Novell Sentinel

6.0

www.novell.com

BAND I – INSTALLATIONSHANDBUCH

Apr. 30, 2007

Novell®

Rechtliche Hinweise

Novell, Inc., leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc., behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Desweiteren übernimmt Novell, Inc., für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc., das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc., die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für anstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen genannte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Exportieren von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc., besitzt Anrechte auf geistiges Eigentum für Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite Novell Legal Patents (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

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

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Novell-Dokumentationswebseite (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Vorwort

Die Technische Dokumentation von Sentinel stellt ein allgemeines Betriebs- und Referenzhandbuch dar. 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™-Installationshandbuch
- Band II – Sentinel™-Benutzerhandbuch
- Band III – Sentinel™-Collector-Benutzerhandbuch
- Band IV – Sentinel™-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
- Collector Builder
- Collector Manager
- Advisor

Band II – Sentinel-Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Verwendung der Sentinel Console
- Sentinel-Funktionen
- Sentinel-Architektur
- Sentinel Communication
- Herunterfahren/Starten von Sentinel
- Anfälligkeitsbewertung
- Ereignisüberwachung
- Ereignisfilterung
- Ereigniskorrelation
- Sentinel Data Manager
- Ereigniskonfiguration für Unternehmensrelevanz
- Zuordnungsservice
- Verlaufsberichte
- Collector-Hostverwaltung
- Vorfälle
- Szenarios
- Benutzerverwaltung
- Workflow

Band III – Collector-Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

- Verwendung von Collector Builder
- Collector Manager
- Collectors
- Collector-Hostverwaltung
- Erstellen und Warten von Collectors

Band IV – Sentinel-Referenzhandbuch für Benutzer

In diesem Handbuch werden die folgenden Themen behandelt:

- Collector-Skriptsprache
- Collector-Analysebefehle
- Collector-Administratorfunktionen
- META-Tags für Collector und Sentinel
- Benutzerberechtigungen
- Sentinel Correlation Engine
- Korrelations-Befehlszeilenoptionen
- Sentinel-Datenbankschema

Band V – Sentinel-Handbuch für Drittanbieter-Integration

- Remedy
- HP OpenView-Operationen
- HP Service Desk

Einführung

1

In diesem Kapitel werden die folgenden Themen behandelt:

Dieses Handbuch führt Sie in Einzelschritten durch eine Standardinstallation. Das Sentinel-Benutzerhandbuch enthält detaillierte Beschreibungen zu Architektur, Betrieb und Verwaltungsvorgängen.

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

1.1 Überblick über Sentinel

Sentinel™ ist eine Sicherheitsinformations- und Ereignisverwaltungslösung, die Informationen aus vielen Quellen in einem Unternehmen erhält, diese standardisiert, Prioritäten setzt und Ihnen diese Informationen zur Verfügung stellt, damit Sie Entscheidungen hinsichtlich Bedrohungen, Risiken und Richtlinien treffen können.

Sentinel automatisiert Vorgänge zur Protokollerfassung, Analyse und Berichterstellung, um sicherzustellen, dass IT-Steuerungen wirksam zur Unterstützung von Bedrohungserkennungs- und Audit-Anforderungen eingesetzt werden. Sentinel ersetzt arbeitsintensive manuelle Vorgänge durch die automatisierte fortlaufende Überwachung von Sicherheits- und Konformitätsereignissen und IT-Steuerungen.

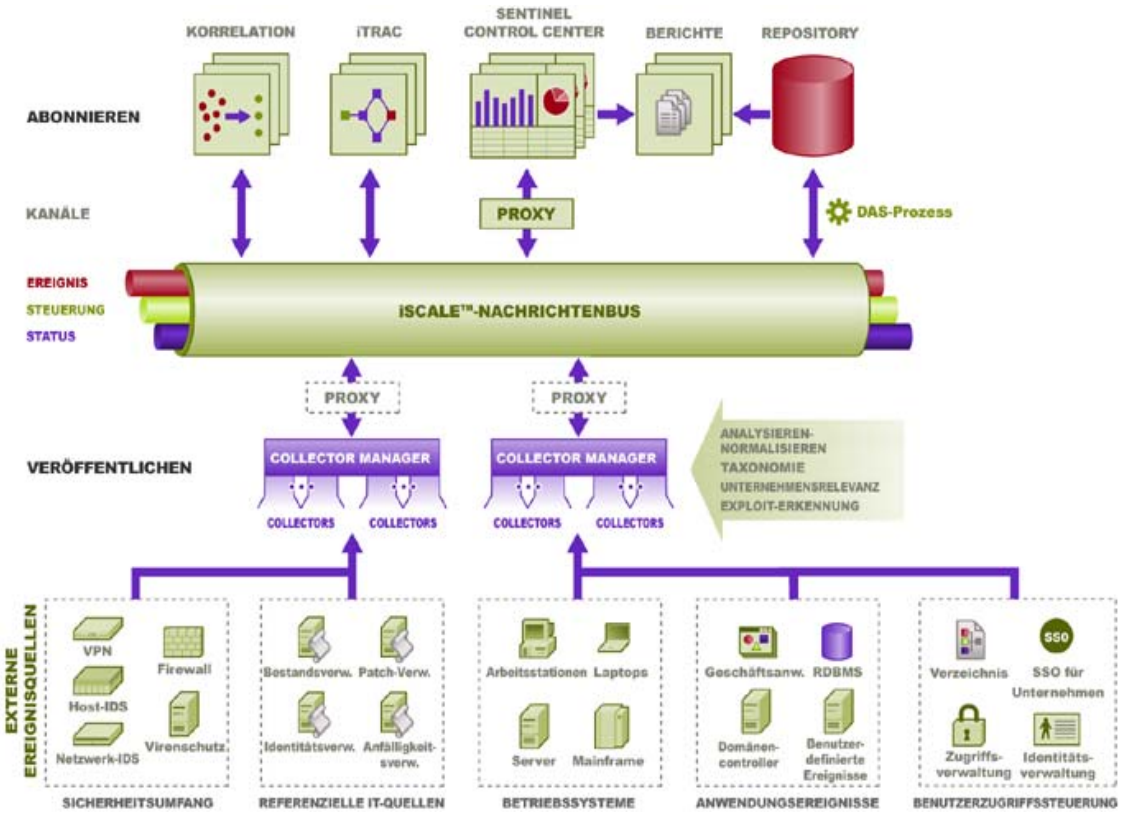
Sentinel erfasst und koordiniert sicherheitsbezogene und nicht sicherheitsbezogene Informationen aus der vernetzten Infrastruktur einer Organisation sowie von Drittanbieter-Systemen, -geräten und -anwendungen. Sentinel stellt die gesammelten Daten in einer umfassenderen grafischen Benutzeroberfläche zur Verfügung, identifiziert Sicherheits- oder Konformitätsprobleme und verfolgt Gegenmaßnahmen. Auf diese Weise werden zuvor fehleranfällige Vorgänge rationalisiert und ein strengeres und sichereres Verwaltungsprogramm wird erstellt.

Die automatisierte Verwaltung der Vorfallbearbeitung ermöglicht Ihnen die Dokumentation und Formalisierung des Vorgangs der Verfolgung und Eskalation von Vorfällen und Richtlinienverletzungen sowie der Reaktion darauf und stellt eine 2-Wege-Integration in Problemberichtsysteme zur Verfügung. Mit Sentinel können Sie unmittelbar reagieren und Vorfälle effizient auflösen.

Sentinel bietet Ihnen Folgendes:

- Integrierte automatisierte Sicherheitsverwaltung und Konformitätsüberwachung in Echtzeit in allen Systemen und Netzwerken
- Ein Bezugssystem, das die Steuerung von IT-Richtlinien und Aktionen durch Geschäftsrichtlinien ermöglicht
- Automatische Dokumentation von Sicherheits-, System- und Zugriffsereignissen im gesamten Unternehmen und Erstellen entsprechender Berichte
- Integrierte Verwaltung und Auflösung von Vorfällen
- Die Möglichkeit zur Demonstration und Überwachung der Konformität mit internen Richtlinien und gesetzlichen Vorschriften wie beispielsweise Sarbanes-Oxley, HIPAA, GLBA und FISMA

In der folgenden Abbildung ist eine konzeptionelle Sentinel-Architektur dargestellt, die die an der Sicherheitsverwaltung beteiligten Komponenten veranschaulicht.



Sentinel setzt sich aus zahlreichen Komponenten zusammen:

- Sentinel Server
- Sentinel Communication Server

- Correlation Engine
- iTRAC
- Sentinel-Datenbank
- Sentinel Collector Manager
- Sentinel-Collectors
- Sentinel Control Center
- Sentinel Collector Builder
- Sentinel Data Manager
- Crystal Report Server
- Sentinel Advisor
- Drittanbieter-Integration
  - HP OpenView-Operationen
  - HP Service Desk
  - Remedy

1.1.1 Sentinel Server

Sentinel Server setzt sich aus mehreren Komponenten zusammen, die die wichtigsten Services der Ereignisverabeitung ausführen. Hierzu zählt der Empfang von Ereignissen von den Collector Manager-Instanzen, das Speichern der Ereignisse in der Datenbank, das Filtern, die Verarbeitung von ActiveView-Ansichten, die Durchführung von Datenbankabfragen und die Verarbeitung der Ergebnisse sowie die Verwaltung administrativer Aufgaben wie zum Beispiel der Benutzerauthentifizierung und der Autorisierung.

1.1.2 Sentinel Communication Server

Der iSCALE-Nachrichtenbus kann in einer Sekunde Tausende von Nachrichtenpaketen zwischen den Sentinel-Komponenten verschieben. Hierdurch ist die unabhängige Skalierung der Komponenten und eine auf Standards basierende Integration in externe Anwendungen möglich.

1.1.3 Correlation Engine

Die Korrelation bietet mehr Intelligenz bei der Verwaltung von Sicherheitsereignissen, indem sie die Analyse des eingehenden Ereignisstroms automatisiert, um Muster zu entdecken, die von Interesse sind. Die Korrelation ermöglicht Ihnen das Definieren von Regeln, die kritische Bedrohungen und komplexe Angriffsmuster identifizieren, sodass Sie Ereignissen Priorität verleihen und eine effektive Vorfallsverwaltung und -reaktion initialisieren können.

1.1.4 iTRAC-Workflow

Sentinel bietet ein iTRAC-Workflow-Verwaltungssystem, mit dem Prozesse für die Vorfallbearbeitung definiert und automatisiert werden können. Vorfälle, die in Sentinel entweder durch eine Korrelationsregel oder manuell identifiziert werden, können mit einem iTRAC-Workflow verknüpft werden.

1.1.5 Sentinel-Datenbank

Das Produkt Sentinel wurde um eine Backend-Datenbank herum erstellt, in der Sicherheitsereignisse sowie sämtliche Sentinel-Metadaten gespeichert sind. Die Ereignisse werden in normalisierter Form gespeichert, zusammen mit Bestands- und Anfälligkeitsdaten, Identitätsdaten, Vorfall- und Workflow-Status sowie zahlreichen anderen Datentypen.

1.1.6 Sentinel Collector Manager

Collector Manager verwaltet die Collectors, überwacht Systemsstatusmeldungen und führt die Ereignisfilterung nach Bedarf durch. Zu den wichtigsten Funktionen von Collector Manager zählen das Umwandeln von Ereignissen, das Ergänzen von Ereignissen um Geschäftsrelevanz über die Taxonomie, das Durchführen globaler Filtervorgänge für Ereignisse, das Routing von Ereignissen sowie das Senden von Zustandsmeldungen an den Sentinel-Server.

Sentinel Collector Manager kann direkt oder über einen SSL-Proxy eine Verbindung zu dem Nachrichtenbus herstellen.

1.1.7 Sentinel-Collectors

Sentinel sammelt Daten von Quellgeräten und stellt einen umfassenderen Ereignisdatenstrom bereit, indem Taxonomie, Exploit-Erkennung sowie Geschäftsrelevanz in den Datenstrom integriert werden, bevor Ereignisse korreliert, 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.

Sentinel-Collectors können Daten der folgenden Gerätetypen analysieren:

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

Vorhandene gerätespezifische Collectors können Sie von der Novell-Website für Produkte (http://support.novell.com/products/sentinel/collectors.html) herunterladen. Collectors können in Collector Builder, einer im Sentinel-System enthaltenen eigenständigen Anwendung, erstellt oder geändert werden.

1.1.8 Sentinel Control Center

Sentinel Control Center bietet eine integrierte Sicherheitsverwaltungskonsole, mit der Analytiker schnell neue Trends oder Angriffe erkennen, grafische Informationen in Echtzeit bearbeiten und

verwenden 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 Kennzahlen
- Ereignisquellenverwaltung: Bereitstellung und Überwachung von Collectors

1.1.9 Sentinel Collector Builder

Sentinel Collector Builder ermöglicht Ihnen das Erstellen von Collectors. Sie können die Schablonen so erstellen und anpassen, dass der Collector die Daten analysieren kann.

1.1.10 Sentinel Data Manager

Sentinel Data Manager (SDM) ermöglicht Ihnen die Verwaltung der Sentinel-Datenbank. In SDM können Sie Folgendes durchführen:

- Auslastung des Datenbankspeichers überwachen
- Datenbankpartitionen anzeigen und verwalten
- Datenbankarchive überwachen
- Daten in die Datenbank importieren
- Datenzuordnung konfigurieren
- Namen von Ereigniskennungen konfigurieren
- Einstellungen für den Zusammenfassungsbericht konfigurieren

1.1.11 Crystal Reporting-Server

Crystal Enterprise Server by Business Objects™ bietet umfassende Services für die Berichterstellung in Sentinel Control Center. Im Lieferumfang von Sentinel sind vordefinierte Berichte enthalten, die auf die häufigsten Berichtsanforderungen von Organisationen ausgerichtet sind, die ihre Sicherheits- und Konformitätsaspekte überwachen. Mit Crystal Report Developer können neue benutzerdefinierte Berichte auch für das veröffentlichte Berichtsansichtsschema von Sentinel entwickelt werden.

1.1.12 Sentinel Advisor

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

1.1.13 Drittanbieter-Integration

Sentinel verwendet API-Plugins von Drittanbietern für die Integration folgender Systeme:

- HP OpenView-Operationen
- HP Service Desk
- Remedy AR

1.2 Sprachunterstützung

Die Sentinel-Komponenten wurden in die folgenden Sprachen übersetzt:

- Englisch
- = Portugiesisch (Brasilien)
- Französisch
- Italienisch
- Deutsch
- Spanisch
- Japanisch
- Chinesisch (Traditionell)
- Chinesisch (Vereinfacht)

Es gibt mehrere Ausnahmen:

- Die Benutzeroberfläche und die Skripts von Collector Builder stehen nur auf Englisch zur Verfügung. Collector Builder kann jedoch auch unter den oben genannten nicht-englischen Betriebssystemen ausgeführt werden.
- Zum aktuellen Zeitpunkt können die Collector Manager-Instanzen nur ASCII- und erweiterte ASCII-Daten (d. h. keine Doppelbyte- oder Unicode-Daten) verarbeiten.
- Von Novell erstellte Collectors wurden für die Analyse von Ereignissen in englischer Sprache entwickelt.
- Interne Ereignisse (zur Prüfung von Sentinel-Operationen) stehen nur auf Englisch zur Verfügung.

1.3 Weitere Novell-Referenzen

Die folgenden Handbücher sind auf der Novell-Dokumentationswebsite (http://www.novell.com/documentation/) verfügbar:

- Sentinel-Installationshandbuch
- Sentinel-Benutzerhandbuch
- Sentinel Collector Builder-Benutzerhandbuch
- Sentinel-Referenzhandbuch für Benutzer
- Sentinel-Handbuch für Drittanbieter-Integration
- Versionshinweise

1.4 Anfragen an Novell

- Website: http://www.novell.com (http://www.novell.com)
- Technischer Support von Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- Self Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Website für das Herunterladen von Patches: http://download.novell.com/index.jsp (http://download.novell.com/index.jsp)
- Support (24 Stunden/7 Tage pro Woche): http://www.novell.com/offices (http://www.novell.com/offices)

Optimale Verfahren

2

In diesem Kapitel werden die folgenden Themen behandelt:

In diesem Kapitel werden optimale Verfahren erörtert und Empfehlungen zur bestmöglichen Nutzung von Sentinel abgegeben.

2.1 Unterstützte Plattformen

Die Sentinel-Komponenten sollten stets auf einer von Novell unterstützten Plattform installiert werden. Zum Zeitpunkt der Drucklegung wurde Sentinel auf den folgenden Plattformen unterstützt. Aktualisierte Informationen finden Sie gegebenenfalls in der Online-Dokumentation unter http://www.novell.com/documentation (http://www.novell.com/documentation).

2.1.1 Betriebssysteme

Die Sentinel-Komponenten (einschließlich der Datenbank) sind für die Ausführung unter folgenden Betriebssystemen zertifiziert:

- SUSE Linux Enterprise Server 9 SP2 und SP3
- SUSE Linux Enterprise Server 10 (Patch vom 01.07.2006)
- Red Hat Enterprise Linux 3 Update 5 ES (x86)
- Solaris 9 (Recommended Patch Cluster DATUM: 03. Mai 2005)
- Sun Solaris 10
- Windows 2003 Standard oder Enterprise Edition SP1
- Windows XP SP1 (nur für Sentinel Control Center, Collector Builder und Sentinel Data Manager)
- Windows 2000 SP4, Standard oder Enterprise Edition (nur für Sentinel Control Center, Collector Builder und Sentinel Data Manager)

2.1.2 Datenbanken

Sentinel ist für die Ausführung mit den folgenden Datenbanken zertifiziert:

- Oracle 10g Enterprise Edition (v 10.2.0.3 mit dem wichtigen Oracle-Patch #5881721)

- Oracle 9i Enterprise Edition (v 9.2.0.7 p. 5490841)
- Microsoft SQL Server 2005 SP1 32-Bit (v.9.00.2047), Standard oder Enterprise Edition
- Microsoft SQL Server 2005 64-Bit (v.9.00.2047), Standard oder Enterprise Edition

---

Hinweis: Alle Datenbanken sollten unter einem Betriebssystem installiert werden, das sowohl von dem Datenbankhersteller als auch von Novell für die Nutzung mit Sentinel-Komponenten zertifiziert ist. Oracle muss unter Linux oder Solaris (nicht Windows) ausgeführt werden.

2.1.3 Report Server

Der unterstützte Reporting-Server ist Crystal Enterprise Server XI R2. Er kann auf jeder der folgenden Plattformen in der Sentinel-Umgebung ausgeführt werden:

- Windows 2003 SP1 Server, Standard oder Enterprise Edition
  - Crystal-Datenbank unter Microsoft SQL 2005
- Red Hat Enterprise Linux 3 Update 5 ES (x86)
  - Crystal-Datenbank unter MySQL
- SUSE Linux Enterprise Server 9 SP2 (x86)
  - Crystal-Datenbank unter MySQL

2.1.4 Unterstützte Stacks

Novell unterstützt Sentinel-Komponenten, die auf einem beliebigen der unterstützten Betriebssysteme installiert sind, und es kann sich um eine gemischte Umgebung (Linux, Solaris und Windows) handeln. Hierbei gibt es nur wenige Ausnahmen und Vorbehalte.

- Collector Builder – kann nur auf Windows-Plattformen ausgeführt werden.
- Crystal Enterprise Server
  - Kann nicht unter Solaris ausgeführt werden.
  - Kann nicht unter Windows 2000 in einer Sentinel-Umgebung ausgeführt werden.
  - Kann nicht mit MSDE als Datenbank in einer Sentinel-Umgebung ausgeführt werden.
- Datenbank
  - Muss SQL Server sein, wenn Sentinel Server unter Windows ausgeführt wird.
  - Muss Oracle sein, wenn Sentinel Server unter Linux oder Solaris (nicht Windows) ausgeführt wird.
  - Oracle unter Windows wird in der Sentinel-Umgebung nicht unterstützt.
- Data Access Service-Prozess (DAS)
  - Die Windows-Authentifizierung kann nicht verwendet werden, wenn DAS in einer gemischten Umgebung installiert ist, wobei DAS unter Windows und Oracle als Datenbank oder DAS unter UNIX oder Linux und SQL Server als Datenbank verwendet wird.

2.2 Hardware-Empfehlungen

Bei einer Installation unter Linux oder Windows können der Sentinel-Server und die Datenbankkomponenten auf Hardware vom Typ x86 (32-Bit) oder x86-64 (64-Bit), einschließlich AMD Opteron- und Intel Xeon-Hardware, installiert werden. Itanium-Server werden nicht unterstützt.

Für Solaris wird die SPARC-Architektur unterstützt.

2.2.1 Architektur

Sentinel weist eine in hohem Maße skalierbare Architektur auf. Wenn hohe Ereignisraten erwartet werden, können die Komponenten auch auf mehrere Computer verteilt werden, um die bestmögliche Leistung des Systems zu erzielen.

Beim Entwurf eines Sentinel-Systems sind zahlreiche Faktoren zu berücksichtigen. Nachfolgend finden Sie eine Liste (nicht vollständig) der Faktoren, die bei der Entwicklung eines Designs beachtet werden müssen:

- Ereignisrate (Ereignisse pro Sekunde oder EPS)
- Geographischer Ort bzw. Standort des Netzwerks mit den Ereignisquellen und Bandbreite zwischen Netzwerken
- Verfügbare Hardware
- Bevorzugte Betriebssysteme
- Pläne für die zukünftige Skalierbarkeit
- Umfang der erwarteten zu filternden Ereignisse
- Lokale Richtlinien für die Datenaufbewahrung
- Gewünschte Anzahl und Komplexität der Korrelationsregeln
- Erwartete Anzahl der Vorfälle pro Tag
- Erwartete Anzahl der Workflows, die pro Tag verwaltet werden
- Anzahl der Benutzer, die sich an dem System anmelden
- Anfälligkeit und Bestandsinfrastruktur

Der wichtigste Faktor für das Design eines Sentinel-Systems ist die Ereignisrate; beinahe jede Komponente der Sentinel-Architektur wird durch steigende Ereignisraten beeinflusst. In einer Umgebung mit einer hohen Ereignisrate unterliegt die Datenbank den höchsten Anforderungen. Sie ist in großem Maße E/A-abhängig und verarbeitet unter Umständen gleichzeitig hunderte oder tausende von Ereigniseingaben pro Sekunde. Weiterhin verarbeitet die Datenbank die Objekterstellung durch mehrere Benutzer, Aktualisierungen von Workflow-Prozessen, einfache historische Abfragen aus dem Sentinel Control Center und langfristige Berichte von Crystal Enterprise Server. Novell empfiehlt daher Folgendes:

- Die Datenbank sollte ohne andere Sentinel-Komponenten installiert werden.
- Der Datenbankserver sollte nur für Sentinel-Operationen vorgesehen sein. Zusätzliche Anwendungen (oder ETL-Prozesse) können sich negativ auf die Datenbankleistung auswirken.
- Für den Datenbankserver sollte ein Hochgeschwindigkeits-Speicher-Array vorhanden sein, das die E/A-Anforderungen auf der Grundlage der Einfügerate für Ereignisse erfüllt.

- Ein dedizierter DBA sollte in regelmäßigen Abständen die folgenden Aspekte der Datenbank auswerten:
  - Größe
  - E/A-Vorgänge
  - Festplattenspeicher
  - Arbeitsspeicher
  - Indizierung

In Umgebungen mit niedriger Ereignisrate (z. B. EPS < 25) müssen die obigen Empfehlungen nicht unbedingt beachtet werden, da die Datenbank und die übrigen Komponenten weniger Ressourcen verbrauchen.

Dieser Abschnitt enthält einige allgemeine Empfehlungen zur Hardware als Leitfaden für das Design des Sentinel-Systems. Grundsätzlich liegen den Empfehlungen für das Design Ereignisratenbereiche zugrunde. Bei den Empfehlungen wird jedoch von folgenden Annahmen ausgegangen:

- Die Ereignisrate liegt am oberen Ende des EPS-Bereichs.
- Die durchschnittliche Ereignisgröße beträgt 600 Byte.
- Alle Ereignisse werden in der Datenbank gespeichert (d. h., es sind keine Filter vorhanden, mit denen Ereignisse verworfen werden).
- Die Daten werden 30 Tage lang online in der Datenbank aufbewahrt.
- Der Speicherplatz für Advisor-Daten ist in den nachstehenden Spezifikationen nicht berücksichtigt.
- Der Sentinel-Server verfügt standardmäßig über 5 GB Festplattenspeicher für das temporäre Caching von Ereignisdaten, die nicht in die Datenbank übernommen werden konnten.
- Der Sentinel-Server verfügt weiterhin standardmäßig über 5 GB Festplattenspeicher für Ereignisse, die nicht in Aggregatereignisdateien geschrieben werden können.

Die Hardwareempfehlungen für eine Sentinel-Implementierung können je nach individueller Implementierung unterschiedlich sein. Es empfiehlt sich daher, vor der Fertigstellung der Sentinel-Architektur die Novell Consulting Services zu Rate zu ziehen. Die nachstehenden Empfehlungen können als Leitfaden dienen.

Hinweis: Aufgrund hoher Auslastung durch Ereignisse und der Notwendigkeit des lokalen Caching benötigt der Sentinel Server-Computer mit DAS ein lokales oder freigegebenes Disk-Array (RAID) mit Striping mit mindestens 4 Datenträgerspindeln.

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

Novell empfiehlt, Crystal Enterprise Server auf einem eigenen dedizierten Computer zu installieren, wenn es sich um eine große Datenbank handelt oder die Berichterstellung in hohem Maße genutzt wird. Crystal kann auf demselben Computer installiert werden wie die Datenbank, wenn es sich um eine kleine Datenbank handelt, die Berichterstellung nur wenig genutzt wird und die Datenbank entweder unter Windows oder unter Linux installiert ist.

Hinweis: Sentinel 6.0 befand sich noch in der Entwicklung, als dieses Dokument erstellt wurde. Daher basieren die folgenden Zahlen auf Tests mit Sentinel 5.1.3. Aktualisierte Informationen finden Sie auf der Novell-Dokumentationswebsite unter http://www.novell.com/documentation (http://www.novell.com/documentation).

1 - 500 EPS: Konfiguration mit 2 Computern (Sentinel 5.1.3)			
Komponenten	**RAM**	**Leerzeichen**	**Prozessor**
Computer 1: Sentinel Server / Collector Manager ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor ◆ Collector Manager / Collectors ◆ Datenbank ◆ Crystal Server (optional für Windows/Linux)	6 GB	250 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5150 (2,66 GHz) oder Sun Solaris – 4 x UltraSPARC IIIi (1,5 GHz)
Computer 2: Report Server ◆ Crystal Server	2 GB	20 GB	Windows oder Linux – 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

500 – 1500 EPS: Konfiguration mit 3 Computern (Sentinel 5.1.3)			
Komponenten	**RAM**	**Leerzeichen**	**Prozessor**
Computer 1: Sentinel Server / Collector Manager ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor ◆ Collector Manager / Collectors	4 GB	40 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 2: Datenbank ◆ Datenbank ◆ Crystal Server (optional für Windows/Linux)	4 GB+	1 TB+	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 3: Report Server (wird nur benötigt bei Sentinel/DB unter Solaris) ◆ Crystal Server	2 GB	20 GB	Windows oder Linux – 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)

1500 – 3000 EPS: Konfiguration mit 4 - 5 Computern (Sentinel 5.1.3)			
Komponenten	**RAM**	**Leerzeichen**	**Prozessor**
Computer 1: Sentinel Server ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor	4 GB	40 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 2: Datenbank ◆ Datenbank ◆ Crystal Server (optional für Windows/Linux)	8 GB+	3 TB+	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 3: Collector Manager ◆ Collector Manager / Collectors	2 GB	20 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) oder Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+
Computer 4: Report Server ◆ Crystal Server	4 GB	20 GB	Windows oder Linux – 1 x Dual Core Intel® Xeon® 5150 (2,66 GHz)
Computer 5: DAS-Komponente (benötigt bei EPS > 2000)	2 GB	40 GB	Windows oder Linux – 2 x Dual Core Intel® Xeon® 5160 (3,0 GHz) Sun Solaris – 2 x 1,8 GHz UltraSPARC IV+

2.3 Leistungsvergleichstests

In den folgenden Tabellen sind verschiedene repräsentative Konfigurationen und Testergebnisse beschrieben.

Diese Ratings dienen als Referenzpunkt für die Festlegung des Architekturdesigns und stellen keine starren Grenzwerte dar. In diesen Tests betrug die Systemauslastung nicht mehr als 75 %, und die Ereignisraten repräsentieren eine stabile Leistung.

Hinweis: Die Vergleichstests konzentrierten sich auf die in Sentinel eingefügten Ereignisse, die Korrelation und den Zuordnungsservice. Weitere Aktivitäten, zum Beispiel die Berichterstellung oder Verlaufsdatenabfragen, wurden bei den Tests nicht berücksichtigt.

Alle nachfolgend beschriebenen Tests wurden auf einem System mit RAID 5 mit Striping mit einer 4 + 1-Konfiguration durchgeführt.

2.3.1 Konfiguration für Machbarkeitsstudien oder als Demonstration

Diese Konfiguration mit einem einzigen Computer eignet sich für Demonstrationen oder eingeschränkte Machbarkeitsstudien und kann mit der Option „Einfach“ im Installationprogramm von Sentinel installiert werden. Es wird dringend empfohlen, diese Konfiguration nicht in einem Produktionssystem anzuwenden.

Hinweis: Sentinel 6.0 befand sich noch in der Entwicklung, als dieses Dokument erstellt wurde. Daher basieren die folgenden Zahlen auf Tests unter Sentinel 5.1.3. Aktualisierte Informationen finden Sie auf der Novell-Dokumentationswebsite unter http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Funktion	RAM	MODEL
Sentinel Server + DB + Collector Manager	5 GB, 5 x 36 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5150 2,66 GHz

Die folgenden Leistungskennzahlen wurden auf diesem System ermittelt.

Attribut	Rating	Kommentar
Pro Tag verarbeitete und gespeicherte Ereignisse (in DB)	86 Million	
Ereignisse pro Sekunde (Collector Manager)	1000	Eine einzelne Xeon CPU (Dual Core) wurde für Collector Manager verwendet.
Ereignisse pro Sekunde (Collector Engine)	300	Bei diesem Test wurden PIX, Snort und weitere Geräte eingesetzt.
Ereignisse pro Sekunde (SYSLOG)	300	1 Syslog-Server wurde auf dem Collector Manager-Host mit 1 Engine ausgeführt.
Pro Collector Manager-Instanz bereitgestellte Collectors	3	1 Collector verwendete syslog, die übrigen verwendeten einen Datei-Connector.
Anzahl der Collector Manager-Instanzen	1	Höchstzahl der unterstützten CM-Instanzen pro Sentinel Server: 20
Anzahl der bereitgestellten Correlation Engines	1	Wird auf dem Sentinel Server-Computer ausgeführt.
Festgelegte Regeln pro Correlation Engine	10	
Ausgeführte Active Views™	10	
Anzahl gleichzeitiger Benutzer	3	
Anzahl der Ansichten pro Active View-Instanz	2	
Anzahl der bereitgestellten Zuordnungen	2	
Größe der umfangreichsten Zuordnung im Zuordnungsservice	1.5 MB	

Attribut	Rating	Kommentar
Anzahl der Zeilen in der umfangreichsten Zuordnung	1.5 Million	

2.3.2 Konfiguration für ein Produktionssystem: Option 1

Diese Konfiguration beinhaltet drei Computer und es werden ca. 2.000 Ereignisse pro Sekunde verarbeitet.

Hinweis: Sentinel 6.0 befand sich noch in der Entwicklung, als dieses Dokument erstellt wurde. Daher basieren die folgenden Zahlen auf Tests unter Sentinel 5.1.3. Aktualisierte Informationen finden Sie auf der Novell-Dokumentationswebsite unter http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Funktion	RAM	MODEL
Sentinel Server	4 GB, 5 x 36 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5150 2,66 GHz
Datenbank	4 GB, 5 x 250 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5150 2,66 GHz
Collector Manager	2 GIG, 72 GIG	SLES9 – 1 x Dual Core Intel® Xeon® 5150 2,66 GHz

Die folgenden Leistungskennzahlen wurden auf diesem System ermittelt:

Attribut	Rating	Kommentar
Pro Tag verarbeitete und gespeicherte Ereignisse (in DB)	173 Million	
Ereignisse pro Sekunde (Collector Manager)	2000	Eine einzelne Xeon CPU (Dual Core) wurde für Collector Manager verwendet.
Ereignisse pro Sekunde (Collector Engine)	1200	Bei diesem Test wurden PIX, Snort und weitere Geräte eingesetzt.
Ereignisse pro Sekunde (SYSLOG)	1200	1 Syslog-Server wurde auf dem Collector Manager-Host mit 1 Engine ausgeführt.
Pro Collector Manager-Instanz bereitgestellte Collectors	10	1 Collector verwendete syslog, die übrigen verwendeten einen Datei-Connector.
Anzahl der Collector Manager-Instanzen	1	Höchstzahl der unterstützten CM-Instanzen pro Sentinel Server: 20
Bereitgestellte Correlation Engines	1	Wird auf dem Sentinel Server-Computer ausgeführt.
Festgelegte Regeln pro Correlation Engine	20	
Ausgeführte Active Views™	20	
Anzahl gleichzeitiger Benutzer	5	

Attribut	Rating	Kommentar
Anzahl der Ansichten pro Active View-Instanz	4	
Anzahl der bereitgestellten Zuordnungen	4	
Größe der umfangreichsten Zuordnung	1.5 MB	
Anzahl der Zeilen in der umfangreichsten Zuordnung	1.5 Million	

2.3.3 Konfiguration für ein Produktionssystem: Option 2

Diese Konfiguration erfordert vier Computer und es werden ca. 3.000 Ereignisse pro Sekunde verarbeitet.

Hinweis: Sentinel 6.0 befand sich noch in der Entwicklung, als dieses Dokument erstellt wurde. Daher basieren die folgenden Zahlen auf Tests unter Sentinel 5.1.3. Aktualisierte Informationen finden Sie auf der Novell-Dokumentationswebsite unter http://www.novell.com/documentation/index.html (http://www.novell.com/documentation/index.html).

Funktion	RAM	MODEL
Sentinel Server	4 GB, 5 x 36 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Datenbank	8 GB, 5 x 250 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Collector Manager	2 GB, 72 GB	SLES9 – 2 x Dual Core Intel® Xeon® 5160 3,0 GHz
Sentinel Server (DAS – Knoten 2)	2 GB, 5 x36 GB RAID	SLES9 – 2 x Dual Core Intel® Xeon® 5160 3,0 GHz

Die folgenden Leistungskennzahlen wurden auf diesem System ermittelt:

Attribut	Rating	Kommentar
Pro Tag verarbeitete und gespeicherte Ereignisse (in DB)	260 Million	
Ereignisse pro Sekunde (Collector Manager)	3000	Für Collector Manager wurde eine duale Xeon CPU (Dual Core) verwendet.
Ereignisse pro Sekunde (Collector Engine)	1200	Bei diesem Test wurden PIX, Snort und weitere Geräte eingesetzt.
Ereignisse pro Sekunde (SYSLOG)	2500	Auf dem Collector Manager-Host wurde ein Syslog-Server ausgeführt.
Pro Collector Manager-Instanz bereitgestellte Collectors	10	3 Collectors verwendeten syslog, die übrigen verwendeten einen Datei-Connector
Anzahl der Collector Manager-Instanzen	1	

Attribut	Rating	Kommentar
Bereitgestellte Correlation Engines	1	Wird auf dem Sentinel Server-Computer ausgeführt.
Festgelegte Regeln pro Correlation Engine	20	
Ausgeführte Active Views™	20	
Anzahl gleichzeitiger Benutzer	5	
Anzahl der Ansichten pro Active View-Instanz	4	
Anzahl der bereitgestellten Zuordnungen	4	
Größe der umfangreichsten Zuordnung	1.5 MB	
Anzahl der Zeilen in der umfangreichsten Zuordnung	1.5 Million	

2.4 Konfiguration für Disk-Array

Der Novell Sentinel-Server in einer Produktionskonfiguration erfordert ein Hochgeschwindigkeits-Disk-Array für die Datenbank und die Sentinel-Hosts. Dieser Abschnitt behandelt typische Empfehlungen für die Datenträgerkonfiguration (RAID). Die folgenden Funktionen werden durch die Leistung der Datenträgerhardware beeinflusst:

- Datenbankkomponente (Microsoft SQL/Oracle): Die Ereignisrate (Ereignisse pro Sekunde) und die Abfragefunktionen werden beeinflusst (einschließlich Verlaufsereignisabfrage, Offline-Abfrage und Crystal Reporting).
- DAS-RT (Data Access Service Real Time-Komponente): Die Active View-Funktion wird beeinflusst.
- DAS-Aggregation: Die Anzahl der Zusammenfassungen, die aktiviert werden können, wird beeinflusst.

2.4.1 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 – Datenbank (Daten, Indizes, Transaktionsprotokolle usw.)
- RAID-Gruppe 2 – Sentinel Server DAS (Datenverzeichnis, Temp DIR*)
- Datenträger (mindestens): 13 pro RAID-Gruppe
- Datenträgertyp: 12K + RPM, Glasfaserkanal oder SCSI
- LUN 1 (RAID-Gruppe 1): 5 GB – 144 GB+ pro Datenträger
- LUN 2 (RAID-Gruppe 2): 5 GB – 144 GB+ pro Datenträger

2.4.2 Optimale Konfiguration

Für eine Konfiguration mit optimaler Leistung und Redundanz kann ein RAID 1+0 mit denselben Einstellungen wie oben verwendet werden. Es sind jedoch möglicherweise weitere RAID-Gruppen und LUNs gemäß den obigen Richtlinien erforderlich, um weiteren Parallelismus und weitere E/A für bestimmte Datenbanken zu erzielen.

