# Novell® Sentinel™

5.1.3

7. Juli 2006

www.novell.com

Band II – SENTINEL-Benutzerhandbuch

Novell®

## Rechtliche Hinweise

Novell, Inc., übernimmt keine Gewährleistung oder Haftung in Bezug auf den Inhalt und die Verwendung dieser Dokumentation und schließt insbesondere jede ausdrückliche oder stillschweigende Gewährleistung bezüglich der handelsüblichen Qualität sowie der Eignung für einen bestimmten Zweck aus.
Darüber hinaus behält sich Novell, Inc., das Recht vor, diese Veröffentlichung ohne vorherige Ankündigung zu überarbeiten und inhaltliche Änderungen vorzunehmen, ohne dass für Novell die Verpflichtung entsteht, Personen oder Organisationen über die vorgenommenen Änderungen zu informieren.

Novell, Inc., übernimmt ferner keine Gewährleistung oder Haftung in Bezug auf Software und schließt insbesondere jede ausdrückliche oder stillschweigende Gewährleistung bezüglich der handelsüblichen Qualität sowie der Eignung für einen bestimmten Zweck aus. Darüber hinaus behält sich Novell, Inc., das Recht vor, die Novell-Software vollständig oder teilweise zu ändern, ohne dass für Novell die Verpflichtung entsteht, Personen oder Organisationen über die vorgenommenen Änderungen zu informieren.

Sämtliche Produkte und technischen Informationen, die im Rahmen dieser Vereinbarung bereitgestellt werden, unterliegen möglicherweise den US-Exportbestimmungen und den Handelsgesetzen anderer Länder. Hiermit erklären Sie sich bereit, sämtliche Exportbestimmungen einzuhalten und ggf. die erforderlichen Lizenzen oder Berechtigungen für den Export, die Wiederausfuhr oder den Import einzuholen. Sie erklären sich bereit, keinen Export oder keine Wiederausfuhr an natürliche oder juristische Personen zu tätigen, die zurzeit auf den Exportausschlusslisten der USA aufgeführt sind, oder in Länder, die einem Embargo unterliegen oder die den US-Exportbestimmungen zufolge den Terrorismus unterstützen. Sie erklären sich bereit, die Lieferbestandteile nicht für die Endnutzung in verbotenen nuklearen, chemischen oder biologischen Waffen oder Raketen einzusetzen.
Weitere Informationen zum Export von Novell-Software finden Sie unter www.novell.com/info/exports/. Novell übernimmt keinerlei Verantwortung, wenn Sie es versäumen, die erforderlichen Exportgenehmigungen einzuholen.



Novell, Inc., besitzt Rechte an geistigem Eigentum für die Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte an geistigem Eigentum umfassen im Besonderen eines oder mehrere der unter http://www.novell.com/company/legal/patents/ aufgelisteten Patente sowie ein oder mehrere andere Patente oder Patentanmeldungen in den USA und in anderen Ländern, sind jedoch nicht darauf beschränkt.

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

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

## Novell-Marken

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

## Materialien von Drittanbietern

Alle Marken von Drittanbietern sind Eigentum der jeweiligen Inhaber.

## Rechltliche Hinweise zu Drittanbieterprodukten

Sentinel 5 enthält möglicherweise folgende Drittanbietertechnologien:

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

  Java 2 Platform kann außerdem folgende Drittanbieterprodukte enthalten:

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

- Eastman Kodak Company © 1992
- Lucinda, eine eingetragene Marke oder Marke von Bigelow and Holmes
- Taligent, Inc.
- IBM, einige Teile verfügbar unter: http://oss.software.ibm.com/icu4j/

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

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

- Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://grinninglizard.com/tinyxmldocs/index.html.
- SecurityNexus. Copyright © 2003 bis 2006. SecurityNexus, LLC. Alle Rechte vorbehalten.
- Xalan und Xerces, jeweils von der Apache Software Foundation lizenziert, Copyright © 1999–2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://xml.apache.org/dist/LICENSE.txt.
- yWorks. Copyright © 2003 bis 2006, yWorks.

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

# Vorwort

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

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

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

## Band I – Sentinel Installationshandbuch

In diesem Handbuch wird die Installation folgender Komponenten erläutert:

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

## Band II – Sentinel Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

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

## Band III – Wizard-Benutzerhandbuch

In diesem Handbuch werden die folgenden Themen behandelt:

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

## Band IV - Sentinel Referenzhandbuch für Benutzer

In diesem Handbuch werden die folgenden Themen behandelt:

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

## Volume V - Sentinel Handbuch für Drittanbieter-Integration

- Remedy
- HP OpenView Operations
- HP Service Desk

# Inhalt

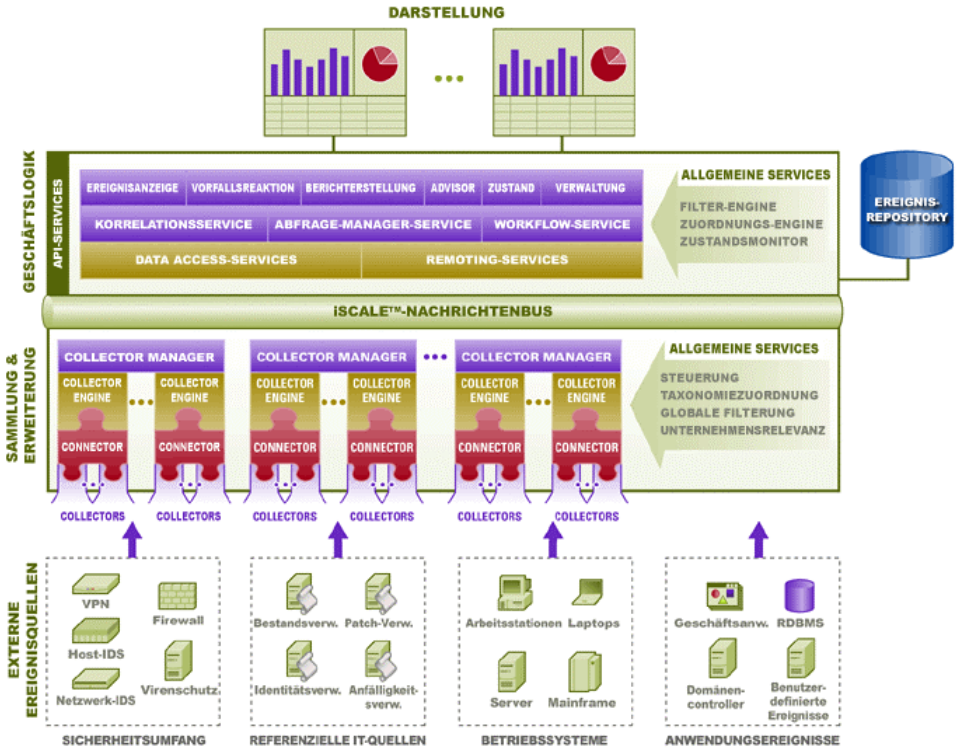
# 1 Einführung in Sentinel

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

Sentinel™ 5 ist die führende Lösung im Bereich Sicherheitsinformationsverwaltung und Überwachung der Einhaltung von Bestimmungen, die in Echtzeit aus vielen verschiedenen Quellen eines Unternehmens gesammelte Informationen empfängt, diese standardisiert sowie nach Priorität ordnet und Korrelationen durchführt. Sentinel sammelt von vielen auf dem Markt erhältlichen Sicherheitsprodukten Daten und bietet die Flexibilität, Daten gemäß der Entwicklung auf dem Softwaremarkt und sich ändernder geschäftlicher Anforderungen von neuen Technologien und Produkten zu sammeln.

Viele der Funktionen in Sentinel 5 sind das Ergebnis einer strukturellen Umgestaltung von Sentinel 4.0 und von den Anforderungen der Kunden von Novell beeinflusst. Aufgrund der zunehmenden Sicherheitsbedrohungen und des steigenden Drucks durch Bestimmungen suchen Unternehmen nach einer Lösung, mit der sie folgende Punkte abdecken können:

- die Sichtbarkeit und den Einblick gewinnen, die erforderlich sind, um eine größere Kosteneffektivität der Sicherheitsumgebung zu erreichen,
- die Einhaltung interner Richtlinien und rechtlicher Vorschriften (z. B. Sarbanes-Oxley, HIPAA, GLBA, FISMA, NISPOM, DCID 6/3 und DITSCAP) fortlaufend überwachen,
- Vorfälle schneller und mit gesteigerter Kosteneffektivität mittels zentralisierter und automatisierter Sammlung und Auflösung von Daten zu Bedrohungen und Richtlinien ermitteln und lösen,
- Betriebs- und Exekutivmetriken bereitstellen, um fortwährend die Position hinsichtlich Sicherheit und Einhaltung von Bestimmungen zu bewerten und um sowohl taktische als auch strategische Ziele zu verfolgen,
- betriebliche Kosten verringern, die mit der Überwachung der Sicherheit und der Einhaltung von Bestimmungen sowie der Ermittlung und Sanierung von Vorfällen verbunden sind.




Bei Ereignissen handelt es sich um Aktionen oder Vorgänge, die Sentinel gemeldet werden. Ereignisse von Sicherheitsgeräten werden als externe Ereignisse bezeichnet. Von Sentinel generierte Ereignisse werden interne Ereignisse genannt. Ereignisse können sich auf die Sicherheit, die Leistung oder auf Informationen beziehen. Bei einem externen Ereignis kann es sich beispielsweise um einen Angriff, der von einem Intrusion Detection System (IDS) ermittelt wird, eine erfolgreiche Anmeldung, die von einem Betriebssystem gemeldet wird, oder einen benutzerdefinierten Vorgang handeln, wie etwa den Zugriff auf eine Datei durch einen Benutzer. Interne Ereignisse werden von Sentinel generiert, um nennenswerte Änderungen am Zustand des Systems anzuzeigen, wie beispielsweise das Anhalten von Collectors oder das Deaktivieren von Korrelationsregeln.

