Sentinel beim Export eines Berichts zum Speichern oder Drucken verwendete Datei.
`GetReports.jsp`	Die Datei, die Sentinel Control Center verwendet, um eine Verbindung mit Crystal Server herzustellen und die Berichtsliste anzuzeigen.

Anwenden von Patches auf Crystal-Berichte

1. ZURZEIT NUR ÜBER SERVICE PACK VERFÜGBAR. Wechseln Sie auf der Sentinel Service Pack-CD-ROM zu \content\reports\patch und kopieren Sie alle *.html- und *.js-Dateien zum Speicherort der Viewer-Datei; standardmäßig ist dies:

   ```
   /opt/crystal_xi/bobje/webcontent/enterprise11/viewer/en/
   ```

2. Wechseln Sie auf der Sentinel Service Pack-CD-ROM zu \content\reports\patch und kopieren Sie alle *.js-Dateien nach:

   ```
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/
   ```

   HINWEIS: Erstellen Sie einen Ordner mit der Bezeichnung **esec-script**

   ```
   Kopieren Sie alle *.jar-Dateien
   ```

   von:

   ```
   /opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
   ```

   nach:

   ```
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib
   ```

   HINWEIS: Erstellen Sie die Ordnerstruktur **WEB-INF/lib**

Veröffentlichen Sie Crystal Report-Schablonen

Diese Berichtsschablonen wurden von Novell für die Verwendung auf den Registerkarten „Analyse“ und „Advisor“ in Sentinel Control Center erstellt.

Es gibt zwei Methoden zur Veröffentlichung von Berichten.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console

Außerdem stehen Beispielberichte im pdf-Format zur Verfügung.

HINWEIS: Bei „List of Attacks by CVE Report“ (Liste der Angriffe von CVE Report) handelt es sich um eine Schnittmenge aus Angriffssignaturen aus dem Advisor-Feed und durch Absuchen entdeckten Anfälligkeiten.

HINWEIS: Zur Ausführung von Top 10-Berichten muss die Aggregation aktiviert und EventFileRedirectService (in DAS_Binary.xml) muss eingeschaltet sein. Informationen zur Aktivierung der Aggregation finden Sie im *Sentinel-Benutzerhandbuch, Kapitel 10 – Sentinel Data Manager*, im Abschnitt zur Registerkarte „Bericht für Daten“ oder hier im Abschnitt Aktivieren der Sentinel Top 10-Berichte.

Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard

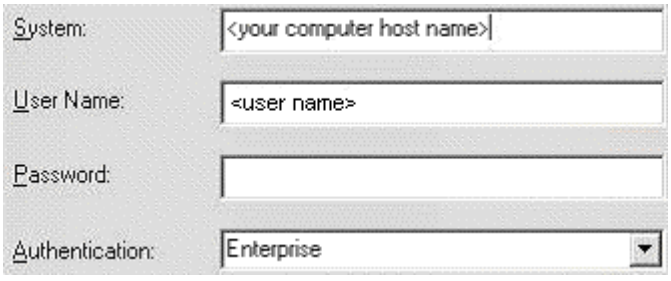
HINWEIS: Zur Ausführung von Crystal Publishing Wizard ist eine Windows-Plattform erforderlich.

Importieren von Crystal Reports-Schablonen

HINWEIS: Wenn Sie Ihre Reports-Schablonen erneut importieren (veröffentlichen), müssen Sie den vorherigen Schablonen-Import löschen.

1. Klicken Sie auf *Start* > *Alle Programme* > *BusinessObjects 11* > *Crystal Reports Server* > *Publishing Wizard*.
2. Klicken Sie auf *Next* (Weiter).
3. Melden Sie sich an. Als System sollte der Name des Host-Computers verwendet werden und als Authentifizierung „Enterprise“. Der Benutzername kann „Administrator“ lauten. Aus Sicherheitsgründen sollten Sie einen anderen Benutzer verwenden als den Administrator. Geben Sie Ihr Passwort ein und klicken Sie auf *Weiter*.

HINWEIS: Auf Berichte, die als Benutzer „Verwalter“ veröffentlicht wurden, haben alle Benutzer Zugriff.

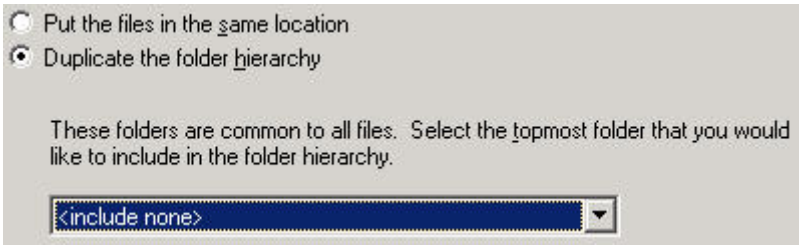


4. Klicken Sie auf *Add Folder* (Ordner hinzufügen).
5. Klicken Sie auf *Include Subfolder* (Unterordner einbeziehen). Rufen Sie die Sentinel Service Pack-CD-ROM auf und wechseln Sie zu:

   ```
   \content\reports\Crystal_v11\Oracle
   ```

   Klicken Sie auf *OK* (OK).
6. Klicken Sie auf *Next* (Weiter).
7. Klicken Sie im Fenster „Specify Location“ (Speicherort angeben) auf die Schaltfläche *New Folder* (Neuer Ordner) in der rechten oberen Ecke und erstellen Sie einen Ordner mit der Bezeichnung *eSecurity_Reports*. Klicken Sie auf *Next* (Weiter).

8. Wählen Sie:
   - *Duplicate the folder hierarchy* (Ordnerhierachie duplizieren).
   - Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie <*include none*> (<keine einschließen>) aus.



Klicken Sie auf *Next* (Weiter).

9. Klicken Sie im Fenster „Confirm Location“ (Speicherort bestätigen) auf *Next* (Weiter).
10. Gehen Sie im Fenster „Specify Categories“ (Kategorien angeben) wie folgt vor:
    - Geben Sie einen beliebigen Kategorienamen an (z. B. sentinel)
    - Markieren Sie den Namen und klicken Sie auf die Schaltfläche „+“.

HINWEIS: Nur der erste Bericht wird nach dem Klicken auf „Next“ (Weiter) unter der Kategorie angezeigt.

    - Klicken Sie auf *Next* (Weiter).
11. Klicken Sie im Fenster „Specify Schedule“ (Zeitplan angeben) auf *Let users update the object* (Zulassen, dass Benutzer das Objekt aktualisieren) (sollte Standard sein). Klicken Sie auf *Next* (Weiter).
12. Klicken Sie im Fenster „Specify Repository Refresh“ (Repository-Aktualisierung angeben) auf *Enable all* (Alle aktivieren), um die Repository-Aktualisierung zu aktivieren. Klicken Sie auf *Next* (Weiter).
13. Klicken Sie im Fenster „Specify Keep Saved Data“ (Angabe für das Beibehalten gespeicherter Daten) auf *Enable all* (Alle aktivieren), um beim Veröffentlichen von Berichten die gespeicherten Daten beizubehalten. Klicken Sie auf *Next* (Weiter).
14. Klicken Sie im Fenster „Change Defaults Values“ (Standardwerte ändern) auf das Optionsfeld *Publish reports without modifying properties* (Berichte veröffentlichen, ohne Eigenschaften zu ändern) (sollte Standard sein). Klicken Sie auf *Next* (Weiter).
15. Klicken Sie auf *Next* (Weiter), um Ihre Objekte hinzuzufügen.
16. Klicken Sie auf *Next* (Weiter).
17. Klicken Sie auf *Finish* (Fertig stellen).

Wenn die Sentinel-Schablonen für Crystal Reports auf dem Crystal Enterprise-Server veröffentlicht werden, müssen sich die Schablonen im Verzeichnis *eSecurity_Reports* befinden.

Veröffentlichen von Reports-Schablonen – Central Management Console

Bei der Veröffentlichung von Berichten mithilfe von Central Management Console kann der Bericht nicht als Batch veröffentlicht werden, wie dies bei der Verwendung des Publishing Wizard unter Windows der Fall ist.

Importieren von Crystal Reports-Schablonen

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/businessobjects/enterprise11/adminla
      unch
   ```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).
3. Melden Sie sich bei Crystal Server an.
4. Klicken Sie im Fenster „Organize“ (Organisieren) auf *Folders* (Ordner).
5. Klicken Sie in der rechten oberen Ecke auf *new Folder…* (Neuer Ordner...).
6. Erstellen Sie einen neuen Ordner mit der Bezeichnung *eSecurity_Reports*. Klicken Sie auf *OK* (OK).
7. Klicken Sie auf *eSecurity_Reports*.
8. Klicken Sie auf die Registerkarte „Subfolders“ (Unterordner) und erstellen Sie die folgenden Unterordner.
   - Advisor_Vulnerability
   - Incident Management
   - Internal Events
   - Security Events
   - Top 10
9. Klicken Sie auf *Home* (Basis).
10. Klicken Sie auf *Objects* (Objekte).
11. Klicken Sie auf *New Object* (Neues Objekt).
12. Markieren Sie auf der linken Seite den Eintrag *Report* (Bericht).
13. Klicken Sie auf die Schaltfläche *Browse* (Durchsuchen) und wechseln Sie zur Sentinel Service Pack-CD:

    ```
    \content\reports\Crystal_v11\Oracle
    ```

    Wählen Sie einen Ordner und darin einen Bericht aus.
14. Markieren Sie *eSecurity_Reports*, klicken Sie auf „Show Subfolders“ (Unterordner anzeigen).
15. Wählen Sie den entsprechenden Ordner für den Bericht aus und klicken Sie auf *Show Subfolders* (Unterordner anzeigen).
16. Klicken Sie auf *OK* (OK).

17. Klicken Sie auf *Update* (Aktualisieren).
18. Klicken Sie auf die Registerkarte *Reports* (Berichte) und fügen Sie weiter Berichte hinzu.
19. Um die verbliebenen Berichte zu einem anderen Ordner hinzuzufügen, klicken Sie links oben auf *Folders* (Ordner) und wiederholen Sie die Schritte 14 bis 17.

Verwenden von Crystal XI Web Server

Crystal Server XI unter Linux installiert einen Webserver, über den Sie Verwaltungsaufgaben durchführen sowie Berichte veröffentlichen und anzeigen können.

Das Verwaltungsportal kann unter folgender URL über den Browser aufgerufen werden:

```
http://<Hostname_oder_IP-Adresse_des_Webservers>:<Webserver-Port-
    Standard_8080>/businessobjects/enterprise11/adminlaunch
```

Das nicht für die Verwaltung bestimmte (allgemeine) Portal kann unter folgender URL über den Browser aufgerufen werden:

```
http://<Hostname_oder_IP-Adresse_des_Webservers>:<Webserver-
    Port-
    Standard_8080>/businessobjects/enterprise11/enterprise11
```

Testen der Konnektivität zum Webserver

Testen der Konnektivität zum Webserver

1. Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.
2. Geben Sie Folgendes ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/businessobjects/enterprise11/adminla
      unch
   ```

3. Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

Festlegen eines Kontos für einen benannten Benutzer

Der im Lieferumfang von Crystal Server enthaltene Schlüssel ist ein Kontoschlüssel für „Named User“ (Benannter Benutzer). Das Gastkonto muss von „Concurrent User“ (Gleichzeitiger Benutzer) in „Named User“ (Benannter Benutzer) geändert werden.