Hinweis: Weitere Informationen dazu, wie DAS TEMP DIR auf einen anderen Speicherplatz verwiesen wird, finden Sie unter Abschnitt 2.7, „Installation und Konfiguration von Sentinel“, auf Seite 34

2.4.3 Speicherkonfiguration für eine Microsoft SQL-Installation: Beispiel

In diesem Beispiel wird das Speichersubsystem EMC2 CLARiiON mit folgenden Eigenschaften verwendet:

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

RAID-Gruppen

Array	LUN	RAID-Typ	RAID-Gruppe	Größe (GB)
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)	Speicherprozessor	Name
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1

Array	LUN	RAID-Typ	RAID-Gruppe	Größe (GB)	Speicherprozessor	Name
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	Laufwerkbuchstabe	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
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

2.4.4 Speicherkonfiguration für eine Oracle-Installation: Beispiel

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

2.5 Netzwerkkonfiguration

Sentinel Server-seitige Komponenten: Diese Komponenten sollten über einen einzelnen 1 GB-Switch miteinander 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 Server verbunden sein.

2.6 Optimale Verfahren: Datenbankinstallation/-konfiguration

Hinweis: Die meisten Installationsparameter für die Datenbank können nach der Datenbankinstallation über Datenverwaltungswerkzeuge oder die Befehlszeile geändert werden.

1. Sentinel bedient sich einer vordefinierten Archivierungsstrategie zur Verwaltung der schnell anwachsenden Tabellen (beispielsweise Ereignistabelle). Diese Tabellen sind partitioniert und ältere Partitionen können archiviert und abgelegt werden, ohne dass sich dies auf neuere Daten auswirkt. Andere Tabellen hingegen sind durch dieses Partitionierungs- und Archivierungsschema nicht abgedeckt und müssen separat verwaltet werden.
2. Um eine möglichst hohe Leistung zu erzielen, sollten die folgenden Protokolle auf der Festplatte mit der höchsten Schreibgeschwindigkeit installiert werden, sofern die Installation in RAID erfolgt und die RAID-Umgebung dies zulässt.
   - Wiederherstellungsprotokoll (Oracle)
   - Transaktionsprotokoll (Microsoft SQL)
3. 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.
4. Zu Wiederherstellungszwecken sollte ein DBA in regelmäßigen Abständen geplante Sicherungen der nicht partitionierten Tabellen in der Datenbank durchführen.
5. Bei Oracle-Installationen deaktiviert das Sentinel-Installationsprogramm 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, wenn die Kapazitätsgrenze des Protokollziels erreicht ist.
6. Zur Erzielung einer möglichst hohen Leistung in Umgebungen mit hohen Ereignisraten sollten die Speicherorte auf andere Orte (z. B. andere Festplattencontroller) verweisen, um E/A-Konflikte zu verhindern.
   - Datenverzeichnis
   - Indexverzeichnis
   - Zusammenfassungsdatenverzeichnis

- Zusammenfassungsindexverzeichnis
- Protokollverzeichnis (nur Microsoft SQL)
- Temporäres Verzeichnis und Tabellenbereichs-Verzeichnis zum Rückgängigmachen (nur Oracle)
- Verzeichnis für Redo-Protokollmitglied A (nur Oracle)
- Verzeichnis für Redo-Protokollmitglied B (nur Oracle)

2.6.1 Sentinel-Datenbank-Patches

Nur bei Microsoft 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.

2.6.2 Empfohlene UNIX-Kernel-Einstellungen für Oracle

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 dazu, wie Sie Kernel-Parameter unter Linux anzeigen und festlegen, finden Sie in Kapitel 3, „Installieren von Sentinel 6“, auf Seite 45 im Installationshandbuch.

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

Mindestwerte für Kernel-Parameter für Solaris

Überprüfen Sie die UNIX-Kernel-Parameter 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
```

2.6.3 Konfigurieren von Parametern beim Erstellen der eigenen Datenbankinstanz

Die Datenbankstruktur (bis zur Tabellenbereichsebene) können Sie bei Bedarf statt durch das Sentinel-Installationsprogramm auch manuell erstellen. Bei der Installation können Sie dann die Option „Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen“ auswählen. Die folgenden Einstellungen werden für das Erstellen Ihrer eigenen Datenbankinstanz empfohlen. Die Einstellungen können je nach Systemkonfiguration und Anforderungen unterschiedlich sein.

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
ESENTD	5 G	Mindestwert Für Ereignisdaten

Empfohlene Mindestgröße für den Tabellenbereich		
Tabellenbereich	**Beispielgröße**	**Hinweise**
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

2.7 Installation und Konfiguration 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 dazu, welche Dateien entfernt werden sollten, finden Sie in Kapitel 11, „Deinstallieren von Sentinel“, auf Seite 157 im Installationshandbuch.
2. Die Leistung von Active Views und der Zuordnung kann erheblich 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:

2a Erstellen Sie auf der schnellen Festplatte ein Verzeichnis für die temporären Dateien. Unter UNIX müssen der Sentinel-Administratorbenutzer und die Gruppe „esec“ Inhaber dieses Verzeichnisses sein und über Schreibrechte dafür verfügen.

2b Erstellen Sie eine Sicherungskopie der Datei %ESEC_HOME%\config\configuration.xml.

2c Öffnen Sie die Datei %ESEC_HOME%\config\configuration.xml in einem Texteditor.

2d 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.

2e Um diese Änderung für den DAS_RT-Prozess vorzunehmen, suchen Sie nach der Zeile mit dem Text

```
-Dsrv_name=DAS_RT
```

und fügen Sie das angegebene Argument daneben hinzu.

```
-Djava.io.tmpdir=<tmp_directory>
```

Nachfolgend finden Sie ein Beispiel dafür, wie die Zeile aussehen sollte (die Argumennte –Xmx, -Xms und –XX können abweichen):

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

2f Um diese Änderung für den DAS_Query-Prozess vorzunehmen, suchen Sie nach der Zeile mit dem Text

```
-Dsrv_name=DAS_Query
```

und fügen Sie das angegebene Argument daneben hinzu.

```
-Djava.io.tmpdir=<tmp_directory>
```

Nachfolgend finden Sie ein Beispiel dafür, wie die Zeile aussehen sollte (die Argumennte –Xmx, -Xms und –XX können abweichen):

```
<process component="DAS" image="&amp;quot;$(ESEC_JAVA_HOME)/
java&amp;quot; -server -Dsrv_name=DAS_Query -
Djava.io.tmpdir=D:\Temp2 -Xmx256m -Xms85m -XX:+UseParallelGC -
Xss128k -Xrs -Desecurity.dataobjects.config.file=/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml -
Djava.util.logging.config.file=../config/das_query_log.prop -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../../lib/krb5.conf -
Desecurity.execution.config.file=../config/execution.properties
-Dcom.esecurity.configurationfile=../../configuration.xml -jar
../../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" post_startup_delay="5" shutdown_command="cmd
//C &amp;quot;$(ESEC_HOME)/bin/stop_container.bat&amp;quot; localhost
DAS_Query" working_directory="$(ESEC_HOME)/bin"/>
```

2.8 Festlegen von Passwörtern – Optimale Verfahren

So werden die für die Common Criteria Certification erforderlichen strikten Sicherheitskonfigurationen eingehalten:

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 weder Ihren Email-Namen noch 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).

2.9 Berichtkonfiguration

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 von Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren. Hierfür können Sie entweder Central Configuration Manager oder die Crystal-Webseite verwenden.

So konfigurieren Sie Crystal Page Server über Central Configuration Manager neu

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 Folgendes hinzu:

   ```
   maxDBResultRecords <value greater than 20000 or 0 to disable the
   default limit>
   ```

5. Starten Sie Crystal Page Server neu.

So konfigurieren Sie Crystal Page Server über die Crystal-Webseite neu

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 Hostcomputers 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 "Anwenden".
9. Sie werden aufgefordert, den Page Server erneut zu starten. Klicken Sie auf OK (OK).

Möglicherweise werden Sie zur Eingabe eines Anmeldenamens und eines Passworts für den Zugriff auf den Service-Manager des Betriebssystems aufgefordert.

So konfigurieren Sie Crystal Page Server neu (Crystal-Server unter Linux oder Windows)

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

   Für Linux Crystal Servers:

   ```
   http://<DNS or IP of Crystal Server>:8080/businessobjects/
   enterprise11/adminlaunch
   ```

   Für Window Crystal Servers:

   ```
   http://<DNS name or IP address of your web server>/businessobjects/
   enterprise11/WebTools/adminlaunch/default.aspx
   ```
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Hostcomputers 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 "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.

2.9.1 Von Sentinel bereitgestellte Berichte

Zur Verbesserung der Leistung fragen die wichtigsten 10 Berichte anstelle der Ereignistabelle Zusammenfassungstabellen ab. Die Zusammenfassungstabellen enthalten eine Anzahl von Ereignissen aus einem gewissen Zeitraum für Kombinationen aus Feldern in den Ereignisdaten. Die Gruppe der Daten für bestimmte Abfragearten wird auf diese Weise wesentlich kleiner. Außerdem führt dies zu erheblich schnelleren Abfragen und einer kürzeren Berichtlaufzeit.

Der Aggregatservice ist für das Auffüllen der Zusammenfassungstabellen mit Zusammenfassungen aller Ereignisse aus der Ereignistabelle verantwortlich. Der Aggregatservice generiert zusammengefasste Daten nur für aktive Zusammenfassungen. Die folgenden Zusammenfassungen werden von den wichtigsten 10 Berichten benötigt und sind standardmäßig aktiviert:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Zusammenfassungen können im Sentinel Control Center auf der Registerkarte „Admin“ im Fenster „Berichtdatenkonfiguration“ aktiviert oder deaktiviert werden.

Der Aggregatservice ist darüber hinaus davon abhängig, dass die Komponente EventFileRedirectService in DAS Binary die Ereignisdaten zur Verfügung stellt, die dieser Service zusammenfasst. Diese Komponente muss also aktiviert sein, damit der Aggregatservice ordnungsgemäß ausgeführt wird. Die Komponente wird aktiviert oder deaktiviert, indem das Attribut „Status“ der Komponente EventFileRedirectService in der Datei das_binary.xml auf „Ein“ oder „Aus“ gesetzt wird. Standardmäßig ist die Komponente aktiviert.

Hinweis: Informationen zu EventFileRedirectService und den drei Aggregatzusammenfassungen finden Sie im Kapitel zu Sentinel Data Manager im Sentinel Control Center-Benutzerhandbuch oder im Kapitel zu Crystal Reports für Windows und in Kapitel 10, „Crystal Reports für Linux“, auf Seite 141 im Sentinel-Installationshandbuch.

Hinweis: Die Ausführung von Berichten, mit denen ein großer Datenbereich abgefragt wird, nimmt möglicherweise einige Zeit in Anspruch. Derartige Berichte sollten geplant und nicht interaktiv ausgeführt werden. Informationen zur Planung von Crystal Reports-Berichten finden Sie in der Dokumentation zu Crystal BusinessObjects Enterprise™ 11.

2.9.2 Tipps für die Entwicklung benutzerdefinierter Crystal-Berichte

Für benutzerdefinierte Berichte wird Folgendes empfohlen:

1. Wenn die Berichte vordefinierte aggregierte Tabellen verwenden können, wählen Sie diejenige aggregierte Tabelle aus, bei der die wenigsten Daten verarbeitet werden.
2. Versuchen Sie, einen möglichst großen Teil der Verarbeitung auf die Datenbank-Engine zu verlagern.
3. Um den Verarbeitungs-Overhead in Crystal Server zu verringern, sollten Sie die in Crystal Server zu ladende Datenmenge so gering wie möglich halten.
4. Erstellen Sie Berichte stets für die von Novell zur Verfügung gestellten Datenbankansichten und nicht für die Basistabellen.

2.10 Datenbankwartung

Sentinel speichert alle Ereignisse sowie die Konfigurationsdaten in der Backend-Datenbank. Diese Datenbank muss sorgfältig verwaltet werden, um sicherzustellen, dass sie stets effizient genutzt werden kann.

2.10.1 Ereignisinformationen in der Datenbank

Der größte Teil der Datenbank besteht aus normalisierten und zusammengefassten Ereignisdaten. Zur Vereinfachung der Verwaltung dieser stetig anwachsenden Datenmenge partitioniert Novell die Tabellen und stellt als Verwaltungswerkzeug Sentinel Data Manager zum Archivieren und Löschen älterer Partitionen zur Verfügung. Es empfiehlt sich, einen Archivierungsplan zu entwickeln, der automatisiert werden kann, um die Benutzerinteraktion möglichst gering zu halten.

Hinweis: Weitere Informationen zu Sentinel Data Manager finden Sie im Kapitel zu "Sentinel Data Manager" im Sentinel Control Center-Benutzerhandbuch.

2.10.2 Weitere Informationen in der Datenbank

Die Sentinel-Datenbank enthält noch zahlreiche weitere Informationen, zum Beispiel Benutzerkonten, Konfigurationsinformationen, Vorfälle, Workflows, Bestandsdaten und Anfälligkeitsdaten. All diese Daten müssen mit normalen Datenbankwerkzeugen gesichert werden, damit sie bei Datenverlust wiederhergestellt werden können. Novell empfiehlt die Entwicklung einer umfassenden Sicherungsstrategie für die gesamte Sentinel-Datenbank (sowie die Server), mit Ausnahme der obigen partitionierten Tabellen.

Bei Verwendung von SQL Server werden Sentinel-Datenbanken standardmäßig gemäß dem Modell für die 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 4 mal 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.

2.10.3 Weitere Datenbankwartung

Zusätzlich zu der Sicherung sollte die Datenbank regelmäßig auf interne Konsistenz überprüft werden. Novell stellt hierfür einige automatisierte Werkzeuge zur Verfügung. Weitere Informationen hierzu finden Sie im Sentinel-Benutzerhandbuch.

Zu diesen Dienstprogrammen gehören:

- Analyze Partitions (Partitionsanalyse) – Sammelt Partitionsstatistiken für Partitionen, die kürzlich mit Daten gefüllt wurden.
- Database Health Check (Zustandsprüfung der Datenbank) – 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.

Hinweis: Diese Dienstprogramme stellen keinen Ersatz für eine regelmäßige Datenbankwartung durch einen qualifizierten DBA dar.

Datenbankanalyse für Oracle

Da Ereignisse laufend 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 prüfen, ob auf der Novell-Website für den technischen Support (http://support.novell.com/techselect/index.html) Aktualisierungen vorliegen.

Analyze Partitions

Das Skript AnalyzePartitions.sh analysiert Partitionen, die vor Kurzem mit Daten gefüllt wurden. Dieses Skript sollte über Cron oder einen anderen Planer für die tägliche Ausführung geplant werden, um Datenbankstatistiken auf Partitionen zu aktualisieren, die am vorherigen Tag aufgefüllt wurden. Es empfiehlt sich, das Skript zu einer Tageszeit mit geringer Datenbankauslastung auszuführen.

Das Skript befindet sich im Verzeichnis $ESEC_HOME/bin. 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.

So installieren Sie sp_esec_dba_utl.sql

1. Melden Sie sich als Eigentümer der Oracle-Software an.
2. Stellen Sie unter Verwendung von SQL*Plus als Sentinel-Datenbankbenutzer eine Verbindung zu 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.

So führen Sie AnalyzePartitions.sh aus

1. Wechseln Sie auf dem Computer mit dem Oracle-Datenbankserver in das Verzeichnis:
   ```
   $ESEC_HOME/bin/
   ```
   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> >> <LogFileName>
   ```

Für Linux:

```
ksh ./AnalyzePartitions.sh <ORACLE_SID> >> <LogFileName>
```

- 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.

2.10.4 Database Health Check für Oracle

Das Skript dbHealthCheck.sh sammelt Informationen über die Sentinel-Datenbank unter Oracle. Das Skript dbHealthCheck.sh befindet sich im Ordner %esec_home%\bin. 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 prüfen, ob auf der Novell-Website für den technischen Support (http://support.novell.com/techselect/index.html) Aktualisierungen vorliegen.

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.

So installieren Sie 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 unter Verwendung von SQL*Plus als Sentinel-Datenbankbenutzer eine Verbindung zu 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.

So führen Sie dbHealthCheck.sh aus

Hinweis: Das Skript muss über das Konto 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 >> <filename>`

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 >> <filename>`

2.10.5 Datenbankwartung

Die Datenbankpartitionierung wird automatisch bei der Installation von Sentinel konfiguriert. Der Administrator sollte die Einstellungen in Sentinel Data Manager überprüfen und bei Bedarf anpassen. Weitere Informationen zu Sentinel Data Manager finden Sie im entsprechenden Kapitel im Sentinel-Benutzerhandbuch.

2.11 Correlation Engine

2.11.1 Zeitsynchronisierung

Die Sentinel Correlation Engine ist äußerst zeitempfindlich. Daher empfiehlt Novell dringend, alle Computer mit Correlation Engine und Collector Manager mit einem NTP-Server (Network Time Protocol) oder einer anderen Art von Zeitserver zu verbinden. Damit die Sentinel Correlation Engine ordnungsgemäß arbeitet, muss die Systemzeit aller Computer mit Collector Manager innerhalb von ± 30 Sekunden synchronisiert werden.

2.11.2 Speichernutzung

In der Korrelationsregelsprache ist den beiden Operatoren „Fenster“ und „Auslöser“ ein Zeitfenster zugeordnet. Je größer das Zeitfenster, um so mehr Ereignisinformationen können für das betreffende Zeitfenster im Arbeitsspeicher abgelegt werden. Dies wirkt sich auf den Umfang des Arbeitsspeichers aus, der für die Arbeitsspeicher-Korrelation von Sentinel benötigt wird. Wenn die Correlation Engine zu viel Arbeitsspeicher verbraucht, sollten Sie Folgendes in Erwägung ziehen:

- Installieren Sie die Correlation Engine auf einem dedizierten Computer und stellen Sie alle aktuellen Regeln für die neue Correlation Engine erneut bereit.
- Installieren Sie eine neue Correlation Engine und stellen Sie ausgewählte aktuelle Regeln für die neue Correlation Engine erneut bereit.
- Optimieren Sie die Fenster-Klausel der Korrelationsregeln.
  - Geben Sie einen spezifischeren Filter für vergangene Ereignisse an.
  - Verkleinern Sie das Zeitfenster.
- Optimieren Sie die Auslöser-Klausel der Korrelationsregeln.
  - Verkleinern Sie das Zeitfenster.
  - Setzen Sie den Schwellwert für die Anzahl der Ereignisse herab, die zur Auslösung der Regel erforderlich sind.
  - Wählen Sie Diskriminatoren mit einer niedrigen Kardinalität aus (z. B. Gerätetyp).
  - Wenn der Diskriminator eine niedrige Kardinalität aufweist (z. B. Quell-IP-Adresse), setzen Sie den Schwellwert für die Anzahl der Ereignisse herab, die zur Auslösung der Regel erforderlich sind. Verkleinern Sie gleichzeitig das Zeitfenster, um ein äquivalentes Ergebnis zu erhalten.

2.11.3 Kurzschlussanalyse

Zahlenvergleiche werden schneller durchgeführt als Zeichenkettenvergleiche, die wiederum schneller durchgeführt werden als Vergleiche zwischen regulären Ausdrücken. Die Filteroperation führt eine Kurzschlussanalyse für die booleschen Ausdrücke durch. Durch eine sorgfältige Anordnung des Ausdrucks können Sie eventuell die Evaluierungsgeschwindigkeit erhöhen.

2.11.4 Formfreie Regeln

Wenn eine Korrelationsregel nicht mit dem Assistenten für Korrelationsregeln ausgedrückt werden kann, können Sie mithilfe der Korrelationsregelsprache eine formfreie Regel erstellen. Weitere Informationen zum Erstellen formfreier Regeln finden Sie unter “Correlation Engine” im Referenzhandbuch.

2.12 Sentinel-Protokolldateien

Es ist sinnvoll, die von Sentinel generierten Protokolldateien in regelmäßigen Abständen auf Fehler zu prüfen. Weitere Informationen zu diesen Dateien und ihren Speicherorten finden Sie im Kapitel zu “Sentinel-Protokollspeicherorten” im Referenzhandbuch.

Installieren von Sentinel 6

3

In diesem Kapitel werden die folgenden Themen behandelt:

3.1 Installieren von Sentinel unter Linux, Solaris und Windows

In diesem Kapitel erhalten Sie Unterstützung zur Installation von Sentinel für Oracle unter SUSE Linux Enterprise Server, Red Hat Enterprise Linux und Solaris sowie Microsoft SQL Server unter Windows.

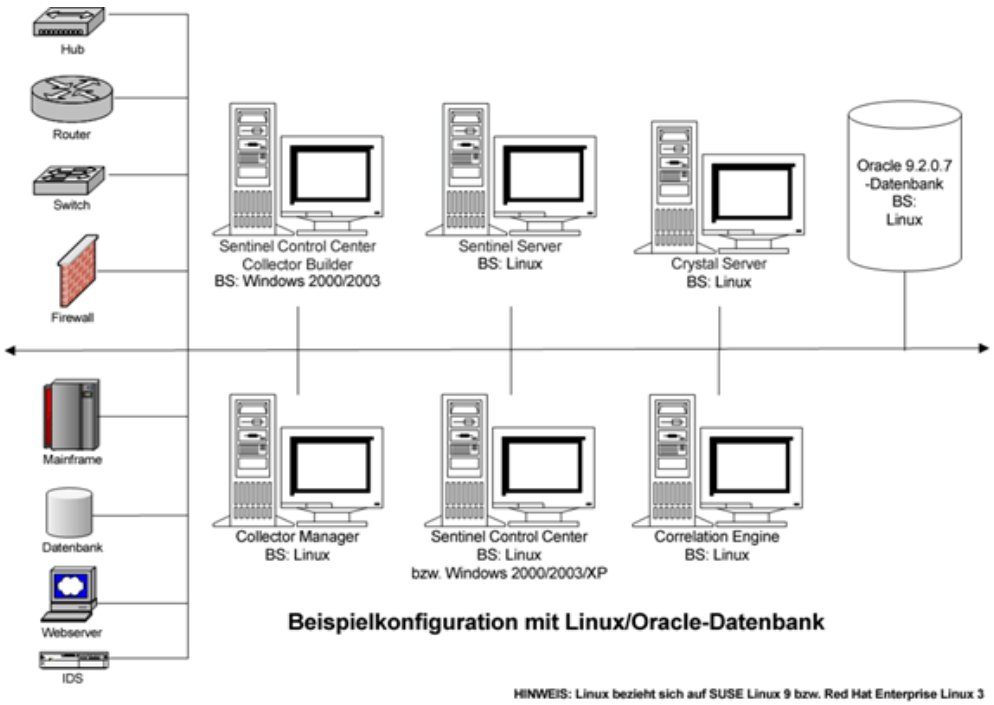
Wenn Sie eine Neuinstallation von Sentinel durchführen möchten, nachdem eine frühere Version von Sentinel deinstalliert wurde, müssen Sie evtl. noch aus einer früheren Version übrig gebliebene Dateien und Systemeinstellungen manuell entfernen. Weitere Informationen zum Deinstallieren von Sentinel 6.0 finden Sie in Kapitel 11, „Deinstallieren von Sentinel“, auf Seite 157. Informationen zum Deinstallieren früherer Versionen von Sentinel finden Sie in den jeweiligen Dokumentversionen auf der Novell-Dokumentationswebsite unter http://www.novell.com/documentation/ (http://www.novell.com/documentation/).

Hinweis: Für die Installation von Sentinel Server unter SLES empfiehlt Novell die Verwendung eines anderen Dateisystems als ReiserFS, da bei der Ausführung von Sentinel unter SLES mit ReiserFS zeitweise Probleme aufgetreten sind. Obwohl zahlreiche Möglichkeiten zur Auswahl stehen, wurden die internen Sentinel-Tests bei Novell mit dem Dateisystem ext3 durchgeführt.

3.1.1 Konfiguration von Sentinel

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.

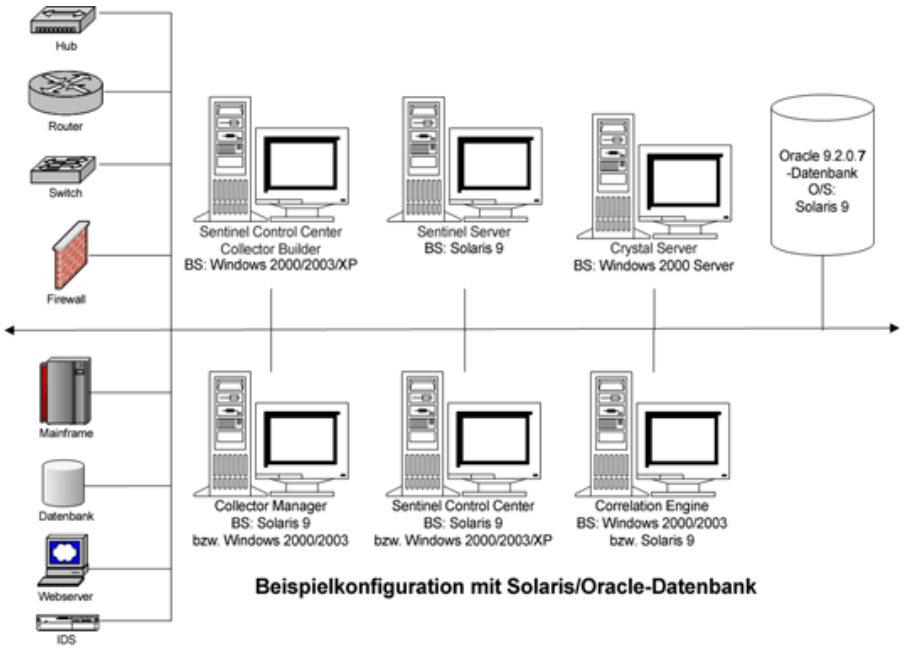
Unter Linux



Beispielkonfiguration mit Linux/Oracle-Datenbank

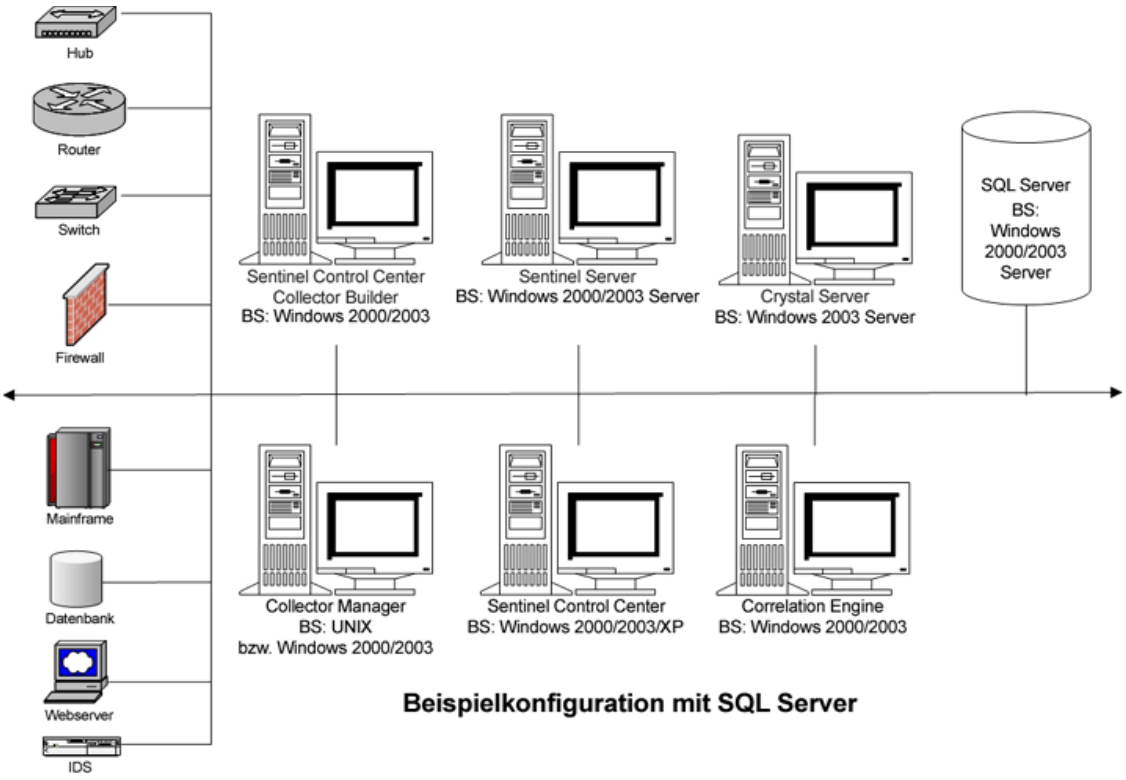
HINWEIS: Linux bezieht sich auf SUSE Linux 9 bzw. Red Hat Enterprise Linux 3

Unter Solaris



Beispielkonfiguration mit Solaris/Oracle-Datenbank

Unter Windows



Beispielkonfiguration mit SQL Server

3.1.2 Voraussetzungen für die Installation von Sentinel 6.0

Bevor Sie Sentinel installieren, müssen Sie Folgendes sicherstellen:

- Ihre Computer müssen die Mindestsystemanforderungen erfüllen und das Betriebssystem muss durch die besten zurzeit verfügbaren Sicherheitsvorkehrungen geschützt sein. Weitere Informationen hierzu finden Sie in Kapitel 2, „Optimale Verfahren“, auf Seite 19
- Installieren Sie für die Installation von Sentinel unter Solaris und Linux Oracle Enterprise mit Partitionierung. Der Sentinel Data Manager benötigt diese Funktion zur Verwaltung der Sentinel-Datenbank.
- Die erforderlichen Bedingungen für die Installation der folgenden Komponenten sind erfüllt:
  - Sentinel-Datenbank
  - Sentinel Server
  - Sentinel Control Center und Sentinel Collector Builder
  - Sentinel Advisor
- Oracle wurde unter Linux, SUSE Linux, Red Hat Linux und Solaris installiert.

Sentinel-Datenbank

Bevor die Sentinel-Datenbank installiert wird, benötigen Sie Folgendes:

Unter Linux/Solaris:

- Unter Linux die Anmeldeberechtigung für das Oracle-Betriebssystem (Standard: „oracle“).
- Unter Solaris:
  - Eine Kopie von Oracle 148673.1 SOLARIS: Quick Start Guide
  - Den Oracle-Betriebssystembenutzer (Standard: oracle).
- Stellen Sie unter Linux/Solaris sicher, dass die folgenden Umgebungsvariablen für den Oracle-Betriebssystembenutzer festgelegt wurden:
  - ORACLE_HOME (Beispiel: echo $ORACLE_HOME bringt /opt/oracle/product/10gR2/db hervor)
  - ORACLE_BASE (Beispiel: echo $ORACLE_BASE bringt /opt/oracle hervor)
  - PATH (muss enthalten $ORACLE_HOME/bin)
- Wenn Sie beabsichtigen, die Oracle-Datenbankinstanz, in der die SentinelDatenbank installiert wird, manuell zu erstellen (auch wenn diese Vorgehensweise NICHT empfohlen wird), finden Sie im Abschnitt zur “Datenbankerstellung und -konfiguration für hohe Ereignisraten” Anweisungen zum Erstellen der Oracle-Instanz, damit diese mit Sentinel kompatibel ist. Wenn Sie diese Option auswählen, müssen Sie dennoch das Sentinel-Installationsprogramm verwenden, um der manuell erstellten Oracle-Datenbankinstanz die Datenbankobjekte hinzuzufügen. Weitere Informationen hierzu finden Sie in Abschnitt 3.3.2, „Angepasste Installation“, auf Seite 62

Hinweis: Falls Sie eine vorhandene oder manuell erstellte Oracle-Datenbankinstanz verwenden, darf diese nur den Sentinel-Datenbankbenutzer enthalten (d. h., sie muss ansonsten leer sein).

Unter Windows:

- Unter Windows muss SQL Server 2005 SP1 installiert sein und ausgeführt werden.

Hinweis: Damit eine optimale Leistung gewährleistet werden kann, wird DRINGEND empfohlen, dass bei einer RAID-Installation und falls hre RAID-Umgebung dies zulässt, das System so konfiguriert wird, dass das Transaktionsprotokoll auf die schnellste beschreibbare Festplatte verweist, bei der es sich um einen eigenen physischen Datenträger handelt, auf dem die Datenbankdateien gespeichert sind.

- Unter Windows muss SQL Server mit der Authentifizierung für den gemischten Modus installiert werden, damit die Anmeldung sowohl mit der Windows- als auch mit der SQL Server-Authentifizierung möglich ist. Wird SQL Server für den nicht gemischten Modus installiert, kann die Anmeldung nur mit der Windows-Authentifizierung durchgeführt werden.
- So ändern Sie die Einstellungen für den Authentifizierungsmodus
  - Klicken Sie in Microsoft SQL Server Management Studio mit der rechten Maustaste auf den Server, dessen Einstellungen Sie ändern möchten.
  - Wählen Sie „Eigenschaften“ aus, und klicken Sie auf „Sicherheit“.
  - Wählen Sie für die Authentifizierung eine der beiden folgenden Optionen aus: „SQL Server- und Windows-Authentifizierungsmodus“ oder „Windows-Authentifizierungsmodus“.
  - Stellen Sie darüber hinaus sicher, dass sich der MSSQLSERVER-Service mit dem lokalen Systemkonto anmeldet.

- Bestimmen Sie den Namen der SQL Server-Instanz (Standard empfohlen).

  Hinweis: Falls Sie die Instanz bei der Installation von SQL Server benannt haben, verwenden Sie diesen Namen, wenn Sie bei der Installation der Sentinel-Datenbank und/oder der DAS-Komponenten zur Eingabe des Namens der SQL Server-Instanz aufgefordert werden. Wenn Sie die Instanz bei der Installation von SQL Server nicht benannt haben, lassen Sie den Instanznamen während der Installation leer (d. h., wenn Sie den Hostnamen eingeben, fügen Sie nicht „\<Instanzname>“ zum Hostnamen der Datenbank hinzu).

- Bestimmen Sie die Portnummer der SQL Server-Instanz (Standard: 1433).
- Wenn Sie die Windows-Authentifizierung für einen oder mehrere der bei der Sentinel-Installation verwendeten Sentinel-Benutzer nutzen, muss der entsprechende Windows-Domänenbenutzer bereits vor der Installation der Sentinel-Datenbank vorhanden sein. Folgende Sentinel-Benutzer können einem Windows-Domänenbenutzer zugewiesen werden:
  - Sentinel-Datenbankadministrator („esecdba“, der Eigentümer des Datenbankschemas)
  - Sentinel-Anwendungsbenutzer („esecapp“, von Sentinel-Anwendungen für die Verbindung mit der Datenbank verwendet)
  - Sentinel-Administrator („esecadm“, Administrator für die Anmeldung an Sentinel Control Center)
  - Sentinel Report-Benutzer („esecrpt“, für das Erstellen von Berichten verwendet)

  Hinweis: Die Datenbank enthält standardmäßig den Sentinel-Datenbankadministratorbenutzer, den Sentinel-Anwendungsbenutzer und den Sentinel-Administrator.

Hinweis: Sentinel bietet keine Unterstützung für Microsoft Clustering oder High Availability für Windows.

Sentinel Server

Hinweis: Wenn Sie die Sentinel-Datenbank nicht auf demselben Computer wie Sentinel Server installieren, muss die Sentinel-Datenbank zuerst installiert werden.

- Falls die DAS-Komponente installiert wird, halten Sie die Sentinel-Seriennummer und den Lizenzschlüssel (für DAS) bereit.
- Entscheiden Sie sich für einen SMTP-Server (DNS-Name). Dies ist erforderlich, um Emails von Sentinel zu senden.
- Unter Windows muss einem Benutzer die Berechtigung „Als Dienst anmelden“ zugewiesen werden, falls DAS installiert und ein Benutzerkonto einer Windows-Domäne für die Sentinel-Anwendung verwendet wird. So weisen Sie diese Berechtigung zu
  - Fügen Sie den Benutzer auf dem Computer, auf dem DAS installiert werden soll, unter „Lokale Sicherheitsrichtlinie“ hinzu („Start“ > „Einstellungen“ > „Systemsteuerung“ > „Verwaltung“ > „Lokale Sicherheitsrichtlinie“).
  - Wechseln Sie im Fenster Lokale Sicherheitsrichtlinie zu Lokale Richtlinien > Zuweisen von Benutzerrechten.
  - Doppelklicken Sie auf die Richtlinie „Als Dienst anmelden“, und fügen Sie den Benutzer hinzu.

Advisor

Zum Installieren von Advisor müssen Sie eine Advisor-ID und ein Passwort von Sentinel anfordern. Die Advisor-ID und das Passwort erhalten Sie, wenn Sie die Software kaufen. Wenn Sie „Direktes Herunterladen vom Internet“ ausgewählt haben, verwenden Sie den ausgehenden Port 443. Um Berichte auszuführen, muss die Crystal Enterprise-Software im System installiert sein.

Hinweis: Wenn Sie Advisor nur für Exploit-Erkennung verwenden, brauchen Sie die Crystal Enterprise-Software nicht zu installieren. Weitere Informationen hierzu finden Sie in Kapitel 4, „Advisor-Konfiguration“, auf Seite 77.

3.2 Installieren von Oracle unter Linux, SUSE Linux, Redhat Linux und Solaris

Stellen Sie für die Installation von Oracle unter Linux/Solaris sicher, dass Folgendes durchgeführt wurde:

- Festlegen von Kernel-Werten
- Konfigurieren der Datei init.ora unter Linux
- Unter Solaris:
  - Erstellen einer Gruppe und eines Benutzerkontos für Oracle
  - Festlegen von Umgebungsvariablen
  - Überprüfen des Solaris-Layouts
- Installation von Oracle 9.2.0.4
- Patch-Aktualisierung für Oracle 9.2.0.7

3.2.1 Festlegen von Kernel-Werten

Wichtig: Die in diesem Abschnitt vorgeschlagenen Kernel-Werte stellen nur Mindestwerte dar. Die Einstellungen sollten geändert werden, wenn die Systemeinstellungen unter den empfohlenen Mindestwerten liegen. Wenden Sie sich jedoch zunächst an den Systemadministrator und lesen Sie in der Oracle-Dokumentation nach, bevor Sie Änderungen vornehmen.

So legen Sie die Kernel-Werte unter Solaris fest

Unter Solaris müssen die folgenden Kernel-Werte in /etc/system festgelegt werden.

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

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.

So legen Sie die Kernel-Werte unter Linux fest

Unter Solaris müssen die folgenden Kernel-Werte in /etc/system festgelegt werden.

shmmax=2147483648 (Mindestwert)	semmni=1024
shmmni=4096	semmsl=1024
semmns=32000	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: Zum Festlegen der aktuellen Einstellung für einen bestimmten Kernel-Parameter führen Sie folgenden Befehl aus:

sysctl <Kernel-Parameter>

Beispiel: Zum Überprüfen des aktuellen Werts des Kernel-Parameters „kernel.sem“ führen Sie den folgenden Befehl aus: sysctl kernel.sem

Unter SUSE LINUX

```
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
vm.disable_cap_mlock=1
```

Unter REDHAT LINUX

```
# 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, um die Änderungen in die Datei /etc/sysctl.conf zu laden:

```
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.

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

3.2.2 Erstellen einer Gruppe und eines Benutzerkontos für Oracle unter Solaris

So erstellen Sie eine Gruppe und ein Benutzerkonto und legen Umgebungsvariablen fest

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
     ```

3.2.3 Festlegen von Umgebungsvariablen für Oracle unter Solaris

So legen Sie Umgebungsvariablen fest

1. Melden Sie sich als „root“ an.
2. 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
   ```

3.2.4 Überprüfen des Solaris-Layouts

So legen Sie Umgebungsvariablen fest

1. Rufen Sie die Website von Sun auf 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.

3.2.5 Installation von Oracle

In diesem Abschnitt wird erläutert, wie Oracle unter folgenden Betriebssystemen installiert wird:

- SUSE Linux
- Red Hat Linux
- Solaris

Wichtig: 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. Bei dieser Dokumentation wird davon ausgegangen, dass das Benutzerverzeichnis des Oracle-Benutzers /home/oracle lautet und dass Oracle im Verzeichnis /opt/oracle installiert wird. Ihre jeweilige Konfiguration kann davon abweichen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Betriebssystem und zu Oracle.

SUSE Linux (SLES 9 SP3)

So installieren Sie Oracle unter SUSE Linux

1 Befolgen Sie die im SLES 9-Installationshandbuch bereitgestellten Installationsanweisungen. Installieren Sie SLES 9 mit den Standardpaketen sowie die C/C++-Compiler und -Werkzeuge und SP2.

   Hinweis: Falls Sie SUSE Linux bereits installiert haben, können Sie YaST (Yet Another Setup Tool) in der SUSE Linux-GUI zur Installation der C/C++-Compiler und -Werkzeuge verwenden.

   ---

2 Melden Sie sich als „root“ an.

3 Installieren Sie gcc_old mithilfe von YaST.

4 Überprüfen Sie, ob SP3 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-SP3
   ```

   oder

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 3
   ```

5 Um den größten Teil der Aufgaben vor der Installation von Oracle zu automatisieren und um den Oracle-Benutzer zu erstellen, installieren Sie die in SLES 9 enthaltene Datei orarun.rpm.

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

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

Hinweis: orarun ist ebenfalls unter http://www.novell.com (http://www.novell.com) verfügbar.

6. 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.
7. Legen Sie ein neues Passwort für den Oracle-Benutzer fest, indem Sie YaST verwenden oder Folgendes eingeben:

   ```
   /usr/bin/passwd oracle
   ```
8. Führen Sie zum Festlegen der Kernel-Parameter Folgendes aus:

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

   Ignorieren Sie dabei möglicherweise auftretende Fehler.

   ```
   /sbin/chkconfig oracle on
   ```
9. Wechseln Sie zum Benutzer „oracle“

   ```
   su - oracle
   ```
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.
    - Wenn Sie zur Eingabe des UNIX-Gruppennamens aufgefordert werden, 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 9.2.0.7 Patch für Oracle auf der Disk1 der Oracle 9.2.0.7 Patch-Distribution führen Sie das Skript aus:

```
./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.
- Je nach Ihrer Version wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option 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.

17 Bearbeiten Sie die Datei init.ora, um den Verzeichnispfad anzugeben, in den archivierte Sentinel-Daten geschrieben werden sollen. Diese Angabe wird im Parameter UTL_FILE_DIR festgelegt. Folgendes muss angegeben werden:

- UTL_FILE_DIR = *****

  oder

- UTL_FILE_DIR = <bestimmer Verzeichnispfad>

SUSE Linux (SLES 10)

So installieren Sie Oracle unter SUSE Linux

1 Befolgen Sie die im SLES 10-Installationshandbuch bereitgestellten Installationsanweisungen. Installieren Sie SLES 10 mit den Standardpaketen sowie Oracle Server Base, C/C++-Compiler und -Werkzeuge.

2 Melden Sie sich als „root“ an.

3 Installieren Sie das SLES 10 Service Pack. Überprüfen Sie die Service Pack-Informationen, indem Sie Folgendes eingeben:

```
SPident
```

oder

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

Zum Zeitpunkt dieser Dokumentation war das SLES 10 Service Pack noch nicht veröffentlicht. Verwenden Sie für die Überprüfung SPident oder cat/etc/SUSE-release.

Folgendes sollte angezeigt werden:

```
CONCLUSION: System is up-to-date!
      Found     SLES-10-x86_64-current
```

4 Um den größten Teil der Aufgaben vor der Installation von Oracle zu automatisieren und um den Oracle-Benutzer zu erstellen, installieren Sie die in SLES 9 enthaltene Datei orarun.rpm.

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

```
rpm -ivh/orarun-1.9-21.2.x86_64.rpm
```

Hinweis: orarun ist ebenfalls unter http://www.novell.com (http://www.novell.com) verfügbar.

5. 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 die Datei /etc/passwd bearbeiten.
6. Legen Sie ein neues Passwort für den Oracle-Benutzer fest, indem Sie YaST verwenden oder Folgendes eingeben:

   ```
   /usr/bin/passwd oracle
   ```
7. Ändern Sie bei Bedarf die durch orarun festgelegte Oracle-Standardumgebung:
   - Ändern Sie das Oracle-Benutzerverzeichnis, indem Sie die Variable ORACLE_HOME in der Datei /etc/profile.d/oracle.sh ändern.
   - Die standardmäßig durch orarun festgelegte ORACLE_SID lautet „orcl“. Ändern Sie sie in der Datei /etc/profile.d/oracle.sh in ESEC.
8. Führen Sie zum Festlegen der Kernel-Parameter Folgendes aus:

   ```
   /usr/sbin/rcoracle start
   ```
9. Wechseln Sie zum Benutzer „oracle“

   ```
   su - oracle
   ```
10. Wechseln Sie zu dem Datenbankverzeichnis und führen Sie ./runinstaller (Oracle Universal Installer) aus. Ein Fehler wird ausgegeben (siehe unten):
11. Beheben Sie den Fehler mit einer der folgenden Maßnahmen:
    - Bearbeiten Sie die Datei database/install/oraparam.ini, um Unterstützung für SUSE Linux 10 hinzuzufügen. Nachdem Sie die Datei oraparam.ini bearbeitet haben, wird die Zeile „[Certified Versions]“ wie folgt angezeigt:

      ```
      [Certified Versions]
      Linux=redhat=3,SuSE-9,SuSE-10,redhat-4,UnitedLinux-1.0.asianux-1,asianux-2
      ```
    - Führen Sie die Installation mit der Option -ignoreSysPrereqs durch.

      ```
      i.e. ./runInstaller -ignoreSysPrereqs
      ```
12. Akzeptieren Sie das standardmäßige Inventarverzeichnis, oder wählen Sie ein neues Verzeichnis aus. Klicken Sie auf „Next“ (Weiter).
13. Wählen Sie als Installationstyp „Enterprise Edition“ aus. Klicken Sie auf „Next“ (Weiter).
14. Für die Überprüfung der Anforderungen an die Netzwerkkonfiguration wählen Sie „User Verified“ (Durch Benutzer überprüft) aus. Klicken Sie auf „Next“ (Weiter).
15. Wählen Sie in den Konfigurationsoptionen „Install Database Software only“ (Nur Datenbanksoftware installieren) aus. Klicken Sie auf „Next“ (Weiter).
16. Es wird eine Zusammenfassung der Installation angezeigt. Überprüfen Sie die Angaben und klicken Sie auf „Install“ (Installieren).
17. Führen Sie die angegebenen Skripts als „root“ aus und klicken Sie nach der Ausführung auf „OK“.
18. Klicken Sie nach der erfolgreichen Installation auf „Exit“ (Beenden).

Red Hat Linux

So installieren Sie Oracle unter Red Hat Linux

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 /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 Sentinel-Administratorbenutzers 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.

- Wenn Sie zur Eingabe des UNIX-Gruppennamens aufgefordert werden, 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 9.2.0.7 Patch für Oracle auf der Disk1 der Oracle 9.2.0.7 Patch-Distribution führen Sie das Skript aus:

```
./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.
- Je nach Ihrer Version wählen Sie auf dem Bildschirm „Produkt zur Installation auswählen“ die Option 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.

20 Unlink gcc:

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

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

```
Exit
```

22 Bearbeiten Sie die Datei init.ora, um den Verzeichnispfad anzugeben, in den archivierte Sentinel-Daten geschrieben werden sollen. Diese Angabe wird im Parameter UTL_FILE_DIR festgelegt. Folgendes muss angegeben werden:

- UTL_FILE_DIR = *

oder

- UTL_FILE_DIR = [bestimmter Verzeichnispfad

Unter Solaris

So installieren Sie Oracle unter Solaris

1 Melden Sie sich als Root an.

2 Führen Sie die in Oracle Note: 148673.1 SOLARIS: Quick Start Guide beschriebenen Schritte durch.

3 Installieren Sie Oracle 9i Release 2 (9.2.0.1) als Benutzer „oracle“. Sie werden aufgefordert, zwei zusätzliche CD-ROMs einzulegen. Sie müssen für jede der zusätzlichen CD-ROMs in verschiedene Verzeichnisse wechseln.

4 Führen Sie eine Patch-Aktualisierung Ihres Systems auf Oracle 9.2.0.7 durch. Weitere Informationen zum Installieren von Patches finden Sie in der Oracle-Dokumentation.

5 Wenn Sie die Patch-Stufe als Oracle UNIX-Benutzer überprüfen möchten, geben Sie Folgendes ein:

```
sqlplus '/as sysdba'
```

Als Ergebnis erhalten Sie das Release 9.2.0.7. Beenden Sie das Programm, indem Sie „quit“ eingeben.

6 Löschen Sie das Verzeichnis, das Sie für den Patch erstellt haben.

7 Nach der Installation der Patches löschen Sie die Patch-Verzeichnisse und -Dateien.

8 Bearbeiten Sie die Datei init.ora, um den Verzeichnispfad anzugeben, in den archivierte Sentinel-Daten geschrieben werden sollen. Diese Angabe wird im Parameter UTL_FILE_DIR festgelegt. Folgendes muss angegeben werden:

- UTL_FILE_DIR = *

oder

- UTL_FILE_DIR = [bestimmter Verzeichnispfad]

9 Booten Sie den Computer neu.

3.3 Installation von Sentinel

Sentinel unterstützt zwei Installationstypen. Dazu gehören:

- **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.

3.3.1 Einfache Installation

Wenn die im vorherigen Abschnitt genannten Voraussetzungen erfüllt sind, können Sie mit der Installation von Sentinel fortfahren.

So installieren Sie Sentinel

1 Melden Sie sich als Benutzer „root“ unter Solaris/Linux oder als Administratorbenutzer unter Windows an.

2 Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.

3 Stellen Sie unter Linux/Solaris sicher, dass die system-umask auf 0027 gesetzt ist, indem Sie den folgenden Befehl in derselben Befehlseingabeaufforderung ausführen, in der das Installationsprogramm ausgeführt wurde:

```
umask 0027
```

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

- Unter Windows: Führen Sie setup.bat aus.
- Unter Solaris/Linux:

GUI-Modus:

```
./setup.sh
```

oder

Textbasierter Modus („serielle Konsole“):

```
./setup.sh -console
```

5 Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:

Englisch	Italienisch
Französisch	= Portugiesisch (Brasilien)
Deutsch	Spanisch
Chinesisch (Vereinfacht)	Japanisch
Chinesisch (Traditionell)	

6 Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.

7 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf „Weiter“.

8 Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie auf „Weiter“.

9 Wählen Sie Einfach aus. Klicken Sie auf „Weiter“.

10 Geben Sie in diesem Bildschirm die Konfigurationsinformationen ein und klicken Sie auf „Weiter“.

- Seriennummer
- Lizenzschlüssel
- SMTP-Server
- Email

  Die IP-Adresse des SMTP-Servers oder der DNS-Name, die hier eingegeben wurden, helfen Ihnen dabei, den Versand von Emails aus Sentinel über die hier eingegebene Email-ID zu konfigurieren.

- Globales Systempasswort

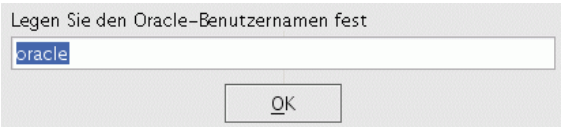
  Das hier eingegebene Passwort ist für alle Standardbenutzer gültig. Hierzu zählen sowohl der Sentinel-Administratorbenutzer als auch die Datenbankbenutzer. Weitere Informationen zu der bei der Installation erstellten Liste der Standard-Datenbankbenutzer finden Sie in Abschnitt 3.4.2, „Sentinel-Datenbank“, auf Seite 74.

- Advisor-Benutzername und -Passwort

  Geben Sie zum Installieren von Advisor den Benutzernamen und das Passwort ein, die Sie beim Kauf der Software erhalten haben. 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.

Hinweis: Falls Advisor installiert wird, wird das Programm bei der einfachen Installation so konfiguriert, dass die Option „Direktes Herunterladen vom Internet“ mit einem Aktualisierungsintervall von 12 Stunden verwendet wird und alle Email-Benachrichtigungen aktiviert sind.

Unter Solaris/Linux werden Sie zur Eingabe des Oracle-Benutzernamens aufgefordert. Geben Sie den Benutzernamen ein und klicken Sie auf „OK“.



11 Konfiguration der Datenbank:

- Wählen Sie die Plattform für die Zieldatenbank aus.
- Geben Sie den Datenbanknamen ein.
  - Geben Sie unter Linux/Solaris die Oracle-JDBC-Treiberdatei an.
  - Geben Sie unter Windows den Benutzerberechtigungsnachweis für die Datenbank und den Namen der SQL Server-Instanz ein.

Klicken Sie auf „Weiter“.

Die Datenbankgröße für die einfache Installation beträgt 10 GB.

12 Es wird eine Zusammenfassung der ausgewählten Datenbankparameter angezeigt. Klicken Sie auf „Weiter“.:

13 Es wird eine Zusammenfassung der Installation angezeigt. Klicken Sie auf Installieren.

14 Klicken Sie nach erfolgreicher Installation auf „Fertig stellen“.

3.3.2 Angepasste Installation

Wenn die im vorherigen Abschnitt genannten Voraussetzungen erfüllt sind, können Sie mit der Installation von Sentinel fortfahren.

So installieren Sie Sentinel

1 Melden Sie sich als Benutzer „root“ unter Solaris/Linux oder als Administratorbenutzer unter Windows an.

2 Legen Sie die Sentinel-Installations-CD ein und mounten Sie sie.

3 Stellen Sie unter Linux/Solaris sicher, dass die system-umask auf 0027 gesetzt ist, indem Sie den folgenden Befehl in derselben Befehlseingabeaufforderung ausführen, in der das Installationsprogramm ausgeführt wurde:

```
umask 0027
```

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

- Unter Windows: Führen Sie setup.bat aus.
- Unter Solaris/Linux:

GUI-Modus:

```
./setup.sh
```

oder

Für Textmodus („kopflos“):

```
./setup.sh -console
```

5 Klicken Sie auf den nach unten zeigenden Pfeil und wählen Sie eine der folgenden Sprachen aus:

Englisch	Italienisch
Französisch	= Portugiesisch (Brasilien)
Deutsch	Spanisch
Chinesisch (Vereinfacht)	Japanisch
Chinesisch (Traditionell)	

6 Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.

7 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf „Weiter“.

8 Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie auf „Weiter“.

9 Wählen Sie „Benutzerdefiniert“ aus. Klicken Sie auf „Weiter“.

10 Wählen Sie die zu installierenden Komponenten von Sentinel aus.

Hinweis: Weitere Informationen zur Installation der einzelnen Komponenten für verschiedene Konfigurationen finden Sie in Kapitel 2, „Optimale Verfahren“, auf Seite 19 im Installationshandbuch.

Mit den zur Verfügung stehenden Optionen können Sie

Datenbank – Installiert die Sentinel-Datenbank	Sentinel Collector Service
Communication Server – Installiert den Nachrichtenbus (iSCALE) und DAS Proxy	Collector Builder
Advisor	Sentinel Control Center
Correlation Engine	Sentinel Data Manager
DAS (für die Kommunikation mit der Datenbank)	HP OpenView Service Desk
	Remedy Integration

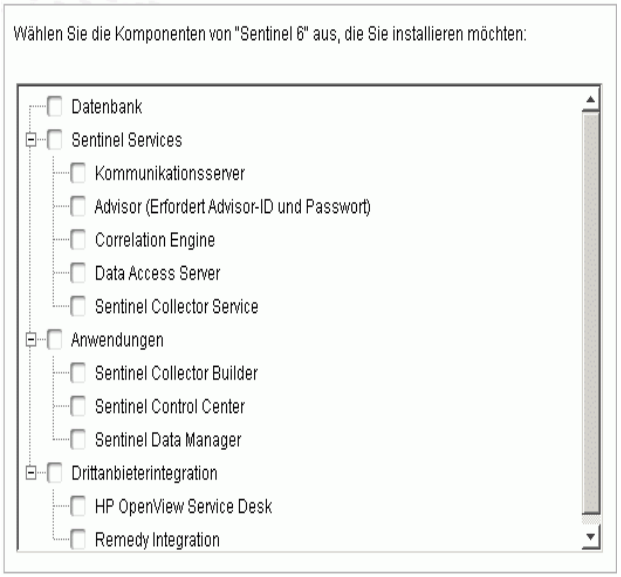
Hinweis: Informationen zum Installieren von HP OpenView Service Desk oder Remedy Integration finden Sie im Handbuch für Drittanbieter-Integration.

Hinweis: Beim Auswählen oder Aufheben der Auswahl einer Komponente tritt in der Schnittstelle eine zeitliche Verzögerung ein.

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 Datenbankorder %ESEC_HOME%\ ab.

Hinweis: Bei der einfachen Installation beträgt die Installationsgröße der Datenbank für MSSQL und ORACLE 10 GB.



11 Wenn Sie ausgewählt haben, dass DAS installiert werden soll, werden Sie zur Eingabe folgender Informationen aufgefordert:

- Seriennummer
- Lizenzschlüssel

12 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.

13 Geben Sie unter Linux/Solaris den Benutzernamen des Sentinel-Administrators für das Betriebssystem und den Speicherort seines Benutzerverzeichnisses an. 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 – Standard: „esecadm“

- Benutzerverzeichnis des Betriebssystem-Administrators – Standard: „/export/home“. Wenn der Benutzername „esecadm“ lautet, ist das dazugehörige Basisverzeichnis /export/home/esecadm.

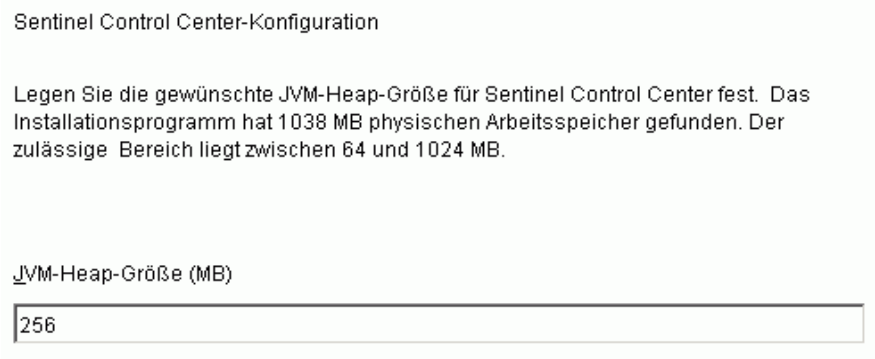
Hinweis: Damit die für die Common Criteria Certification erforderlichen strikten Sicherheitskonfigurationen eingehalten werden, beachten Sie die Angaben im Abschnitt „Festlegen von Passwörtern – Optimale Verfahren in Kapitel 2, „Optimale Verfahren“, auf Seite 19.

Hinweis: Der Benutzer „esecadm“ wird erstellt, ohne dass ein Passwort festgelegt wird. Wenn Sie sich als dieser Benutzer anmelden möchten, müssen Sie zunächst ein Passwort hierfür festlegen.

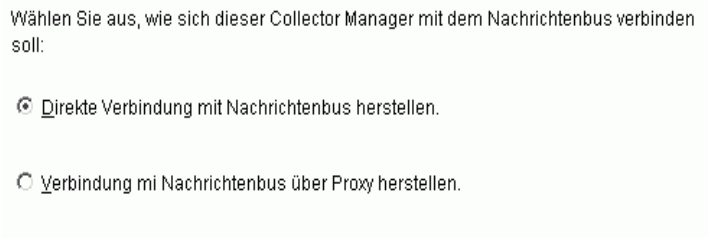
---

14 Wenn Sie ausgewählt haben, dass Sentinel Control Center installiert werden soll, fordert das Installationsprogramm Sie auf, die maximale Menge des Arbeitsspeichers einzugeben, der für Sentinel Control Center reserviert werden soll. Geben Sie die maximale JVM-Heap-Größe (MB) ein, die nur von Sentinel Control Center verwendet werden soll.

- JVM-Heap-Größe (MB): Standardmäßig ist dieser Wert als die Hälfte des auf dem Computer erkannten physischen Arbeitsspeichers festgelegt (maximal 1.024 MB).



15 Für die Kommunikation zwischen den Sentinel-Clients und dem Server stehen zwei Möglichkeiten zur Verfügung. Sie können zwischen dem Kommunikationstyp für den direkten Nachrichtenbus oder dem Proxytyp wählen. Weitere Informationen zu diesen beiden Optionen finden Sie in Kapitel 8, „Kommunikationsschicht (iSCALE)“, auf Seite 105 im Installationshandbuch.



16 Sie werden aufgefordert, Informationen zum Port und zum Namen des Hostservers einzugeben. Geben Sie die erforderlichen Informationen ein und klicken Sie auf „Weiter“. Wenn Sie den

Proxytyp ausgewählt haben, werden Sie außerdem zur Eingabe des Sentinel Communication Center-Proxy-Ports aufgefordert.

- Nachrichtenbus-Port: Der Port, den der Nachrichtenbus überwacht. Dieser Port wird von den Komponenten verwendet, die eine direkte Verbindung zu dem Nachrichtenbus herstellen.
- Sentinel Control Center-Proxy-Port: Der Port, den der SSL-Proxyserver (DAS Proxy) überwacht, um auf Benutzername und Passwort basierende authentifizierte Verbindungen zu akzeptieren. Da Sentinel Control Center zur Eingabe eines Benutzernamens und eines Passworts auffordert, wird dieser Port für die Verbindung zu Sentinel Server verwendet.
- Authentifizierungs-Proxy-Port für Zertifikatbasis: Der Port, den der SSL-Proxyserver (DAS Proxy) überwacht, um auf Zertifikaten basierende authentifizierte Verbindungen zu akzeptieren. Da Collector Manager nicht zur Eingabe eines Benutzernamens und eines Passworts auffordern kann, verwendet Collector Manager diesen Port für die Verbindung zu Sentinel Server, wenn die Verbindung der Konfiguration zufolge über den Proxy hergestellt wird.

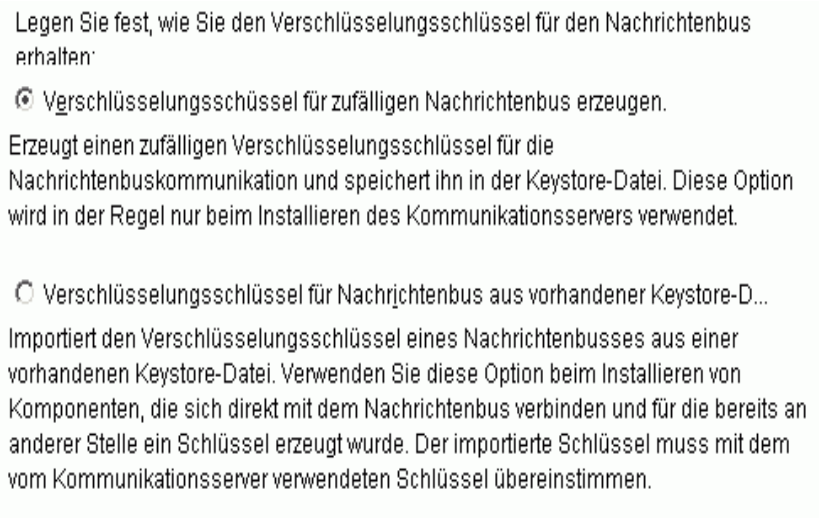
Hinweis: Eine Kommunikation ist nur dann möglich, wenn die Portnummern auf allen Computern im Sentinel-System identisch sind. Notieren Sie sich diese Informationen für zukünftige Installationen auf anderen Computern.

---

17 Wenn Sie eine Komponente installieren, die eine direkte Verbindung zu dem Nachrichtenbus herstellt, oder wenn Sie den Kommunikationsserver installieren, werden Sie aufgefordert anzugeben, wie Sie den Verschlüsselungsschlüssel für den Nachrichtenbus erhalten möchten:

- Zufälligen Verschlüsselungsschlüssel generieren (empfohlen, wenn der Kommunikationsserver installiert wird)
- Verschlüsselungsschlüssel aus Keystore-Datei importieren (empfohlen, wenn andere Komponenten installiert werden) Sie werden aufgefordert, die Datei auszuwählen, aus der der Verschlüsselungsschlüssel importiert werden soll.
- Die Keystore-Datei wird unter Linux und Solaris im Verzeichnis $ESEC_HOME/config und unter Windows im Verzeichnis %ESEC_HOME%\config abgelegt.

18 Geben Sie an, ob eine zufällige Keystore-Datei generiert oder eine vorhandene Keystore-Datei von einem anderen Computer im Sentinel-System importiert werden soll.



Hinweis: Alle Komponenten, die eine direkte Verbindung zu dem Nachrichtenbus herstellen, müssen denselben Verschlüsselungsschlüssel verwenden. Novell empfiehlt das Generieren eines zufälligen Verschlüsselungsschlüssels, wenn der Kommunikationsserver installiert wird, und das Importieren des Schlüssels, wenn Komponenten auf anderen Computern installiert werden. Komponenten, die eine Verbindung über den Proxy herstellen, benötigen den gemeinsamen Verschlüsselungsschlüssel für den Nachrichtenbus nicht.

19 Wenn Sie eine vorhandene Keystore-Datei importieren möchten, müssen Sie zum Speicherort der Datei navigieren und die Keystore-Datei auswählen. Klicken Sie auf „Weiter“.

20 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. Bei verteilten Umgebungen empfiehlt es sich, den maximalen Arbeitsspeicher auszuwählen, da ein Teil des Speichers für die Datenbank benötigt wird.

21 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 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 Sentinel-Datenbank, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten.
- Datenbankname: Der Name der Sentinel-Datenbankinstanz, für die Sie die DAS-Komponente für die Verbindung konfigurieren möchten (standardmäßig ESEC).
- Datenbankport (standardmäßig für Microsoft SQL: 1433 und für Oracle: 1521)
- Sentinel-Anwendungsdatenbankbenutzer: Geben Sie den Anmeldenamen „esecapp“ an und geben Sie das Passwort ein, das bei der Installation der Sentinel-Datenbank für diesen Benutzer festgelegt wurde.

22 Konfigurieren Sie die Datenbank für die Installation:

Unter Windows:

- Wählen Sie Microsoft SQL Server 2005 als Serverplattform für die Zieldatenbank aus.
  - Eine neue Datenbank mit Datenbankobjekten erstellen: Hiermit wird eine neue Microsoft SQL-Datenbank erstellt und die Datenbank wird mit Datenbankobjekten gefüllt.
  - Datenbankobjekte zu einer vorhandenen leeren Datenbank hinzufügen: Hiermit werden nur Datenbankobjekte zu einer vorhandenen Microsoft SQL 2005-Datenbank hinzugefügt. Die bestehende Datenbank muss leer sein.
  - Geben Sie das Verzeichnis für das Protokoll der Datenbankinstallation an.

Klicken Sie auf „Weiter“.

- Geben Sie den Speicherort für folgende Verzeichnisse an:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis
  - Protokollverzeichnis

Klicken Sie auf „Weiter“.

- Wählen Sie die Option zur Unterstützung des Zeichensatzes für die Datenbak aus: entweder Unicode oder Nur ASCII-Datenbank. Wenn Sie nicht-asiatische Sprachen (andere Sprachen als vereinfachtes/traditionelles Chinesisch & Japanisch in der Liste) auswählen, werden Sie aufgefordert, zwischen Unicode- und Nicht-Unicode-Datenbanken zu wählen. Wählen Sie ein Datenbankformat aus und klicken Sie auf „OK".

  Hinweis: Für die Unicode-Datenbankinstallation wird zusätzlicher Festplattenspeicher benötigt.

  Hinweis: Wenn Sie eine asiatische Sprache auswählen, wird automatisch die Unicode-Datenbank installiert. Klicken Sie auf „Weiter“.

- Geben Sie die Größe der Datenbank an. Klicken Sie auf „Weiter“.
- Konfigurieren Sie Datenbankpartitionen.
  - Sie können die Option zum Aktivieren automatischer Datenbankpartitionen auswählen.
  - Geben Sie für die Datenpartitionen das Archivverzeichnis an. Machen Sie Zeitangaben für das Hinzufügen und Archivieren der Daten.

Klicken Sie auf „Weiter“.

Unter Linux/Solaris:

- Wählen Sie die Serverplattform für die Zieldatenbank aus.
  - Wählen Sie in der Dropdown-Liste „Oracle 10g“ aus.
  - Wählen Sie „Eine neue Datenbank mit Datenbankobjekten erstellen“ aus.

Klicken Sie auf „Weiter“.

- Geben Sie einen Oracle-Benutzernamen an, oder akzeptieren Sie den Standardbenutzernamen. Klicken Sie auf OK
- Wenn Sie ausgewählt haben, dass eine neue Datenbank erstellt werden soll, geben Sie Folgendes ein:
  - **Pfad für die Oracle JDBC-Treiberdatei:** (der übliche 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. Das Installationsprogramm unterstützt nur das Erstellen einer neuen Datenbankinstanz auf dem lokalen Host.
  - **Datenbankname** Der Name der zu installierenden Datenbankinstanz.
- Wenn Sie einer vorhandenen leeren Oracle-Datenbank Datenbankobjekte hinzufügen, werden Sie um die folgenden Informationen gebeten.

  Pfad für die Oracle JDBC-Treiberdatei: (der übliche 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 Hosts mit der Oracle-Datenbank, der Sie die Datenbankobjekte hinzufügen möchten. Das kann der lokale Hostname oder ein Remote-Hostname sein.

Datenbankname: Der Name der vorhandenen 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.

Datenbank-Port: Der Standardwert ist 1521

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

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.

Hinweis: Das Installationsprogramm sichert die Dateien tnsnames.ora und listener.ora im Verzeichnis $ORACLE_HOME/network/admin. Die Datei listener.ora wird mit den Verbindungsinformationen der Sentinel-Datenbank überschrieben und diese Verbindungsinformationen werden an die Datei tnsnames.ora angehängt. Wenn sich andere Datenbanken auf demselben Server wie die Sentinel-Datenbank befinden, muss der Administrator die Informationen aus den gesicherten listener.ora-Dateien manuell in der neuen Datei zusammenführen und den Oracle-Listener neu starten, sodass die anderen Anwendungen weiterhin mit der Datenbank verbunden sind.

- Akzeptieren Sie beim Erstellen einer Datenbank die Standardwerte für den Speicherplatz und den Listener-Port, oder geben Sie neue Werte an.
- Geben Sie SYS und den SYS-Berechtigungsnachweis ein und klicken Sie auf „Weiter“.
- Geben Sie die Größe der Datenbank an. Sie können zwischen „Standard“, „Groß“ und „Benutzerdefiniert“ wählen. Bei Auswahl von „Benutzerdefiniert“ 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)
- Geben Sie die Gesamtgröße der Datenbank an, die für die Tabellenbereiche der Ereignisse und Ereigniszusammenfassungen zugeteilt ist.

- Geben Sie den Speicherort für folgende Verzeichnisse an:
  - Datenverzeichnis
  - Indexverzeichnis
  - Zusammenfassungsdatenverzeichnis
  - Zusammenfassungsindexverzeichnis
  - Protokollverzeichnis

  Klicken Sie auf „Weiter“.

  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.

  Um die bestmögliche Leistung zu erzielen, sollte das Wiederherstellungsprotokoll auf die schnellste beschreibbare Festplatte verweisen, die verfügbar ist.

  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 <directory_path>
  chmod –R 770 <directory_path>
  ```

- Dabei wird davon ausgegangen, dass „oracle“ Ihr Oracle-Benutzername und „dba“ Ihr Oracle-Gruppenname ist.
- Konfigurieren Sie Datenbankpartitionen.
  - Wählen Sie die Option zum automatischen Aktivieren von Datenbankpartitionen aus.
  - Geben Sie das Archivverzeichnis für die Datenpartition an.
  - Machen Sie Zeitangaben für das Hinzufügen und Archivieren von Daten.

  Klicken Sie auf „Weiter“.

23 Geben Sie Authentifizierungsinformationen für folgende Benutzer an:

- Sentinel-Datenbankadministratorbenutzer
- Sentinel-Anwendungsdatenbankbenutzer
- Sentinel-Administratorbenutzer
- Sentinel Report-Benutzer (nur Windows)

Klicken Sie auf „Weiter“.

24 Es wird eine Zusammenfassung der ausgewählten Datenbankparameter angezeigt. Klicken Sie auf „Weiter“.

25 Wenn Sie ausgewählt haben, dass DAS installiert werden soll, müssen Sie Email-Unterstützung für Sentinel konfigurieren. Geben Sie den SMTP-Server und die Email-Adresse an, von der Execution Service Nachrichten senden soll. (Optional: Sie können diese Angaben nach der Installation manuell ändern [$ESEC_HOME\sentinel\config\execution.properties unter Linux/Solaris und %ESEC_HOME%\sentinel\config\execution.properties unter Windows.])

26 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.
- **Einzelplatzbetrieb:** Advisor ist als isoliertes System konfiguriert, in das manuell eingegriffen werden muss, um eine Aktualisierung von Sentinel zu empfangen.

27 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. Klicken Sie anschließend auf "Weiter". Sie werden gefragt, ob Sie fortfahren möchten, wenn der Benutzername und das Passwort nicht bestätigt werden können (nicht empfohlen). Wenn Sie fortfahren, geben Sie Ihr Advisor-Passwort noch einmal in das Fenster „Passwortbestätigung“ ein. Berichtigen Sie anderenfalls Ihr Advisor-Passwort.

28 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 bearbeiten. Weitere Informationen finden Sie im Abschnitt zur “Registerkarte „Advisor“” im Sentinel-Benutzerhandbuch.

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

Hinweis: Fehlerbenachrichtigungen werden immer gesendet.

---

29 Klicken Sie anschließend auf "Weiter". Ein Übersichtsfenster mit den für die Installation ausgewählten Funktionen wird angezeigt. Klicken Sie auf Installieren.

Hinweis: 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.

---

30 Nach erfolgreicher Installation werden Sie aufgefordert, das System neu zu booten. Klicken Sie auf Fertig stellen, um das System neu zu booten.

Hinweis: 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.

Hinweis: Wenn Sie eine hohe Ereignisrate (mehr als 500 Ereignisse pro Sekunde) erwarten, müssen Sie die zusätzlichen Konfigurationsanweisungen im Abschnitt zum “Einrichten der OCI-Ereigniseinfügestrategie (Oracle Call Interface) bei der Datenbankerstellung” befolgen.