Festlegen des Gastkontos als „Named User“ (Benannter Benutzer) ’

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/businessobjects/enterprise11/adminla
      unch
   ```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).

3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Klicken Sie im Fenster „Organize“ (Organisieren) auf *Users* (Benutzer).
5. Klicken Sie auf „Guest“ (Gast).
6. Ändern Sie den Verbindungstyp von *Concurrent User* (Gleichzeitiger Benutzer) in *Named User* (Benannter Benutzer).
7. Klicken Sie auf *Update* (Aktualisieren).
8. Melden Sie sich ab und schließen Sie das Fenster.

Konfigurieren von Berichten

In diesem Verfahren wird erläutert, wie Administration Launchpad so konfiguriert werden kann, dass Sie Berichte anzeigen und bearbeiten können.

Konfigurieren von Administration Launchpad

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/businessobjects/enterprise11/adminla
      unch
   ```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht der Fall, wählen Sie *Enterprise* aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *Log On* (Anmelden).
5. Klicken Sie im Fenster „Organize“ (Organisieren) auf *Folders* (Ordner).
6. Klicken Sie einmal (nicht doppelt) auf *eSecurity_Reports*.
7. Wählen Sie *All* (Alle).
8. Klicken Sie auf die Registerkarte „Rights“ (Rechte).
9. Wählen Sie im Dropdown-Menü für „Everyone“ (Alle) die Option *View on Demand* (Auf Verlangen anzeigen) aus. Klicken Sie auf *Update* (Aktualisieren).
10. Melden Sie sich ab und schließen Sie das Fenster.

Aktivieren von Sentinel Top 10-Berichten

Gehen Sie wie folgt vor, um Sentinel Top 10-Berichte zu aktivieren:

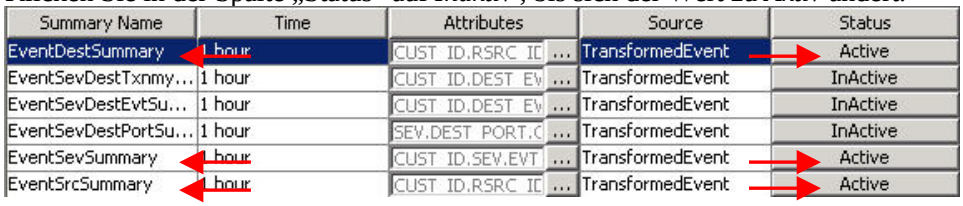
- Schalten Sie die Aggregation ein.
- Aktivieren Sie „EventFileRedirectService”.

Einschalten der Aggregation

1. Starten Sie Sentinel Data Manager.
2. Melden Sie sich an.
3. Klicken Sie auf die Registerkarte *Bericht für Daten.*

4. Aktivieren Sie folgende Zusammenfassungen:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Klicken Sie in der Spalte „Status“ auf *Inaktiv* , bis sich der Wert zu *Aktiv* ändert.



Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active
EventSevDestTxnmy...	1 hour	CUST_ID.DEST_Ev ...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID.DEST_Ev ...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV.DEST_PORT.C ...	TransformedEvent	InActive
EventSevSummary	1 hour	CUST_ID.SEV.EVT ...	TransformedEvent	Active
EventSrcSummary	1 hour	CUST_ID.RSRC_ID ...	TransformedEvent	Active

Aktivieren von EventFileRedirectService

1. Öffnen Sie auf Ihrem DAS-Computer mithilfe des Texteditors folgende Datei:

   ```
   $ESEC_HOME/sentinel/config/das_binary.xml
   ```

2. Ändern Sie den Status von EventFileRedirectService auf „on“ (ein).

   ```
   <property name="status">on</property>
   ```

3. Starten Sie den Prozess DAS_Binary neu. Dies ist mithilfe von Sentinel Control Center oder durch erneutes Booten des Computers möglich.

   Mithilfe von Sentinel Control Center:

   - Melden Sie sich als Benutzer mit Administratorrechten bei Sentinel Control Center an. Dieser Benutzer benötigt folgende Berechtigungen für „Serveransichten“:
     - Server anzeigen
     - Server steuern
   - Öffnen Sie über die Registerkarte „Admin“ eine Serveransicht, um alle Sentinel Server-Prozesse anzuzeigen.
   - Klicken Sie mit der rechten Maustaste auf den DAS_Binary-Prozess und wählen Sie die *Neu starten* aus.
   - Der Zähler „Starten“ für diesen Prozess erhöht sich um den Wert 1, wenn der Prozess erfolgreich neu gestartet wurde.

Maximieren der Ereignisberichterstellung

Je nachdem, wie viele Ereignisse Crystal abfragt, erhalten Sie möglicherweise eine Fehlermeldung bezüglich der maximalen Verarbeitungszeit oder der maximalen Datensatzgrenze. Um den Server für die Verarbeitung einer größeren oder unbegrenzten Anzahl an Berichten einzurichten, müssen Sie den Crystal Page-Server erneut konfigurieren.

Neukonfiguration von Crystal Page Server

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/businessobjects/enterprise11/adminla
      unch
   ```

2. Klicken Sie auf *Central Management Console* (Zentrale Verwaltungskonsole).

3. Als Systemname sollte der Name des Host-Computers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits der Fall, wählen Sie „Enterprise“ aus.
4. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *Log On* (Anmelden).
5. Klicken Sie auf *Servers* (Server).
6. Klicken Sie auf <*Servername*>.*pageserver*.
7. Klicken Sie unter *Database Records to Read When Previewing Or Refreshing a report* (Bei Vorschau oder Aktualisierung eines Berichts zu lesende Datenbankdatensätze) auf *Unlimited records* (Unbegrenzt viele Datensätze).
8. Klicken Sie auf *Apply* (OK).
9. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf *OK* (OK).
10. Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager Betriebssystems aufgefordert.

Konfigurieren von Sentinel für den Crystal Enterprise Server

Nach der Installation von Crystal Enterprise benötigt Sentinel Control Center die URLs für die Analyseberichte.

Konfigurieren von Sentinel für Crystal Enterprise Server

1. Melden Sie sich bei Sentinel Control Center als Benutzer mit Rechten für die Registerkarte „Admin“ an.
2. Wählen Sie auf der Registerkarte „Admin“ die Option *Berichtkonfiguration*.
3. Geben Sie in das Feld „Analyse-URL“ Folgendes ein:

```
http://<Hostname_oder_IP-
   Adresse_des_Webservers>:<Webserver-Port-
   Standard_8080>/esec-
   script/GetReports.jsp?APS=<Hostname>&user=Guest&pas
   sword=&tab=Analysis
```

HINWEIS: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse bzw. den Hostnamen des Crystal Enterprise Server ersetzt werden.

HINWEIS: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS nicht die IP-Adresse angegeben ist. Es muss sich um den Hostnamen handeln.

HINWEIS: <Webserver-Port-Standard_8080> muss durch den Port ersetzt werden, den der Crystal-Webserver überwacht.

4. Klicken Sie neben dem Feld „Analyse-URL“ auf *Aktualisieren*.

5. Wenn Advisor auf Ihrem Computer installiert ist, geben Sie Folgendes in das Feld „Advisor-URL“ ein:

   ```
   http://<Hostname_oder_IP-
      Adresse_des_Webservers>:<Webserver-Port-
      Standard_8080>/esec-
      script/GetReports.jsp?APS=<Hostname>&user=Guest&pas
      sword=&tab=Advisor
   ```

   HINWEIS: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse bzw. den Hostnamen des Crystal Enterprise Server ersetzt werden.

   HINWEIS: Die oben angegebene URL funktioniert nicht ordnungsgemäß, wenn für APS nicht die IP-Adresse angegeben ist. Es muss sich um den Hostnamen handeln.

   HINWEIS: <Webserver-Port-Standard_8080> muss durch den Port ersetzt werden, den der Crystal-Webserver überwacht.

6. Klicken Sie neben dem Feld „Advisor URL“ auf *Aktualisieren*.
7. Klicken Sie auf *Speichern*.
8. Melden Sie sich bei Sentinel Control Center ab und erneut wieder an. Die Crystal Reports-Bäume auf den Registerkarten „Analyse“ und „Advisor“ (wenn Advisor installiert ist), sollten nun im Navigatorfenster angezeigt werden.

Dienstprogramme und Fehlersuche

Starten von MySQL

So stellen Sie sicher, dass MySQL ausgeführt wird:

1. Melden Sie sich als Crystal-Benutzer an.
2. Wechseln Sie zu /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

Starten von Tomcat

So vergewissern Sie sich, dass Tomcat ausgeführt wird:

1. Melden Sie sich als Crystal-Benutzer an
2. cd /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

Starten von Crystal Server-Instanzen

So stellen Sie sicher, dass Crystal Server-Instanzen ausgeführt werden:

1. Melden Sie sich als Crystal-Benutzer an
2. Wechseln Sie zu /opt/crystal_xi/bobje
3. ./startservers

Fehler beim Crystal-Hostnamen

Fehler beim Hostnamen

1. Wenn Sie folgende Fehlermeldung erhalten:

```
Warning: ORB::BOA_init: hostname lookup returned
   `localhost' (127.0.0.1)

Use the -OAhost option to select some other hostname
```

   Vergewissern Sie sich, dass Ihre IP-Adresse und Ihr Hostname sich in der Datei /etc/hosts befinden. Beispiel:

```
192.0.2.46  linuxCE02
```

Verbindung mit CMS nicht möglich

Wenn das System meldet, dass es keine Verbindung zu CMS herstellen kann, versuchen Sie das Problem, durch Ausführung folgender Befehle zu lösen.

Fehlersuche bei CMS-Verbindungsfehler

1. Wenn der Befehl „netstat –an | grep 6400“ zu keinen Ergebnissen führt, versuchen Sie folgende Vorgehensweise:
   - Geben Sie die MySQL-Verbindungsinformationen erneut ein:

   a. Melden Sie sich als Crystal-Benutzer an
   b. Wechseln Sie zu /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Drücken Sie die Eingabetaste, wenn „[<Hostname>.cms]“ angezeigt wird.
   e. Wählen Sie *select* (Auswählen) und geben Sie alle MySQL-Datenbankinformationen erneut ein, die zum Zeitpunkt der Installation eingegeben wurden (siehe Installationsanweisungen).
   f. Beenden Sie abschließend cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers

   - Initialisieren Sie die MySQL-Datenbank neu:

   a. Melden Sie sich als Crystal-Benutzer an.
   b. Wechseln Sie zu /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Drücken Sie die Eingabetaste, wenn „[<Hostname>.cms]“ angezeigt wird.
   e. Wählen Sie„reinitialize“ (Neu initialisieren) und befolgen Sie die Anweisungen.
   f. Beenden Sie abschließend cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers

2. Vergewissern Sie sich, dass alle CCM-Server aktiviert sind:
   a. Melden Sie sich als Crystal-Benutzer an.
   b. Wechseln Sie zu /opt/crystal_xi/bobje
   c. ./ccm.sh -enable all

11 Advisor-Konfiguration

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Sentinel Advisor, powered by SecurityNexus, bietet Echtzeit-Informationen zu Unternehmens-Anfälligkeiten, Expertenrat und empfohlene Schritte zur Sanierung. Advisor bietet einen Querverweis zwischen Echtzeit-IDS-Angriffssignaturen und der Advisor Knowledge Base für Anfälligkeiten. Weitere Informationen finden Sie unter http://www.esecurity.net/Software/Products/Advisor.asp.

Die Installation von Advisor ist optional. Die Komponente ist allerdings notwendig, wenn Sie die Sentinel-Funktion zur Exploit-Erkennung oder die Advisor-Berichtsfunktion nutzen möchten.

Crystal BusinessObjects Enterprise™ 11 ist eines der Berichterstellungswerkzeuge, die sich mit Sentinel integrieren lassen. Informationen zur Installation von Crystal BusinessObjects Enterprise™ 11 finden Sie im Kapitel *Crystal Reports* für die jeweilige Plattform, auf der Crystal Enterprise Server ausgeführt werden soll (Windows bzw. Linux). Wenn Sie Advisor nur für Exploit-Erkennung verwenden möchten, brauchen Sie keine Instanz von Crystal Server zu installieren. Crystal Server ist nur erforderlich, wenn Sie vorhaben, Berichte auszuführen.

In diesem Kapitel wird erörtert, wie Sentinel so konfiguriert werden kann, dass eine direkte Ausführung von Advisor-Berichten über Sentinel Control Center möglich ist. Advisor-Berichte werden von Novell zu Berichterstellungs- und Analysezwecken erstellt und erscheinen auf der Registerkarte „Advisor“ von Sentinel Control Center, sobald die Sentinel Control Center-Integration ordnungsgemäß konfiguriert ist.

Installation von Advisor

Advisor kann nur auf dem Computer installiert werden, auf dem sich Database Access Service (DAS) befindet.

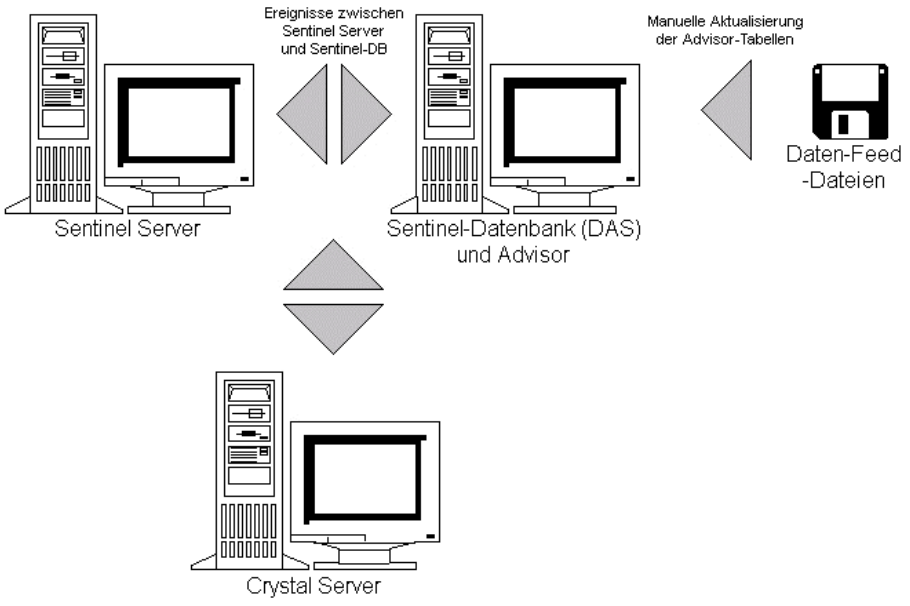
Es sind zwei verschiedene Installationsoptionen verfügbar. Hierbei handelt es sich um:

- Einzelplatzbetrieb
- Direktes Herunterladen vom Internet

Wenn Sie Advisor Crystal Reports ausführen möchten, schlagen Sie zuerst im Kapitel *Crystal Reports* zum Thema Installation und Konfiguration Ihrer Crystal Server-Instanz nach. Veröffentlichen Sie anschließend die Advisor Crystal Reports auf Crystal Server. Anweisungen zum Veröffentlichen Ihrer Berichte finden Sie unter Importieren von Berichtsschablonen.

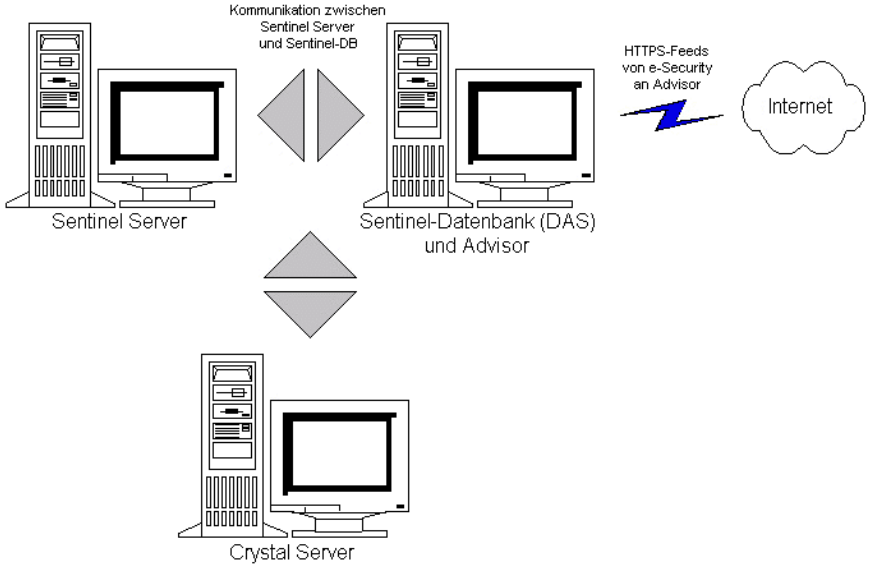
Einzelplatzkonfiguration

Bei einer Einzelplatzinstallation ist Advisor ein isoliertes System, in das manuell eingegriffen werden muss, um eine Aktualisierung von Novell zu empfangen.



Konfiguration für direktes Herunterladen vom Internet

Beim direkten Herunterladen vom Internet ist der Advisor-Computer direkt mit dem Internet verbunden. In dieser Konfiguration werden regelmäßig automatisch Aktualisierungen von Novell über das Internet heruntergeladen.



Advisor-Installation

HINWEIS: Vor der Installation von Advisor müssen Sie sicherstellen, dass Sie von Novell den Advisor-Benutzernamen und das zugehörige Passwort erhalten haben. Während der Installation werden Sie zur Eingabe von Benutzernamen und Passwort aufgefordert.

Wenn Sie vorhaben, Advisor-Berichte (Crystal Reports) auszuführen, führen Sie die folgenden Schritte in der angegebenen Reihenfolge aus. Die folgenden Schritte sind nicht erforderlich, wenn Sie lediglich vorhaben, Advisor für die Exploit-Erkennung zu nutzen.

- Wenn nicht bereits erfolgt, führen Sie folgende Aktionen aus (siehe Kapitel *Crystal Reports*):
  - Installieren Sie Microsoft Internet Information Server (IIS).
  - **Für die Sentinel-Database auf Oracle (Linux)** – Führen Sie eine Vorinstallation von Crystal BusinessObjects Enterprise aus.
  - Installieren Sie Crystal BusinessObjects Enterprise™ 11.
  - **Mit Sentinel-Database unter Oracle (Solaris)** – Konfigurieren Sie den nativen Oracle-Treiber (für Oracle-Installationen)
  - **Mit Sentinel-Datenbank unter MS SQL (Windows)** – Konfigurieren Sie Open Database Connectivity (ODBC).
  - Wenden Sie Patches auf Crystal Reports an – Siehe Kapitel *Crystal Reports*.
- Installieren Sie Advisor – wenn Advisor noch nicht installiert ist, lesen Sie im Kapitel *Hinzufügen von Komponenten zu einer bestehenden Installation* nach.
- Importieren Sie Crystal Report-Schablonen.
- Erstellen Sie eine Crystal-Webseite.
- Konfigurieren Sie Sentinel Control Center für die Integration mit Crystal Enterprise Server.

Importieren von Berichtsschablonen

Ziehen Sie, je nach verwendetem Betriebssystem, eines der folgenden Kapitel zurate:

- *Kapitel 9 – Crystal Reports für Windows und Solaris*
- *Kapitel 10 – Crystal Reports für Linux*

Konfigurieren von Administration Launchpad

Ziehen Sie, je nach verwendetem Betriebssystem, eines der folgenden Kapitel zurate:

- *Kapitel 9 – Crystal Reports für Windows und Solaris*
- *Kapitel 10 – Crystal Reports für Linux*

Einrichten der Sentinel Control Center-Integration mit Advisor-Berichten

Sentinel Control Center bietet über die Registerkarte „Advisor“ die Möglichkeit zur Integration mit Advisor-Berichten. Mit dieser Funktion können Sie Advisor-Berichte direkt aus Sentinel Control Center anzeigen.

Um diese Funktion zu aktivieren, installieren Sie zunächst Crystal Server, importieren Sie die Advisor-Berichtsschablonen in Crystal Server und installieren Sie dann Advisor. Wenn diese Vorbedingungen erfüllt sind, befolgen Sie die Anweisungen im Abschnitt „Konfigurieren von Sentinel für die Integration mit Crystal Enterprise Server“ in:

- *Kapitel 9 – Crystal Reports für Windows und Solaris*
- *Kapitel 10 – Crystal Reports für Linux*

Aktualisieren von Daten in Advisor-Tabellen

Sofern Sie keine Einzelplatzkonfiguration verwenden, werden die Daten in den Advisor-Tabellen automatisch während des nächsten geplanten Herunterladens des Advisor-Feed aktualisiert. Die Daten können jedoch auch manuell aktualisiert werden. Informationen zur manuellen Aktualisierung finden Sie im *Sentinel-Benutzerhandbuch*.

Zurücksetzen des Advisor-Passworts (nur beim direkten Herunterladen)

Wenn Sie Advisor im Modus zum direkten Herunterladen ausführen und ein neues Advisor-Passwort erhalten haben bzw. das während der Installation festgelegte Advisor-Passwort falsch war, müssen Sie das verschlüsselte Advisor-Passwort, das in der Konfigurationsdatei von Advisor gespeichert ist, zurücksetzen.

Sie können das verschlüsselte Advisor-Passwort nicht aktualisieren, wenn Sie Advisor in einer Einzelplatzkonfiguration ausführen, da das Passwort in diesem Modus nicht in der Advisor-Konfigurationsdatei gespeichert ist.

Um das in der Advisor-Konfigurationsdatei gespeicherte Passwort zurückzusetzen, müssen Sie folgende Schritte ausführen:

1. Melden Sie sich unter UNIX als esecadm bzw. unter Windows mit Administratorrechten an. Melden Sie sich bei dem Computer an, auf dem Advisor installiert ist.
2. Wechseln Sie in folgendes Verzeichnis:

   Bei UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Bei Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

3. Führen Sie folgenden Befehl aus, wobei <neuesPasswort> das Advisor-Passwort ist, das Sie festlegen möchten:

   Bei UNIX:

   ```
   ./adv_change_passwd.sh <neuespasswort>
   ```

   Bei Windows:

   ```
   adv_change_passwd.bat <neuespasswort>
   ```

12 Testen der Installation

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Die folgenden Test-Collectors werden zusammen mit der Collector-Service-Komponente (Collector Manager) installiert, um Sie beim Testen der Installation zu unterstützen. Name und Beschreibung der einzelnen Collectors lauten:

Zum Testen des grundlegenden Ereignisflusses:

- SendOneEvent – Sendet genau ein Ereignis durch Sentinel und stoppt dann.
- SendMultipleEvents – Sendet 20 Ereignisse durch Sentinel und stoppt dann.

Zum Testen der Ereignisbestandszuordnung und der Exploit-Erkennung:

- DemoEvents – Sendet 13 Ereignisse durch Sentinel und stoppt dann.
- DemoAssetUpload – Lädt Demobestandsdaten in Sentinel. Wenn der DemoEvents-Collector nach diesem Collector ausgeführt wird, werden die Bestandsdaten aus diesem Collector infolge der Ereigniszuordung in den Ereignissen des DemoEvents-Collector angezeigt. Dieser Collector generiert keine externen Ereignisse.
- DemoVulnerabilityUpload – Lädt Demo-Anfälligkeitsdaten in Sentinel. Wenn der DemoEvents-Collector nach diesem Collector und nach dem Herunterladen des Advisor-Feed ausgeführt wird, lösen einige der Ereignisse des DemoEvents-Collector eine Exploit-Erkennung aus (d. h. das Feld „Anfälligkeit“ des Ereignisses wird auf „1“ gesetzt). Dieser Collector generiert keine externen Ereignisse.

Weitere Informationen (einschließlich Konfiguration) zu anderen Collectors finden Sie unter:

```
%ESEC_HOME%\wizard\Elements\<Collector-Name>\docs\
```

Testen der Installation mithilfe der Test-Collectors

In Sentinel v5.1.2 und höher sind die Test-Collectors vorkonfiguriert auf allen Collector Managers installiert. Daher können Sie bei Verwendung dieser Sentinel-Version direkt zur Ausführung der Test-Collectors zum Testen Ihrer Installation übergehen.

In Sentinel v5.1.1 und früher müssen die Collectors vor der Verwendung manuell auf einem Collector Manager konfiguriert werden. Zur Konfiguration der Test-Collectors befolgen Sie die Anweisungen im Abschnitt Konfigurieren der Test-Collectors. Kehren Sie anschließend zu diesem Abschnitt zurück, um die Installation mithilfe der Test-Collectors zu testen.

Ausführen der Test-Collectors zum Testen der Installation

1. Öffnen Sie die Anwendung Sentinel Control Center.
2. Klicken Sie auf die Registerkarte *Collectors*.
3. Doppelklicken Sie im Dialogfeld „Collector-Ansichts-Manager“ auf die Ansicht für ALLE AGENTEN, um eine Ansicht aller Collector-Ports zu öffnen.

4. In der geöffneten Collector-Ansicht werden alle aktuell konfigurierten Collector-Ports, nach dem Namen des Collector Manager gruppiert, angezeigt. Wenn keine Collector-Ports angezeigt werden, bedeutet dies, dass zurzeit keine der Collector Manager-Instanzen mit Sentinel verbunden ist. Wenn Sie davon ausgehen, dass ein oder mehrere Collector Manager-Instanzen mit Sentinel verbunden sein werden, müssen Sie sicherstellen, dass die Collector Manager-Instanzen ausgeführt werden, und überprüfen, ob Fehler in den Protokolldateien von Collector Manager bzw. Sentinel Server vorliegen.
5. Öffnen Sie vor der Ausführung eines Collectors einen Active View, um die von den Test-Collectors generierten Ereignisse anzeigen zu können. Gehen Sie dazu wie folgt vor:
   - Klicken Sie auf die Registerkarte *Active Views*.
   - Wählen Sie in der Menüleiste die Optionsfolge *Active Views > Aktive Ansicht erstellen*.
   - Wählen Sie den Filter *PUBLIC::External_Events*.
   - Klicken Sie auf *Fertig stellen*.
6. So führen Sie einen Collector aus, um den grundlegenden Ereignisfluss zu testen:
   - Rufen Sie die Registerkarte *Collectors* auf.
   - Klicken Sie mit der rechten Maustaste in der Collector-Ansicht auf den Port des *SendMultipleEvents*-Collector und wählen Sie die Aktion „Starten“ aus. Da die Test-Collectors nur kurze Zeit laufen und dann stoppen, wird der Status des Collector-Ports kurz auf „Ein“ und dann wieder auf „Aus“ gesetzt.
   - Um sicherzustellen, dass Ereignisse das System durchlaufen, kehren Sie zur Registerkarte „Active Views“ zurück und überwachen Sie den erstellten Activ View. Beachten Sie, dass es eine Minute dauern kann, bis das Ereignis nach der Ausführung des Collector im Active View angezeigt wird.
7. So führen Sie einen Collector aus, um die Ereignisbestandszuordnung zu testen:
   - Rufen Sie die Registerkarte „Collectors“ auf.
   - Klicken Sie mit der rechten Maustaste in der Collector-Ansicht auf den Port des *DemoAssetUpload*-Collector und wählen Sie die Aktion „Starten“ aus. Da die Test-Collectors nur kurze Zeit laufen und dann stoppen, wird der Status des Collector-Ports kurz auf „Ein“ und dann wieder auf „Aus“ gesetzt.
   - Warten Sie ein bis zwei Minuten, bis die Bestandsdaten in Sentinel geladen, vom Zuordnungsservice in einer Zuordnung generiert und an die Collector Manager-Instanzen verteilt wurden. Sie erkennen, dass dies geschehen ist, wenn Sie nach einem internen Ereignis des Typs Ausschau halten, in dessen Ereignismeldung „Asset“ (Bestand) vorkommt. Um dieses interne Ereignis anzuzeigen, müssen Sie einen Active View mit einem Filter verwenden, der interne Ereignisse durchlässt (z. B. PUBLIC::Internal_Events). Der Filter PUBLIC::External_Events lässt keine internen Ereignisse durch.
   - Klicken Sie mit der rechten Maustaste in der Collector-Ansicht auf den Port des *DemoEvents*-Collector und wählen Sie die Aktion „Starten“ aus. Da die Test-Collectors nur kurze Zeit laufen und dann stoppen, wird der Status des Collector-Ports kurz auf „Ein“ und dann wieder auf „Aus“ gesetzt.

- Um zu überprüfen, ob die Ereignisbestandzuordnungen vorgenommen wurden, doppelklicken Sie auf ein Ereignis (in der Ereignistabelle unten im Active View), das soeben vom DemoEvents-Collector erstellt wurde, um die Ereignisdetails anzuzeigen. Erweitern Sie in den Ereignisdetails, die links neben der Ereignistabelle angezeigt werden, die Gruppe „Bestand“, um de Bestandszuordnungsdaten anzuzeigen. Beachten Sie, dass es eine Minute dauern kann, bis das Ereignis nach der Ausführung des Collector im Active View angezeigt wird.

8. So führen Sie einen Collector aus, um die Exploit-Erkennung zu testen (Advisor-Komponente muss installiert sein):

   - Führen Sie das Herunterladen des Advisor-Feed aus (kann einige Zeit in Anspruch nehmen):

   Unter Windows:

   - Melden Sie sich bei dem Computer an, auf dem Advisor installiert ist. Führen Sie den geplanten Advisor-Task aus (*Start* > *Systemsteuerung* > *Geplante Tasks* > *{e-Security_Advisor | at1}*)

   Unter UNIX:

   - Melden Sie sich bei dem Computer an, auf dem Advisor als esecadm-Benutzer installiert ist, und führen Sie folgenden Befehl aus:

     ```
     $ESEC_HOME/sentinel/bin/advisor.sh
     ```

   - Rufen Sie in Sentinel Control Center die Registerkarte „Collectors“ auf.
   - Klicken Sie mit der rechten Maustaste in der Collector-Ansicht auf den Port des *DemoVulnerabilityUpload*-Collector und wählen Sie die Aktion „Starten“ aus. Da die Test-Collectors nur kurze Zeit laufen und dann stoppen, wird der Status des Collector-Ports kurz auf „Ein“ und dann wieder auf „Aus“ gesetzt.
   - Warten Sie, bis die aktualisierten Exploit-Erkennungs-Daten in die Collector Manager-Instanz geladen wurden. Sie erkennen, dass dies geschehen ist, wenn Sie nach einem internen Ereignis des Typs Ausschau halten, in dessen Ereignismeldung „IsExploitWatchlist“ vorkommt. Um dieses interne Ereignis anzuzeigen, müssen Sie einen Active View mit einem Filter verwenden, der interne Ereignisse durchlässt (z. B. PUBLIC::Internal_Events). Der Filter PUBLIC::External_Events lässt keine internen Ereignisse durch. Es kann etwas länger als eine halbe Stunde dauern, bis die aktualisierten Exploit-Erkennungs-Daten an Collector Manager gesendet werden, da DAS die Exploit-Erkennungs-Daten standardmäßig mindestens einmal alle 30 Minuten aktualisiert.
   - Klicken Sie mit der rechten Maustaste in der Collector-Ansicht auf den Port des *DemoEvents*-Collector und wählen Sie die Aktion „Starten“ aus. Da die Test-Collectors nur kurze Zeit laufen und dann stoppen, wird der Status des Collector-Ports kurz auf „Ein“ und dann wieder auf „Aus“ gesetzt.
   - Um zu überprüfen, ob die Exploit-Erkennung vorgenommen wurde, doppelklicken Sie auf ein Ereignis (in der Ereignistabelle unten im Active View), das soeben vom DemoEvents-Collector erstellt wurde, um die Ereignisdetails anzuzeigen. Erweitern Sie in den Ereignisdetails, die links neben der Ereignistabelle angezeigt werden, die Exploit-Gruppe, um die Exploit-Erkennungs-Daten anzuzeigen. Einige der Ereignisse sollten mit dem Wert „1“ für das Feld „Anfälligkeit“ angezeigt werden. Beachten Sie, dass es eine Minute dauern kann, bis das Ereignis nach der Ausführung des Collector im Active View angezeigt wird.

Konfigurieren der Test-Collectors

Bei Sentinel v5.1.1 und früher sind die Test-Collectors zum Zeitpunkt der Installation nicht vorkonfiguriert. Daher müssen Sie die Collectors (auf einem Windows-Computer) mithilfe von Collector Builder konfigurieren, damit sie ausgeführt werden können.

In Sentinel v5.1.2 und höher sind diese Konfigurationsschritte nicht erforderlich, es sei denn, die Test-Collector-Ports wurden gelöscht.

Konfigurieren des SendOneEvent-Collector

Konfigurieren, Heraufladen und Ausführen des SendOneEvent-Collector

1. Öffnen Sie die Collector Builder-Anwendung.
2. Klicken Sie auf die Registerkarte *Wizard-Hosts*.
3. Markieren Sie den Hostnamen Ihres Computers. Der Hostname wird in dem Feld unterhalb des Menüs oben in der Anwendung angezeigt.
4. Doppelklicken Sie unter dem Header „Portname“ auf *Neu.*….
5. Geben Sie einen Wizard-Portnamen ein (z. B. SendOneEvent).
6. Wählen Sie für „Rx/Tx-Typ“ den Wert *Ohne* aus.
7. Lassen Sie „Rx/Tx-Wert“ leer.
8. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Collector-Spalte und wählen Sie „SendOneEvent“ aus.
9. Klicken Sie auf *Speichern*.
10. Klicken Sie auf die Registerkarte *Collectors*.
11. Erweitern Sie den SendOneEvent-Collector.
12. Klicken Sie mit der rechten Maustaste auf die Schablonendatei SendOneEvent und klicken Sie auf *Skripts erstellen*.
13. Klicken Sie mit der rechten Maustaste auf den SendOneEvent-Collector und klicken Sie auf *Collector heraufladen*.
14. Auf der Registerkarte „Collectors“ sollte Ihr Computer ausgewählt sein. Klicken Sie auf *Heraufladen*.
15. Wenn Sie dazu aufgefordert werden, geben Sie das Collector Manager-Passwort ein.
16. Klicken Sie auf *OK*.

Konfigurieren des SendMultipleEvents-Collector

Konfigurieren, Heraufladen und Ausführen des SendMultiple Events-Collector

1. Öffnen Sie die Collector Builder-Anwendung.