Konsoleninstallation unter Linux/Solaris

```
Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0] 2
    1. Deselect 'Sentinel Services'
    2. View 'Sentinel Services' subfeatures
   Enter command [1] 2

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [ ] Communication Server
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] 1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view its children, type its
number:
        1. [x] Communication Server
        2. [ ] Advisor (Install requires Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [x] Sentinel Collector Service
      Other options:
       -1. View this feature's parent
        0. Continue installing
      Enter command [0] -1

Select the features for "Sentinel 6" you would like to install:
   Sentinel 6
   To select/deselect a feature or to view its children, type its
number:
     1. [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
```

```
  4. +[ ] 3rd Party Integration
Other options:
  0. Continue installing
Enter command [0]
```

Client-Installation

Sentinel Control Center, Collector Builder und Sentinel Data Manager können mit dem vollständigen Installationsprogramm oder dem Client-Installationsprogramm installiert werden. Das Hauptinstallationsprogramm bietet Ihnen die Möglichkeit, unter den drei Anwendungen zu wählen, während das Client-Installationsprogramm alle drei Anwendungen installiert.

Hinweis: Da das Client-Installationsprogramm automatisch auch Collector Builder installiert, kann dieses Installationsprogramm nur unter Windows-Betriebssystemen verwendet werden. Diese Windows-basierten Anwendungen können alle mit einem Linux-basierten Sentinel Server zusammenarbeiten.

So installieren Sie Sentinel Control Center und Collector Builder mit dem Client-Installationsprogramm

1. Rufen Sie die CD auf und führen Sie setup.sh (Linux und Solaris) oder setup.bat (Windows) aus. Der Installationsassistent wird initialisiert.
2. Wählen Sie die Sprache für den Assistenten aus und klicken Sie auf „OK“.
3. Der Sentinel-Begrüßungsbildschirm wird angezeigt. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.
4. Der Bildschirm mit der Sentinel-Endbenutzer-Lizenzvereinbarung wird angezeigt. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie dann auf „Weiter“.
5. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um den Speicherort für die Installation anzugeben. Klicken Sie auf „Weiter“.
6. Geben Sie die Adresse des Hosts ein, auf dem der Kommunikationsserver installiert ist.
7. Wählen Sie die Option zum Generieren einer zufälligen Keystore-Datei aus und klicken Sie auf „Weiter“.
8. Klicken Sie auf „Weiter“.
9. Eine Zusammenfassung der Installation wird angezeigt. Klicken Sie auf Installieren.
10. Klicken Sie nach erfolgreicher Installation auf „Fertig stellen“.

3.4 Konfiguration im Anschluss an die Installation

3.4.1 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

Hinweis: Dieses Beispiel gilt für das Betriebssystem Linux/Solaris. Für Windows muss eine ähnliche Konfiguration durchgeführt werden.

1. Melden Sie sich auf dem Computer, auf dem DAS installiert ist, als Sentinel-Administratorbenutzer 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 Sentinel-Administratorbenutzer 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
   ```

3.4.2 Sentinel-Datenbank

Hinweis: Standardmäßig setzt das Installationsprogramm alle Tabellenbereiche auf automatisches Wachstum. Standardmäßig beträgt die Größe, auf die eine Datei anwachsen kann, 200 MB. Die maximale Dateigröße richtet sich jedoch nach dem Wert, der bei der Installation angegeben wurde (z. B. 2.000 MB).

Die automatische Partitionsverwaltung für Sentinel-Datenbanken (Archivieren, Ablegen und Hinzufügen von Partitionen) sollte aktiviert werden, um die Größe der Ereignisdaten überschaubar zu halten. Die automatische Partitionsverwaltung kann mithilfe von Sentinel Data Manager (SDM) konfiguriert werden.

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

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

- **esecdba:** Eigentümer des Datenbankschemas. Aufgrund von Sicherheitsbeschränkungen wird dem Sentinel-Datenbankbenutzer keine DBA-Berechtigung erteilt. 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. Dies ist nicht dasselbe Benutzerkonto wie der Sentinel-Administrator-Betriebssystembenutzer.
- **esecrpt:** Datenbankreport-Benutzer
- SYS: SYS-Datenbankbenutzer
- SYSTEM: SYSTEM-Datenbankbenutzer

3.4.3 Collector-Service

Bei der Installation des Collector Service wird ein Collector mit der Bezeichnung „Allgemeiner Collector“ konfiguriert. Dieser Collector kann zum Testen der Installation verwendet werden.

Hinweis: Weitere Informationen hierzu finden Sie in Kapitel 5, „Testen der Installation“, auf Seite 83

Hinweis: Weitere Informationen zu Collectors finden Sie unter http://support.novell.com/products/sentinel/collectors.html (http://support.novell.com/products/sentinel/collectors.html).

3.4.4 Aktualisieren des Lizenzschlüssels (von einem Evaluierungsschlüssel)

Wenn Sie das Produkt nach Ablauf des Evaluierungszeitraums kaufen, müssen Sie die folgenden Schritte durchführen, um den Lizenzschlüssel im System zu aktualisieren, damit eine Neuinstallation verhindert wird.

So aktualisieren Sie den Lizenzschlüssel

1. Melden Sie sich an dem Computer, auf dem die Komponente DAS installiert ist, als „esecadm“ an.
2. Wechseln Sie in der Befehlseingabeaufforderung zu folgendem Verzeichnis: $ESEC_HOME/bin.

3. Führen Sie die folgende ausführbare Datei aus: ./softwarekey. Ihnen wird ein Menü mit folgenden Angaben angezeigt.
   - Primärschlüssel eingeben
   - Sekundärschlüssel eingeben
   - Primärschlüssel anzeigen
   - Sekundärschlüssel anzeigen
   - Beenden
4. Geben Sie „1“ ein, um einen neuen Primärschlüssel einzugeben.

Advisor-Konfiguration

4

In diesem Kapitel werden die folgenden Themen behandelt:

In diesem Kapitel wird erläutert, wie Sentinel so konfiguriert wird, dass Advisor-Berichte direkt über Sentinel Control Center ausgeführt werden können. Advisor-Berichte werden von Novell für die Berichterstellung und Analyse erstellt. Nachdem die Integration von Sentinel Control Center ordnungsgemäß konfiguriert wurde, werden sie auf der Registerkarte „Advisor“ angezeigt.

4.1 Überblick über Advisor

Sentinel Advisor bietet Echtzeitinformationen zu Unternehmensanfälligkeiten, Expertenrat und empfohlene Schritte zur Sanierung. Advisor bietet Erkennungsauswertung, einen Kreuzverweis zwischen IDS-Angriffssignaturen in Echtzeit und der Advisor Knowledge Base für Anfälligkeiten.

Hinweis: 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. Advisor ist ein abonnementbasierter Datenservice.

Folgende System werden unterstützt:

Eindringversuchssysteme	Anfälligkeits-Absuchprogramme
Cisco Secure IDS	eEYE Retina
Enterasys Dragon Host Sensor	Foundstone Foundscan
Enterasys Dragon Network Sensor	ISS Database Scanner
Intrusion.com (SecureNet_Provider)	ISS Internet Scanner
ISS BlackICE	ISS System Scanner
ISS RealSecure Desktop	ISS Wireless Scanner
ISS RealSecure Network	Nessus
ISS RealSecure Server	nCircle IP360
ISS RealSecure Guard	Qualys QualysGuard
Snort	**Firewalls**
Symantec Network Security 4.0 (ManHunt)	Cisco IOS Firewall
Symantec Intruder Alert	
McAfee IntruShield	

4.2 Installation von Advisor

Hinweis: Advisor muss auf demselben Computer installiert werden, auf dem sich auch Database Access Service (DAS) befindet.

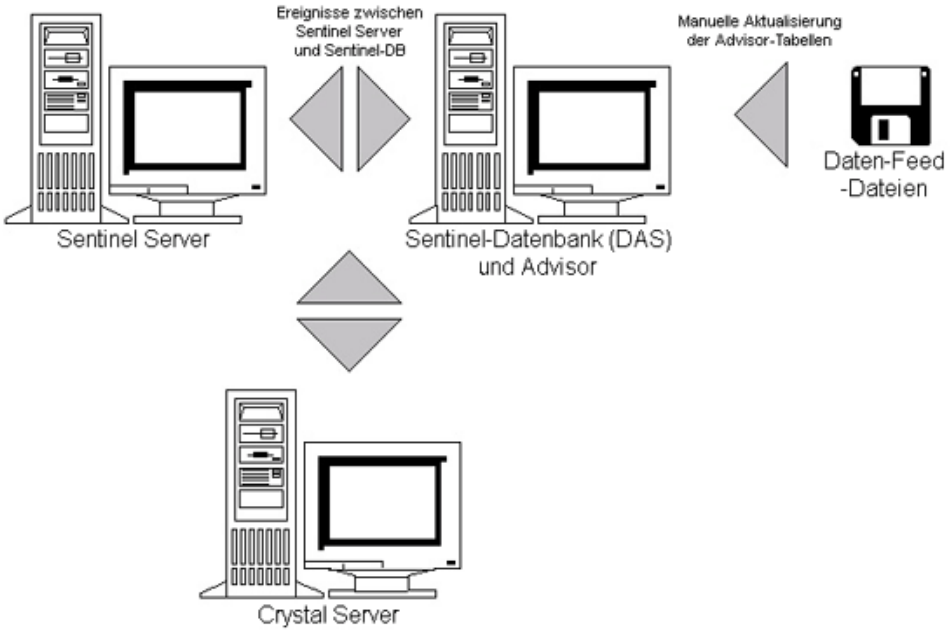
Es sind zwei verschiedene Installationsoptionen verfügbar. Dazu gehören:

- Einzelplatzbetrieb
- Direktes Herunterladen vom Internet

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.

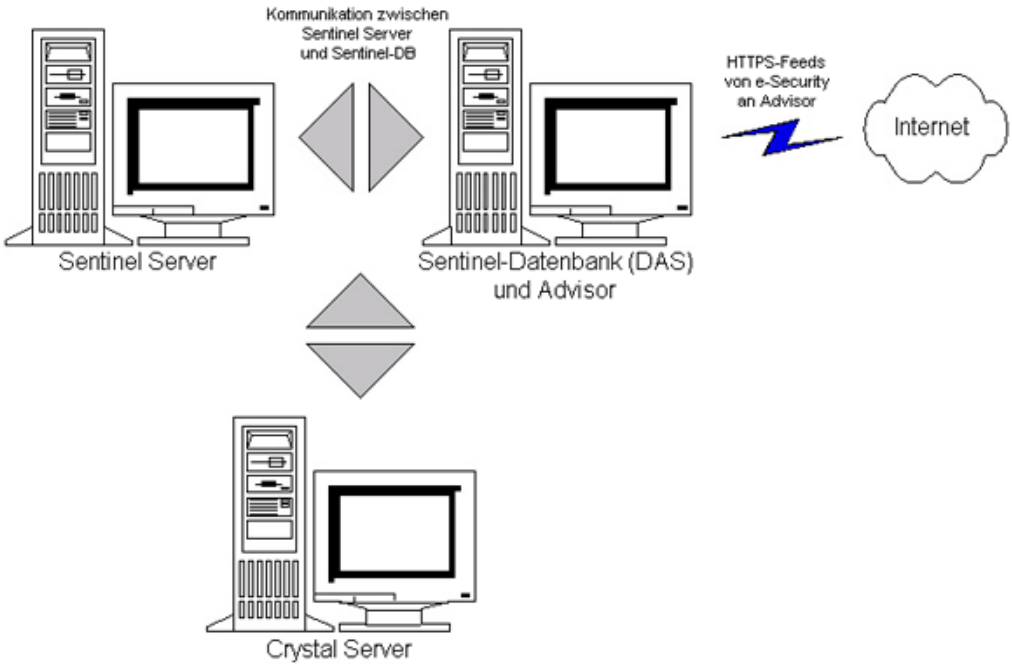
4.2.1 Einzelplatzkonfiguration

Bei einer Einzelplatzinstallation ist Advisor ein isoliertes System, in das manuell eingegriffen werden muss, um eine Aktualisierung von Novell zu empfangen.



4.2.2 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.



4.3 Advisor-Berichte

Crystal BusinessObjects Enterprise™ XI ist ein Werkzeug für die Berichterstellung, das eng mit Sentinel zusammenarbeitet. Weitere Informationen zur Installation von Crystal BusinessObjects Enterprise™ XI finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 und Kapitel 10, „Crystal Reports für Linux“, auf Seite 141 im Installationshandbuch.

Hinweis: Crystal Server ist nur dann erforderlich, wenn Sie beabsichtigen, Berichte auszuführen. Wenn Sie Advisor nur für Exploit-Erkennung verwenden möchten, brauchen Sie keine Instanz von Crystal Server zu installieren.

So führen Sie Crystal Reports-Berichte unter Advisor aus

- Installieren und konfigurieren Sie Crystal Server. Weitere Informationen finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 im Installationshandbuch.
- Veröffentlichen Sie die Advisor Crystal Reports-Berichte auf Crystal Server. Weitere Informationen finden Sie im Kapitel zum Importieren von Berichtsvorlagen.

4.3.1 Konfiguration von Advisor-Berichten

Wenn Sie beabsichtigen, Advisor-Berichte (Crystal Reports) auszuführen, führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch. Die folgenden Schritte sind nicht erforderlich, wenn Sie lediglich vorhaben, Advisor für die Exploit-Erkennung zu nutzen.

- Falls dies noch nicht geschehen ist, führen Sie die folgenden Aktionen durch. (Weitere Informationen hierzu finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 im Installationshandbuch.)
  - Installieren Sie Microsoft Internet Information Server (IIS).
  - Installieren Sie Crystal BusinessObjects Enterprise™ 11.

- Sentinel-Datenbank unter Oracle (Solaris/Linux): Konfigurieren Sie den systemeigenen Oracle-Treiber (für Oracle-Installationen)
- Sentinel-Datenbank unter Microsoft SQL 2005 (Windows): Konfigurieren Sie Open Database Connectivity (ODBC).
- Installieren Sie die notwendigen Patches für Crystal Reports. Weitere Informationen finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 im Installationshandbuch.

- Installieren Sie Advisor. Weitere Informationen zur Installation von Advisor finden Sie in Kapitel 7, „Installieren der Sentinel-Komponenten“, auf Seite 99 im Installationshandbuch.
- Importieren Sie Crystal Report-Schablonen.
- Erstellen Sie eine Crystal-Webseite.
- Konfigurieren Sie Sentinel Control Center für die Integration mit Crystal Enterprise Server.

Hinweis: Weitere Informationen zum Importieren von Berichtsschablonen und zum Konfigurieren von Sentinel Control Center, sodass die Advisor-Berichte angezeigt werden, finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 und Kapitel 10, „Crystal Reports für Linux“, auf Seite 141 im Installationshandbuch.

4.4 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. Weitere Informationen zur manuellen Aktualisierung finden Sie im Sentinel-Benutzerhandbuch im Kapitel zur Verwendung und Wartung von Advisor.

4.5 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. Navigation:

   Bei UNIX:

   `$ESEC_HOME/bin`

   Für Windows:

```
%ESEC_HOME%\bin
```

3 Führen Sie den folgenden Befehl aus:

Bei UNIX:

```
./adv_change_passwd.sh <newpassword>
```

Für Windows:

```
adv_change_passwd.bat <newpassword>
```

wobei <neues Passwort> das Advisor-Passwort ist, das Sie festlegen möchten.

Testen der Installation

5

In diesem Kapitel werden die folgenden Themen behandelt:

5.1 Testen der Installation

Sentinel wird mit einem Collector zu Demonstrationszwecken installiert, mit dem zahlreiche Basisfunktionen des Systems getestet werden können. Mit diesem Collector können Sie Active Views, die Vorfallerstellung, Korrelationsregeln und Berichte testen. Nachfolgend werden die Schritte erläutert, mit denen sich das System und die erwarteten Ergebnisse testen lassen. Möglicherweise erhalten Sie nicht genau die gleichen Ergebnisse. Ihre Ergebnisse sollten den folgenden Ergebnissen jedoch ähneln.

Auf einer Basisebene können Sie mit diesen Tests überprüfen, ob Folgendes zutrifft:

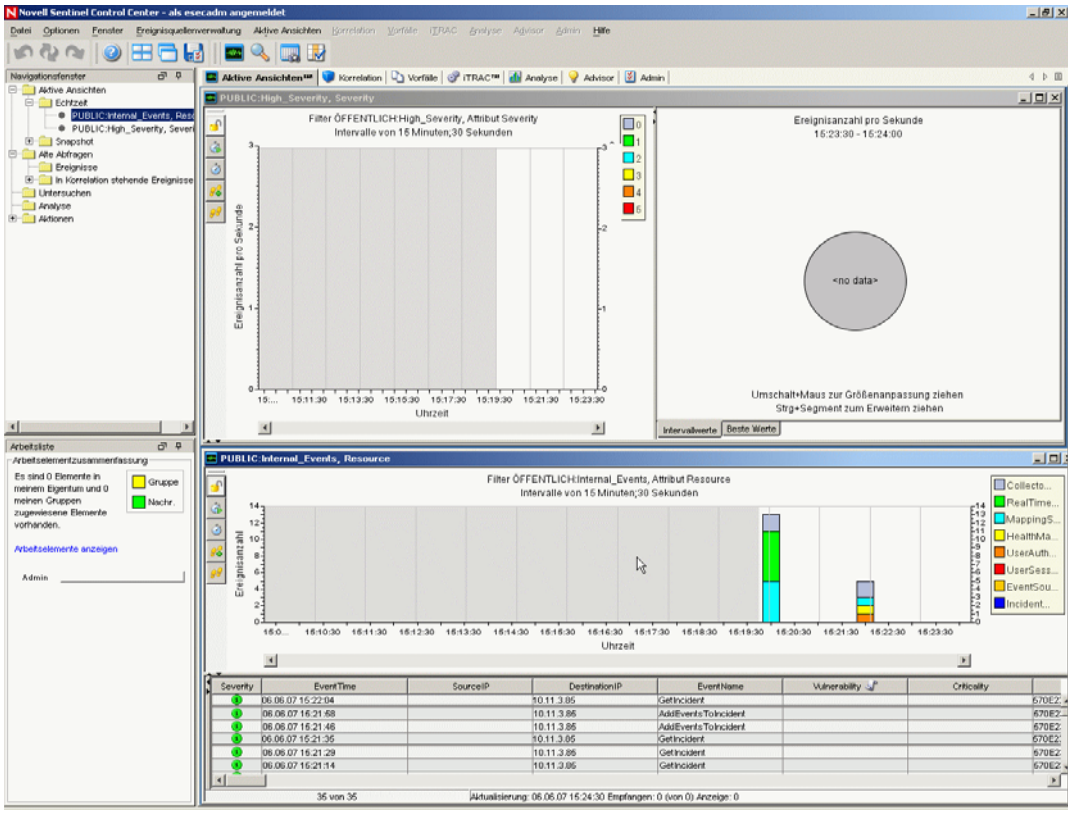
- Sentinel Services sind aktiv und werden ausgeführt.
- Die Kommunikation über den Nachrichtenbus funktioniert.
- Interne Audit-Ereignisse werden gesendet.
- Ereignisse können von einem Collector Manager gesendet werden.
- Ereignisse werden in die Datenbank eingefügt und können entweder mit der Verlaufsereignisabfrage oder dem Reporting-Server abgerufen werden.
- Vorfälle können erstellt und angezeigt werden.
- Correlation Engine wertet Regeln aus und löst korrelierte Ereignisse aus.
- Sentinel Data Manager kann eine Verbindung mit der Datenbank herstellen und Partitionsinformationen lesen.

Falls einer dieser Tests fehlschlägt, überprüfen Sie das Installationsprotokoll und die übrigen Protokolldateien und wenden Sie sich, falls notwendig, an den technischen Support von Novell.

So testen Sie die Installation

1. Doppelklicken Sie auf das Symbol für Sentinel Control Center auf dem Desktop.
2. Melden Sie sich als der bei der Installation festgelegte Sentinal-Administratorbenutzer an (standardmäßig „esecadm“). Sentinel Control Center wird geöffnet. Gebenenfalls wird die

Registerkarte „Active Views“ angezeigt, in der das Fenster „ÖFFENTLICH:Alle, Schweregrad“ angezeigt wird.

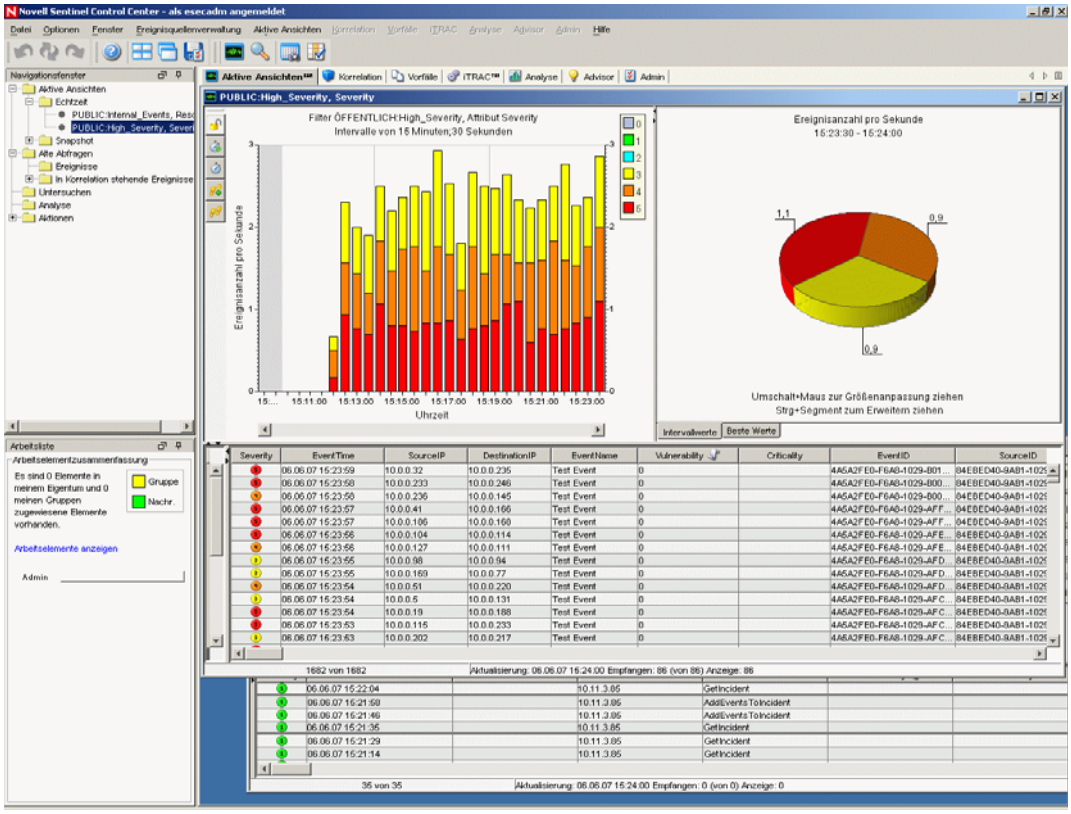


3 Wählen Sie im Menü „Ereignisquellenverwaltung“ die Option „Live-Ansicht“ aus.

4 Klicken Sie in der grafischen Ansicht mit der rechten Maustaste auf „Ereignisquelle mit 5 EPS“ und wählen Sie „Start“ aus.

5 Schließen Sie das Fenster „Ereignisquellenverwaltung [Live-Ansicht]“.

6 Wechseln Sie zu der Registerkarte „Active Views“. Hier wird das aktive Fenster „ÖFFENTLICH: High_Severity, Schweregrad“ angezeigt. Es dauert möglicherweise einige Zeit, bis der Collector startet und die Daten in diesem Fenster angezeigt werden.



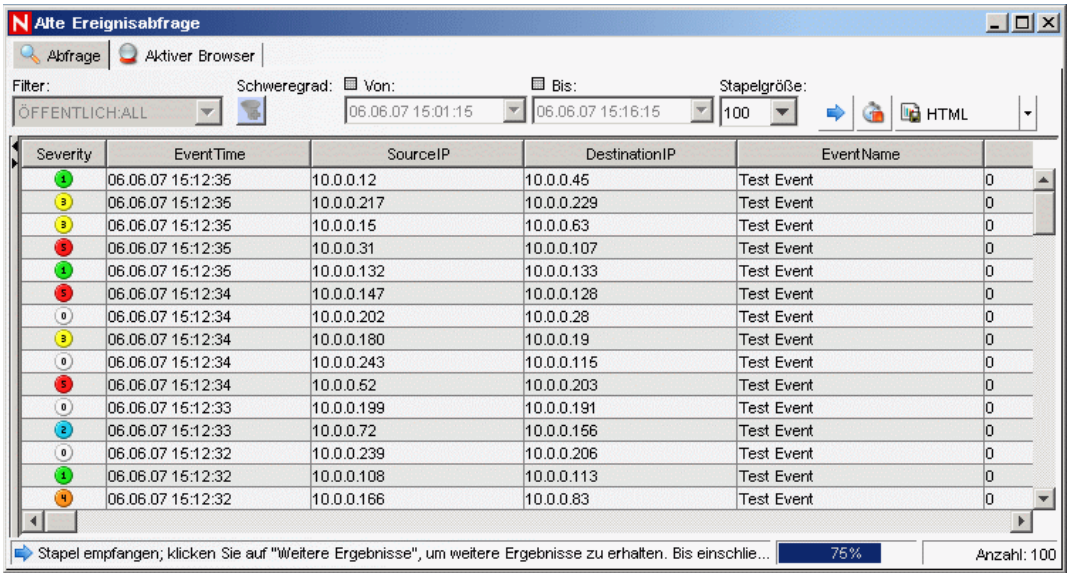
7 Klicken Sie auf der Symbolleiste auf die Schaltfläche „Ereignisabfrage“. Das Fenster „Alte Ereignisabfrage“ wird angezeigt.

8 Klicken Sie im Fenster „Alte Ereignisabfrage“ auf den Pfeil im Feld für den Filter, um den Filter auszuwählen. Markieren Sie den Filter „Öffentlich: Alle“, und klicken Sie dann auf „Auswählen“.

9 Wählen Sie einen Zeitraum für die Aktivität des Collectors aus. Wählen Sie mithilfe der Dropdown-Felder „Von“ und „Bis“ einen Datumsbereich aus.

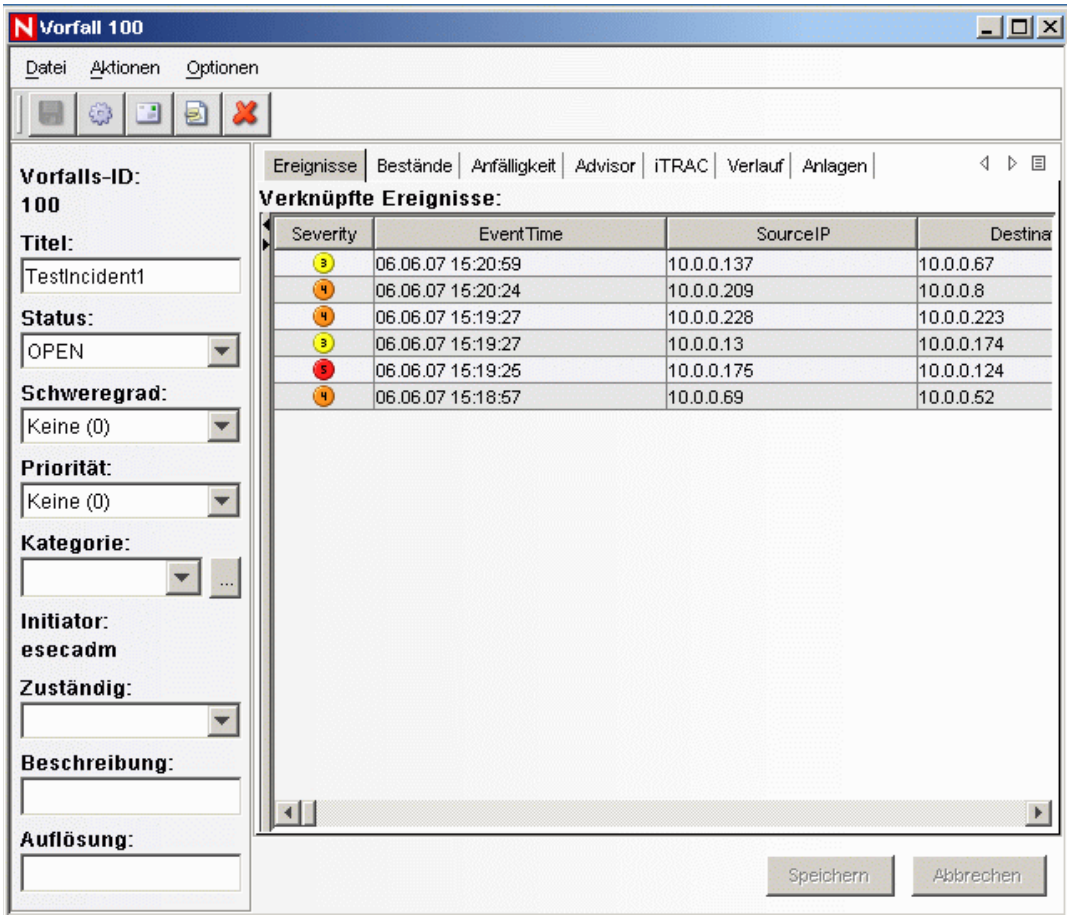
10 Wählen Sie im Dropdown-Feld „Stapelgröße“ eine Stapelgröße aus.

11 Klicken Sie auf die Lupe, um die Abfrage auszuführen.



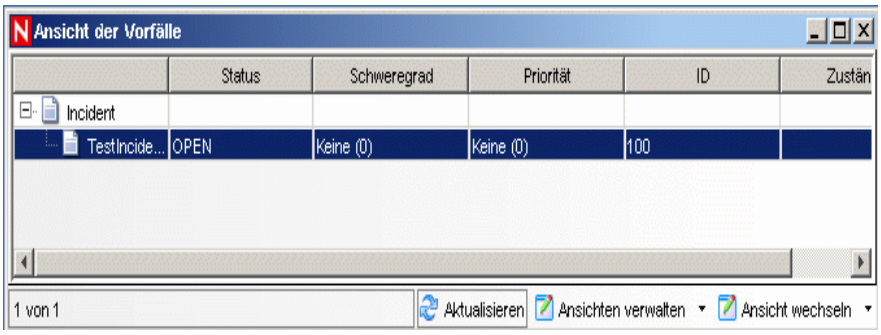
12 Halten Sie die Strg-Taste oder die Umschalttaste gedrückt, und wählen Sie im Fenster „Alte Ereignisabfrage“ weitere Ereignisse aus.

13 Klicken Sie mit der rechten Maustaste und wählen Sie „Vorfall erstellen“ aus.

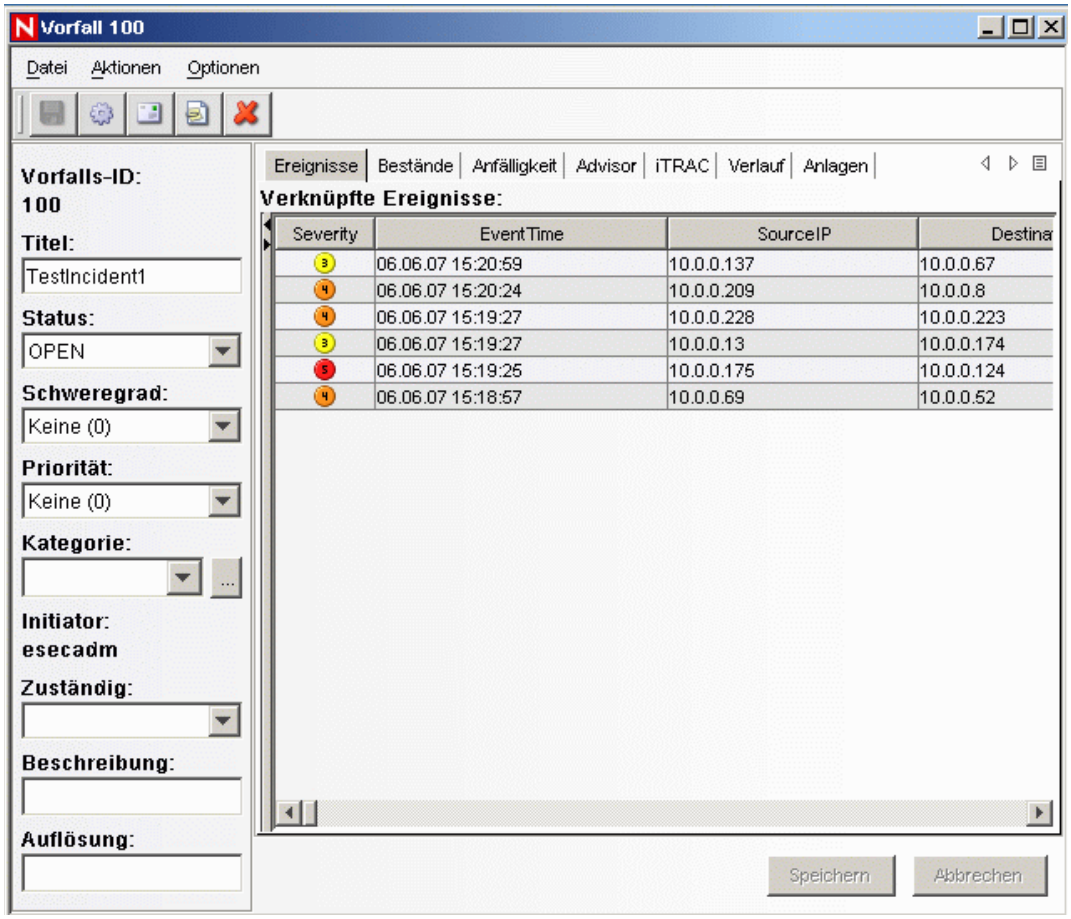


14 Benennen Sie den Vorfall als „TestVorfall1“ und klicken Sie auf „Erstellen“. Es wird eine Benachrichtigung angezeigt, dass der Vorfall erfolgreich erstellt wurde. Klicken Sie auf "OK".

15 Wechseln Sie zu der Registerkarte „Vorfall“. Der Vorfallsansichts-Manager wird angezeigt. Im Vorfallsansichts-Manager wird der soeben erstellte Vorfall angezeigt.



16 Doppelklicken Sie auf den Vorfall, um ihn zu öffnen.



17 Schließen Sie das Vorfallsfenster, wählen Sie „Datei“ > „Beenden“ aus, oder klicken Sie auf das „X“ oben rechts im Fenster.

18 Klicken Sie auf die Registerkarte Analyse. Öffnen Sie im Analysenavigator den Ordner „Verlaufsberichte“.

19 Klicken Sie auf Ereignisabfrage.

20 Klicken Sie auf „Analyse“ > „Bericht erstellen“, oder klicken Sie auf das Symbol „Bericht erstellen“. Ein Ereignisabfragefenster wird geöffnet. Legen Sie Folgendes fest:

- Zeitrahmen
- Filter
- Schweregrad
- Stapelgröße (Dies ist die Anzahl der angezeigten Ereignisse – ältere Ereignisse werden vor neueren Ereignissen angezeigt.)

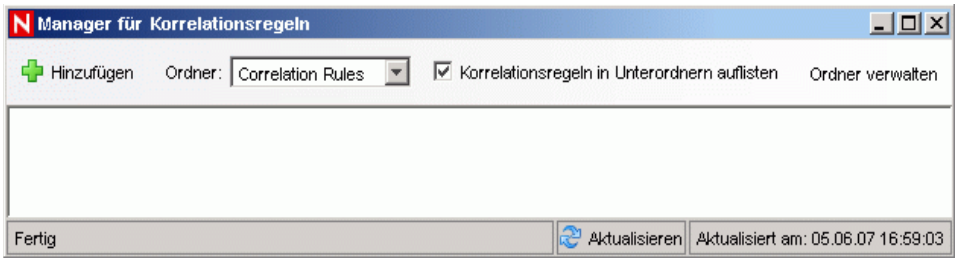
21 Klicken Sie auf Abfrage aktualisieren.

22 Klicken Sie zum Anzeigen des nächsten Ereignisstapels auf Weitere Optionen.

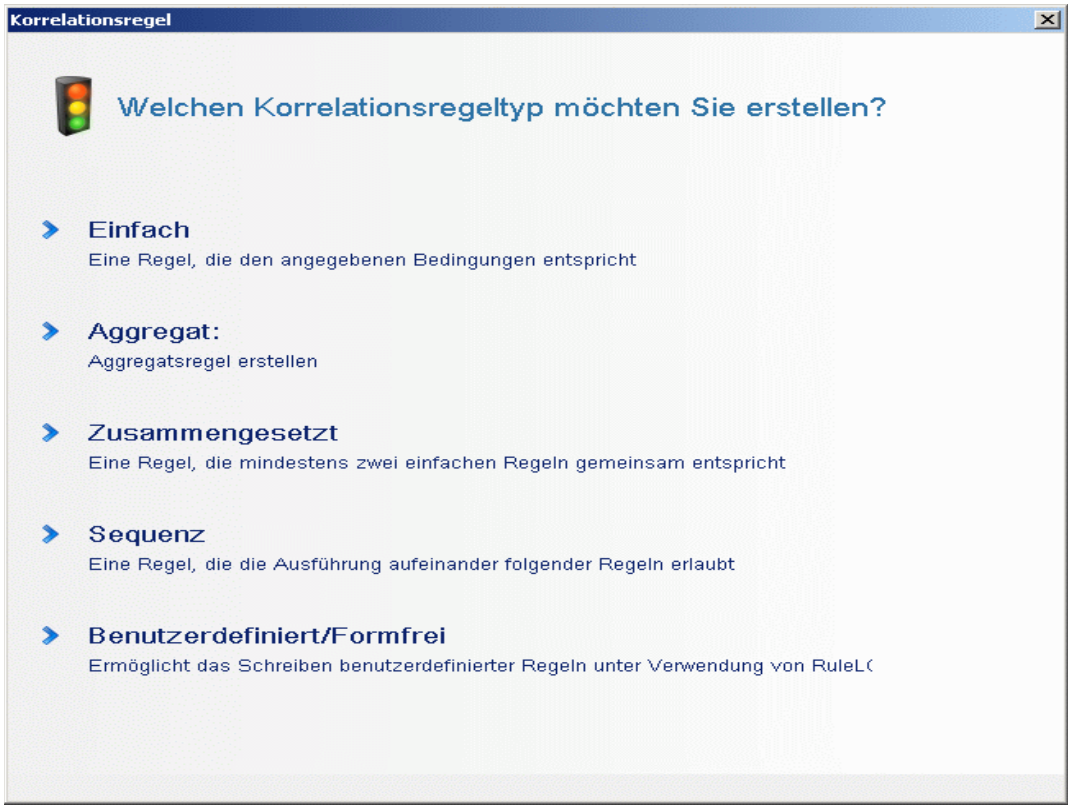
23 Ordnen Sie die Spalten neu an, indem Sie diese ziehen und ablegen, und ändern Sie die Sortierreihenfolge, indem Sie auf die Spaltenüberschrift klicken.

24 Wenn Ihre Abfrage fertig ist, wird sie im Navigator der Liste der Schnellabfragen hinzugefügt.

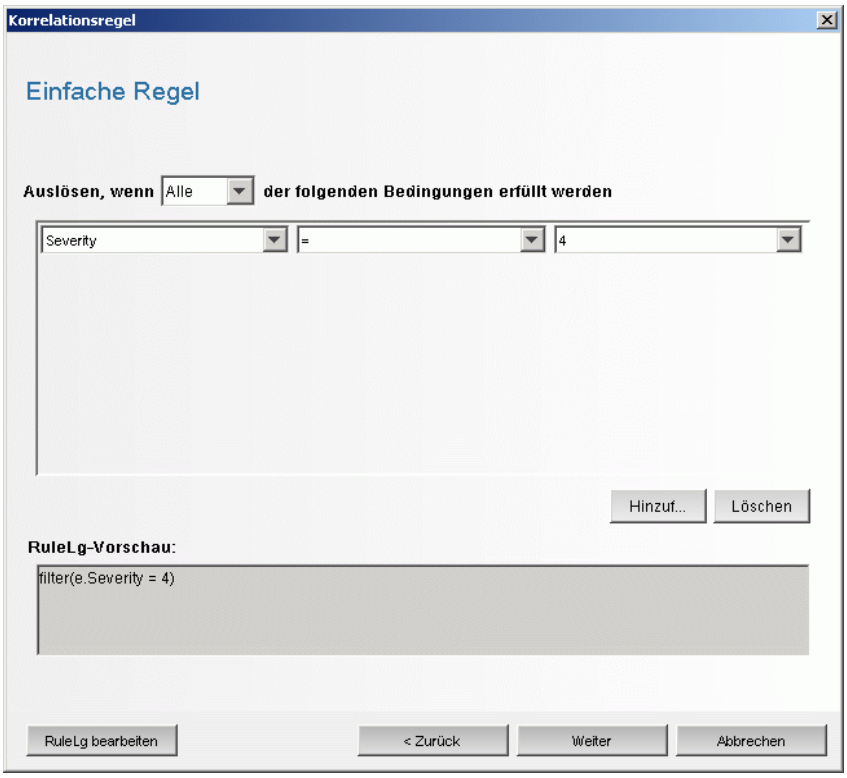
25 Wechseln Sie zu der Registerkarte „Korrelation“. Der Manager für Korrelationsregeln wird angezeigt.



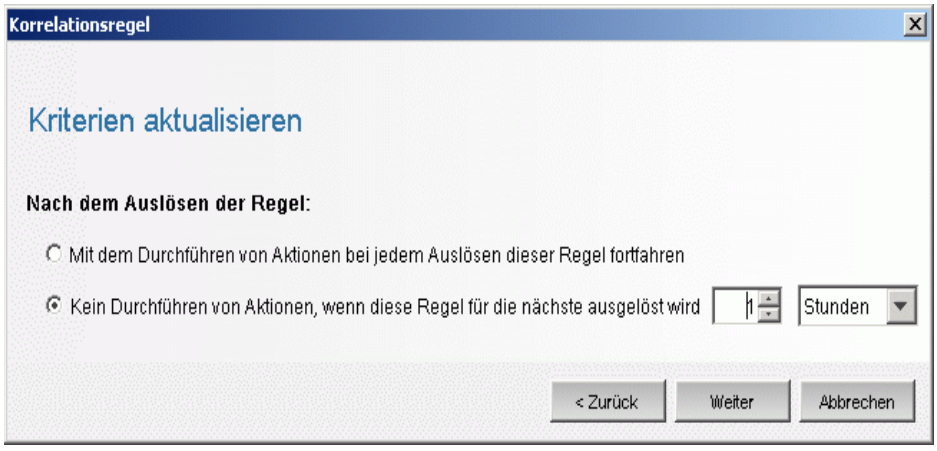
26 Klicken Sie auf Hinzufügen. Der Assistent für Korrelationsregeln wird geöffnet.



27 Klicken Sie auf „Einfach“. Das Fenster „Einfache Regel“ wird geöffnet.

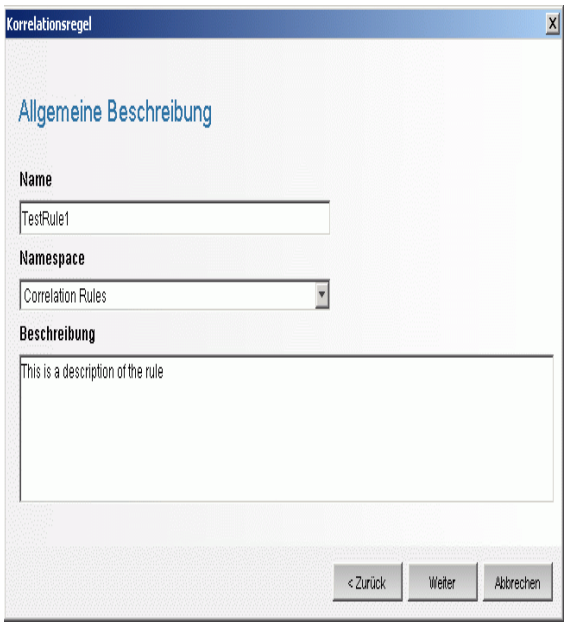


28 Verwenden Sie die Dropdown-Menüs, um als Kriterium „Schweregrad = 4“ festzulegen. Klicken Sie anschließend auf "Weiter". Das Fenster „Kriterien aktualisieren“ wird angezeigt.



29 Wählen Sie „Kein Durchführen von Aktionen, wenn diese Regel für die nächste ausgelöst wird“ aus und legen Sie den Zeitraum mithilfe des Dropdown-Menüs auf 1 Minute fest.

Klicken Sie anschließend auf "Weiter". Das Fenster „Allgemeine Beschreibung“ wird angezeigt.

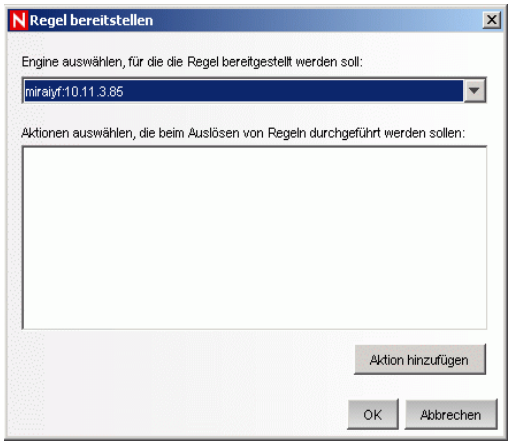


30 Geben Sie als Namen für die Regel „TestRegel1“ an, geben Sie eine Beschreibung ein und klicken Sie dann auf „Weiter“.

31 Wählen Sie „Nein, erstellen Sie keine andere Regel“ und klicken Sie auf „Weiter“.

32 Öffnen Sie das Fenster „Manager für Korrelationsregeln“.

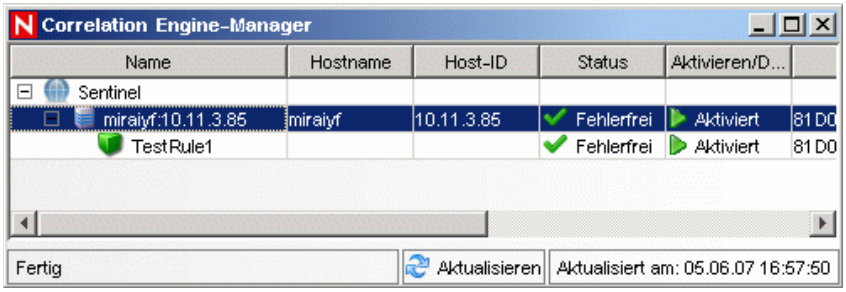
33 Markieren Sie eine Regel und klicken Sie auf die Verknüpfung zur Bereitstellung von Regeln. Das Fenster „Regel bereitstellen“ wird angezeigt.



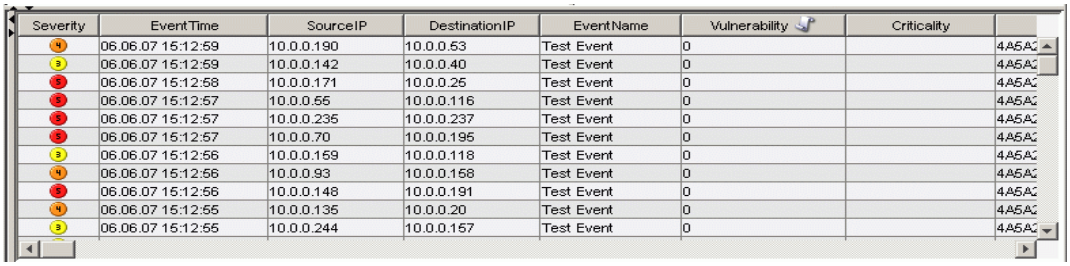
34 Wählen Sie im Fenster „Regel bereitstellen“ in der Dropdown-Liste die Engine zum Bereitstellen der Regel aus.

35 Wählen Sie die Aktion „Email senden“ aus, um sie mit der Regel zu verknüpfen, und klicken Sie auf „OK“.

36 Wählen Sie den Correlation Engine-Manager aus. Im Correlation Engine-Manager können Sie sehen, dass die Regel bereitgestellt/aktiviert wurde.



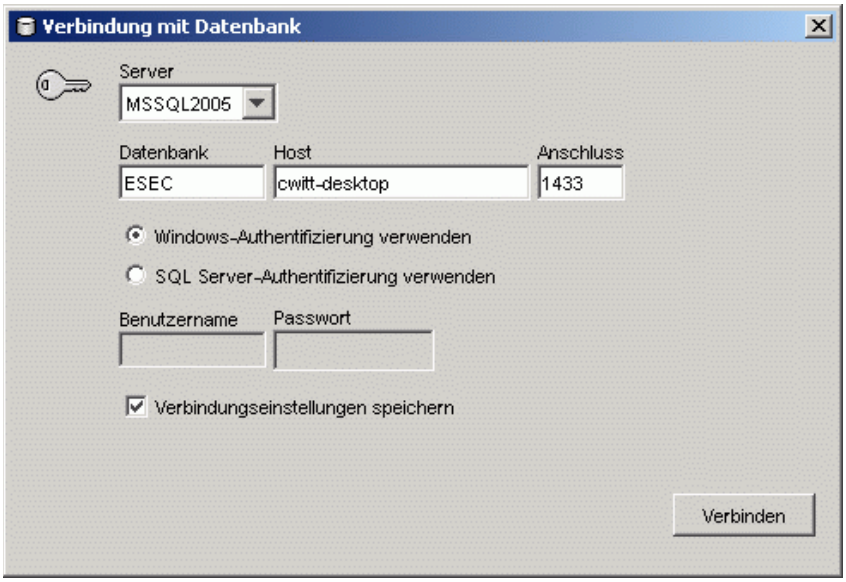
37 Wechseln Sie zur Registerkarte „Active Views“ und überprüfen Sie, ob das korrelierte Ereignis erstellt wurde.



38 Schließen Sie Sentinel Control Center.

39 Doppelklicken Sie auf dem Desktop auf das Symbol für Sentinel Data Manager (SDM).

40 Melden Sie sich als der bei der Installation festgelegte Datenbankadministratorbenutzer an (standardmäßig „esecadm“).



41 Klicken Sie auf die einzelnen Registerkarten, um zu überprüfen, ob Sie darauf zugreifen können.

42 Schließen Sie Sentinel Data Manager.

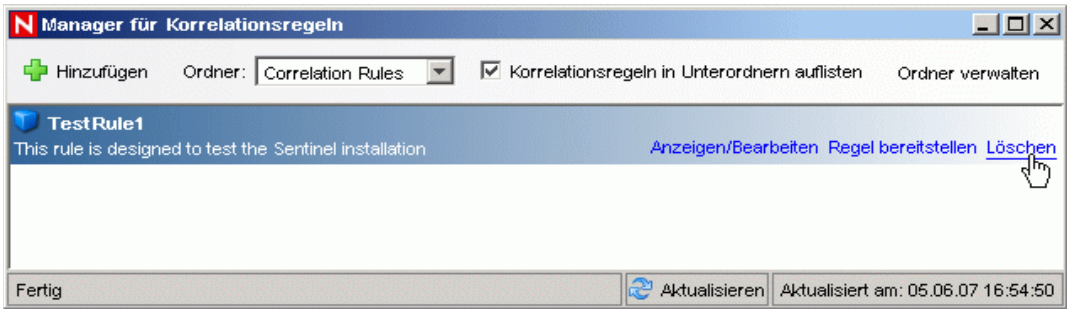
Wenn Sie alle Schritte fehlerfrei durchführen konnten, haben Sie die grundlegende Überprüfung der Installation des Sentinel-Systems erfolgreich abgeschlossen.

5.2 Bereinigung nach dem Testen

Nach Abschluss der Systemüberprüfung sollten Sie die für die Tests erstellten Objekte löschen.

So führen Sie nach dem Systemtest eine Bereinigung durch

1. Melden Sie sich als der bei der Installation festgelegte Sentinal-Administratorbenutzer an (standardmäßig „esecadm“).
2. Wechseln Sie zu der Registerkarte „Korrelation“.
3. Öffnen Sie den Correlation Engine-Manager.
4. Klicken Sie im Correlation Engine-Manager mit der rechten Maustaste auf „TestRegel1“ und wählen Sie „Bereitstellung der Regel aufheben“ aus.
5. Öffnen Sie den Manager für Korrelationsregeln.
6. Wählen Sie „TestRegel1“ aus und klicken Sie auf „Löschen“.



7. Wählen Sie im Menü „Ereignisquellenverwaltung“ die Option „Live-Ansicht“ aus.
8. Klicken Sie in der grafischen Ereignisquellenhierarchie mit der rechten Maustaste auf „Allgemeiner Collector“ und wählen Sie „Stoppen“ aus.
9. Schließen Sie das Fenster „Ereignisquellenverwaltung“.
10. Wechseln Sie zu der Registerkarte „Vorfälle“.
11. Öffnen Sie den Vorfallansichts-Manager.
12. Wählen Sie „TestVorfall1“ aus, klicken Sie mit der rechten Maustaste und wählen Sie „Löschen“ aus.

5.3 Einführung

Sie können das System jetzt nutzen. Weitere Informationen finden Sie im SCC-Benutzerhandbuch unter “Quick Start” (Schnellstart).

Aufrüstung auf Sentinel 6

6

In diesem Kapitel werden die folgenden Themen behandelt:

Dieses Kapitel bietet einen anspruchsvollen Überblick über die Aufrüstung früherer Versionen von Sentinel auf Sentinel 6.0. Bei den grundlegenden Schritten handelt es sich um die Sicherung früherer Sentinel-Versionen, die Installation/Deinstallation der Software, die Konfigurationsänderungen und die Datenmigration.

Hinweis: In diesem Dokument werden keine detaillierten Verfahren zur Durchführung der Aufrüstung vorgestellt. Detaillierte Informationen finden Sie in der Dokumentation zur Patch-Installation auf der Novell-Dokumentationswebsite (http://www.novell.com/documentation/).

Für die Patch-Aktualisierung auf Sentinel 6.0 stehen die folgenden Patch-Installationsprogramme zur Verfügung:

- Sentinel 4.x auf Sentinel 6.0
- Sentinel 5.x auf Sentinel 6.0

Es gibt zahlreiche wichtige Änderungen zwischen Sentinel 6.0 und früheren Versionen, die sich gegebenenfalls auf Ihre Aufrüstung auswirken. Weitere Einzelheiten finden Sie in der Dokumentation zur Patch-Installation.

- Es gibt kleinere Änderungen beim Datenbankschema zwischen Sentinel 5.x und 6.0 und größere zwischen Sentinel 4.x und 6.0. Aufgrund dieser Schemaänderungen wird mit Sentinel 6.0 eine neue Berichtsbibliothek zur Verfügung gestellt und an benutzerdefinierten Berichten müssen möglicherweise Änderungen vorgenommen werden.
- Die neue Ereignisquellenverwaltung erfordert gegebenenfalls einige kleinere Änderungen an Collectors, um neue Connectors zu verwenden.
- Für Benutzer von Sentinel Control Center sind neue Benutzerberechtigungen verfügbar.
- Die Systemanforderungen haben sich geändert, einschließlich der Unterstützung verschiedener neuer Plattformen.
- Die Verzeichnisstruktur wurde geändert, sodass Skripts, die sich auf Verzeichnispfade beziehen, unter Umständen aktualisiert werden müssen.

6.1 Aufrüstung von Sentinel 5.x auf Sentinel 6.0

Folgendes ist zu beachten:

- Bei der Aufrüstung von Sentinel 5.x auf Sentinel 6.0 handelt es sich um eine Vor-Ort-Aufrüstung, die mit dem Sentinel-Patch-Installationsprogramm durchgeführt wird.
- Die Datenmigration von Microsoft SQL Server 2000 für Sentinel 5.x auf Microsoft SQL Server 2005 für Sentinel 6.0 wird unterstützt. (SQL Server 2000 wird in Sentinel 6 nicht mehr unterstützt.)

- Die Datenmigration von Oracle 9i für Sentinel 5.x auf Oracle 10g für Sentinel 6.0 wird unterstützt.
- Die Datenmigration von einer nicht-Unicode-Datenbank auf eine Unicode-Datenbank wird nicht unterstützt.
- Bei einer erfolgreichen Datenmigration werden Korrelationsregeln und iTRAC-Workflow-Schablonen nicht migriert. Korrelationsregeln können aus Version 5.x exportiert und in Version 6.0 importiert werden. Die iTRAC-Workflow-Schablonen müssen in Sentinel 6.0 neu erstellt werden.

So führen Sie die Aufrüstung von Sentinel 5.x auf Sentinel 6.0 durch

- Überprüfen der Systemanforderungen.
  - Überprüfen Sie, ob die Hardwarespezifikationen des Systems den in Kapitel 2, „Optimale Verfahren“, auf Seite 19 genannten Hardwareanforderungen entsprechen.
  - Überprüfen Sie, ob die Version des Betriebssystems und der Datenbank den in Kapitel 2, „Optimale Verfahren“, auf Seite 19 genannten Systemanforderungen entspricht.
- Sichern der erforderlichen Komponenten
  - Sentinel Server
  - Sentinel Collector Manager
  - Crystal Reporting-Server
  - Datenbankserver
  - Collector-Skripts
  - Exportieren der Korrelationsregeln
  - Sichern der iTRAC-Workflows
- Ausführen des Patch-Installationsprogramms von Novell
- Installieren der Sentinel 6.0-Datenbank
- Durchführen der Datenmigration
- Installieren von Sentinel 6.0 (ausgenommen Datenbank)
- Konfigurieren der Objekte
  - Benutzerberechtigungen aktualisieren
  - Menükonfigurationen aktualisieren
  - Email-Einstellungen neu konfigurieren
  - Collectors neu bereitstellen (für ausgewählte Collectors sind gegebenenfalls Änderungen erforderlich)
  - Berichte neu bereitstellen

6.2 Aufrüstung von Sentinel 4.x auf Sentinel 6.0

Folgendes ist zu beachten:

- Die Datenmigration von Microsoft SQL Server 2000 für Sentinel 4.x auf Microsoft SQL Server 2005 für Sentinel 6.0 wird unterstützt. (SQL Server 2000 wird in Sentinel 6 nicht mehr unterstützt.)

- Die Datenmigration von Oracle 9i für Sentinel 4.x auf Oracle 10g für Sentinel 6.0 wird unterstützt.
- Bei einer erfolgreichen Datenmigration werden die folgenden Objekte von Sentinel 4.x auf Sentinel 6.0 migriert:
  - Benutzer und zugewiesene Berechtigungen
  - Filter
  - Konfigurationsoptionen für das Kontextmenü
  - Umbenannte CV-Tags
  - Partitionskonfigurationen
  - Fallbeispiele aus Version 4.x werden als Vorfälle zu Version 6.0 migriert.
  - Vorfälle und vorfallsbezogene Ereignisse
- Bei einer erfolgreichen Datenmigration werden keinerlei Korrelationsregeln und Ereignisse migriert. Korrelationsregeln können aus Version 5.x exportiert und in Version 6.0 importiert werden. Ereignisse, die Teil eines Vorfalls sind, werden migriert, andere Ereignisse hingegen nicht.

So führen Sie die Aufrüstung von Sentinel 4.x auf Sentinel 6.0 durch

- Systemanforderungen
  - Überprüfen Sie, ob die Hardwarespezifikationen des Systems den in Kapitel 2, „Optimale Verfahren“, auf Seite 19 genannten Hardwareanforderungen entsprechen. Unter Umständen müssen Sie Ihre Hardware aktualisieren, da die Hardwarespezifikationen für Sentinel 4.x und Sentinel 6.0 unterschiedlich sind.
  - Überprüfen Sie, ob die Version des Betriebssystems und der Datenbank den in Kapitel 2, „Optimale Verfahren“, auf Seite 19 genannten Systemanforderungen entspricht.
  - Sichern der erforderlichen Komponenten
  - Sentinel Server
  - Sentinel Collector Manager
  - Crystal Reporting-Server
  - Datenbankserver
  - Collector-Skripts
  - Exportieren der Korrelationsregeln
  - Sichern der iTRAC-Workflows
- Ausführen des Patch-Installationsprogramms von Novell
- Installieren der Sentinel 6.0-Datenbank
  - Sie müssen eine neue Datenbank oder eine neue Instanz der Datenbank installieren. Das Datenbankschema für Sentinel 4.x weicht von dem für Sentinel 6.0 ab. Es gibt nur wenige Tabellen, die in Sentinel 6.0 berücksichtigt/gelöscht werden. Beim Installieren einer neuen Datenbank oder einer neuen Datenbankinstanz werden diese Tabellen in Sentinel 6.0 erstellt/gelöscht.
- Durchführen der Datenmigration
- Installieren von Sentinel 6.0 (ausgenommen Datenbank)

- Konfigurieren der Objekte
  - Benutzerberechtigungen aktualisieren
  - Menükonfigurationen aktualisieren
  - Email-Einstellungen neu konfigurieren
  - Collectors neu bereitstellen (für ausgewählte Collectors sind gegebenenfalls Änderungen erforderlich)
  - Ändern Sie Berichte und stellen Sie sie erneut bereit.

Installieren der Sentinel-Komponenten

7

In diesem Kapitel werden die folgenden Themen behandelt:

Es gibt verschiedene Szenarios, in denen Sie unter Umständen Komponenten zu einer bestehenden Installation hinzufügen müssen:

- Es befinden sich bereits Sentinel-Komponenten auf einem Computer und es werden weitere Komponenten benötigt. (Beispiel: Collector Manager ist auf einem Computer installiert und es wäre hilfreich, auch Sentinel Control Center hinzuzufügen.)
- Um eine möglichst hohe Leistung zu erzielen, empfiehlt es sich, in einer Umgebung mit hoher Ereignisrate eine neue Collector Manager-Instanz oder eine neue Correlation Engine hinzuzufügen.

Die Aufgaben in jedem dieser Szenarios können problemlos mit dem Sentinel-Installationsprogramm gelöst werden.

7.1 Installieren einer neuen Komponente auf einem Sentinel-Computer

Zeitweise kann es notwendig sein, einen weiteren Computer in der Sentinel-Umgebung hinzuzufügen. Wenn die Speicherauslastung auf dem Correlation Engine-Computer hoch ist, sollten Sie unter Umständen einen entsprechenden zusätzlichen Computer hinzufügen. Sie möchten möglicherweise eine Collector Manager-Instanz an einem Remotestandort hinzufügen, um Daten lokal zu sammeln, oder ein neuer Mitarbeiter benötigt Sentinel Control Center auf seinem Desktop.

Für die Installation von Sentinel-Komponenten auf einem neuen Computer müssen verschiedene Voraussetzungen erfüllt sein:

- IP-Adresse oder Hostname des Computers, auf dem sich der Kommunikationsserver befindet
- Zugriff auf eine Kopie der Keystore-Datei auf einem beliebigen Computer in der bestehenden Sentinel-Installation
- Diese Datei befindet sich im Verzeichnis %ESEC_HOME%\config (Windows) oder $ESEC_HOME/config (Linux und Solaris).
- Sie müssen in der Lage sein, von dem Computer aus, auf dem Sie die Installation durchführen, zu der Keystore-Datei zu navigieren.
- Die bei der ursprünglichen Sentinel-Installation verwendeten Portnummern.

Hinweis: Die Keystore-Datei und die Portnummern müssen auf allen Computern im Sentinel-System identisch sein, um die Kommunikation zu ermöglichen. Es gibt zwei Ausnahmen: Die

Keystore-Datei wird nicht benötigt, wenn Sentinel Control Center installiert wird oder wenn Collector Manager mithilfe der SSL-Proxykommunikation installiert wird.

So fügen Sie Komponenten hinzu

1. Melden Sie sich als Benutzer mit Administratorrechten (Windows) oder als Benutzer „root“ (Solaris) an.
2. Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.
3. Wechseln Sie zu der CD und doppelklicken Sie auf:
   - Solaris:

     GUI-Modus:

     `./setup.sh`

     oder

     Für Textmodus („kopflos“):

     `./setup.sh -console`
   - Windows: setup.bat.

   Hinweis: Die Installation im Konsolenmodus wird unter Windows nicht unterstützt.
4. Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.
5. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf „Weiter“.
6. Wenn Sie eine weitere Komponente installieren, wird ein Fenster angezeigt, in dem der Speicherort der früheren Installation und die bereits installierten Komponenten angegeben sind. Bei einer Neuinstallation von Sentinel wird ein Fenster mit Informationen zum Standardinstallationsverzeichnis angezeigt. Klicken Sie auf „Durchsuchen“, um das Installationsverzeichnis zu ändern. Klicken Sie auf „Weiter“.
7. Wählen Sie die Komponenten aus, die Sie hinzufügen möchten.

   Szenario 1: Es werden nur Anwendungen installiert.

   7a Wählen Sie als Installationstyp „Benutzerdefiniert“ aus und klicken Sie auf „Weiter“.

   7b Wählen Sie die Anwendungen (Sentinel Collector Builder, Sentinel Control Center und Sentinel Data Manager) aus und klicken Sie auf „Weiter“.

   7c Eine Eingabeaufforderung für die JVM-Heap-Größe (Java Virtual Machine) wird angezeigt. Klicken Sie auf „Weiter“.

   JVM-Heap-Größe (MB): Standardmäßig ist dieser Wert als die Hälfte des auf dem Computer erkannten physischen Arbeitsspeichers festgelegt (maximal 1.024 MB). Dies ist die maximal von Sentinel Control Center verwendete JVM-Heap-Größe.

   7d Sie werden aufgefordert, Informationen zum Port und zum Namen des Hostservers einzugeben. Geben Sie die erforderlichen Informationen ein und klicken Sie auf „Weiter“.

Szenario 2: Installation von Correlation Engine (weitere Komponenten) nach der Installation der Anwendung:

7e Wählen Sie Correlation Engine aus und klicken Sie auf „Weiter“.

7f Wählen Sie die Methode für den Erhalt des Nachrichtenbusschlüssels aus. Geben Sie an, ob eine zufällige Keystore-Datei generiert oder eine vorhandene Keystore-Datei von einem anderen Computer im Sentinel-System importiert werden soll. Wenn Sie eine

vorhandene Keystore-Datei importieren möchten, müssen Sie zum Speicherort der Datei navigieren und die Keystore-Datei auswählen. Klicken Sie auf „Weiter“.

Szenario 3: Installation von Correlation Engine und Anwendungen

7g Wählen Sie als Installationstyp „Benutzerdefiniert“ aus und klicken Sie auf „Weiter“.

7h Wählen Sie die Anwendungen (Sentinel Collector Builder, Sentinel Control Center und Sentinel Data Manager) sowie Correlation Engine aus und klicken Sie auf „Weiter“.

7i Eine Eingabeaufforderung für die JVM-Heap-Größe (Java Virtual Machine) wird angezeigt. Klicken Sie auf „Weiter“.

7j Sie werden aufgefordert, den Proxy-Port für Sentinel Control Center und den Hostnamen für den Kommunikationsserver einzugeben. Geben Sie die erforderlichen Informationen ein und klicken Sie auf „Weiter“.

7k Wählen Sie die Methode für den Erhalt des Verschlüsselungsschlüssels für den Nachrichtenbus aus. Geben Sie an, ob eine zufällige Keystore-Datei generiert oder eine vorhandene Keystore-Datei von einem anderen Computer im Sentinel-System importiert werden soll. Wenn Sie eine vorhandene Keystore-Datei importieren möchten, müssen Sie zum Speicherort der Datei navigieren und die Keystore-Datei auswählen. Klicken Sie auf „Weiter“.

Szenario 4: Installation von Sentinel Collector Service und Anwendungen

7l Wählen Sie als Installationstyp „Benutzerdefiniert“ aus und klicken Sie auf „Weiter“.

7m Wählen Sie die Anwendungen (Sentinel Collector Builder, Sentinel Control Center und Sentinel Data Manager) sowie Sentinel Collector Service aus und klicken Sie auf „Weiter“.

7n Eine Eingabeaufforderung für die JVM-Heap-Größe (Java Virtual Machine) wird angezeigt. Klicken Sie auf „Weiter“.

7o Für die Kommunikation zwischen den Sentinel-Clients und dem Server stehen zwei Möglichkeiten zur Verfügung. Sie können zwischen „Direkte Verbindung mit Nachrichtenbus herstellen“ und „Verbindung mit Nachrichtenbus über Proxy herstellen“ wählen. Klicken Sie auf „Weiter“.

7p Sie werden zur Eingabe des Nachrichtenbus-Ports, des Sentinel Control Center-Proxy-Ports und des Hostnamens für den Kommunikationsserver aufgefordert. Geben Sie die erforderlichen Informationen ein und klicken Sie auf „Weiter“.

Hinweis: Wenn Sie „Verbindung mit Nachrichtenbus über Proxy herstellen“ ausgewählt haben, ist die zusätzliche Option „Authentifizierungsport für Collector Manager-Zertifikat“ verfügbar.

7q Wählen Sie die Methode für den Erhalt des Nachrichtenbusschlüssels aus. Geben Sie an, ob eine zufällige Keystore-Datei generiert oder eine vorhandene Keystore-Datei von einem anderen Computer im Sentinel-System importiert werden soll. Wenn Sie eine vorhandene Keystore-Datei importieren möchten, müssen Sie zum Speicherort der Datei navigieren und die Keystore-Datei auswählen. Klicken Sie auf „Weiter“.

8 Der Bildschirm „Zusammenfassung“ wird angezeigt. Überprüfen Sie die Installationszusammenfassung und klicken Sie auf „Installieren“.

9 Nach Abschluss der Installation werden Sie aufgefordert, das System neu zu booten. Wählen Sie die Option zum Neustarten des Computers aus und klicken Sie anschließend auf „Fertig stellen“, um das System neu zu booten.

7.1.1 Installieren der Sentinel-Datenbank

So installieren Sie die Sentinel 6-Datenbank

1 Bevor Sie mit der Installation beginnen, müssen Sie unter Windows die folgenden Umgebungsvariablen löschen, wenn Sentinel zuvor installiert wurde.

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

2 Melden Sie sich als Benutzer mit Administratorrechten (Windows) oder als Benutzer „root“ (Solaris oder Linux) an.

3 Legen Sie die Sentinel-Installations-CD in das CD-ROM-Laufwerk ein.

4 Wechseln Sie zu der CD und doppelklicken Sie auf:

- Linux/Solaris:

  GUI-Modus:

  ```
  ./setup.sh
  ```

  oder

  Für Textmodus („kopflos“):