2. Klicken Sie auf die Registerkarte *Wizard-Hosts*.
3. Markieren Sie den Hostnamen Ihres Computers. Der Hostname wird in dem Feld unterhalb des Menüs oben in der Anwendung angezeigt.
4. Doppelklicken Sie unter dem Header „Portname“ auf „Neu…“, geben Sie einen Wizard-Portnamen ein (z. B. SendMultipleEvents).
5. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Spalte „ Rx/Tx-Typ“ und wählen Sie „Alle in Datei speichern“ aus.

6. Klicken Sie in derselben Zeile in das Textfeld der Spalte „Rx/Tx-Wert“ und geben Sie den Pfad zur Eingabedatei ein:

   ```
   Elements\SendMultipleEvents\config\test_events.csv
   ```

7. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Collector-Spalte und wählen Sie „SendMultipleEvents“ aus.
8. Klicken Sie auf *Speichern*.
9. Klicken Sie auf die Registerkarte *Collectors*.
10. Erweitern Sie den SendMultipleEvents-Collector.
11. Klicken Sie mit der rechten Maustaste auf die Schablonendatei SendMultipleEvents und klicken Sie auf *Skripts erstellen*.
12. Klicken Sie mit der rechten Maustaste auf den SendMultipleEvents-Collector und klicken Sie auf *Collector heraufladen*.
13. Auf der Registerkarte „Collectors“ sollte Ihr Computer ausgewählt sein. Klicken Sie auf *Heraufladen*.
14. Wenn Sie dazu aufgefordert werden, geben Sie das Collector Manager-Passwort ein.
15. Klicken Sie auf *OK*.

Konfigurieren des DemoEvents-Collector

Konfigurieren, Heraufladen und Ausführen des DemoEvents-Collector

1. Öffnen Sie die Collector Builder-Anwendung.
2. Klicken Sie auf die Registerkarte „Wizard-Hosts“.
3. Markieren Sie den Hostnamen Ihres Computers. Der Hostname wird in dem Feld unterhalb des Menüs oben in der Anwendung angezeigt.
4. Doppelklicken Sie unter dem Header „Portname“ auf „Neu…“, geben Sie einen Wizard-Portnamen ein (z. B. DemoEvents).
5. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Spalte „ Rx/Tx-Typ“ und wählen Sie „Alle in Datei speichern“ aus.
6. Klicken Sie in derselben Zeile in das Textfeld der Spalte „Rx/Tx-Wert“ und geben Sie den Pfad zur Eingabedatei ein:

   ```
   Elements\DemoEvents\data\Generic_Events.csv
   ```

7. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Collector-Spalte und wählen Sie „DemoEvents“ aus.
8. Klicken Sie auf *Speichern*.
9. Klicken Sie auf *Heraufladen*.
10. Wählen Sie die Registerkarte „Collectors“.
11. Klicken Sie auf den nach unten weisenden Pfeil und wählen Sie den DemoEvents-Collector aus.
12. Klicken Sie auf *Heraufladen*.
13. Wenn Sie dazu aufgefordert werden, geben Sie das Collector Manager-Passwort ein.
14. Klicken Sie auf *OK*.

Konfigurieren des DemoAssetUpload-Collector

Konfigurieren, Heraufladen und Ausführen des DemoAssetUpload-Collector

1. Öffnen Sie die Collector Builder-Anwendung.
2. Klicken Sie auf die Registerkarte „Wizard-Hosts“.
3. Markieren Sie den Hostnamen Ihres Computers. Der Hostname wird in dem Feld unterhalb des Menüs oben in der Anwendung angezeigt.
4. Doppelklicken Sie unter dem Header „Portname“ auf *Neu.*…, geben Sie einen Wizard-Portnamen ein (z. B. DemoAssetUpload).
5. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Spalte „ Rx/Tx-Typ“ und wählen Sie „Alle in Datei speichern“ aus.
6. Klicken Sie in derselben Zeile in das Textfeld der Spalte „Rx/Tx-Wert“ und geben Sie den Pfad zur Eingabedatei ein:

   ```
   Elements\DemoAssetUpload\data\asset_info.csv
   ```

7. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Collector-Spalte und wählen Sie „DemoAssetUpload“ aus.
8. Klicken Sie auf *Speichern*.
9. Klicken Sie auf *Heraufladen*.
10. Wählen Sie die Registerkarte „Collectors“.
11. Klicken Sie auf den nach unten weisenden Pfeil und wählen Sie „DemoAssetUpload“ aus.
12. Klicken Sie auf *Heraufladen*.
13. Wenn Sie dazu aufgefordert werden, geben Sie das Collector Manager-Passwort ein.
14. Klicken Sie auf *OK*.

Konfigurieren des DemoVulnerabiltyUpload-Collector

Konfigurieren, Heraufladen und Ausführen des DemoVulnerabiltyUpload-Collector

1. Öffnen Sie die Collector Builder-Anwendung.
2. Klicken Sie auf die Registerkarte „Wizard-Hosts“.
3. Markieren Sie den Hostnamen Ihres Computers. Der Hostname wird in dem Feld unterhalb des Menüs oben in der Anwendung angezeigt.
4. Doppelklicken Sie unter dem Header „Portname“ auf *Neu.*…, geben Sie einen Wizard-Portnamen ein (z. B. DemoVulnerabiltyUpload).
5. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Spalte „ Rx/Tx-Typ“ und wählen Sie „Alle in Datei speichern“ aus.
6. Klicken Sie in derselben Zeile in das Textfeld der Spalte „Rx/Tx-Wert“ und geben Sie den Pfad zur Eingabedatei ein:

   ```
   Elements\DemoVulnerabiltyUpload\data\vuln_info.csv
   ```

7. Klicken Sie in derselben Zeile auf das Dropdown-Menü für die Collector-Spalte und wählen Sie „DemoVulnerabiltyUpload“ aus.
8. Klicken Sie auf *Speichern*.
9. Klicken Sie auf *Heraufladen*.
10. Wählen Sie die Registerkarte „Collectors“.

11. Klicken Sie auf den nach unten weisenden Pfeil und wählen Sie „DemoVulnerabiltyUpload“ aus.
12. Klicken Sie auf *Heraufladen*.
13. Geben Sie das Collector Manager-Passwort ein.
14. Klicken Sie auf *OK*.

13 Änderungen an der Kommunikationsebene (iSCALE)

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Bei der Kommunikationsebene (iSCALE), die alle Komponenten der Architektur miteinander verbindet, handelt es sich um eine auf verschlüsseltem TCP/IP beruhende Verbindung. Standardmäßig ist diese Kommunikation mit AES 256 Bit verschlüsselt. ARC4 ist für die Verwendung verfügbar.

Mit keymgr können sie auch auswählen, welche Verschlüsselungsmethode verwendet werden soll oder den Schlüssel ändern. Das Programm generiert eine Datei mit dem Namen „.keystore“ im Verzeichnis „lib“ einer Sentinel-Installation ($ESEC_HOME/lib or %ESEC_HOME%\lib). Diese Datei muss auf jeden Computer kopiert werden, auf dem eine Sentinel-Komponente installiert ist.

Sentinel empfiehlt als optimales Verfahren, den Standard-Sicherheitsschlüssel zu ändern, um eindeutige Verschlüsselungs- und Authentifizierungsparameter zu erzielen.

HINWEIS: Wenn Sie Advisor, DBConnector oder RDEP-Collecto-Connector verwenden, müssen Sie die in der Konfigurationsdatei der jeweiligen Komponente gespeicherten Passwörter aktualisieren. Dies ist erforderlich, da der Verschlüsselungsschlüssel, mit dem das Passwort vor der Speicherung in diesen Konfigurationsdateien verschlüsselt wird, auf dem Schlüssel in der zu aktualisierenden .keystore-Datei beruht.

Änderungen am Verschlüsselungsschlüssel

Vornehmen von Schlüsseländerungen oder Aktivieren anderer Verschlüsselungsmethoden

1. Melden Sie sich unter UNIX als „esecadm“ an. Melden Sie sich unter Windows als Benutzer mit Administratorrechten an.
2. Wechseln Sie in das folgende Verzeichnis:

   Bei Windows:

   ```
   %ESEC_HOME%\lib
   ```

   Bei UNIX:

   ```
   $ESEC_HOME/lib
   ```

3. Führen Sie den folgenden Befehl aus:

   Unter Windows:

   ```
   „%ESEC_JAVA_HOME%\java“ -jar keymgr.jar -–keyalgo
      <encryption [AES or ARC4]> --keysize 256
   ```

   Unter UNIX:

   ```
   $ESEC_JAVA_HOME/java -jar keymgr.jar -–keyalgo
      <encryption [AES or ARC4]> --keysize 256
   ```

   Dadurch können Sie Ihre Verschlüsselungsmethode festlegen. Die Datei .keystore wird im Verzeichnis lib erstellt.

4. Kopieren Sie .keystore auf die einzelnen Computer, auf denen eine Sentinel-Komponente installiert ist. Die Datei sollte an folgenden Speicherort kopiert werden:

   Bei Windows:

   ```
   %ESEC_HOME%
   ```

   Bei UNIX:

   ```
   $ESEC_HOME
   ```

5. Wenn Sie DBConnector oder den RDEP-Collector-Connector auf einem Collector Manager-Computer konfiguriert haben, müssen Sie die Passwörter in allen Instanzen der Connector-Konfigurationsdatei aktualisieren. Dies ist erforderlich, da der Verschlüsselungsschlüssel, mit dem das Passwort vor der Speicherung in der Connector-Konfigurationsdatei verschlüsselt wird, auf dem Schlüssel in der soeben aktualisierten .keystore-Datei beruht. Anweisungen zur Festlegung der Passwörter in den Connector-Konfigurationsdateien können Sie der Dokumentation zu DBConnector und zum RDEP-Collector-Connector entnehmen.

6. Wenn Sie Advisor im Modus zum direkten Herunterladen auf Ihrem System ausführen, müssen Sie das in der Advisor-Konfigurationsdatei gespeicherte verschlüsselte Advisor-Passwort aktualisieren. Dies ist erforderlich, da der Verschlüsselungsschlüssel, mit dem das Passwort vor der Speicherung in der Advisor-Konfigurationsdatei verschlüsselt wird, auf dem Schlüssel in der soeben aktualisierten .keystore-Datei beruht. Sie können das verschlüsselte Advisor-Passwort nicht aktualisieren, wenn Sie Advisor in einer Einzelplatzkonfiguration ausführen, da das Passwort in diesem Modus nicht in der Advisor-Konfigurationsdatei gespeichert ist. Um das in der Advisor-Konfigurationsdatei gespeicherte Passwort zu aktualisieren, müssen Sie die folgenden Schritte in der angegebenen Reihenfolge ausführen:

   - Melden Sie sich unter UNIX als esecadm bzw. unter Windows mit Administratorrechten an. Melden Sie sich bei dem Computer an, auf dem Advisor installiert ist.
   - Wechseln Sie in folgendes Verzeichnis:

   Bei UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

Bei Windows:

```
%ESEC_HOME%\sentinel\bin
```

- Geben Sie die folgenden Befehle ein:

Bei UNIX:

```
./adv_change_passwd.sh <neuespasswort>
```

Bei Windows:

```
adv_change_passwd.bat <neuespasswort>
```

14 Hinzufügen von Komponenten zu einer bestehenden Installation

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Das Installationsprogramm von Sentinel 5 Enterprise Security Management unterstützt das Hinzufügen von Sentinel-Komponenten zu einer bestehenden Installation. Ein Beispiel für das Hinzufügen einer Komponente: Sie installieren zunächst lediglich Wizard Collector Manager auf einem Computer und entscheiden sich zu einem späteren Zeitpunkt, auch Sentinel Control Center auf diesem Computer zu installieren. In diesem Fall fügen Sie die Sentinel Control Center-Komponente zur Wizard Collector Manager-Installation hinzu.

HINWEIS: Stellen Sie vor dem Hinzufügen einer Komponente sicher, dass sie die richtigen Sentinel-Variablen festgelegt haben.

```
ESEC_HOME
ESEC_JAVA_HOME
WORKBENCH_HOME
ESEC_CONF_FILE
ESEC_VERSION
ESEC_USER
LD_LIBRARY_PATH
```

Hinzufügen von Komponenten unter Solaris bzw. Linux

Hinzufügen von Komponenten unter Solaris

1. Melden Sie sich als Benutzer „root“ an.
2. Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.
3. Starten Sie das Installationsprogramm, indem Sie zum Installationsverzeichnis auf der CD-ROM wechseln und Folgendes eingeben:

   ```
   ./setup.sh
   ```

   oder

   ```
   ./setup.sh -console (wenn X Windows nicht verfügbar
     ist.)
   ```

4. Es wird eine Meldung angezeigt, die den Speicherort der vorherigen Installation sowie die bereits installierten Komponenten angibt. Klicken Sie auf *Next* (Weiter).
5. Wählen Sie aus, welche Komponenten Sie hinzufügen möchten und klicken Sie auf *Weiter*.

6. Folgen Sie den Eingabeaufforderungen und geben Sie jeweils die entsprechenden Informationen ein. Weitere Informationen zu einer bestimmten Eingabeaufforderung finden Sie im entsprechenden Installationskapitel.

Hinzufügen von Komponenten unter Windows

Hinzufügen von Komponenten unter Windows

1. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
2. Wechseln Sie zu der CD und doppelklicken Sie auf *setup.bat*.

   HINWEIS: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.
3. Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.
4. Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.
5. Es wird eine Meldung angezeigt, die den Speicherort der vorherigen Installation sowie die bereits installierten Komponenten angibt. Klicken Sie auf *Next* (Weiter).
6. Wählen Sie aus, welche Komponenten Sie hinzufügen möchten, und klicken Sie auf *Weiter*.
7. Folgen Sie den Eingabeaufforderungen und geben Sie jeweils die entsprechenden Informationen ein. Weitere Informationen zu einer speziellen Eingabeaufforderung finden Sie in Kapitel 3 (für Solaris), Kapitel 4 (für Linux) bzw. Kapitel 5 (für Windows).

15 Deinstallieren der Software

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Deinstallieren von Sentinel, Collector Manager und Advisor

Deinstallation unter Solaris und Linux

Starten des Sentinel-Deinstallationsprogramms für Solaris

1. Melden Sie sich als Benutzer „root“ an.
2. Stoppen Sie Sentinel Server.
3. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/_uninst
   ```

4. Geben Sie Folgendes ein:

   ```
   ./uninstall.bin
   ```

HINWEIS: Unter Solaris und Linux muss nach der Deinstallation von Sentinel Server ggf. der Benutzer „esecadm“ manuell aus dem Betriebssystem entfernt werden.

Deinstallation unter Windows

Mit dem Sentinel-Deinstallationsprogramm für Windows

1. Melden Sie sich als Administrator an.
2. Stoppen Sie Sentinel Server.
3. Wählen Sie die Optionsfolge *Start > Programme > Sentinel > Sentinel 5.x deinstallieren.*

Folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie die zu deinstallierenden Anwendungen aus:

- Datenbank
- Kommunikationsserver (Nachrichtenbus)
- Advisor
- Sentinel-Basisservices
- Korrelation
- DAS
- Collector-Service (Collector Manager)

- Sentinel Control Center
- Sentinel Database Manager (SDM)
- HP OpenView Service Desk
- Remedy Integration

Deinstallation über die Systemsteuerung

So deinstallieren Sie Sentinel-Anwendungen unter Windows

1. Wählen Sie die Optionsfolge *Start* > *Programme* > *Einstellungen* > *Systemsteuerung* > *Software*.
2. Klicken Sie auf *Sentinel 5.x*.
3. Befolgen Sie die Anweisungen. Sie werden aufgefordert, die zu deinstallierenden Anwendungen auszuwählen. Wählen Sie aus, welche Anwendungen Sie deinstallieren möchten.

Nach der Deinstallation

Das Deinstallationsprogramm belässt einige wenige Dateien auf dem Computer, die nach der Deinstallation von Sentinel 5 manuell gelöscht werden müssen. Möglicherweise müssen Sie das $ESEC_HOME-Verzeichnis bzw. das %ESEC_HOME%-Verzeichnis und alle Unterverzeichnisse löschen. Bei Advisor empfiehlt es sich möglicherweise, Ihre Ordner mit Angriffsinformationen und Warnmeldungen zu löschen, die für die Advisor-Datendateien verwendet werden.

Hier einige der nach der Deinstallation weiterhin vorhandenen Dateien:

- Sentinel-Protokolldateien
- Wizard-Protokolldateien
- DAS-Protokolldateien
- Collector Manager-Protokolldateien

In einigen Fällen sind nach der Deinstallation noch Systemeinstellungen vorhanden. In *Anhang E* finden Sie Anweisungen dazu, wie verbleibende Systemeinstellungen manuell entfernt werden können.

A Fragebogen vor der Installation

HINWEIS: Bei MS SQL 2000 darf die Ereignisgröße 8 KB nicht überschreiten.

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Fragen vor der Installation

1. Nachdem Sie bestimmt haben, welcher Computer als DAS-Computer verwendet werden soll und sichergestellt haben, dass er die nötigen Anforderungen für Betriebssystem und Hardware erfüllt:
   a. Rufen Sie die Host-ID-Nummer Ihres DAS-Computers ab.
   b. Nehmen Sie Kontakt mit Novell auf, um Ihren Lizenzschlüssel zu erhalten.
2. Zu welchem Zweck bzw. mit welchem Ziel verwenden Sie Novell Sentinel?
   a. Einhaltung von Bestimmungen
   b. SEM
   c. Sonstiges_____
3. Welche Netzwerkarchitektur verwenden die Quellgeräte hinsichtlich des Sicherheitssegments, in dem sich die Sentinel/Wizard-Hardware befinden soll?

   HINWEIS: Dies ist wichtig, um die Hierarchie der Datensammlung des Assistenten zu verstehen und alle Firewalls zu identifizieren, die durchdrungen werden müssen, um die Kommunikation zwischen Wizard und Sentinel bzw. Sentinel und Datenbank oder zwischen Crystal Server und Datenbank zu ermöglichen.

   Geben Sie unten Informationen (Text und/oder Zeichnung) bzw. einen Link zu Informationen ein.

4. Welche Berichte sollen über das System erstellt werden? Dies ist wichtig, um sicherzustellen, dass die Collectors die richtigen Daten für die Weitergabe an die Sentinel-Datenbank sammeln.

   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____

5. Aus welchen Quellgeräten möchten Sie Daten sammeln (IDS, HIDS, Router, Firewalls, usw…), Ereignisrate (EPS – Ereignisse pro Sekunde), Versionen, Verbindungsmethoden, Plattformen und Patches?

Gerät (Hersteller/Modell)	**Ereignisrate (EPS)**	**Version**	**Verbindungsmethode**	**Plattform**	**Patches**

   Können Sie Beispiele für Daten angeben, die die Sentinel Collectors sammeln und analysieren sollen? Dies ist wichtig, damit Sentinel die gewünschten Ergebnisse liefern kann.

6. Welche Sicherheitsmodelle/Standards sind an Ihrem Standort vorhanden?
   - Wie ist Ihre Haltung in Bezug auf lokale Konten gegenüber Domänenauthentifizierung?
     - Für Windows mit Domänenauthentifizierung müssen die richtigen Domänenkontoeinstellungen erstellt werden, damit Sentinel installiert werden kann.
     - Für Solaris-Installationen gilt dies nicht. Sentinel unterstützt jedoch nicht NIS.
7. Welche Hardware wurde für die Installation von Sentinel zugeordnet? Entspricht sie den in Kapitel 1 und 2 des Installationshandbuchs angegebenen Hardware-Spezifikationen?
8. Wie lange müssen die Daten beibehalten werden (in Tagen)? Normalerweise sind 30 Tage ein guter Wert. MS SQL hat Schwierigkeiten bei Werten über 60 Tage. Oracle funktioniert problemlos.

9. Welche Datenträgergröße möchten Sie auf der Grundlage der Informationen über die Datenbeibehaltung und EPS verwenden? Verwenden Sie 500 bis 800 Byte/Ereignis für Größenschätzungen.
10. Haben Sie die Sentinel-Anforderungen für den Betrieb anhand Ihrer Konfiguration gemäß Kapitel 1 und 2 des Installationshandbuchs bestätigt?
    - Betriebssystem-Patch-Stufe
    - Service-Patches
    - Hot Fixes usw.

B Wartung vor und nach der Installation für Oracle-Datenbank unter Solaris

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Vor-Installations-Checkliste

Diese Oracle-Checkliste für die Anwendung vor der Installation ist in erster Linie für verteilte Installationen gedacht. Sie kann jedoch auch für eigenständige Installationen verwendet werden. Wenn Sie über mehr als 3 Instanzen von Collector Manager und Correlation Engine verfügen, notieren Sie sie. Diese Checkliste ist für bis zu drei Collector Manager- und Correlation Engine-Instanzen geeignet.

Weitere Informationen finden Sie in *Kapitel 3 – Installation von Sentinel 5 für Oracle*.

	Konfigurationsvariable			
1.	*Sentinel-Version:*			*Aktuelles Datum:*
	Betriebssystem			
	▪ Richtiges Betriebssystem für Datenbank	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▪ Richtige Oracle-Datenbank mit Partitionierung	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▫ Version		▫ Patch-Stufe	
	▪ Kopie von Oracle Note: 148673.1	: Ja | : Nein		
	▪ Richtige Umgebungsvariablen für Benutzer des Oracle-Betriebssystems festgelegt.	: Ja | : Nein		
	▪ Richtiges Betriebssystem für Sentinel-Komponenten	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
2.	*DAS-Computer*			
	▪ Host-ID			
	▪ Seriennummer			
	▪ Lizenzschlüssel			
3.	*DAS-Installation*			
	▪ DB-Hostname oder IP			Standard: ESEC
	▪ Datenbankname			Standard: 1521
	▪ Datenbank-Port			
	▪ Speicherort der JDBC-Datei			

	Konfigurationsvariable			
4.	*UNIX-Kernel-Werte für Oracle. Im Folgenden sind die Mindestwerte angegeben.*			
	▪ shminfo_shmmax	4294967295	: Ja | : Nein	Wert, wenn höher:
	▪ shminfo_shmmin	1	: Ja | : Nein	Wert, wenn höher:
	▪ shminfo_shmseg	50	: Ja | : Nein	Wert, wenn höher:
	▪ shminfo_shmmni	400	: Ja | : Nein	Wert, wenn höher:
	▪ seminfo_semmns	14000	: Ja | : Nein	Wert, wenn höher:
	▪ seminfo_semmni	1024	: Ja | : Nein	Wert, wenn höher:
	▪ seminfo_semmsl	1024	: Ja | : Nein	Wert, wenn höher:
	▪ seminfo_shmopm	100	: Ja | : Nein	Wert, wenn höher:
	▪ seminfo_shmvmx	32767	: Ja | : Nein	Wert, wenn höher:
5.	*Datenbankinstanz (SID)*			
6.	*Datenbankname*			
7.	Wert, wenn höher:			
	▪ Sentinel-Datenbank (IP oder DNS)			Betriebssystem: Patch:
	▫ DB-Installationsprotokoll			
	▫ Oracle-Speicher (RAM)			
	▫ Instanzname			
	▫ Listener-Port		Standard: 1521	
	▫ SYS-Passwort			
	▫ SYSTEM-Passwort			
	▪ Kommunikationsserver (iSCALE) (IP bzw. DNS)			Betriebssystem: Patch:
	▪ Sentinel-Basisservices (IP oder DNS)			Betriebssystem: Patch:
	▪ DAS/Advisor (IP oder DNS) (Advisor ist optional)			Betriebssystem: Patch:
	▫ DAS RAM			
	▪ Correlation Engine (IP und Betriebssystem)			
		IP:		Betriebssystem:
		IP:		Betriebssystem:
		IP:		Betriebssystem:
	▪ Crystal Server (IP oder DNS)			

	Konfigurationsvariable		
	▫ MS SQL (optional, aber empfohlen)	MS SQL-Version: MS SQL-Patch: sa-Passwort oder Passwortinhaber:	
	▪ Collector Builder (IP oder DNS) (genau eine Installation empfohlen)		
	▪ Collector Manager (Collector-Services)	**HINWEIS**: Collector Manager kann ohne Passwort festgelegt werden.	
	▫ IP: ▫ IP: ▫ IP:	PW: PW: PW:	Betriebssystem: Betriebssystem: Betriebssystem:
8.	*Advisor (optional)*		
	▪ Speicherort der Datei für Datenfeed		
	▪ „Von“-Adresse des Advisors		
	▪ „An“-Adresse des Advisors		
	▪ Benutzername und Passwort	Benutzername:	PW:
9.	*Speicherorte für Datenbankdateien:*		
	▪ Datendateien		
	▪ Indexdateien		
	▪ Zusammenfassung Datendateien		
	▪ Zusammenfassung Indexdateien		
	▪ Temporäre Dateien und Tablespace-Dateien zum Rückgängigmachen		
	▪ Verzeichnis für Redo-Protokollmitglied A		
	▪ Verzeichnis für Redo-Protokollmitglied A		
10.	*Datenbankgröße::*		
	▪ Standard (20 GB)		
	▪ Groß (400 GB)		
	▪ Benutzerdefiniert (Größe)		
11.	*SMTP-Server (DNS oder IP)*		

12.	*Benutzerpasswörter*		
	▪ esecadm	PW:	
	▫ Basisverzeichnis		Standard: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Wartung nach der Installation

Es sind einige Dienstprogramme für die regelmäßige Durchführung von Wartungsarbeiten an Ihrer Datenbank verfügbar. Zu diesen Dienstprogrammen gehören:

- Analyze Partitions – Sammelt Partitionsstatistiken für Partitionen, die vor Kurzem mit Daten gefüllt wurden.
- Analyze Tables– Sammelt globale Tabellenstatistiken für die Ereignistabellen und die Tabellen mit korrelierten Ereignissen.
- Database Health Check – Sammelt Datenbankinformationen. Das Programm bietet folgende Meldungen:
  - Überprüft, ob die Datenbankinstanz aktiv ist.
  - Überprüft, ob Oracle Listener aktiv ist
  - Zeigt die Speicherplatzauslastung an.
  - Prüft auf nicht verwendbare Indizes.
  - Prüft auf ungültige Datenbankobjekte
  - Prüft auf Datenbankanalyse.