  ```
  ./setup.sh -console
  ```

- Windows: setup.bat.

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

5 Klicken Sie nach dem Lesen des Begrüßungsbildschirms auf Weiter.

6 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf „Weiter“.

7 Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf Durchsuchen, um einen anderen Speicherort für die Installation anzugeben. Klicken Sie auf „Weiter“.

8 Wählen Sie als Installationstyp „Benutzerdefiniert“ (Standard) aus. Klicken Sie auf „Weiter“.

9 Heben Sie im Fenster zum Auswählen von Funktionen die Auswahl aller Optionen auf und wählen Sie dann „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.

---

10 Konfigurieren Sie die Datenbank für die Installation:

- Unter Windows:

10a Wählen Sie die Serverplattform für die Zieldatenbank aus.

- Wählen Sie Microsoft SQL Server 2005 aus.
- Geben Sie das Verzeichnis für das Protokoll der Datenbankinstallation an.

Klicken Sie auf „Weiter“.

10b Geben Sie den Speicherort für folgende Verzeichnisse an:

- Datenverzeichnis
- Indexverzeichnis
- Zusammenfassungsdatenverzeichnis
- Zusammenfassungsindexverzeichnis
- Protokollverzeichnis

Klicken Sie auf „Weiter“.

10c Wählen Sie die Option zur Unterstützung des Zeichensatzes für die Datenbak aus: entweder Unicode oder Nur ASCII-Datenbank. Klicken Sie auf „Weiter“.

10d Geben Sie die Größe der Datenbank an. Klicken Sie auf „Weiter“.

10e Konfigurieren Sie Datenbankpartitionen.

- Sie können die Option zum Aktivieren automatischer Datenbankpartitionen auswählen.
- Geben Sie für die Datenpartitionen das Archivverzeichnis an. Machen Sie Zeitangaben für das Hinzufügen und Archivieren der Daten.

Klicken Sie auf „Weiter“.

Unter Linux/Solaris:

10f Wählen Sie die Serverplattform für die Zieldatenbank aus.

- Wählen Sie in der Dropdown-Liste „Oracle 10g“ aus.
- Wählen Sie „Eine neue Datenbank mit Datenbankobjekten erstellen“ aus.

Klicken Sie auf „Weiter“.

10g Geben Sie einen Oracle-Benutzernamen an, oder akzeptieren Sie den Standardbenutzernamen. Klicken Sie auf OK

10h Wählen Sie den Oracle JDBC-Treiber aus und geben Sie den Datenbanknamen an. Klicken Sie auf „Weiter“.

10i Übernehmen Sie die Standardwerte für den Arbeitsspeicher und den Listener-Port, oder geben Sie neue Werte ein.

10j Geben Sie SYS und den SYS-Berechtigungsnachweis ein und klicken Sie auf „Weiter“.

10k Geben Sie die Größe der Datenbank an. Klicken Sie auf „Weiter“.

10l Geben Sie den Speicherort für folgende Verzeichnisse an:

- Datenverzeichnis

- Indexverzeichnis
- Zusammenfassungsdatenverzeichnis
- Zusammenfassungsindexverzeichnis
- Protokollverzeichnis

Klicken Sie auf „Weiter“.

10m Konfigurieren Sie Datenbankpartitionen.

- Wählen Sie die Option zum automatischen Aktivieren von Datenbankpartitionen aus.
- Geben Sie das Archivverzeichnis für die Datenpartition an.
- Machen Sie Zeitangaben für das Hinzufügen und Archivieren von Daten.

Klicken Sie auf „Weiter“.

11 Geben Sie Authentifizierungsinformationen für folgende Benutzer an:

- Sentinel-Datenbankadministratorbenutzer
- Sentinel-Anwendungsdatenbankbenutzer
- Sentinel-Administratorbenutzer
- Sentinel Report-Benutzer (nur Windows)

Klicken Sie auf „Weiter“.

12 Es wird eine Zusammenfassung der ausgewählten Datenbankparameter angezeigt. Klicken Sie auf „Weiter“.

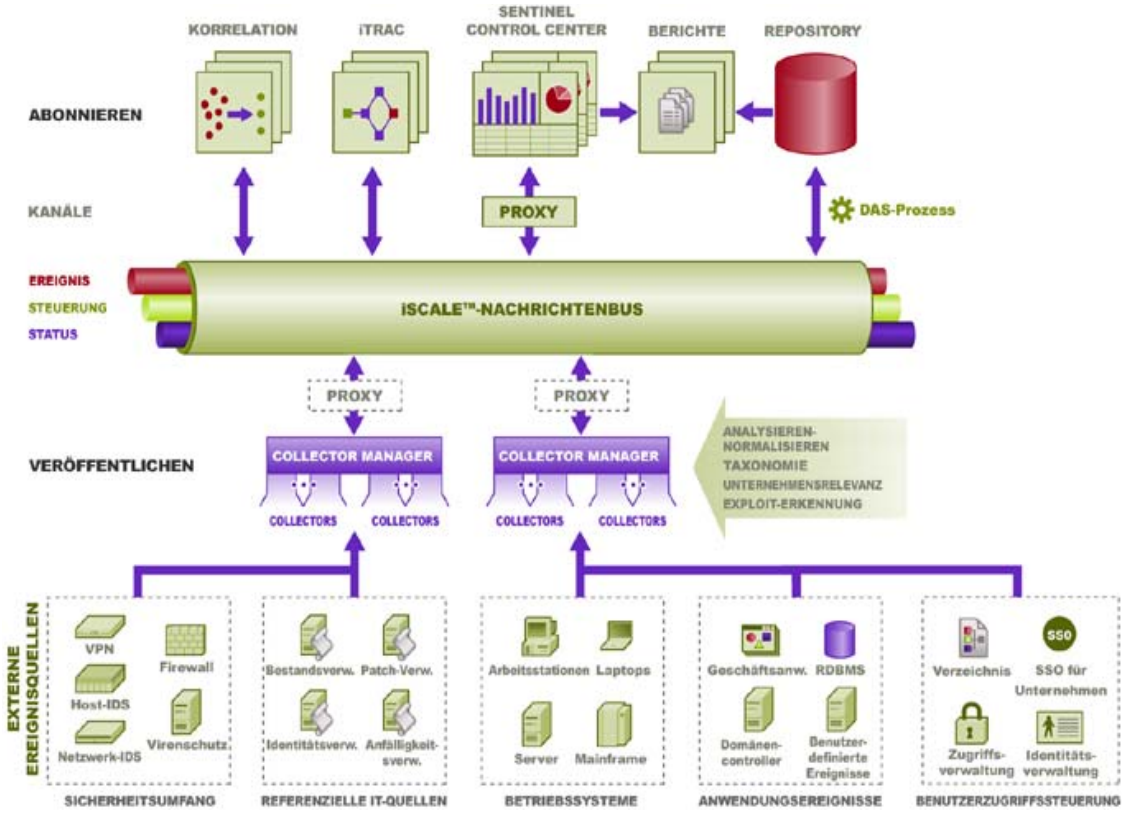
13 Die Installationszusammenfassung wird angezeigt. Klicken Sie auf Installieren.

14 Wählen Sie nach erfolgreicher Installation die Option zum Neustarten des Systems aus und klicken Sie dann auf „Fertig stellen“.

Kommunikationsschicht (iSCALE) 8

In diesem Kapitel werden die folgenden Themen behandelt:

Bei der Kommunikationsschicht (iSCALE), die alle Komponenten der Architektur miteinander verbindet, handelt es sich um eine verschlüsselte TCP/IP-basierte Verbindung, die auf einem JMS-Backbone (Java Messaging Service) aufgebaut wird. Mit Sentinel 6 wurde ein optionaler SSL-Proxy hinzugefügt, um die Komponenten Collector Manager und Sentinel Control Center zu schützen, falls diese außerhalb der Firewall installiert sind.



Bei der Installation von Collector Manager stehen zwei Kommunikationsoptionen zur Verfügung:

- **Direkte Verbindung mit Nachrichtenbus herstellen (Standard):** Dies ist die einfachste und schnellste Option. Sie erfordert, dass Collector Manager den Verschlüsselungsschlüssel für den gemeinsamen Nachrichtenbus kennt. Dies kann jedoch ein Sicherheitsrisiko darstellen, wenn Collector Manager auf einem Computer ausgeführt wird, der Sicherheitsbedrohungen ausgesetzt ist (z. B. ein Computer in der DMZ). Mit dieser Option wird die Kommunikation mithilfe der AES 128-Bit-Verschlüsselung basierend auf dem Wert in einer als Keystore-Datei bezeichneten Datei verschlüsselt.
- **Verbindung mit Nachrichtenbus über Proxy herstellen:** Mit dieser Option wird eine zusätzliche Sicherheitsebene hinzugefügt, indem Collector Manager so konfiguriert wird, dass

Verbindungen über einen SSL-Proxyserver hergestellt werden. In diesem Fall wird die zertifikatbasierte Authentifizierung und Verschlüsselung verwendet, sodass die Keystore-Datei nicht auf dem Collector Manager-Computer gespeichert werden muss. Diese Option ist sinnvoll, wenn Collector Manager in einer weniger sicheren Umgebung installiert wird.

Jede dieser Optionen kann beim Installieren von Collector Manager gewählt werden. Für Sentinel Control Center wird standardmäßig die Proxyeinstellung verwendet.

8.1 SSL-Proxy und direkte Kommunikation

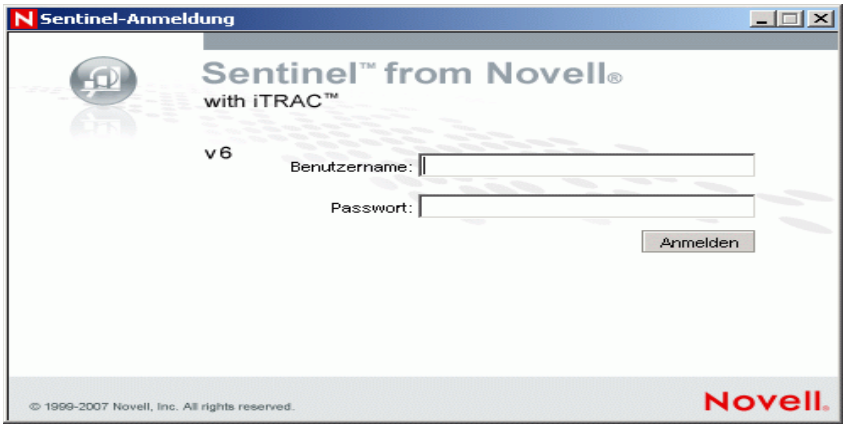
Bei den Sentinel-Komponenten, die den SSL-Proxy verwenden können, handelt es sich um Sentinel Control Center und Collector Manager.

8.1.1 Sentinel Control Center

Sentinel Control Center verwendet den SSL-Proxy als Standardeinstellung. Sentinel Control Center stellt die Verbindung zu SSL über den proxied_client-Port her. Dieser Port ist für die ausschließliche Verwendung der serverseitigen SSL-Zertifikatauthentifizierung eingerichtet. Für die Authentifizierung auf der Clientseite wird der Benutzername und das Passwort des Sentinel Control Center-Benutzers verwendet.

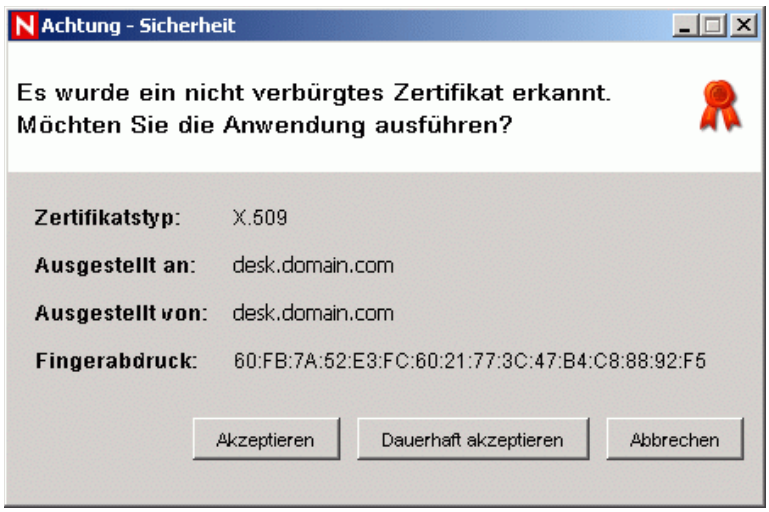
So melden Sie sich zum ersten Mal an Sentinel Control Center an

1. Wählen Sie „Start“ > „Programme“ > „Sentinel“ und dann „Sentinel Control Center“ aus. Das Sentinel-Anmeldefenster wird angezeigt.



2. Geben Sie Ihren Benutzerberechtigungsnachweis ein, um sich an Sentinel Control Center anzumelden.
   - Benutzername und Passwort bei SQL Server-Authentifizierung ODER
   - Domäne\Benutzername und Passwort bei Windows-Authentifizierung
3. Klicken Sie auf Anmelden.

4 Für den ersten Anmeldeversuch wird eine Warnmeldung (siehe Abbildung) angezeigt.



5 Wenn Sie „Akzeptieren“ auswählen, wird diese Meldung jedes Mal angezeigt, wenn Sie versuchen, Sentinel auf Ihrem System zu öffnen. Um dies zu vermeiden, können Sie „Dauerhaft akzeptieren“ auswählen.

So starten Sie Sentinel Control Center unter Linux und Solaris

1 Ändern Sie als Sentinel-Administratorbenutzer („esecadm“) das Verzeichnis wie folgt:
`$ESEC_HOME/bin`

2 Führen Sie den folgenden Befehl aus:
`control_center.sh`

3 Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf „OK“.

4 Klicken Sie in dem daraufhin angezeigten Zertifikatfenster auf „Akzeptieren“.

Benutzer von Sentinel Control Center müssen das obige Verfahren wiederholen, um unter folgenden Umständen ein neues Zertifikat zu akzeptieren:

- Der Sentinel-Kommunikationsserver wurde neu installiert.
- Der Sentinel-Kommunikationsserver wurde auf einen neuen Server verschoben.

8.1.2 Collector Manager

Collector Manager kann im Proxymodus (Verwendung von SSL-Proxy) oder im direkten Modus (direkte Verbindung mit dem Nachrichtenbus) installiert werden.

- Für Collector Manager-Instanzen, die eher Gefährdungen ausgesetzt sind (zum Beispiel ein Computer in der DMZ) bietet die Kommunikationsmethode, bei der die Verbindung über den SSL-Proxy hergestellt wird, mehr Sicherheit.
- Für Collector Manager-Instanzen in einer Umgebung mit höherer Sicherheit, wenn ein hoher Ereignisdurchsatz wichtig ist oder wenn die Collector Manager-Instanzen auf demselben Computer wie Data Access Service (DAS) installiert sind, empfiehlt sich die direkte Kommunikation mit dem Nachrichtenbus.

Collector Manager stellt die Verbindung zu SSL über den proxied_trusted_client her. Um den Neustart von Collector Manager nach einem Reboot ohne menschliches Eingreifen zu ermöglichen, wird dieser Port so eingerichtet, dass sowohl die Server- als auch die Client-SSL-Zertifikatauthentifizierung verwendet wird. Zwischen dem Proxy und Collector Manager wird eine Vertrauensstellung eingerichtet (Zertifikataustausch), wobei das Zertifikat bei zukünftigen Verbindungen für die Authentifizierung verwendet wird. Diese Vertrauensstellung wird bei der Installation automatisch eingerichtet.

Die Vertrauensstellung muss unter den folgenden Umständen für jede Collector Manager-Instanz, die den SSL-Proxy verwendet, zurückgesetzt werden:

- Der Sentinel-Kommunikationsserver wurde neu installiert.
- Der Sentinel-Kommunikationsserver wurde auf einen neuen Server verschoben.

So setzen Sie die Vertrauensstellung für eine Collector Manager-Instanz zurück

1. Melden Sie sich bei dem Collector Manager-Server als Sentinel-Administrator an (standardmäßig „esecadm“).
2. Öffnen Sie die Datei configuration.xml im Verzeichnis $ESEC_HOME/config oder %ESEC_HOME%\config in einem Texteditor.
3. Ändern Sie die Services „Collector_Manager“, „agentmanager_events“ und „Sentinel“ in der Datei configuration.xml so, dass die Strategie-ID „proxied_trusted_client“ verwendet wird. Nachfolgend finden Sie einen Auszug aus einer Beispieldatei.

```
<service name="Collector_Manager" plugins=""
strategyid="proxied_trusted_client"/>
<service name="agentmanager_events" plugins=""
strategyid="proxied_trusted_client"/>
<service name="Sentinel" plugins=""
strategyid="proxied_trusted_client"/>
```

4. Speichern und schließen Sie die Datei.
5. Öffnen Sie die Datei sentinel.xml im Verzeichnis $ESEC_HOME/config oder %ESEC_HOME%\config in einem Texteditor.
6. Entfernen Sie die folgende Komponente aus der Datei sentinel.xml:

```
<obj-component id="SentinelRemoteLoggingService">
<!-- Must be after the service manager -->
<class>esecurity.ccs.comp.audit.LogHandlerService</class>
<property name="Level">SEVERE</property>
</obj-component>
```

7. Speichern und schließen Sie die Datei.
8. Führen Sie %ESEC_HOME%\bin\register_trusted_client.bat aus (oder die .sh-Datei unter UNIX). Eine Ausgabe ähnlich der Folgenden wird angezeigt:

```
E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
Please review the following server certificate:
Type:X.509
Issued To:foo.bar.net
Issued By:foo.bar.net
Would you like to accept this certificate? [Y/N] (defaults to N): Y
Please enter a Sentinel username and password that has permissions
to register a trusted client.
Username: esecadm
```

```
Password:*********
*Writing to keystore file: E:\Program
Files\novell\sentinel6\config\.proxyClientKeystore
```

9 Starten Sie Sentinel Service auf dem Server neu, auf dem sich der Kommunikationsserver befindet. Warten Sie, bis die Initialisierung von DAS Proxy abgeschlossen ist.

10 Starten Sie Sentinel Service auf dem Server neu, auf dem sich Collector Manager befindet.

11 Wiederholen Sie diese Schritte für alle Collector Manager-Instanzen, die sich der Proxykommunikation bedienen.

8.2 Änderungen bei Verschlüsselungsschlüsseln

Die Sentinel-Installation bietet dem Administrator die Möglichkeit, einen neuen zufälligen Verschlüsselungsschlüssel (gespeichert in der Keystore-Datei) zu generieren oder eine vorhandene Keystore-Datei zu importieren. Unabhängig vom gewählten Verfahren muss die Keystore-Datei auf allen Computern in der Sentinel-Umgebung identisch sein, damit eine ordnungsgemäße Kommunikation möglich ist.

Hinweis: Die Keystore-Datei wird auf dem Datenbankcomputer nicht benötigt, wenn auf diesem Computer als einzige Sentinel-Komponente die Datenbank installiert ist.

Der Verschlüsselungsschlüssel kann mit dem Dienstprogramm keymgr geändert werden. Das Programm generiert im Verzeichnis lib einer Sentinel-Installation ($ESEC_HOME/lib or %ESEC_HOME%\lib) eine Datei mit der Bezeichnung .keystore. Diese Datei muss auf jedem Computer, auf dem eine Sentinel-Komponente installiert ist, in das gleiche Verzeichnis kopiert werden.

So ändern Sie den Verschlüsselungsschlüssel für die direkte Kommunikation

1 Melden Sie sich unter UNIX als Sentinel-Administratorbenutzer an (standardmäßig „esecadm“). Melden Sie sich unter Windows als Benutzer mit Administratorrechten an.

2 Navigation:

Für Windows:

```
%ESEC_HOME%\bin
```

Bei UNIX:

```
$ESEC_HOME/bin
```

3 Führen Sie den folgenden Befehl aus:

Unter Windows:

```
"%ESEC_JAVA_HOME%\java" -jar keymgr.jar --keyalgo AES --keysize 256
--keystore <filename, usually .keystore>
```

Unter UNIX:

```
$ESEC_JAVA_HOME/java -jar keymgr.jar --keyalgo AES --keysize 256 --
keystore <filename, usually .keystore>
```

4 Kopieren Sie die Keystore-Datei auf jeden Computer, auf dem eine Sentinel-Komponente installiert ist (es sei denn, auf dem betreffenden Computer erfolgt die Kommunikation über einen Proxy). Die Datei sollte an folgenden Speicherort kopiert werden:

Für Windows:

```
%ESEC_HOME%\config
```

Bei UNIX:

```
$ESEC_HOME/config
```

8.2.1 Änderungen des Advisor-Passworts

Wenn Sie Advisor im Modus für das direkte Herunterladen verwenden, müssen Sie die in den Advisor-Konfigurationsdateien gespeicherten Passwörter aktualisieren. Dieses Passwort wurde mithilfe der Informationen aus der Keystore-Datei verschlüsselt und muss mit den neuen Keystore-Werten neu erstellt werden.

So verschlüsseln Sie das Advisor-Passwort nach einer Änderung des Verschlüsselungsschlüssels

1. Melden Sie sich unter UNIX an dem Computer, auf dem Advisor installiert ist, als Sentinel-Administratorbenutzer an (standardmäßig „esecadm“). Melden Sie sich unter Windows als Benutzer mit Administratorrechten an.
2. Wechseln Sie in folgendes Verzeichnis:

   Bei UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   Für Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```
3. Geben Sie die folgenden Befehle ein:

   Bei UNIX:

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   Für Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

Crystal Reports für Windows

9

In diesem Kapitel werden die folgenden Themen behandelt:

Crystal BusinessObjects Enterprise™ ist ein Berichterstellungswerkzeug.

In diesem Kapitel wird die Installation und Konfiguration von Crystal Reports Server für Sentinel erläutert.

Sentinel unterstützt die Ausführung von Crystal Reports Server auf den folgenden Plattformen:

- Windows – Wird unterstützt, wenn die Sentinel-Datenbank unter Windows oder Linux ausgeführt wird.
- Linux – Wird unterstützt, wenn die Sentinel-Datenbank unter Linux ausgeführt wird.

In diesem Kapitel wird die Ausführung von Crystal Reports Server unter Windows erläutert. Weitere Informationen zum Ausführen von Crystal Reports Server unter Linux finden Sie in Kapitel 10, „Crystal Reports für Linux“, auf Seite 141.

So installieren Sie Crystal Reports Server

1. Installieren von Microsoft IIS und ASP.NET
2. Installieren von Microsoft SQL (je nach Konfiguration als Windows-Authentifizierung oder SQL Server-Authentifizierung)
3. Installieren von Crystal Server
   - Konfigurieren von Open Database Connectivity (ODBC) für SQL-Authentifizierung

     oder
   - Installieren und Konfigurieren der Oracle 9i-Clientsoftware
4. Konfigurieren von inetmgr

5 Anwenden von Patches auf Crystal Reports-Berichte

6 Veröffentlichen (Importieren) von Crystal Reports-Berichten

7 Einrichten eines Kontos für einen benannten Benutzer

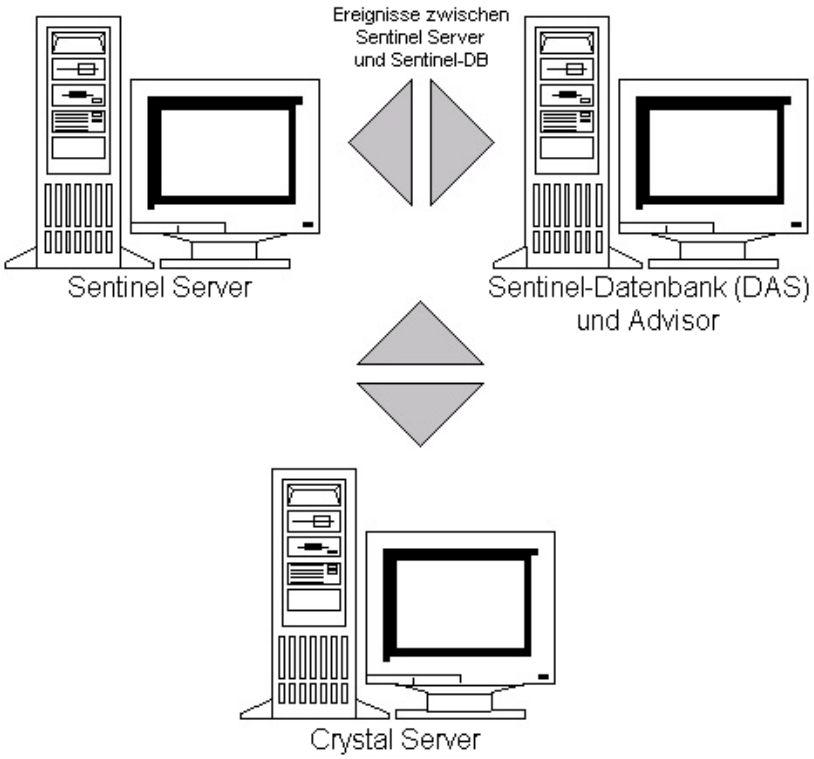
8 Testen der Konnektivität zum Webserver

9 Erhöhen der Datensatzgrenze für die Berichtsaktualisierung in Crystal Enterprise Server (empfohlen)

10 Konfigurieren von Sentinel Control Center für die Integration in Crystal Enterprise Server

Die Installation sollte in der angegebenen Reihenfolge vorgenommen werden.

Hinweis: Die Installation von Crystal Reports Server muss in der obigen Reihenfolge durchgeführt werden.



9.1 Überblick

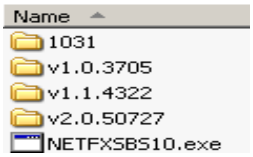
Crystal Reports Server benötigt eine Datenbank zum Speichern von Informationen über das System und dessen Benutzer. Diese Datenbank ist als Central Management Server-(CMS-)Datenbank bekannt. Der CMS ist ein Server, der Informationen über das Crystal Reports Server-System speichert. Nach Bedarf können weitere Komponenten von Crystal Reports Server Zugriff auf diese Informationen erlangen.

Eine CMS-Datenbank muss über einer lokalen Microsoft SQL Server-Datenbank eingerichtet werden. Mit dem Installationsprogramm von Crystal Reports Server können Sie die CMS-Datenbank über der MSDE-Datenbank einrichten, wenn kein lokaler Microsoft SQL 2005 Server installiert ist. Sentinel unterstützt keine MSDE-Konfiguration.

9.2 Systemanforderungen

Windows® 2003 Server mit SP1 mit einer NTFS-formatierten Partition und installiertem IIS (Microsoft Internet Information Server) und NET.ASP. Sentinel unterstützt Crystal XI auf Windows® 2000 Server nicht.

.NET Framework 1.1 (Unter Windows 2003 standardmäßig installiert. BusinessObjects Enterprise™ XI bietet keine Unterstützung für .NET Framework 2.0). 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:

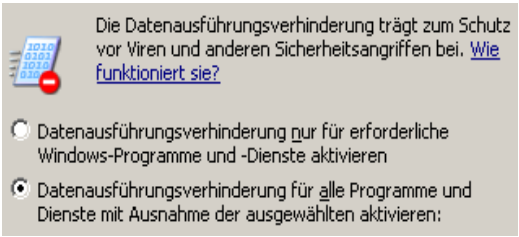


9.3 Konfigurationsanforderungen

1. Vergewissern Sie sich, dass das für die Installation von Crystal Reports Server verwendete Konto über lokale Administratorrechte verfügt.
2. Richten Sie die Datenausführungsverhinderung so ein, dass sie nur für erforderliche Windows-Programme und -Services ausgeführt wird. Dies ist insbesondere hilfreich zur Vermeidung des folgenden Fehlers „Error 1920. Service Crystal Report Cache Server on Windows 2003“.

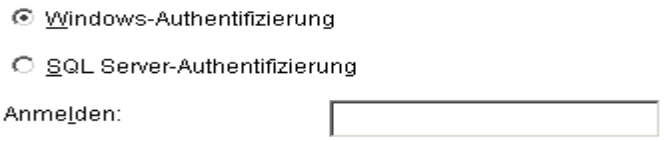
   Der Zugriff auf die Datenausführungsverhinderung erfolgt über die „Systemsteuerung“ > „System“ > Registerkarte „Erweitert“ > „Leistungseinstellungen“ > „Datenausführungsverhinderung“.

   Wählen Sie die Option „Datenausführungsverhinderung nur für erforderliche Windows-Programme und -Dienste aktivieren“ aus.

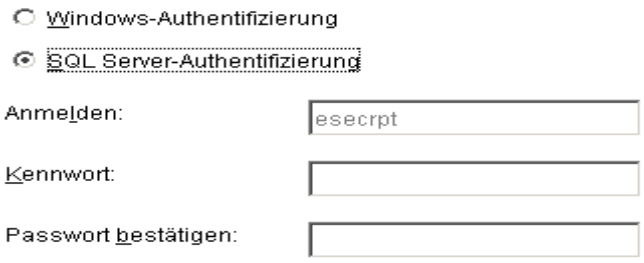


   Wenn Sie vorhaben, Sentinel-Berichte mithilfe der Windows NT-Authentifzierung auszuführen, müssen Sie sicherstellen, dass das Windows-Domänenkonto für Sentinel Report-Benutzer bereits in der Sentinel-Datenbank vorhanden ist. Dies erfolgt während der Sentinel-Installation durch Auswahl von Windows-Authentifizierung bei der Einstellung von

Authentifizierungsmethode für den Sentinel Report-Benutzer, wie in der Abbildung unten gezeigt.



3. 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 Microsoft SQL-Datenbank erfolgt dies während der Sentinel-Installation für Microsoft SQL durch Auswahl der SQL Server-Authentifizierung bei der Festlegung der Authentifizierungsmethode für den Sentinel Report-Benutzer (siehe folgende Abbildung).



   - Bei Sentinel Oracle-Datenbanken erfolgt dies während der Sentinel-Installation für Oracle. esecrpt nimmt dasselbe Passwort an wie esecadm.
4. Bei Oracle 9i Client Release 2 (9.2.0.1.0) müssen Sie dies vor der Installation von Crystal BusinessObjects Enterprise™ installieren.
5. Bei Microsoft SQL Server müssen Sie Microsoft SQL 2005 vor der Installation von Crystal Reports Server installieren.
6. Video-Auflösung von 1024 x 768 oder höher
7. Installieren Sie Microsoft Internet Information Server (IIS) und NET.ASP

Hinweis: Sentinel unterstützt MSDE nicht. Installieren Sie Microsoft SQL 2005 vor der Installation von Crystal Reports Server XI.

9.3.1 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.

So installieren Sie IIS und ASP.NET

1. Öffnen Sie die Windows-Systemsteuerung und wählen Sie „Software“ aus.

2 Klicken Sie im linken Fensterbereich auf Windows-Komponenten hinzufügen/entfernen.

3 Wählen Sie Anwendungsserver aus.

4 Klicken Sie auf "Details".

5 Wählen Sie ASP.NET und Internet Information Services (IIS) aus.

6 Klicken Sie auf "OK".

7 Klicken Sie anschließend auf "Weiter". Möglicherweise werden Sie aufgefordert, die Windows-Installations-CD einzulegen.

8 Klicken Sie auf Fertig stellen.

9.4 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 werden Verfahren für die manuelle Deinstallation von BusinessObjects Enterprise XI erläutert: http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

Hinweis: Die oben stehende URL war zum Veröffentlichungszeitpunkt dieses Dokuments korrekt.

9.5 Verwenden von Crystal Reports

Weitere Informationen zur Verwendung von Crystal Reports für die Sentinel-Berichterstellung finden Sie in der Crystal Reports-Dokumentation und im Sentinel-Benutzerhandbuch.

9.6 Installationsüberblick

9.6.1 Installationsüberblick für Microsoft SQL 2005 Server mit Windows-Authentifizierung

So installieren Sie Microsoft SQL Server mit Windows-Authentifizierung

1. Installieren von Crystal Reports Server XI – Wenn Sie bei der Installation der Sentinel-Anwendung die Windows-Authentifizierung für den Sentinel Report-Benutzer ausgewählt haben, folgen Sie dem Link in Abschnitt 9.7.1, „Installieren von Crystal Server für Microsoft SQL 2005 Server mit Windows-Authentifizierung“, auf Seite 117.
2. Konfigurieren von Open Database Connectivity (ODBC)
3. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
4. Anwenden von Patches auf Crystal Reports
5. Veröffentlichen von Berichten
6. Einrichten des Benutzers als benanntes Benutzerkonto
7. Importieren von Crystal Report-Schablonen
8. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
9. Konfigurieren von Sentinel für Crystal Enterprise Server

Hinweis: Bei der Installation von Microsoft SQL Server mit Windows-Authentifizierung muss die obige Reihenfolge beachtet werden.

9.6.2 Installationsüberblick für Microsoft SQL 2005 Server mit SQL Server-Authentifizierung

So installieren Sie Microsoft SQL Server mit SQL Server-Authentifizierung

1. Installieren von Crystal Reports Server XI

   Hinweis: Wenn Sie beim Installieren der Sentinel-Anwendung die SQL Server-Authentifizierung für den Sentinel Report-Benutzer ausgewählt haben, folgen Sie dem Link in Abschnitt 9.7.2, „Installieren von Crystal Server für Microsoft SQL 2005 Server mit SQL-Authentifizierung“, auf Seite 124.

   ---

2. Konfigurieren von Open Database Connectivity (ODBC)
3. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
4. Importieren von Crystal Report-Schablonen
5. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
6. Konfigurieren von Sentinel für Crystal Enterprise Server

Hinweis: Bei der Installation von Microsoft SQL Server mit SQL Server-Authentifizierung muss die obige Reihenfolge beachtet werden.

9.6.3 Installationsüberblick für Oracle

So installieren Sie Oracle

Führen Sie zur ordnungsgemäßen Installation von Crystal Reports folgendes Verfahren in der angegebenen Reihenfolge durch.

1. Installation von Oracle 9i Client
2. Installieren von Crystal Reports Server XI Weitere Informationen hierzu finden Sie in Abschnitt 9.7.2, „Installieren von Crystal Server für Microsoft SQL 2005 Server mit SQL-Authentifizierung“, auf Seite 124.
3. Konfigurieren des systemeigenen Oracle-Treibers
4. Zuordnen von Crystal Reports zur Verwendung mit Sentinel
5. Importieren von Crystal Report-Schablonen
6. Erstellen einer Crystal-Webseite (Konfigurieren von .NET Administration Launchpad)
7. Konfigurieren von Sentinel für Crystal Enterprise Server

Hinweis: Die Installation von Oracle muss in der obigen Reihenfolge durchgeführt werden.

9.7 Installation

In diesem Abschnitt wird die Installation von Crystal Server für folgende Elemente beschrieben:

- Microsoft SQL 2005 Server Sentinel-Datenbank mit Windows-Authentifizierung
- Microsoft SQL 2005 Server Sentinel-Datenbank mit SQL Server-Authentifizierung
- Oracle Sentinel-Datenbank

9.7.1 Installieren von Crystal Server für Microsoft SQL 2005 Server mit Windows-Authentifizierung

So installieren Sie BOE XI Crystal Server mit Windows-Authentifizierung

1. Installieren Sie Microsoft SQL 2005 im gemischten Modus.
2. Starten Sie Microsoft SQL Management Studio.
3. Erweitern Sie im Navigationsbereich „Datenbanken“.

   Markieren Sie Datenbank, klicken Sie mit der rechten Maustaste darauf und wählen Sie Neue Datenbank…

4 Geben Sie im Feld „Datenbankname“ die Bezeichnung „BOE11“ ein und klicken Sie auf „OK“.

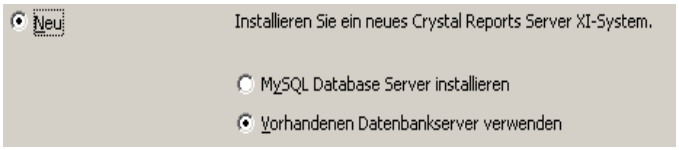
5 Beenden Sie Microsoft SQL Management Studio.

6 Legen Sie die Crystal Reports XI Server-CD in das CD-ROM-Laufwerk ein.

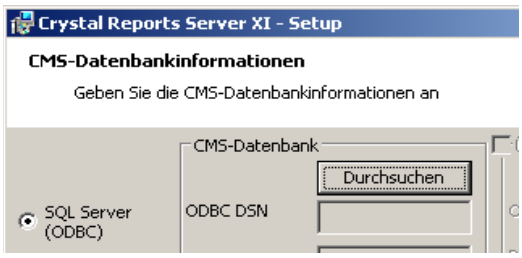
7 Wenn auf Ihrem Computer Autoplay deaktiviert ist, führen Sie die Datei setup.exe aus.

8 Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option „Perform Server Installation“ (Serverinstallation durchführen)+++ aus.

9 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)+++.



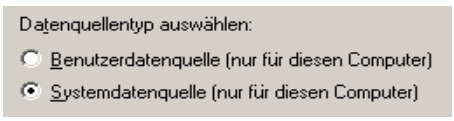
10 Klicken Sie im Bereich „CMS Database“ (CMS-Datenbank) auf „Browse“ (Durchsuchen).



11 Klicken Sie auf die Registerkarte Machine Data Source (Computer-Datenquelle).

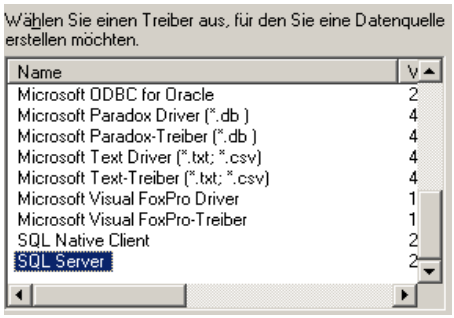
12 Klicken Sie auf "Neu".

13 Wählen Sie „System Data Source“ (Systemdatenquelle) aus.

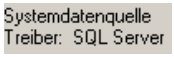


Klicken Sie auf „Next“ (Weiter).

14 Blättern Sie nach unten, wählen Sie SQL Server und klicken Sie auf Next (Weiter).

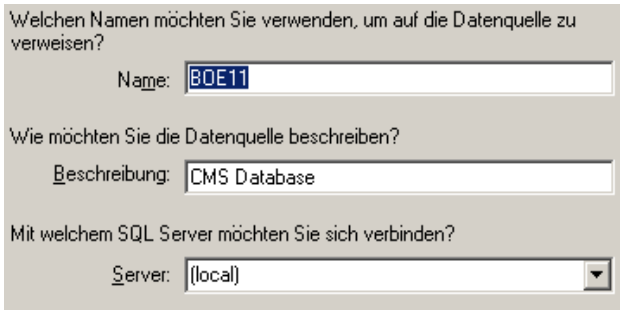


15 Eine neue Quelle wird angezeigt. Klicken Sie auf Finish (Fertig stellen).



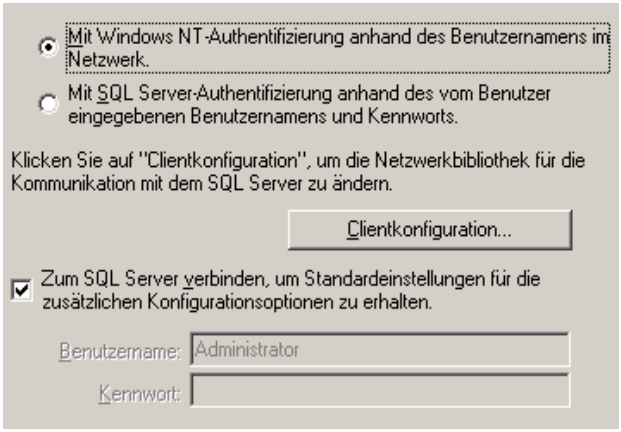
16 Geben Sie im Fenster „New Data Source to SQL Server“ (Neue Datenquelle für SQL Server) Folgendes ein:

- 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.



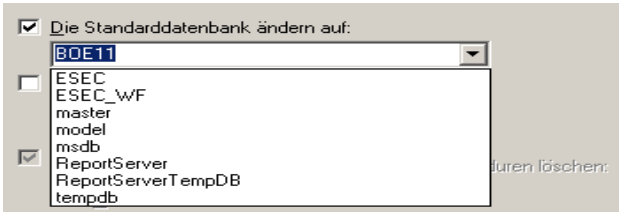
Klicken Sie auf „Next“ (Weiter).

Falls noch nicht geschehen, wählen Sie „With Windows NT“ (Mit Windows NT) aus und klicken Sie dann auf „Next“ (Weiter).



Hinweis: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

Aktivieren Sie das Kontrollkästchen „Change the default database to“ (Standarddatenbank ändern in). Ändern Sie Ihre Standarddatenbank in BOE11. Klicken Sie auf Next (Weiter).



17 Klicken Sie im Fenster „Create a New Data Source to SQL Server“ (Neue Datenquelle für SQL Server erstellen) auf „Finish“ (Fertig stellen).

18 Klicken Sie auf „Test Data Source“ (Datenquelle testen) und führen Sie einen Test der Datenquelle durch. Klicken Sie nach einem erfolgreichen Test der Datenquelle auf „OK“.

Markieren Sie im Fenster „Select Data Source“ (Datenquelle auswählen) die Option „BOE11“ und klicken Sie so oft auf „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".

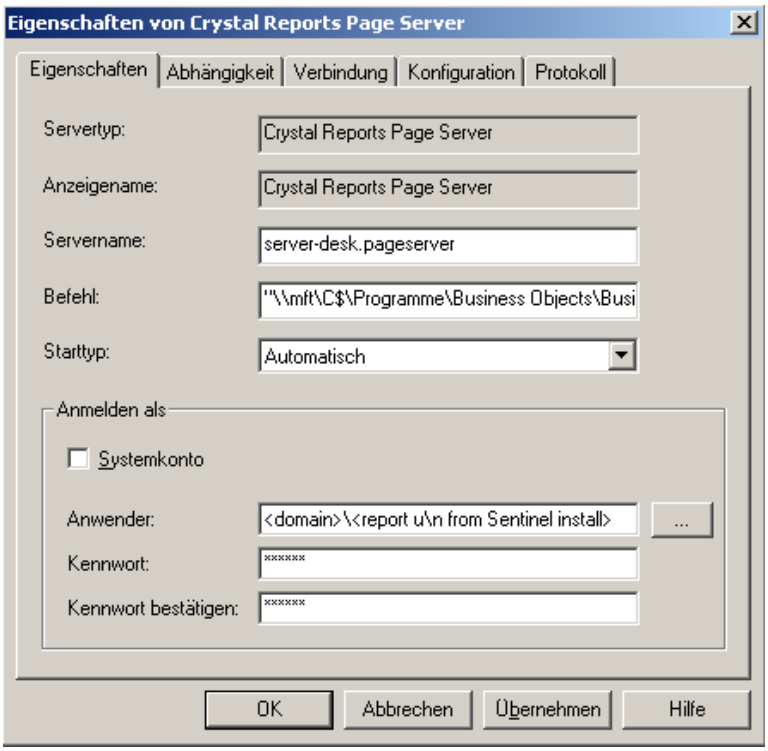
Hinweis: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

19 Wählen Sie im Fenster „Web Component Adapter Type“ (Adaptertyp der Webkomponente) die Option IIS ASP.NET aus.

Hinweis: Wenn IIS and ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert wurde, ist IIS ASP.NET abgeblendet.

1 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.

- Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „Central Configuration Manager“.
- Klicken Sie mit der rechten Maustaste auf „Crystal Reports Page Server“ (Crystal Reports Page Server) und wählen Sie stop (stopp).
- Klicken Sie mit der rechten Maustaste erneut auf Crystal Reports Page Server (Crystal Reports Page Server) und wählen Sie Properties (Eigenschaften).
- 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 für den Sentinel Report-Benutzer verwendet wurden. Klicken Sie auf "OK".



2 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.

So richten Sie eine ODBC-Datenquelle für die Windows-Authentifizierung ein

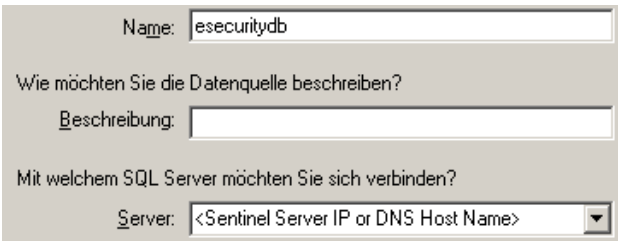
1 Wechseln Sie zur Windows-Systemsteuerung > „Verwaltung“ > „Datenquellen (ODBC)“.

2 Klicken Sie auf die Registerkarte System-DSN und dann auf Hinzufügen.

3 Wählen Sie SQL Server. Klicken Sie auf Fertig stellen.

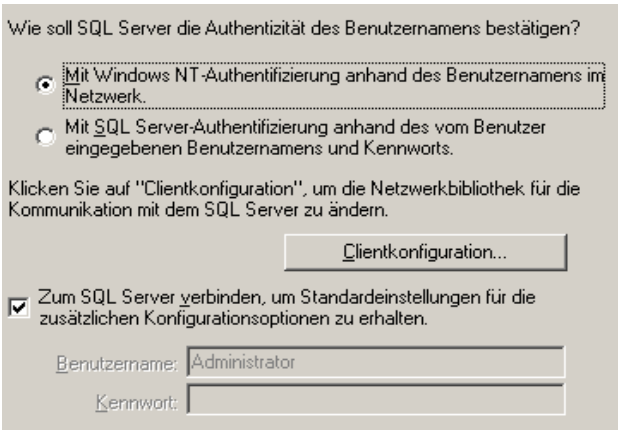
4 Ein Bildschirm wird angezeigt, in dem Sie nach Informationen zur Treiberkonfiguration gefragt werden:

- 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).

Wählen Sie im nächsten Bildschirm die Option für die Windows-Authentifizierung.



Hinweis: Die Anmelde-ID (abgeblendet) ist Ihr Windows-Anmeldename.

---

5 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).

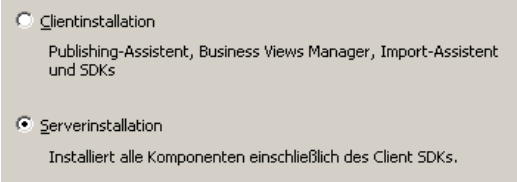
6 Klicken Sie auf Fertig stellen.

7 Klicken Sie auf „Test Data Source…“ (Datenquelle testen). Die Verbindungsherstellung sollte erfolgreich sein. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

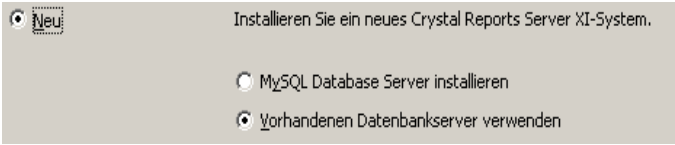
9.7.2 Installieren von Crystal Server für Microsoft SQL 2005 Server mit SQL-Authentifizierung

So führen Sie die Authentifizierung von BOE XI Crystal Server SQL durch

Wählen Sie im Fenster zur Auswahl der Client- oder Serverinstallation die Option „Perform Server Installation“ (Serverinstallation durchführen)+++ aus.



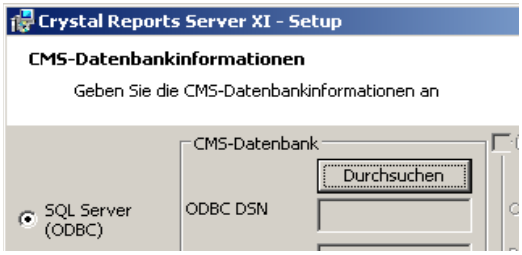
1 Installieren Sie ein neues BusinessObjects Enterprise System mithilfe von „Install MSDE or use existing local SQL Server“ (MSDE installieren oder lokalen SQL-Server verwenden).



Hinweis: Crystal Server und Microsoft SQL Server müssen sich auf demselben Computer befinden.

---

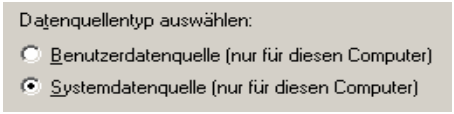
2 Klicken Sie im Bereich „CMS Database“ (CMS-Datenbank) auf „Browse“ (Durchsuchen).



3 Klicken Sie auf die Registerkarte Machine Data Source (Computer-Datenquelle).

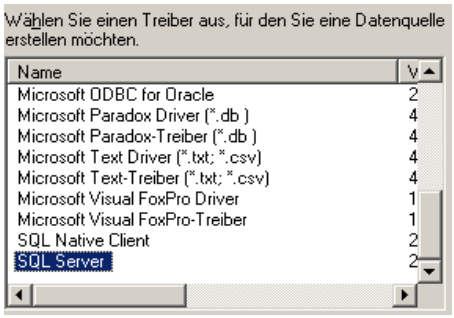
4 Klicken Sie auf "Neu".

Wählen Sie „System Data Source“ (Systemdatenquelle) aus.

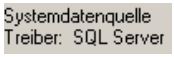


Klicken Sie auf „Next“ (Weiter).

Blättern Sie nach unten, wählen Sie SQL Server und klicken Sie auf Next (Weiter).

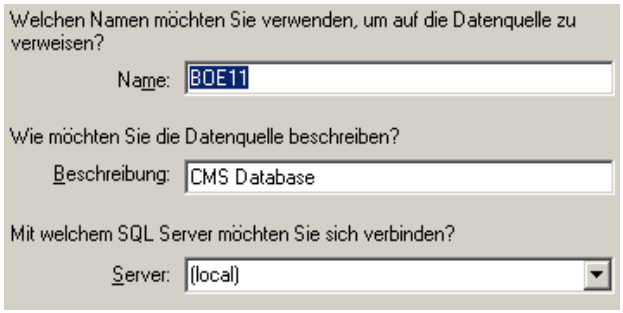


Eine neue Quelle wird angezeigt. Klicken Sie auf Finish (Fertig stellen).



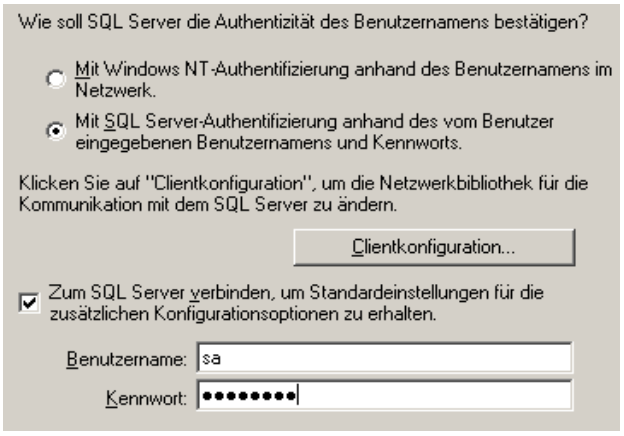
5 Geben Sie im Fenster „New Data Source to SQL Server“ (Neue Datenquelle für SQL Server) Folgendes ein:

- 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.

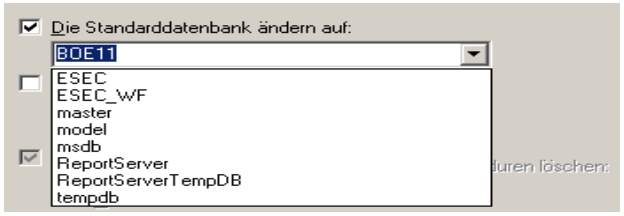


Klicken Sie auf „Next“ (Weiter).

6 Falls noch nicht geschehen, wählen Sie „With SQL Server“ (Mit SQL Server) aus, geben Sie „sa“ als Benutzername ein und geben Sie als Passwort ebenfalls „sa“ ein. Klicken Sie auf „Next“ (Weiter).



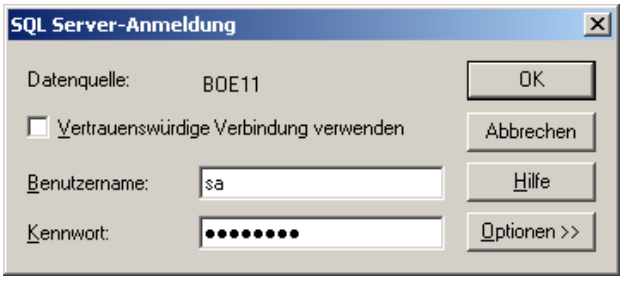
Aktivieren Sie das Kontrollkästchen „Change the default database to:“ (Standarddatenbank ändern in:). Ändern Sie Ihre Standarddatenbank in BOE11. Klicken Sie auf Next (Weiter).



7 Klicken Sie im Fenster „Create a New Data Source to SQL Server“ (Neue Datenquelle für SQL Server erstellen) auf „Finish“ (Fertig stellen).

8 Klicken Sie auf „Test Data Source“ (Datenquelle testen) und führen Sie einen Test der Datenquelle durch. Klicken Sie nach einem erfolgreichen Test der Datenquelle auf „OK“.

Markieren Sie im Fenster „Select Data Source“ (Datenquelle auswählen) die Option „BOE11“ und klicken Sie so oft auf „OK“, bis das Dialogfeld „SQL Server Login“ (SQL Server-Anmeldung) angezeigt wird. Vergewissern Sie sich, dass Use Trusted Connection (Vertrauenswürdige Verbindung verwenden) NICHT ausgewählt ist. Klicken Sie auf OK. Klicken Sie auf „Next“ (Weiter).



9 Wählen Sie im Fenster „Web Component Adapter Type“ (Adaptertyp der Webkomponente) die Option IIS ASP.NET aus.

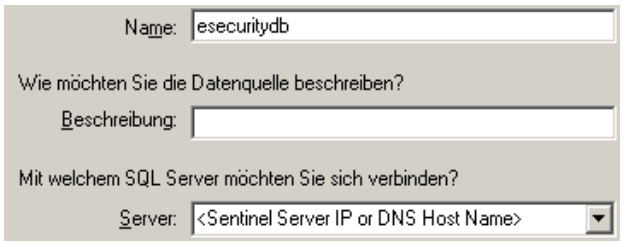
Hinweis: Wenn IIS and ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert wurde, ist IIS ASP.NET abgeblendet.

Konfigurieren 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.

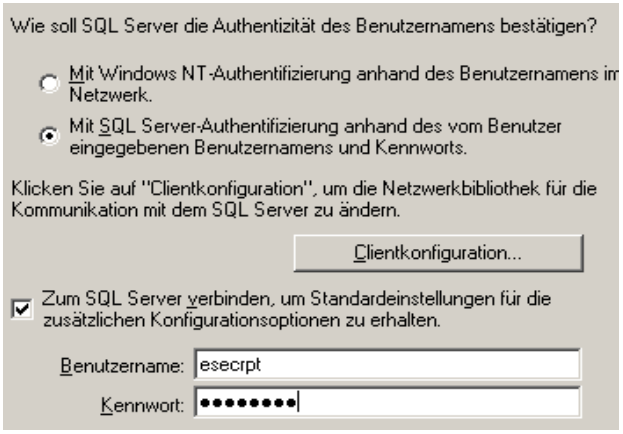
So richten Sie eine ODBC-Datenquelle für Windows ein

1. Wechseln Sie zur 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 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).

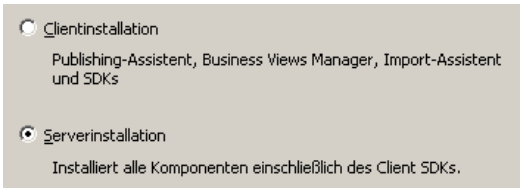
7 Klicken Sie auf Fertig stellen.

8 Klicken Sie auf „Test Data Source“ (Datenquelle testen) und führen Sie einen Test der Datenquelle durch. Klicken Sie nach einem erfolgreichen Test der Datenquelle auf „OK“. Klicken Sie auf OK (OK), bis das Fenster geschlossen wird.

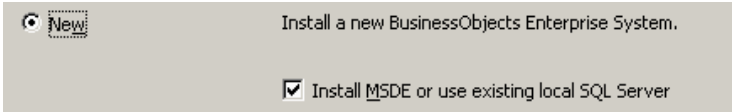
9.7.3 Installation von Crystal Server für Oracle

So installieren Sie Crystal Reports Server XI für Oracle

- „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).

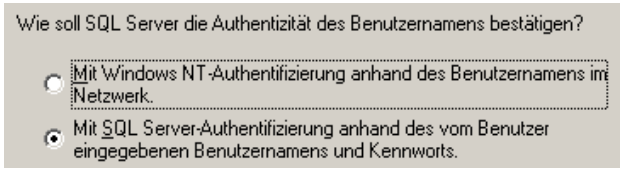


Hinweis: Crystal Server und Microsoft SQL Server 2005 müssen sich auf demselben Server befinden.

- IIS ASP.NET.

Hinweis: Wenn IIS and ASP.NET nicht über „Systemsteuerung“ > „Software“ > „Windows-Komponenten hinzufügen/entfernen“ installiert wurde, 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.

Installieren und Konfigurieren der Oracle 9i-Clientsoftware

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: ESEC
- Benutzer (optional): esecrpt

Erstellen Sie nach der Installation eine lokale Net Service Name-Konfiguration.

So erstellen Sie eine Net Service Name-Konfiguration (Konfiguration des systemeigenen Oracle-Treibers)

1. Wählen Sie „Oracle-OraHome92“ > „Configuration and Migration Tools“ (Konfigurations- und Migrationswerkzeuge) > „Net Manager“ aus.
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“ auf „Test...“. Klicken Sie anschließend auf "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".

   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.

9.8 Konfiguration für alle Authentifizierungen und Konfigurationen

9.8.1 Zuordnen von Crystal Reports zur Verwendung mit Sentinel

Folgende Verfahren sind erforderlich, damit Crystal Server mit Sentinel Control Center zusammenarbeiten kann.

Konfiguration von inetmgr

So konfigurieren Sie inetmgr

1. Kopieren Sie die Datei web.config aus:

   ```
   C:\Program Files\Business Objects\BusinessObjects Enterprise
   11.5\Web Content
   ```

   nach c:\Inetpub\wwwroot.
2. Starten Sie Internet Service Manager, indem Sie auf „Start“ > „Ausführen“ klicken. 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 auf „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 auf „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. Diese Dateien finden Sie in der Sentinel Reports Distribution, die beim technischen Support von Novell heruntergeladen werden kann.

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.
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.

So installieren Sie die notwendigen Patches für Crystal Reports

1. Fordern Sie die Sentinel Reports Distribution beim technischen Support von Novell an.

   Hinweis: Es wird dringend empfohlen, vor Durchführung dieser Aufgabe die Versionshinsweise zu Sentinel Reports zu lesen. Möglicherweise sind aktualisierte Dateien und Skripts vorhanden sowie weitere Schritte zu beachten.

2. Wechseln Sie in der Sentinel Reports Distribution zu dem Patch-Verzeichnis und kopieren Sie alle *.html- und *.js-Dateien in das Verzeichnis der Viewer-Datei. Dies lautet standardmäßig:

   ```
   C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\viewer\en
   ```

3. Wechseln Sie in der Sentinel Reports Distribution zu dem Patch-Verzeichnis und kopieren Sie alle *.asp- und *.js-Dateien in folgendes Verzeichnis:

   ```
   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 Report-Schablonen werden mithilfe von Crystal Publishing Wizard auf dem Crystal Reports Server veröffentlicht. Der neueste Satz der Berichtsschablonen kann von der Novell-Website für den technischen Support heruntergeladen werden.

Veröffentlichen von Berichtsschablonen mithilfe von Crystal Publishing Wizard

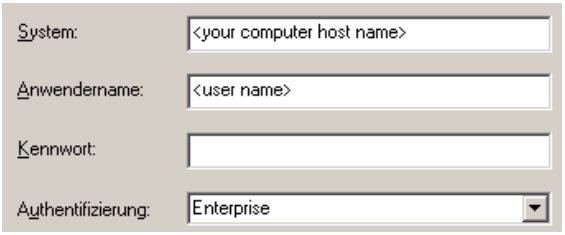
Hinweis: Es wird dringend empfohlen, vor Durchführung dieser Aufgabe die Versionshinsweise zu Sentinel Reports zu lesen. Möglicherweise sind aktualisierte Dateien und Skripts vorhanden sowie weitere Schritte zu beachten.

Veröffentlichen Sie 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“ > „Crystal Reports Server“ > „Publishing Wizard“ (Veröffentlichungsassistent).
2. Klicken Sie auf „Next“ (Weiter).
3. Anmelden. Als System sollte der Name des Hostcomputers 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) aus. Navigieren Sie in der Sentinel Reports Distribution zu:

   Sentinel-Datenbank unter Microsoft SQL:

   `Crystal_v11\SQL-Server`

   Sentinel-Datenbank unter Oracle:

   `Crystal_v11\Oracle`

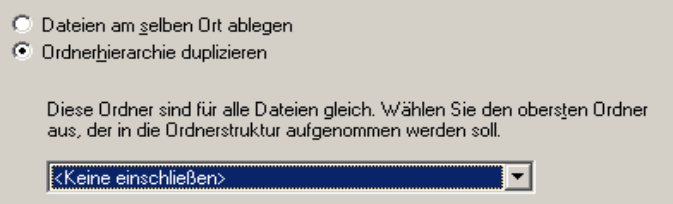
   Klicken Sie auf "OK".
6. Klicken Sie auf „Next“ (Weiter).

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 SentinelReports. Klicken Sie auf „Next“ (Weiter).

7 Auswählen:

- Duplicate the folder hierarchy (Ordnerhierachie duplizieren).

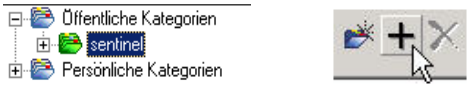
Klicken Sie auf den nach unten weisenden Pfeil und wählen Sie <include none> aus.



Klicken Sie auf „Next“ (Weiter).

8 Klicken Sie im Fenster „Confirm Location“ (Speicherort bestätigen) auf Next (Weiter).

Geben Sie im Fenster „Specify Categories“ (Kategorien angeben) einen Kategorienamen Ihrer Wahl (zum Beispiel Sentinel) ein, markieren Sie den Namen und klicken Sie auf die Schaltfläche mit dem Pluszeichen.



Hinweis: Nur der erste Bericht wird nach dem Klicken auf „Next“ (Weiter) unter der Kategorie angezeigt.

klicken Sie auf „Weiter“.

9 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).

10 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).

11 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).

12 Klicken Sie auf Next (Weiter), um Ihre Objekte hinzuzufügen.

13 Klicken Sie auf „Next“ (Weiter).

14 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 SentinelReports-Verzeichnis befinden.

9.8.2 Einrichten 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“ geändert werden.

So richten Sie das Gastkonto als „Named User“ (Benannter Benutzer) ein

1. Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects“ > „Crystal Reports Server > „.NET Administration Launchpad“.
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Hostcomputers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits 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 "Aktualisieren".
9. Melden Sie sich ab und schließen Sie das Fenster oder gehen Sie weiter zum Abschnitt Konfigurieren von .NET Administration Launchpad.

9.8.3 Konfigurieren von Berechtigungen für Berichte

Bei diesem Verfahren wird gezeigt, wie .NET Administration Launchpad zum Konfigurieren der Berechtigungen für Berichte eingesetzt wird, um Ihnen das Anzeigen und Ändern von Berichten bei Bedarf zu ermöglichen.

So konfigurieren Sie Berechtigungen für Berichte

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad (Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects“ > „Crystal Reports Server“ > „.NET Administration Launchpad“).
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).

   Als Systemname sollte der Name des Hostcomputers verwendet werden und als Authentifizierungstyp „Enterprise“. Ist dies nicht bereits 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 auf „SentinelReports“.
6. Alles auswählen.
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.
9. Klicken Sie auf "Aktualisieren".
10. Melden Sie sich ab und schließen Sie das Fenster.

Testen auf Webserver-Verbindung mit der Datenbank

So testen Sie, ob eine Webserver-Verbindung mit der Datenbank besteht

1. Wenn nicht bereits geschehen, starten Sie .NET Administration Launchpad („Start“ > „Alle Programme“ > „BusinessObjects“ > „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. Navigieren Sie zu „Folders“ (Ordner) > „SentinelReports“ > „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. Ein Bericht sollte angezeigt werden.

Testen der Konnektivität zum Webserver

So testen Sie die Konnektivität zum Webserver

1. Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.
2. Geben Sie ein:

```
http://<DNS name or IP address of your web server>/businessobjects/
enterprise11/WebTools/adminlaunch/default.aspx
```

Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

9.8.4 Deaktivieren der 10 wichtigsten Sentinel-Berichte

Standardmäßig sind die 10 wichtigsten Sentinel-Berichte aktiviert. Gehen Sie wie folgt vor, um die 10 wichtigsten Sentinel-Berichte zu deaktivieren

- Schalten Sie die Aggregation ab.
- Deaktivieren Sie den EventFileRedirectService.

So schalten Sie die Aggregation ab

1. Starten Sie Sentinel Data Manager.
2. Anmelden.

3 Klicken Sie auf die Registerkarte Bericht für Daten.

4 Deaktivieren Sie die folgenden Zusammenfassungen:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Klicken Sie in der Spalte „Status“ auf den Eintrag „Aktiv“, bis er in „Inaktiv“ geändert wird.

Zusammenfassungsna...	Uhrzeit	Attribute	Quelle	Status
EventDestSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv
EventSevDestTxnmyS...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestEvtSum...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestPortSum...	1 Stunde	SEV.DEST_PORT.(...	TransformedEvent	Inaktiv
EventSevSummary	1 Stunde	CUST_ID.SEV.EVT ...	TransformedEvent	Aktiv
EventSrcSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv

So deaktivieren Sie den EventFileRedirectService

1 Öffnen Sia auf Ihrem DAS-Computer mithilfe des Texteditors folgende Datei:

Bei UNIX:

```
$ESEC_HOME/config/das_binary.xml
```

Für Windows:

```
%ESEC_HOME%\config\das_binary.xml
```

2 Ändern Sie den Status von EventFileRedirectService in „Aus“.

```
<property name="status">off</property>
```

3 Starten Sie die DAS-Komponente folgendermaßen erneut:

Unter Windows:

```
Use Service Manager to stop then start the “sentinel” service.
```

9.8.5 Erhöhen der Datensatzgrenze für die Berichtsaktualisierung bei Crystal Enterprise

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 von Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren. Hierfür können Sie entweder Central Configuration Manager oder die Crystal-Webseite verwenden.

So konfigurieren Sie Crystal Page Server über Central Configuration Manager neu

1 Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects“ > „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 Folgendes hinzu:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the
default limit>
```

5 Starten Sie Crystal Page Server neu.

So konfigurieren Sie Crystal Page Server über die Crystal-Webseite neu

1 Klicken Sie auf „Start“ > „Alle Programme“ > „BusinessObjects“ > „Crystal Reports Server > „.NET Administration Launchpad“.

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

3 Als Systemname sollte der Name des Hostcomputers 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 "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.

9.8.6 Konfigurieren von Sentinel Control Center für die Integration in Crystal Enterprise Server

Sentinel Control Center kann für die Integration von Crystal Enterprise Server konfiguriert werden, sodass Sie Crystal Reports-Berichte in Sentinel Control Center anzeigen können.

Gehen Sie wie folgt vor, um die Integration von Crystal Enterprise Server in Sentinel Control Center zu aktivieren.

Hinweis: Diese Konfiguration kann erst durchgeführt werden, nachdem Crystal Enterprise Server installiert wurde und Crystal Reports-Berichte darin veröffentlicht wurden.

So konfigurieren Sie Sentinel für die Integration von 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_or_IP_of_web_server>/
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Hinweis: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse oder den Hostnamen von 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_or_IP_of_web_server>/
   GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
   ```

   Hinweis: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse oder den Hostnamen von 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 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.

Crystal Reports für Linux

10

In diesem Kapitel werden die folgenden Themen behandelt:

Crystal BusinessObjects Enterprise™ XI ist eines der Berichterstellungswerkzeuge für Sentinel.

In diesem Kapitel wird die Installation und Konfiguration von Crystal Reports Server für Sentinel erläutert.

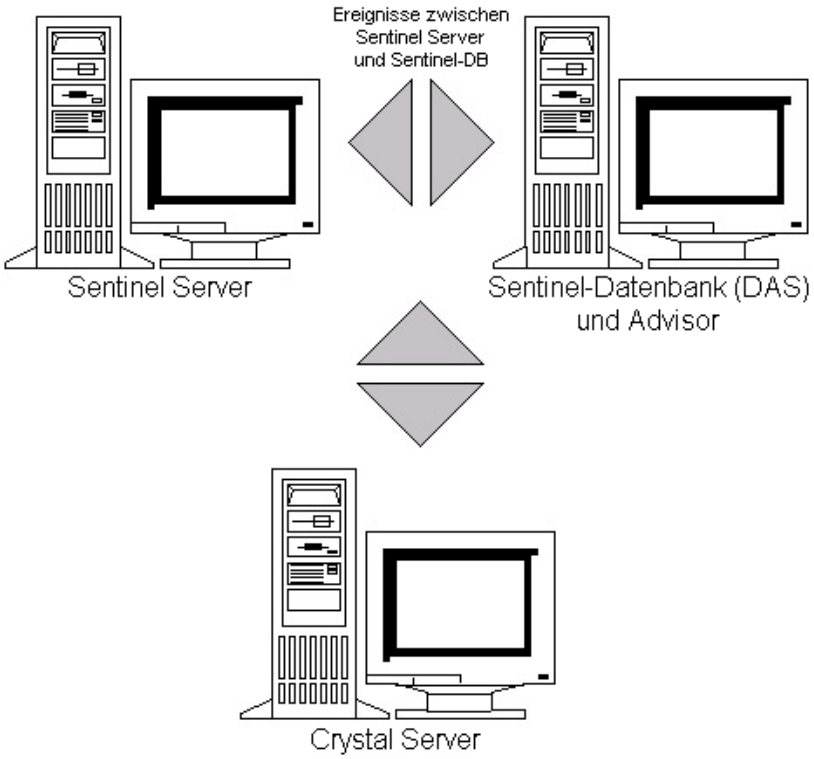
Sentinel unterstützt die Ausführung von Crystal Reports Server auf den folgenden Plattformen:

- Windows – Wird unterstützt, wenn die Sentinel-Datenbank unter Windows, Linux oder Solaris ausgeführt wird.
- Linux – Wird unterstützt, wenn die Sentinel-Datenbank unter Linux oder Solaris ausgeführt wird.

In diesem Kapitel wird die Ausführung von Crystal Reports Server unter Linux behandelt. Weitere Informationen zum Ausführen von Crystal Reports Server unter Windows finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 im Installationshandbuch.

Hinweis: Die Installation sollte in der angegebenen Reihenfolge vorgenommen werden.

- Durchführen der Aufgaben vor der Installation und Installieren von Crystal BusinessObjects Enterprise™ XI
- 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)
- Erhöhen der Datensatzgrenze für die Berichtsaktualisierung in Crystal Enterprise Server (empfohlen)
- Konfigurieren von Sentinel Control Center für die Integration in Crystal Enterprise Server



10.1 Verwenden von Crystal Reports

Informationen zum Verwenden von Crystal Reports für Sentinel Reporting finden Sie in Kapitel 9, „Crystal Reports für Windows“, auf Seite 111 im Installationshandbuch.

10.2 Konfiguration

- Die Linux-Versionen:
  - SUSE Linux Enterprise Server 9 (SLES 9) mit SP2
  - 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)

10.3 Installation

10.3.1 Aufgaben vor der Installation von Crystal BusinessObjects Enterprise™ XI

So führen Sie die Aufgaben vor der Installation von Crystal BusinessObjects Enterprise durch

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 Benutzerverzeichnis ist in diesem Fall /export/home/crystal. Ändern Sie es bei Bedarf. 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:

    10a Melden Sie sich als Oracle-Benutzer an.

    10b Wechseln Sie in das Verzeichnis $ORACLE_HOME/network/admin

10c Erstellen Sie eine Sicherungskopie der Datei tnsnames.ora.

10d Öffnen Sie die Datei tnsnames.ora zur Bearbeitung.

10e 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)
 )
)
```

10f 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.

10g 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 Servicenamen 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)
 )
)
```

10h 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).

10i Speichern Sie die Änderungen an der Datei tnsnames.ora.

10j Führen Sie folgenden Befehl aus, um zu überprüfen, dass der Service-Name esecuritydb ordnungsgemäß konfiguriert wurde:

```
tnsping esecuritydb
```

10k Wenn der Befehl erfolgreich ausgeführt wurde, sollten Sie eine Meldung erhalten, die besagt, dass die Verbindung in Ordnung ist.

10.3.2 Installieren von Crystal BusinessObjects Enterprise™ XI

So installieren Sie Crystal BusinessObjects Enterprise

1 Melden Sie sich als Crystal-Benutzer an.

2 Wechseln Sie in das Verzeichnis DISK_1des Crystal-Installationsprogramms.

3 Ausführen:

```
./install
```

4. Wählen Sie als Sprache „English“ (Englisch) aus+++.
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. Auswählen: „User install“ (Benutzerdefinierte Installation)
10. Auswählen: „New Install“ (Neue Installation)
11. Auswählen: „Install MySQL“ (MySQL installieren)
12. Geben Sie Konfigurationsinformationen für MySQL ein:
    - **12a** „Use default port 3306“ (Standardport 3306 verwenden)
    - **12b** „Admin password“ (Administrator-Passwort)
13. Geben Sie weitere Konfigurationsinformationen für MySQL ein:
    - **13a** Standardname der Datenbank: BOE11
    - **13b** Benutzer-ID: mysqladm
    - **13c** Passwort
14. Geben Sie weitere Konfigurationsinformationen für MySQL ein:
    - **14a** „Local Name Server“ (Name des lokalen Servers): <Hostname des lokalen Computers>
    - **14b** „Default CMS Port Number“ (CMS-Standardportnummer): 6400
15. Auswählen: „Install Tomcat“ (Tomcat installieren)
16. Geben Sie Tomcat-Konfigurationsinformationen ein:
    - **16a** „Default Receive HTTP requests port“ (Standardport zum Empfangen von HTTP-Anforderungen): 8080
    - **16b** „Default Redirect jsp requests port“ (Standardport für die Umleitung von JSP-Anforderungen): 8443
    - **16c** „Default Shutdown Hook port“ (Standardport für Herunterfahren des Hook): 8005
17. Drücken Sie die Eingabetaste, um den Installationsvorgang zu starten.

10.3.3 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. Diese Dateien finden Sie in der Sentinel Reports Distribution, die beim technischen Support von Novell heruntergeladen werden kann.

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.
GetReportURL.jsp	Zur Unterstützung von Hyperlinks zwischen Berichten verwendete Datei.

So installieren Sie die notwendigen Patches für Crystal Reports

1. Fordern Sie die Sentinel Reports Distribution beim technischen Support von Novell an.

   Hinweis: Es wird dringend empfohlen, vor Durchführung dieser Aufgabe die Versionshinsweise zu Sentinel Reports zu lesen. Möglicherweise sind aktualisierte Dateien und Skripts vorhanden sowie weitere Schritte zu beachten.

2. Wechseln Sie in der Sentinel Reports Distribution zu dem Patch-Verzeichnis und kopieren Sie alle *.html- und *.js-Dateien in das Verzeichnis der Viewer-Datei. Dies lautet standardmäßig:
   `/opt/crystal_xi/bobje/webcontent/enterprise11/viewer/en/`
3. Wechseln Sie in der Sentinel Reports Distribution zu dem Patch-Verzeichnis und kopieren Sie alle *.jsp-Dateien in folgendes Verzeichnis:
   `/opt/crystal_xi/bobje/tomcat/webapps/esec-script/`

   Hinweis: Erstellen Sie einen Ordner mit der Bezeichnung esec-script.

4. Kopieren Sie alle *.jar-Dateien:
   ```
   From:
   /opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
   To:
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib
   ```

   Hinweis: Erstellen Sie die Ordnerstruktur WEB-INF/lib.

10.4 Veröffentlichen Sie Crystal Reports-Schablonen

Hinweis: Es wird dringend empfohlen, vor Durchführung dieser Aufgabe die Versionshinsweise zu Sentinel Reports zu lesen. Möglicherweise sind aktualisierte Dateien und Skripts vorhanden sowie weitere Schritte zu beachten.

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

Hinweis: Um einen oder mehrere der wichtigsten 10 Berichte auszuführen, muss die Aggregation aktiviert sein und EventFileRedirectService in DAS_Binary.xml muss auf „Ein“ gesetzt sein. Informationen zum Aktivieren der Aggregation finden Sie im Abschnitt zur Registerkarte „Berichtdaten“ von Sentinel Data Manager im Sentinel-Benutzerhandbuch oder in Abschnitt 10.8, „Aktivieren von Sentinel Top 10-Berichten“, auf Seite 151.

10.4.1 Veröffentlichen von Berichtsschablonen – Crystal Publishing Wizard

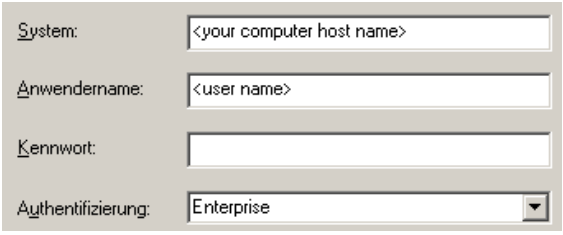
Hinweis: Zur Ausführung von Crystal Publishing Wizard ist eine Windows-Plattform erforderlich.

So importieren Sie Crystal Report-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“ (Veröffentlichungsassistent).
2. Klicken Sie auf „Next“ (Weiter).
3. Anmelden. Als System sollte der Name des Hostcomputers 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 Next (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). Navigieren Sie in der Sentinel Reports Distribution zu:

   `Crystal_v11\Oracle`

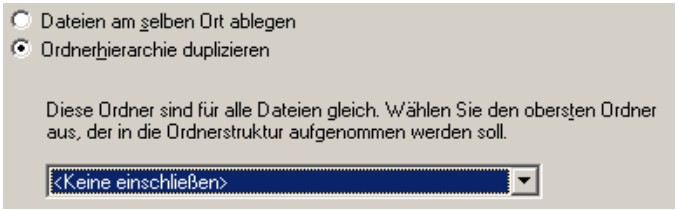
   Klicken Sie auf "OK".

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 Auswählen:

- Duplicate the folder hierarchy (Ordnerhierachie duplizieren).
- Klicken Sie auf den nach unten weisenden Pfeil und wählen Sie <include none> 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 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.

10.4.2 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.

So importieren Sie Crystal Report-Schablonen

1 Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
`http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch`

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".

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 „Browse“ (Durchsuchen) und navigieren Sie zu dem folgenden Ordner mit der Sentinel Reports Distribution:
`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".