Weitere Informationen finden Sie in ***Kapitel 2 –Optimale Verfahren***, im Abschnitt *Optimale Verfahren für die Wartung*.

Im Lieferumfang von Sentinel ist die Anwendung Sentinel Data Manager enthalten. Mit dieser Anwendung können Sie die Datenbankverwaltung durchführen. Weitere Informationen finden Sie im *Sentinel-Benutzerhandbuch, Kapitel 10 – Sentinel Data Manager*.

C Wartung vor und nach der Installation für Oracle-Datenbank unter Linux

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Vor-Installations-Checkliste

Diese Oracle-Checkliste für die Anwendung vor der Installation ist in erster Linie für verteilte Installationen gedacht. Sie kann jedoch auch für eigenständige Installationen verwendet werden. Wenn Sie über mehr als 3 Instanzen von Collector Manager und Correlation Engine verfügen, notieren Sie sie. Diese Checkliste ist für bis zu drei Collector Manager- und Correlation Engine-Instanzen geeignet.

Weitere Informationen finden Sie in *Kapitel 3 – Installation von Sentinel 5 für Oracle*.

	Konfigurationsvariable			
1.	*Sentinel-Version:*			*Aktuelles Datum:*
	Betriebssystem			
	▪ Richtiges Betriebssystem für Datenbank	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▫ Version		▫ Patch-Stufe	
	▪ Richtige Oracle-Datenbank mit Partitionierung	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▫ Version		▫ Patch-Stufe	
	▪ Richtige Umgebungsvariablen für Benutzer des Oracle-Betriebssystems festgelegt.	: Ja | : Nein		
	▪ Start-Skripts (Datenbank-Computer)	: Ja | : Nein		
	▪ Prozesse (Datenbank-Computer)	: Ja | : Nein		
	▪ Sockets	: Ja | : Nein		
	▪ Richtiges Betriebssystem für Sentinel-Komponenten	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
2.	*DAS-Computer*			
	▪ Host-ID			
	▪ Seriennummer			
	▪ Lizenzschlüssel			

3.	*DAS-Installation*			
	▪ DB-Hostname oder IP			
	▪ Datenbankname			Standard: ESEC
	▪ Datenbank-Port			Standard: 1521
	▪ Speicherort der JDBC-Datei			
4.	*UNIX-Kernel-Werte für Oracle. Im Folgenden sind die Mindestwerte angegeben.*			
	▪ shmmax	2147483648	: Ja | : Nein	Wert, wenn höher:
	▪ shmmin	1	: Ja | : Nein	Wert, wenn höher:
	▪ shmseg	4096	: Ja | : Nein	Wert, wenn höher:
	▪ shmmni	400	: Ja | : Nein	Wert, wenn höher:
	▪ semmns	500	: Ja | : Nein	Wert, wenn höher:
	▪ semmni	1024	: Ja | : Nein	Wert, wenn höher:
	▪ semmsl	1024	: Ja | : Nein	Wert, wenn höher:
	▪ shmopm	100	: Ja | : Nein	Wert, wenn höher:
	▪ shmvmx	32767	: Ja | : Nein	Wert, wenn höher:
5.	*Datenbankinstanz (SID)*			
6.	*Datenbankname*			
7.	*Sentinel-Komponenten:*			
	▪ Sentinel-Datenbank (IP oder DNS)			Betriebssystem: Patch:
	▫ DB-Installationsprotokoll			
	▫ Oracle-Speicher (RAM)			
	▫ Instanzname			
	▫ Listener-Port		Standard: 1521	
	▫ SYS-Passwort			
	▫ SYSTEM-Passwort			
	▪ Kommunikationsserver (iSCALE) (IP bzw. DNS)			Betriebssystem: Patch:
	▪ Sentinel-Basisservices (IP oder DNS)			Betriebssystem: Patch:
	▪ DAS/Advisor (IP oder DNS) (Advisor ist optional)			Betriebssystem: Patch:
	▫ DAS RAM			

	▪ Correlation Engine (IP und Betriebssystem)			
		▫ IP:		Betriebssystem:
		▫ IP:		Betriebssystem:
		▫ IP:		Betriebssystem:
	▪ Crystal Server (IP oder DNS)			
	▫ MS SQL (optional, aber empfohlen)	MS SQL-Version: MS SQL-Patch: sa-Passwort oder Passwortinhaber:		
	▪ Collector Builder (IP oder DNS) (genau eine Installation empfohlen)			
	▪ Collector Manager (Collector-Services)	**HINWEIS**: Collector Manager kann ohne Passwort festgelegt werden.		
	▫ IP: ▫ IP: ▫ IP:	Benutzername: Benutzername: Benutzername:	PW: PW: PW:	Betriebssystem: Betriebssystem: Betriebssystem:
8.	*Advisor (optional)*			
	▪ Speicherort der Datei für Datenfeed			
	▪ „Von“-Adresse des Advisors			
	▪ „An“-Adresse des Advisors			
	▪ Benutzername und Passwort	Benutzername:		PW:
9.	*Speicherorte für Datenbankdateien:*			
	▪ Datendateien			
	▪ Indexdateien			
	▪ Zusammenfassung Datendateien			
	▪ Zusammenfassung Indexdateien			
	▪ Temporäre Dateien und Tablespace-Dateien zum Rückgängigmachen			
	▪ Verzeichnis für Redo-Protokollmitglied A			
	▪ Verzeichnis für Redo-Protokollmitglied A			
10.	*Datenbankgröße::*			
	▪ Standard (20 GB)			
	▪ Groß (400 GB)			
	▪ Benutzerdefiniert (Größe)			

11.	*SMTP-Server (DNS oder IP)*		
12.	*Benutzerpasswörter*		
	▪ esecadm	PW:	
	▫ Basisverzeichnis		Standard: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Wartung nach der Installation

Es sind einige Dienstprogramme für die regelmäßige Durchführung von Wartungsarbeiten an Ihrer Datenbank verfügbar. Zu diesen Dienstprogrammen gehören:

- Analyze Partitions – Sammelt Partitionsstatistiken für Partitionen, die vor Kurzem mit Daten gefüllt wurden.
- Analyze Tables– Sammelt globale Tabellenstatistiken für die Ereignistabellen und die Tabellen mit korrelierten Ereignissen.
- Database Health Check – Sammelt Datenbankinformationen. Das Programm bietet folgende Meldungen:
  - Überprüft, ob die Datenbankinstanz aktiv ist.
  - Überprüft, ob Oracle Listener aktiv ist
  - Zeigt die Speicherplatzauslastung an.
  - Prüft auf nicht verwendbare Indizes.
  - Prüft auf ungültige Datenbankobjekte
  - Prüft auf Datenbankanalyse.

Weitere Informationen finden Sie in ***Kapitel 2 –Optimale Verfahren***, im Abschnitt *Optimale Verfahren für die Wartung*.

Im Lieferumfang von Sentinel ist die Anwendung Sentinel Data Manager enthalten. Mit dieser Anwendung können Sie die Datenbankverwaltung durchführen. Weitere Informationen finden Sie im *Sentinel-Benutzerhandbuch, Kapitel 10 – Sentinel Data Manager*.

D Wartung vor und nach der Installation für MS SQL-Datenbank unter Windows

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

HINWEIS: Bei MS SQL 2000 darf die Ereignisgröße 8 KB nicht überschreiten.

Vor-Installations-Checkliste

Diese MS SQL-Checkliste für die Anwendung vor der Installation ist in erster Linie für verteilte Installationen gedacht. Sie kann jedoch auch für eigenständige Installationen verwendet werden. Wenn Sie über mehr als 3 Instanzen von Collector Manager und Correlation Engine verfügen, notieren Sie sie. Diese Checkliste ist für bis zu drei Collector Manager- und Correlation Engine-Instanzen geeignet.

Weitere Informationen finden Sie in *Kapitel 4 – Installation von Sentinel 5 für MS SQL*.

	Konfigurationsvariable			
1.	*Sentinel-Version:*			*Aktuelles Datum:*
	Betriebssystem			
	▪ Richtiges Betriebssystem für Datenbank	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▪ Richtige SQL-Datenbank	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
	▫ Version		▫ Patch-Stufe	
	▪ Richtiges Betriebssystem für Sentinel-Komponenten	: Ja | : Nein	▪ Richtiges Patch	: Ja | : Nein
2.	*Für DAS-Installationen unter dem Konto der Windows-Domäne„Als Dienst anmelden“ zuweisen*	: Ja | : Nein		
3.	*DAS-Computer*			
	▪ Host-ID			
	▪ Seriennummer			
	▪ Lizenzschlüssel			
4.	*Datenbank-Hostname oder IP:*	*<Hostname>[\<Instanzname>]*		
5.	*Datenbankname*			Standard: ESEC
6.	*Port:*		Standard: 1433	
7.	*SQL-Installation*	: gemischt : nicht gemischt		

	Konfigurationsvariable		
8.	*sa-Passwort für SQL Server bzw. Passwortinhaber.*	PW:	
9.	*Sentinel-Komponenten:*		
	▪ Sentinel-Datenbank (IP oder DNS)		Betriebssystem: Patch:
	▪ Kommunikationsserver (iSCALE) (IP bzw. DNS)		Betriebssystem: Patch:
	▪ Sentinel-Basisservices (IP oder DNS)		Betriebssystem: Patch:
	▪ DAS/Advisor (IP oder DNS) (Advisor ist optional)		Betriebssystem: Patch:
	▪ Correlation Engine (IP und Betriebssystem)		
		IP:	Betriebssystem:
		IP:	Betriebssystem:
		IP:	Betriebssystem:
	▪ Crystal Server (IP oder DNS)		Betriebssystem: Patch:
	▫ MS SQL (optional, aber empfohlen)	MS SQL-Version: MS SQL-Patch: sa-Passwort oder Passwortinhaber:	
	▪ Collector Builder (IP oder DNS) (genau eine Installation empfohlen)		
	▪ Collector Manager (Passwörter für Collector-Services mit IP oder DNS und Betriebssystem)	**HINWEIS**: Collector Manager kann ohne Passwort festgelegt werden.	
	▫ IP: ▫ IP: ▫ IP:	PW: PW: PW:	Betriebssystem: Betriebssystem: Betriebssystem:
10.	*Advisor (optional)*		
	▪ Speicherort der Datei für Datenfeed		
	▪ „Von“-Adresse des Advisors		
	▪ „An“-Adresse des Advisors		
	▪ Benutzername und Passwort	Benutzername:	PW:
11.	*Speicherorte für Datenbankdateien:*		
	▪ Datendateien		
	▪ Indexdateien		

	Konfigurationsvariable		
	▪ Zusammenfassung Datendateien		
	▪ Zusammenfassung Indexdateien		
	▪ Protokolldateien		
12.	*Datenbankgröße::*		
	▪ Standard (20 GB)		
	▪ Groß (400 GB)		
	▪ Benutzerdefiniert (Größe)		
13.	*SMTP-Server (DNS oder IP)*		
14.	*Für SQL-Authentifizierung (Passwörter)*		
	▪ esecadm	PW:	
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
15.	*Für Windows-Authentifizierung (Passwörter)*		
	▪ DBA (Anmeldung)	Benutzername:	
	▪ Anwendungsbenutzer (Anmeldung und Passwort)	Benutzername:	PW:
	▪ Sentinel-Administrator (Anmeldung)	Benutzername:	
	▪ Benutzer von Sentinel-Berichterstellung (Anmeldung)	Benutzername:	

Wartung nach der Installation

Mit dem Betriebssystem Windows können Sie automatisch Daten archivieren und Partitionen hinzufügen. Weitere Informationen finden Sie in *Kapitel 2 – Optimale Verfahren,* im Abschnitt *Automatisches Archivieren von Daten und Hinzufügen von Partitionen*.

E Manuelle Bereinigung früherer Installationen

HINWEIS: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Wenn Sie eine Neuinstallation von Sentinel durchführen, sollten Sie UNBEDINGT jeden der folgenden Schritte ausführen, um sicherzustellen, dass keine Dateien oder Systemeinstellungen von einer früheren Sentinel-Installation verblieben sind, die zu einem Scheitern der Neuinstallation führen können. Führen Sie folgende Schritte an jedem Computer durch, für den Sie eine Neuinstallation durchführen möchten, BEVOR Sie das Installationsprogramm ausführen.

ACHTUNG: Diese Anweisungen beinhalten Änderungen an Betriebssystemeinstellungen und Dateien. Wenn Sie keine Erfahrung im Ändern dieser Systemeinstellungen bzw. Dateien haben, wenden Sie sich an den Systemadministrator.

Solaris

Manuelle Sentinel-Bereinigung unter Solaris

1. Melden Sie sich als „root“ an.
2. Vergewissern Sie sich, dass keiner der Sentinel-Prozesse ausgeführt wird.
3. Entfernen Sie den Inhalt von /opt/sentinelXX (bzw. dem Verzeichnis, in dem die Sentinel-Software installiert und benannt wurde)
4. Entfernen Sie folgende Dateien im Verzeichnis /etc/rc3.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (sofern SDEE-Connector installiert ist)
5. Entfernen Sie folgende Dateien im Verzeichnis /etc/rc0.d:
   - K01wizard
   - K02sentinel
   - K01esdee (sofern SDEE-Connector installiert ist)
   - K01esyslogserver (v5.1.1.1)
6. Entfernen Sie folgende Dateien im Verzeichnis /etc/init.d:
   - sentinel
   - wizard
   - esdee (sofern SDEE-Connector installiert ist)
   - esyslogserver (v5.1.1.1)

7. Entfernen Sie folgende Dateien aus /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
8. Entfernen Sie Installshield-Verweise in /var/sadm/pkg. Entfernen Sie folgende Dateien aus dem Verzeichnis /var/sadm/pkg:
   - Alle Dateien, die mit IS beginnen (IS* in der Befehlszeile)
   - Alle Dateien, die mit ES beginnen (ES* in der Befehlszeile)
   - Alle Dateien, die mit MISCwp beginnen (MISCwp* in der Befehlszeile)
9. Entfernen Sie den Benutzer „esecadm“ (und das Basisverzeichnis) und die Gruppe „esec“ (stellen Sie sicher, dass niemand als Benutzer „esecadm“ angemeldet ist, bevor Sie diesen Schritt durchführen)
   - Führen Sie Folgendes aus: userdel -r esecadm
   - Führen Sie Folgendes aus: groupdel esec
10. Entfernen Sie den Installshield-Abschnitt von /etc/profile, /etc/.login
11. Entfernen Sie das Verzeichnis /InstallShield, sofern vorhanden.
12. Entfernen Sie die Sentinel Oracle-Datenbank gemäß den Anweisungen im Abschnitt „Manuelle Bereinigung der Sentinel Oracle-Datenbank unter Solaris“.
13. Starten Sie das Betriebssystem neu.

Manuelle Bereinigung der Sentinel Oracle-Datenbank unter Solaris

1. Halten Sie als Oracle-Benutzer Oracle Listener an:
   - Führen Sie Folgendes aus: lsnrctl stop
2. Stoppen Sie die Sentinel-Datenbank:
   - Wechseln Sie zum Oracle-Benutzer
   - Setzen Sie die Umgebungsvariable ORACLE_SID auf den Namen Ihrer Sentinel-Datenbankinstanz (normalerweise ESEC).
   - Führen Sie Folgendes aus: sqlplus '/ as sysdba'
   - Führen Sie an der sqlplus-Eingabeaufforderung Folgendes aus: shutdown immediate
3. Entfernen Sie den Eintrag für die Sentinel-Datenbank in der Datei /var/opt/oracle/oratab
4. Entfernen Sie die Datei init<Name_Ihrer_Instanz>.ora (normalerweise initESEC.ora) aus dem Verzeichnis $ORACLE_HOME/dbs.
5. Entfernen Sie die Einträge für Ihre Sentinel-Datenbank aus folgenden Dateien im Verzeichnis $ORACLE_HOME/network/admin:
   - tnsnames.ora
   - listener.ora
6. Löschen Sie die Datendateien der Datenbank aus dem Verzeichnis, in dem Sie sie installiert haben.

Linux

Manuelle Sentinel-Bereinigung unter Linux

1. Melden Sie sich als „root“ an.
2. Vergewissern Sie sich, dass keiner der Sentinel-Prozesse ausgeführt wird.
3. Entfernen Sie den Inhalt von /opt/sentinelXX (bzw. dem Verzeichnis, in dem die Sentinel-Software installiert und benannt wurde)
4. Entfernen Sie folgende Dateien im Verzeichnis /etc/rc5.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (sofern SDEE-Connector installiert ist)
5. Entfernen Sie folgende Dateien im Verzeichnis /etc/rc3.d:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (sofern SDEE-Connector installiert ist)
6. Entfernen Sie folgende Dateien im Verzeichnis /etc/rc0.d:
   - K01esyslogserver (v5.1.1.1)
   - K01wizard
   - K02sentinel
   - K01esdee (sofern SDEE-Connector installiert ist)
7. Entfernen Sie folgende Dateien im Verzeichnis /etc/init.d:
   - sentinel
   - wizard
   - esyslogserver (v5.1.1.1)
   - esdee (sofern SDEE-Connector installiert ist)
8. Entfernen Sie folgende Dateien aus /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
9. Entfernen Sie das Verzeichnis /root/InstallShield
10. Entfernen Sie die Datei /root/vpd.properties
11. Entfernen Sie den Benutzer „esecadm“ (und das Basisverzeichnis) und die Gruppe „esec“ (stellen Sie sicher, dass niemand als Benutzer „esecadm“ angemeldet ist, bevor Sie diesen Schritt durchführen)
    - Führen Sie Folgendes aus: userdel -r esecadm
    - Führen Sie Folgendes aus: groupdel esec
12. Entfernen Sie den Installshield-Abschnitt von /etc/profile, /etc/.login
13. Entfernen Sie die Sentinel Oracle-Datenbank gemäß den Anweisungen im Abschnitt „Manuelle Bereinigung der Sentinel Oracle-Datenbank unter Linux“.

14. Starten Sie das Betriebssystem neu.

Manuelle Bereinigung der Sentinel Oracle-Datenbank unter Linux

1. Halten Sie als Oracle-Benutzer Oracle Listener an:
   - Führen Sie Folgendes aus: lsnrctl stop
2. Stoppen Sie die Sentinel-Datenbank:
   - Wechseln Sie zum Oracle-Benutzer
   - Setzen Sie die Umgebungsvariable ORACLE_SID auf den Namen Ihrer Sentinel-Datenbankinstanz (normalerweise ESEC).
   - Führen Sie Folgendes aus: sqlplus '/ as sysdba'
   - Führen Sie an der sqlplus-Eingabeaufforderung Folgendes aus: shutdown immediate
3. Entfernen Sie den Eintrag für die Sentinel-Datenbank in der Datei /etc/oratab
4. Entfernen Sie die Datei init<Name_Ihrer_Instanz>.ora (normalerweise initESEC.ora) aus dem Verzeichnis $ORACLE_HOME/dbs.
5. Entfernen Sie die Einträge für Ihre Sentinel-Datenbank aus folgenden Dateien im Verzeichnis $ORACLE_HOME/network/admin:
   - tnsnames.ora
   - listener.ora
6. Löschen Sie die Datendateien der Datenbank aus dem Verzeichnis, in dem Sie sie installiert haben.

Windows

Manuelle Sentinel-Bereinigung unter Windows

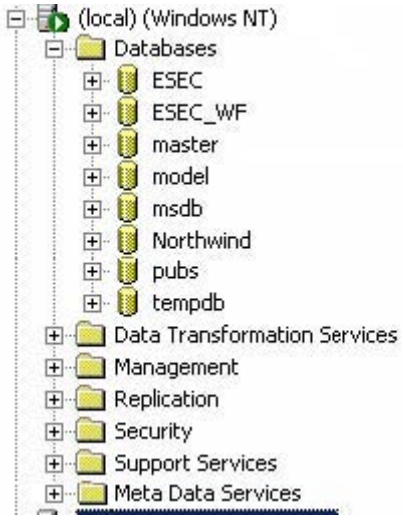
1. Löschen Sie den Ordner C:\Programme\Gemeinsame Dateien\InstallShield\Universal und seinen gesamten Inhalt.
2. Löschen Sie den alten Sentinel-Installationsordner (z. B. C:\Programme\sentinel [%ESEC_HOME%]).
3. Löschen Sie folgende Umgebungsvariablen (sofern vorhanden), indem Sie mit der rechten Maustaste auf „Arbeitsplatz“ klicken, „Eigenschaften“ auswählen, auf die Registerkarte „Erweitert“ klicken und dann auf die Schaltfläche „Umgebungsvariablen“ klicken:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
4. Entfernen Sie alle Einträge in der Umgebungsvariable „Path“, die auf eine frühere Installation verweisen.

ACHTUNG: Achten Sie darauf, nur Pfade zu alten Sentinel-Installationen zu entfernen. Wenn Sie andere Einträge in „Path“ entfernen, funktioniert das System möglicherweise nicht mehr ordnungsgemäß.

5. Löschen Sie alle Sentinel-Verknüpfungen vom Desktop.
6. Löschen Sie den Verknüpfungsordner *Start > Programme > Sentinel* aus dem Startmenü.
7. Entfernen Sie die Sentinel Microsoft SQL Server-Datenbank gemäß den Anweisungen im Abschnitt *Manuelle Bereinigung der Sentinel Microsoft SQL Server-Datenbank unter Windows.*
8. Starten Sie das Betriebssystem neu.

Manuelle Bereinigung der Sentinel Microsoft SQL Server-Datenbank unter Windows

1. Öffnen Sie Microsoft SQL Server Enterprise Manager und stellen Sie eine Verbindung zu der SQL Server-Instanz her, auf der Sie Ihre Sentinel-Datenbank erstellt haben.
2. Erweitern Sie den Datenbank-Baum und suchen Sie die Sentinel-Datenbank.



3. Klicken Sie für jede ESEC- und ESEC_WF-Datenbank (bzw. den von Ihnen während der Installation zugewiesenen Datenbanknamen) mit der rechten Maustaste auf die Datenbank und wählen Sie *Löschen* aus.
4. Bestätigen Sie das Löschen der Datenbank mit *Ja*.