17 Klicken Sie auf "Aktualisieren".

18 Um die übrigen Berichte hinzuzufügen, wiederholen Sie die Schritte 9 bis 17, bis alle Berichte hinzugefügt wurden.

10.5 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_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11/adminlaunch
```

Das nicht für die Verwaltung bestimmte (allgemeine) Portal kann unter folgender URL über den Browser aufgerufen werden:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11
```

10.5.1 Testen der Konnektivität zum Webserver

So testen Sie die Konnektivität zum Webserver

1 Wechseln Sie zu einem anderen Computer, der sich im selben Netzwerk befindet wie Ihr Webserver.

2 Geben Sie ein:

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11/adminlaunch
```

3 Es sollte eine Crystal BusinessObjects-Webseite geöffnet werden.

10.6 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“ geändert werden.

So richten Sie das Gastkonto als „Named User“ (Benannter Benutzer) ein

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

```
http://
<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise11/adminlaunch
```

2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Hostcomputers 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 "Aktualisieren".
8. Melden Sie sich ab und schließen Sie das Fenster.

10.7 Konfigurieren von Berechtigungen für Berichte

Bei diesem Verfahren wird gezeigt, wie Administration Launchpad zum Konfigurieren der Berechtigungen für Berichte eingesetzt wird, um Ihnen das Anzeigen und Ändern von Berichten bei Bedarf zu ermöglichen.

So konfigurieren Sie Berechtigungen für Berichte

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
   ```
   http://
   <hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
   businessobjects/enterprise11/adminlaunch
   ```
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Hostcomputers 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 im Fenster „Organize“ (Organisieren) auf Folders (Ordner).
6. Klicken Sie einmal (nicht doppelt) auf eSecurity_Reports.
7. Alles auswählen.
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.
10. Klicken Sie auf "Aktualisieren".
11. Melden Sie sich ab und schließen Sie das Fenster.

10.8 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.

So schalten Sie die Aggregation ein

1. Klicken Sie auf der Benutzeroberfläche von Sentinel Control Center auf die Registerkarte „Admin“.
2. Klicken Sie im Navigationsbereich auf „Berichtdaten“, oder klicken Sie auf die Schaltfläche „Berichtdaten“.
3. Aktivieren Sie folgende Zusammenfassungen:
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

   Klicken Sie in der Spalte „Status“ auf Inaktiv , bis sich der Wert zu Aktiv ändert.

Zusammenfassungsna...	Uhrzeit	Attribute	Quelle	Status
EventDestSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv
EventSevDestTxnmyS...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestEvtSum...	1 Stunde	CUST_ID.DEST_EV ...	TransformedEvent	Inaktiv
EventSevDestPortSum...	1 Stunde	SEV.DEST_PORT.(...	TransformedEvent	Inaktiv
EventSevSummary	1 Stunde	CUST_ID.SEV.EVT ...	TransformedEvent	Aktiv
EventSrcSummary	1 Stunde	CUST_ID.RSRC_ID ...	TransformedEvent	Aktiv

So aktivieren Sie EventFileRedirectService

1. Öffnen Sia 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.

10.9 Erhöhen der Datensatzgrenze für die Berichtsaktualisierung bei Crystal Enterprise

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 von Datensätzen einzurichten, müssen Sie Crystal Page Server neu konfigurieren.

So konfigurieren Sie Crystal Page Server neu

1. Öffnen Sie einen Webbrowser und geben Sie folgende URL ein:
   `http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch`
2. Klicken Sie auf Central Management Console (Zentrale Verwaltungskonsole).
3. Als Systemname sollte der Name des Hostcomputers 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 "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.

10.10 Konfigurieren von Sentinel Control Center für die Integration in Crystal Enterprise Server

Sentinel Control Center kann für die Integration von Crystal Enterprise Server konfiguriert werden, sodass Sie Crystal Reports-Berichte in Sentinel Control Center anzeigen können.

Gehen Sie wie folgt vor, um die Integration von Crystal Enterprise Server in Sentinel Control Center zu aktivieren.

Hinweis: Diese Konfiguration kann erst durchgeführt werden, nachdem Crystal Enterprise Server installiert wurde und Crystal Reports-Berichte darin veröffentlicht wurden.

So konfigurieren Sie Sentinel für die Integration von 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_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

Hinweis: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse oder den Hostnamen von 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 Hostnamen handeln.

Hinweis: <Standardport_8080_für_Webserver> 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_or_IP_of_web_server>:<web_server_port_default_8080>/
esec-script/
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

Hinweis: <Hostname_oder_IP-Adresse_des_Webservers> muss durch die IP-Adresse oder den Hostnamen von 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 Hostnamen handeln.

Hinweis: <Standardport_8080_für_Webserver> 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.

10.11 Dienstprogramme und Fehlersuche

10.11.1 Starten von MySQL

So vergewissern Sie sich, dass MySQL ausgeführt wird

1. Melden Sie sich als Crystal-Benutzer an.
2. Wechseln Sie zu /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

10.11.2 Starten von Tomcat

So vergewissern Sie sich, dass Tomcat ausgeführt wird:

1. Melden Sie sich als Crystal-Benutzer an
2. Wechseln Sie zu /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

10.11.3 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

10.11.4 Fehler beim Crystal-Hostnamen

So beheben Sie Fehler im Zusammenhang mit dem 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:

   ```
   192.0.2.46linuxCE02
   ```

10.11.5 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.

So beheben Sie CMS-Verbindungsfehler

1. Wenn der Befehl „netstat –an | grep 6400“ zu keinerlei 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. Weitere Informationen finden Sie in den 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) aus 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:

2a Melden Sie sich als Crystal-Benutzer an

2b Wechseln Sie zu /opt/crystal_xi/bobje

2c ./ccm.sh -enable all

Deinstallieren von Sentinel

11

In diesem Kapitel werden die folgenden Themen behandelt:

Zum Entfernen einer Sentinel-Installation stehen Deinstallationsprogramme für Linux, Solaris und Windows zur Verfügung. Zahlreiche Dateien, einschließlich Protokolldateien, werden aufbewahrt und können, falls gewünscht, manuell entfernt werden. Darüber hinaus wird dringend empfohlen, alle nachfolgenden Schritte auszuführen, um sicherzustellen, dass keine Dateien oder Systemeinstellungen aus einer früheren Version übrig bleiben, die zu Konflikten mit einer neuen Installation führen könnten.

Warnung: 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.

11.1 Deinstallieren von Sentinel

11.1.1 Deinstallation unter Solaris und Linux

So starten Sie das Sentinel-Deinstallationsprogramm für Solaris

1. Melden Sie sich als Benutzer „root“ an.
2. Stoppen Sie Sentinel Server.
3. Navigation:
   `$ESEC_HOME/_uninst`
4. Geben Sie folgenden Befehl ein:
   `./uninstall.bin`
5. Wählen Sie eine Sprache aus und klicken Sie auf „OK“.
6. Der Sentinel-Installationsassistent wird angezeigt. Klicken Sie auf „Weiter“.
7. Wählen Sie die Komponenten aus, die deinstalliert werden sollen, und klicken Sie auf „Weiter“.

   Hinweis: Sentinel fordert Sie in einer Warnmeldung dazu auf, sämtliche geöffneten Sentinel-Anwendungen zu schließen.

8 Sie werden aufgefordert, unter den folgenden beiden Optionen zu wählen:

- Gesamte Datenbankinstanz löschen
- Nur die Datenbankobjekte löschen

Wählen Sie die gewünschte Option aus und klicken Sie auf „Weiter“.

9 Klicken Sie auf "Deinstallieren".

11.1.2 Deinstallation unter Windows

So verwenden Sie das Sentinel-Deinstallationsprogramm für Windows

1 Melden Sie sich als Administrator an.

2 Stoppen Sie Sentinel Server.

3 Wählen Sie „Start“ > „Programme“ > „Sentinel“ > „Sentinel deinstallieren“ aus.

4 Wählen Sie eine Sprache aus und klicken Sie auf „OK“.

5 Der Sentinel-Installationsassistent wird angezeigt. Klicken Sie auf „Weiter“.

6 Wählen Sie die Komponenten aus, die Sie deinstallieren möchten, und klicken Sie auf „Weiter“.

Hinweis: Sentinel fordert Sie in einer Warnmeldung dazu auf, sämtliche geöffneten Sentinel-Anwendungen zu schließen.

---

7 Sie werden aufgefordert, unter den folgenden beiden Optionen zu wählen:

- Gesamte Datenbankinstanz löschen
- Nur die Datenbankobjekte löschen

Wählen Sie die gewünschte Option aus und klicken Sie auf „Weiter“.

8 Geben Sie die Authentifizierungsinformationen an, wählen Sie entweder „Windows-Authentifizierung“ oder „SQL-Authentifizierung“ aus und geben Sie den Benutzerberechtigungsnachweis ein, wenn Sie dazu aufgefordert werden. Klicken Sie auf „Weiter“.

9 Es wird eine Zusammenfassung der zur Deinstallation ausgewählten Funktionen angezeigt. Klicken Sie auf "Deinstallieren".

10 Wählen Sie aus, dass das System neu gebootet werden soll, und klicken Sie dann auf „Fertig stellen“.

11.1.3 Deinstallation über die Systemsteuerung

So deinstallieren Sie die Sentinel-Anwendungen für Windows

1 Klicken Sie auf „Start“ > „Systemsteuerung“ > „Software“ > „Sentinel“ > „Entfernen/Ändern“.

2 Wählen Sie eine Sprache aus und klicken Sie auf „OK“.

3 Der Sentinel-Installationsassistent wird angezeigt. Klicken Sie auf „Weiter“.

4 Wählen Sie die Komponenten aus, die Sie deinstallieren möchten, und klicken Sie auf „Weiter“.

Hinweis: Sentinel fordert Sie in einer Warnmeldung dazu auf, sämtliche geöffneten Sentinel-Anwendungen zu schließen.

5 Sie werden aufgefordert, unter den folgenden beiden Optionen zu wählen:

- Gesamte Datenbankinstanz löschen
- Nur die Datenbankobjekte löschen

Wählen Sie die gewünschte Option aus und klicken Sie auf „Weiter“.

6 Geben Sie die Authentifizierungsinformationen an, wählen Sie entweder „Windows-Authentifizierung“ oder „SQL-Authentifizierung“ aus und geben Sie den Benutzerberechtigungsnachweis ein, wenn Sie dazu aufgefordert werden. Klicken Sie auf Weiter

7 Es wird eine Zusammenfassung der zur Deinstallation ausgewählten Funktionen angezeigt. Klicken Sie auf "Deinstallieren".

8 Wählen Sie aus, dass das System neu gebootet werden soll, und klicken Sie dann auf „Fertig stellen“.

11.2 Nach der Deinstallation

11.2.1 Sentinel-Datendateien

Um potenziell wertvolle Informationen auch nach der Deinstallation von Sentinel zu bewahren, werden zahlreiche Dateien nicht entfernt. Falls diese Informationen nicht mehr benötigt werden, können die folgenden Dateien und Ordner manuell entfernt werden.

- 3rd Party
  - SonicMQ
    - Docs7.0
    - InstallLogs7.0
    - MQ7.0
    - Installationsprogramm
    - mq_documentation_7.0.htm
    - sonicsw.properties
    - uninstall.sh
    - wizard.jar
- Bin
  - control_center.ja
  - sdm_gui.jac
- Config
  - .proxyServerKeystore
  - .primary_key
  - .Keystore

- Daten
  - .cache
  - .sessionState
  - .uuid
  - .uuidlock
  - DatabaseManager.log
  - agent-84EBED40-9AB1-1029-9C3F-0003BAC9707D.lck
  - collector_mgr.cache
  - eventfiles
  - map_data
  - portcfg_84EBED40-9AB1-1029-9C3F-0003BAC9707D.dat
  - uuid.dat
- Install_log
  - CreateAdminUserSimpleErr.txt
  - CreateAdminUserSimpleOut.txt
  - PostInstallSetup2Err.log
  - PostInstallSetup2Out.log
  - PostInstallSetupErr.log
  - PostInstallSetupOut.log
  - advcronjoberr.txt
  - advcronjobout.txt
  - configupdateerr.txt
  - configupdateout.txt
  - containerFileUpdate.log
  - cronjoberr.txt
  - cronjobout.txt
  - db
  - dbupdateerr.txt
  - dbupdateout.txt
  - extractJre64_err.log
  - extractJre64_out.log
  - key_generation.log
  - sentinelInstall.log
  - sentinelUninstall.log
  - shutdown_database_err.log
  - shutdown_database_out.log
  - sonic_silent_install_err.log
  - sonic_silent_install_out.log

- sonic_silent_uninstall_err.log
- sonic_silent_uninstall_out.log
- stopAM_err.txt
- stopAM_out.txt
- stopSentinel_err.txt
- stopSentinel_out.txt
- uninstallDB_err.log
- uninstallDB_out.log
- Sämtliche Dateien befinden sich im Verzeichnis $ESEC_HOME or %ESEC_HOME% und dessen Unterverzeichnissen.
- Für Advisor bleiben die für die Advisor-Datendateien verwendeten Angriffs- und Warnungsordner bestehen.

11.2.2 Sentinel-Einstellungen

Nach der Deinstallation von Sentinel bleiben bestimmte Systemeinstellungen bestehen, die manuell entfernt werden können. Diese Einstellungen sollten entfernt werden, bevor eine erneute Installation von Sentinel durchgeführt wird, insbesondere dann, wenn bei der Deinstallation von Sentinel Fehler aufgetreten sind.

Hinweis: Unter Solaris und Linux wird bei der Deinstallation von Sentinel Server der Sentinel-Administratorbenutzer nicht aus dem Betriebssystem entfernt. Sie müssen diesen Benutzer bei Bedarf manuell entfernen.

Entfernen der Sentinel-Systemeinstellungen unter Linux mit Oracle

So bereinigen Sie Sentinel manuell unter Linux

1. Melden Sie sich als „root“ an.
2. Stellen Sie sicher, dass alle Sentinel-Prozesse gestoppt wurden.
3. Entfernen Sie den Inhalt von /opt/sentinelXX (bzw. dem Verzeichnis, in dem die Sentinel-Software installiert und benannt wurde)
4. Entfernen Sie die Datei S98sentinel aus dem Verzeichnis /etc/rc.d/rc5.d.
5. Entfernen Sie die Datei S98sentinel aus dem Verzeichnis /etc/rc.d/rc3.d.
6. Entfernen Sie die Datei K02sentinel aus dem Verzeichnis /etc/rc.d/rc0.d.
7. Entfernen Sie die Datei sentinel aus dem Verzeichnis /etc/init.d.
8. Entfernen Sie das Verzeichnis /root/Install Shield.
9. Entfernen Sie die Datei /root/vpd.properties
10. Stellen Sie sicher, dass kein Benutzer als Sentinel-Administratorbenutzer (standardmäßig „esecadm“) angemeldet ist und entfernen Sie dann den Sentinel-Administratorbenutzer (und home dir) sowie die Gruppe „esec“.
    - Führen Sie den folgenden Befehl aus: userdel -r esecadm
    - Führen Sie den folgenden Befehl aus: groupdel esec

11 Wenn die Datei .login vorhanden ist, müssen Sie den Abschnitt /etc/profile, /etc/.login des Installationsassistenten entfernen.

12 Entfernen Sie die Sentinel Oracle-Datenbank. Weitere Informationen hierzu finden Sie in „So bereinigen Sie die Sentinel Oracle-Datenbank manuell unter Linux“ auf Seite 162.

13 Starten Sie das Betriebssystem neu.

So bereinigen Sie die Sentinel Oracle-Datenbank manuell unter Linux

---

Hinweis: Stellen Sie vor dem Entfernen der Datenbank sicher, dass diese nicht von anderen Anwendungen genutzt wird.

---

1 Melden Sie sich als Benutzer „oracle“ an.

2 Stoppen Sie Oracle-Listener.

- Führen Sie den folgenden Befehl aus: lsnrctl stop

3 Stoppen Sie die Sentinel-Datenbank.

- Setzen Sie die Umgebungsvariable ORACLE_SID auf den Namen Ihrer Sentinel-Datenbankinstanz (normalerweise ESEC).
- Führen Sie den folgenden Befehl aus: sqlplus '/ as sysdba'
- Führen Sie an der sqlplus-Eingabeaufforderung den folgenden Befehl aus: shutdown immediate

4 Entfernen Sie den Eintrag für die Sentinel-Datenbank in der Datei /etc/oratab

5 Entfernen Sie die Datei init<Name_Ihrer_Instanz>.ora (normalerweise initESEC.ora) aus dem Verzeichnis $ORACLE_HOME/dbs.

6 Entfernen Sie die Einträge für Ihre Sentinel-Datenbank aus folgenden Dateien im Verzeichnis $ORACLE_HOME/network/admin:

- tnsnames.ora
- listener.ora

7 Löschen Sie die Datendateien der Datenbank aus dem Verzeichnis, in dem Sie sie installiert haben.

Entfernen der Sentinel-Systemeinstellungen unter Solaris mit Oracle

So bereinigen Sie Sentinel manuell unter Solaris

Hinweis: Die manuelle Bereinigung wird normalerweise dann durchgeführt, wenn bei der Deinstallation von Sentinel ein Fehler auftritt.

---

1 Melden Sie sich als „root“ an.

2 Stellen Sie sicher, dass keine Sentinel-Prozesse ausgeführt werden.

3 Entfernen Sie den Inhalt von /opt/sentinelXX (bzw. dem Verzeichnis, in dem die Sentinel-Software deinstalliert wurde).

4 Entfernen Sie die Datei S98sentinel aus dem Verzeichnis /etc/rc3.d.

5 Entfernen Sie die Datei K02sentinel aus dem Verzeichnis /etc/rc0.d.

6 Entfernen Sie die Datei sentinel aus dem Verzeichnis /etc/init.d.

7. Entfernen Sie Verweise des Installationsassistenten 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)
8. Stellen Sie sicher, dass kein Benutzer als Sentinel-Administratorbenutzer angemeldet ist, und entfernen Sie dann den Sentinel-Administratorbenutzer (und home dir) sowie die Gruppe „esec“.
   - Führen Sie den folgenden Befehl aus: userdel -r esecadm
   - Führen Sie den folgenden Befehl aus: groupdel esec
9. Wenn die Datei .login vorhanden ist, müssen Sie den Abschnitt /etc/profile, /etc/.login des Installationsassistenten entfernen.
10. Entfernen Sie das Verzeichnis /Install Shield, sofern vorhanden.
11. Starten Sie das Betriebssystem neu.

So bereinigen Sie die Sentinel Oracle-Datenbank manuell unter Solaris

Hinweis: Stellen Sie vor dem Entfernen der Datenbank sicher, dass diese nicht von anderen Anwendungen genutzt wird.

1. Melden Sie sich als Benutzer „oracle“ an.
2. Stoppen Sie Oracle-Listener.
   - Führen Sie den folgenden Befehl aus: lsnrctl stop
3. Stoppen Sie die Sentinel-Datenbank:
   - Setzen Sie die Umgebungsvariable ORACLE_SID auf den Namen Ihrer Sentinel-Datenbankinstanz (normalerweise ESEC).
   - Führen Sie den folgenden Befehl aus: sqlplus '/ as sysdba'
   - Führen Sie an der sqlplus-Eingabeaufforderung den folgenden Befehl aus: shutdown immediate
4. Entfernen Sie den Eintrag für die Sentinel-Datenbank in der Datei /var/opt/oracle/oratab
5. Entfernen Sie die Datei init<Name_Ihrer_Instanz>.ora (normalerweise initESEC.ora) aus dem Verzeichnis $ORACLE_HOME/dbs.
6. Entfernen Sie die Einträge für Ihre Sentinel-Datenbank aus folgenden Dateien im Verzeichnis $ORACLE_HOME/network/admin:
   - tnsnames.ora
   - listener.ora
7. Löschen Sie die Datendateien der Datenbank aus dem Verzeichnis, in dem Sie sie installiert haben.

Entfernen der Sentinel-Systemeinstellungen unter Windows mit SQL Server

So bereinigen Sie Sentinel manuell unter Windows

1. Löschen Sie den Ordner %CommonProgramFiles%\InstallShield\Universal und seinen gesamten Inhalt.
2. Löschen Sie den Ordnder %ESEC_HOME% (standardmäßig unter C:\Programme\novell\sentinel6).
3. Klicken Sie mit der rechten Maustaste auf „Arbeitsplatz“ > „Eigenschaften“ > Registerkarte „Erweitert“.
4. Klicken Sie auf die Schaltfläche „Umgebungsvariablen“.
5. Löschen Sie die folgenden Variablen (sofern vorhanden):
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
6. Entfernen Sie alle Einträge in der Umgebungsvariablen PATH, die auf die Sentinel-Installation verweisen.

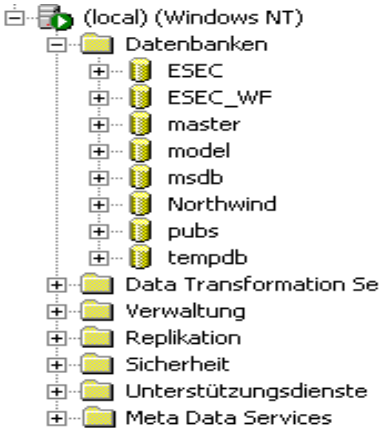
   Warnung: Entfernen Sie ausschließlich Pfade für die alte Sentinel-Installation. Andernfalls kann es geschehen, dass das System nicht ordnungsgemäß funktioniert.
7. Löschen Sie alle Sentinel-Verknüpfungen vom Desktop.
8. Löschen Sie den Verknüpfungsordner „Start“ > „Programme“ > „Sentinel“ aus dem Startmenü.
9. Starten Sie das Betriebssystem neu.

So bereinigen Sie die Sentinel Microsoft SQL Server-Datenbank manuell unter Windows

Hinweis: Stellen Sie vor dem Entfernen der Datenbank sicher, dass diese nicht von anderen Anwendungen genutzt wird.

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 Es sollte eine Sentinel-Datenbank mit Daten (üblicherweise mit der Bezeichnung ESEC) und eine Workflow-Datenbank (üblicherweise mit der Bezeichnung ESEC_WF vorhanden sein). Klicken Sie mit der rechten Maustaste auf die einzelnen Datenbanken und wählen Sie „Löschen“ aus.

4 Bestätigen Sie das Löschen der Datenbank mit Ja.

Fragebogen vor der Installation

A

Fragen vor der Installation

1. Zu welchem Zweck bzw. mit welchem Ziel verwenden Sie Novell Sentinel?
   - **1a** Einhaltung von Bestimmungen
   - **1b** SEM
   - **1c** Sonstiges_____
2. Welche Hardware wurde für die Installation von Sentinel zugeordnet? Stimmt die Hardware mit den im Sentinel-Installationshandbuch genannten Hardwarespezifikationen überein?
3. Haben Sie Ihre Konfiguration im Hinblick auf die im Sentinel-Installationshandbuch erläuterten geltenden Anforderungen an die Sentinel-Hardware und das Betriebssystem überprüft?
   - Betriebssystem-Patch-Stufe
   - Service-Patches
   - Hot Fixes usw.
4. Erfüllt Ihr DAS-Computer die erforderlichen Anforderungen an das Betriebssystem und die Hardware?
5. Welche Netzwerkarchitektur verwenden die Quellgeräte hinsichtlich des Sicherheitssegments, in dem sich die Sentinel- und Collector-Hardware befinden soll?

   Hinweis: Dies ist wichtig, um die Hierarchie der Collector-Datensammlung zu verstehen und um Firewalls zu erkennen, die überwunden werden müssen, um die Kommunikation zwischen Sentinel und Collector, 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.

6 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.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 Von 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? Sentinel kann so konfiguriert werden, dass die gewünschte Ausgabe basierend auf den hier angegebenen Informationen erstellt wird.

8 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.
  - Dies gilt nicht für Solaris-Installationen. Sentinel unterstützt jedoch nicht NIS.

9 Wie lange müssen die Daten beibehalten werden (in Tagen)?

10 Welche Datenträgergröße möchten Sie auf der Grundlage der Informationen über die Datenbeibehaltung und EPS verwenden? Verwenden Sie 500 bis 800 Byte/Ereignis für Größenschätzungen.

Installationsbericht für Sentinel unter Linux mit Oracle

B

Diese Checkliste kann für verteilte Installationen mit maximal drei Collector Manager- und Correlation Engine-Instanzen verwendet werden.

Weitere Informationen finden Sie im Installationshandbuch im Abschnitt zu den Anforderungen an die Hardware und das Betriebssystem und zum Installationsverfahren.

	Konfigurationsvariable			
1.	Sentinel-Version:		Aktuelles Datum:	
2.	UNIX-Kernel-Werte für Oracle. Im Folgenden sind die Mindestwerte angegeben. In SLES und RHEL können Sie Parameter in etc/sysctl.conf festlegen.			
	◆ shmmax	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ shmmin	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ shmseg	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ shmmni	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ semmns	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ semmni	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ semmsl	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ shmopm	☐ : Ja | ☐ : Nein		Wert, wenn höher:
	◆ shmvmx	☐ : Ja | ☐ : Nein		Wert, wenn höher:
3.	Datenbanksystem			
	◆ Richtiges Betriebssystem für Sentinel-Komponenten	☐ : Ja | ☐ : Nein	◆ Richtiges Patch	☐ : Ja | ☐ : Nein
	◆ 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		
	◆ Datei Init.ora konfiguriert	☐ : Ja | ☐ : Nein		

	Konfigurationsvariable			
4.	DAS-Computer			
	◆ Richtiges Betriebssystem für Sentinel-Komponenten	: Ja | : Nein	◆ Richtiges Patch	: Ja | : Nein
	◆ Seriennummer			
	◆ Lizenzschlüssel			
5.	DAS-Installation			
	◆ DB-Hostname oder IP			
	◆ Datenbankname			Standard: ESEC
	◆ Datenbank-Port			Standard: 1521
	◆ Speicherort der JDBC-Datei			
6.	Datenbankinstanz (SID)			
7.	Datenbankname			
8.	Sentinel-Komponenten:			
	◆ Sentinel-Datenbank (IP oder DNS)			BS: Patch:
	◆ DB-Installationsprotokoll			
	◆ Oracle-Speicher (RAM)			
	◆ Instanzname			
	◆ Listener-Port		Standard: 1521	
	◆ SYS-Passwort			
	◆ SYSTEM-Passwort			
	◆ Keystore-Datei bei der Installation importiert:			
	◆ Korrelation	☐ : Ja | ☐ : Nein		
	◆ DAS	☐ : Ja | ☐ : Nein		
	◆ Collector Manager	☐ : Ja | ☐ : Nein		
	◆ Communication Server	☐ : Ja | ☐ : Nein		
	◆ Kommunikationsserver (iSCALE) (IP bzw. DNS)	◆ IP/DNS:		BS: Patch:
	◆ DAS/Advisor (IP oder DNS) (Advisor ist optional)	◆		BS: Patch:
	◆ DAS RAM	◆		
	◆ Correlation Engine (IP und Betriebssystem)			

Konfigurationsvariable		
	◆ IP:	BS:
	◆ IP:	BS:
	◆ IP:	BS:
◆ Collector Builder (IP oder DNS) (genau eine Installation empfohlen)		
◆ Collector Manager	Geben Sie die Details für jede bereitgestellte Collector Manager-Instanz ein.	
◆ Collector Manager	☐ : Ja | ☐ : Nein	
◆ IP: ◆ BS:	◆ Nachrichtenbus-Port ◆ Sentinel Control Center-Proxy-Port ◆ Kommunikationsserver-Hostname ◆ Authentifizierungsport für Collector Manager-Zertifikat	

9. Advisor (optional)

◆ Auf demselben Computer wie DAS installiert?	☐ : Ja | ☐ : Nein
◆ Advisor-Download	☐ : Einzelplatzbetrieb | ☐ : Direktes Herunterladen vom Internet
◆ Speicherort der Datei für Datenfeed	
◆ „Von“-Adresse des Advisors	
◆ „An“-Adresse des Advisors	
◆ Benutzername	Benutzername:

10. 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

11. Datenbankgröße::

Konfigurationsvariable		
◆ Standard (20 GB)		
◆ Groß (400 GB)		
◆ Benutzerdefiniert (Größe)		
12. SMTP-Server (DNS oder IP)		
13. Benutzerpasswörter		
◆ esecadm	PW:	
◆ Basisverzeichnis		Standard: /export/home
◆ esecapp	PW:	
◆ esecdba	PW:	
◆ esecrpt	PW:	
Crystal-Installation		
1. Crystal Version:		
◆ BS		
◆ Crystal-Datenbank		
◆ Crystal Server (IP oder DNS)		
◆ Webserver (IP oder DNS)		
2. Crystal Reports		
◆ Alle Berichte veröffentlicht	☐ : Ja | ☐ : Nein	
◆ Konfigurierte Berichte in SCC	☐ : Ja | ☐ : Nein	

Installationsbericht für Sentinel unter Solaris mit Oracle

C

Diese Checkliste kann für verteilte Installationen mit maximal drei Collector Manager- und Correlation Engine-Instanzen verwendet werden.

Weitere Informationen finden Sie im Installationshandbuch im Abschnitt zu den Anforderungen an die Hardware und das Betriebssystem und zum Installationsverfahren.

	Konfigurationsvariable			
1.	Sentinel-Version:			Aktuelles Datum:
2.	UNIX-Kernel-Werte für Oracle. Im Folgenden sind die Mindestwerte angegeben. In SLES und RHEL können Sie Parameter in etc/sysctl.conf festlegen.			
	shmmax		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	shmmin		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	shmseg		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	shmmni		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	semmns		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	semmni		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	semmsl		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	shmopm		☐ : Ja | ☐ : Nein	Wert, wenn höher:
	shmvmx		☐ : Ja | ☐ : Nein	Wert, wenn höher:
3.	Datenbanksystem			
	Richtiges Betriebssystem für Sentinel-Komponenten	☐ : Ja | ☐ : Nein	Richtiges Patch	☐ : Ja | ☐ : Nein
	◆ 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		

	Konfigurationsvariable			
	◆ Datei Init.ora konfiguriert	☐ : Ja | ☐ : Nein		
	◆ Richtiges Betriebssystem für Sentinel-Komponenten	☐ : Ja | ☐ : Nein	◆ Richtiges Patch	☐ : Ja | ☐ : Nein
4.	DAS-Computer			
	◆ Seriennummer			
	◆ Lizenzschlüssel			
5.	DAS-Installation			
	◆ DB-Hostname oder IP			
	◆ Datenbankname			Standard: ESEC
	◆ Datenbank-Port			Standard: 1521
	◆ Speicherort der JDBC-Datei			
6.	Datenbankinstanz (SID)			
7.	Datenbankname			
8.	Sentinel-Komponenten:			
	◆ Sentinel-Datenbank (IP oder DNS)			BS: Patch:
	◆ DB-Installationsprotokoll			
	◆ Oracle-Speicher (RAM)			
	◆ Instanzname			
	◆ Listener-Port		Standard: 1521	
	◆ SYS-Passwort			
	◆ SYSTEM-Passwort			
	◆ Keystore-Datei bei der Installation importiert:			
	◆ Korrelation	☐ : Ja | ☐ : Nein		
	◆ DAS	☐ : Ja | ☐ : Nein		
	◆ Collector Manager	☐ : Ja | ☐ : Nein		
	◆ Collector Manager			
	◆ Collector Manager installieren:	☐ : Ja | ☐ : Nein	Proxy | Nachrichtenbus direkt	
	◆ IP: ◆ BS:	◆ Nachrichtenbus-Port ◆ Sentinel Control Center-Proxy-Port ◆ Kommunikationsserver-Hostname ◆ Authentifizierungsport für Collector Manager-Zertifikat		

Konfigurationsvariable			
◆ Communication Server	☐ : Ja | ☐ : Nein		
◆ Kommunikationsserver (iSCALE) (IP bzw. DNS)	☐ : Ja | ☐ : Nein		BS: Patch:
◆ DAS/Advisor (IP oder DNS) (Advisor ist optional)			BS: Patch:
◆ DAS RAM			
◆ Correlation Engine (IP und Betriebssystem)			
	IP:		BS:
	IP:		BS:
	IP:		BS:
◆ Crystal Server (IP oder DNS)			
◆ MySQL für Crystal Server	MySQL Version: MySQL-Patch: sa-Passwort oder Passwortinhaber:		
◆ IP:	Benutzername:	PW:	BS:
◆ Collector Builder (IP oder DNS) (genau eine Installation empfohlen)			
◆ Collector Manager			
◆ Installation von Collector Manager unter Verwendung von:	☐ : Ja | ☐ : Nein	☐ : Proxy | ☐ : Nachrichtenbus direkt	
◆ IP:	PW:		BS:
◆ IP:	PW:		BS:
◆ IP:	PW:		BS:

9. Advisor (optional)

Auf demselben Computer wie DAS installiert?	☐ : Ja | ☐ : Nein		
◆ Advisor-Download	☐ : Einzelplatzbetrieb	☐ : Direktes Herunterladen vom Internet	
◆ Speicherort der Datei für Datenfeed			
◆ „Von“-Adresse des Advisors			
◆ „An“-Adresse des Advisors			
◆ Benutzername und Passwort	Benutzername:		

	Konfigurationsvariable		
10.	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		
11.	Datenbankgröße:: ◆ Standard (20 GB) ◆ Groß (400 GB) ◆ Benutzerdefiniert (Größe)		
12.	SMTP-Server (DNS oder IP)		
13.	Benutzerpasswörter		
	◆ esecadm	PW:	
	◆ Basisverzeichnis		Standard: /export/home
	◆ esecapp	PW:	
	◆ esecdba	PW:	
	◆ esecrpt	PW:	
	Crystal-Installation		
1.	◆ Crystal Version: ◆ BS ◆ Crystal-Datenbank ◆ Crystal Server (IP oder DNS) ◆ Webserver (IP oder DNS)		
2.	Crystal Reports		
	◆ Alle Berichte veröffentlicht	☐ : Ja | ☐ : Nein	

Konfigurationsvariable
◆ Konfigurierte Berichte in SCC ☐ : Ja | ☐ : Nein

Installationsbericht für Sentinel unter Windows mit Microsoft SQL Server

D

Diese Checkliste kann für verteilte Installationen mit maximal drei Collector Manager- und Correlation Engine-Instanzen verwendet werden.

Weitere Informationen finden Sie im Installationshandbuch im Abschnitt zu den Anforderungen an die Hardware und das Betriebssystem und zum Installationsverfahren.

	Konfigurationsvariable			
1.	Sentinel-Version:			Aktuelles Datum:
	Datenbanksystem			
	◆ Richtiges Betriebssystem für Datenbank	☐ : Ja | ☐ : Nein	◆ Richtiges Patch	☐ : Ja | ☐ : Nein
	◆ Richtige SQL-Datenbank	☐ : Ja | ☐ : Nein	◆ Richtiges Patch	☐ : Ja | ☐ : Nein
	◆ Version		◆ Patch-Stufe	
	◆			◆
2.	Für DAS-Installationen unter dem Konto der Windows-Domäne„Als Dienst anmelden“ zuweisen	☐ : Ja | ☐ : Nein		
3.	DAS-Computer			
	◆ Seriennummer			
	◆ Lizenzschlüssel			
4.	Datenbank-Hostname oder IP:	<Hostname>[\<Instanzname>]		
5.	Datenbankname			Standard: ESEC
6.	Anschluss:			Standard: 1433
7.	Authentifizierungsmodus	☐ : gemischt		
		☐ : nicht gemischt		
8.	sa-Passwort für SQL Server bzw. Passwortinhaber.	PW:		
9.	Sentinel-Komponenten:			
	◆ Sentinel-Datenbank (IP oder DNS)			BS: Patch:

	Konfigurationsvariable		
	◆ Keystore-Datei bei der Installation importiert:		
	◆ Korrelation	☐ : Ja | ☐ : Nein	
	◆ DAS	☐ : Ja | ☐ : Nein	
	◆ Collector Manager-Service	☐ : Ja | ☐ : Nein	
	◆ Communication Server	☐ : Ja | ☐ : Nein	
	◆ Kommunikationsserver (iSCALE) (IP bzw. DNS)		BS: Patch:
	◆ DAS/Advisor (IP oder DNS) (Advisor ist optional)		BS: Patch:
	◆ Correlation Engine (IP und Betriebssystem)		
		IP:	BS:
		IP:	BS:
		IP:	BS:
	◆ Crystal Server (IP oder DNS)		BS: Patch:
	◆ Microsoft SQL Server für Crystal Server	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)		
	◆ Collector Manager	☐ : Ja | ☐ : Nein ☐ Proxy | ☐ Nachrichtenbus direkt	
	◆ IP: ◆ BS:	◆ Nachrichtenbus-Port ◆ Sentinel Control Center-Proxy-Port ◆ Kommunikationsserver-Hostname ◆ Authentifizierungsport für Collector Manager-Zertifikat	
10.	Advisor (optional)		
	Auf demselben Computer wie DAS installiert?	☐ : Ja | ☐ : Nein	
	◆ Advisor-Download	☐ : Einzelplatzbetrieb | ☐ : Direktes Herunterladen vom Internet	

	Konfigurationsvariable		
	◆ Speicherort der Datei für Datenfeed		
	◆ „Von“-Adresse des Advisors		
	◆ „An“-Adresse des Advisors		
	◆ Benutzername und Passwort	Benutzername:	
11.	Speicherorte für Datenbankdateien:		
	◆ Datendateien		
	◆ Indexdateien		
	◆ 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:	

	Konfigurationsvariable			
	Crystal-Installation			
1.	Crystal Version:			
	BS			
	DB			
	Crystal Server (IP oder DNS)			
	Microsoft SQL (optional, jedoch empfohlen)	Microsoft SQL-Version:		
		Microsoft SQL-Patch:		
		sa-Passwort oder Passwortinhaber:		
	IP:	Benutzername:	PW:	BS:
2.	Crystal Reports			
	Berichtstyp	☐ : SQL	☐ : Oracle	
	◆ Alle Berichte veröffentlicht	☐ : Ja | ☐ : Nein		
	◆ Konfigurierte Berichte in SCC	☐ : Ja | ☐ : Nein		