Als Korrelation wird der Vorgang des Analysierens von Sicherheitsereignissen zum Ermitteln von Mustern innerhalb eines Ereignisses bzw. einer Abfolge von Ereignissen bezeichnet. Es kann beispielsweise eine Korrelationsregel erstellt werden, um zu ermitteln, wann dreißig oder mehr ICMP-Ereignisse innerhalb eines Zeitraums von einer Minute auftreten. Hoher ICMP-Datenverkehr („Flood“) kann zu einem Denial-of-Service-Angriff führen. Mittels Korrelation können Muster in einer Abfolge von Ereignissen von einem einzelnen Gerät, einer Reihe ähnlicher Geräte oder einer willkürlichen Sammlung von Geräten ermittelt werden. Dadurch können Benutzer die Risiken und den Schweregrad von Vorfällen besser abschätzen.

Sentinel nimmt darüber hinaus noch weitere Informationen im Bericht auf, so etwa Informationen zu den Computern im Netzwerk und ihren bekannten Services und Anfälligkeiten. Diese Informationen werden in Echtzeit zur Verfügung gestellt, wodurch die Aussagekraft der überwachten Ereignisse weiter verbessert wird.

Sentinel Control Center verwendet Vorgänge im Hintergrund, um Ergebnisse in Echzeit und Zusammenfassungen von Ergebnissen (Active Views™), Vorfälle, Verlaufsberichte (Analyse) und Advisor-Berichte anzuzeigen.

Ereignisse besonderer Wichtigkeit können zu einem Objekt gruppiert werden, das als *Vorfall* bezeichnet wird. Vorfälle können manuell vom Benutzer oder automatisch von der Correlation Engine erstellt werden. Vorfälle können zusätzliche Informationen enthalten, beispielsweise Informationen zu den angegriffenen Beständen, den Anfälligkeiten dieser Bestände und Informationen zum Angriff, der von der Sentinel Advisor-Komponente empfangen wird. Darüber hinaus können weitere Informationen als Anlage angefügt werden.

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

In diesem Kapitel wird die funktionelle und logische Architektur von Sentinel 5, gefolgt von dessen wichtigsten Produktmodulen beschrieben.

# Funktionelle Architektur

Sentinel 5 besteht aus drei Komponentenuntersystemen, die den Kern der funktionellen Architektur bilden:

- iSCALE-Plattform – ein ereignisorientiertes, skalierbares System
- Data Source Integration – ein erweiterbares Collector-System
- Application Integration – ein erweiterbares Anwendungssystem

Sentinel behandelt sowohl „Services“ als auch „Anwendungen“ als abstrakte Endpunkte von Services, die umgehend auf asynchrone Ereignisse reagieren können. Bei Services handelt es sich um „Objekte“, die nicht mit Protokollen bzw. mit der Art, wie Meldungen an Peer-Services weitergeleitet werden, kompatibel sein müssen.

# Sentinel-Funktionen

Sentinel ist eine mit vielen Funktionen ausgestattete Anwendung für Endbenutzer, die es ermöglicht, verschiedene Funktionen zu überwachen und zu verwalten. Zu den Hauptfunktionen gehören:

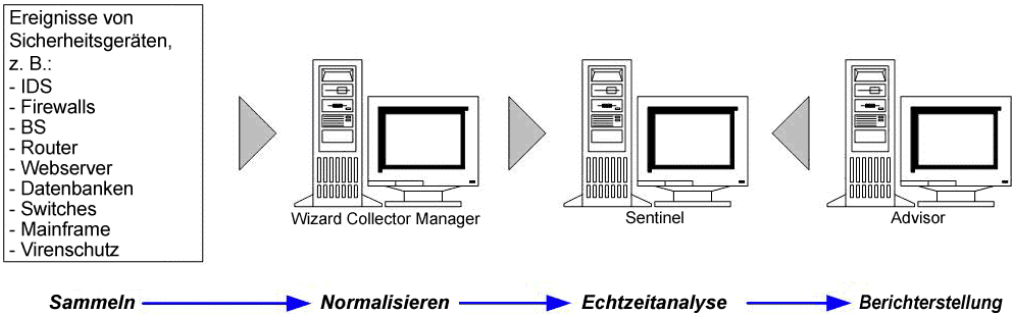
- Ansichten in Echzeit von vielen Ereignisabfolgen
- Auf Ereignissen in Echzeit und Ereignissen aus Verläufen basierende Berichtsfunktionen
- Regulierung von Benutzern sowie deren Anzeige- und Bearbeitungsberechtigungen nach Berechtigungszuweisung
- Einschränkung des Zugriffs für Benutzer auf Ereignisse
- Organisation von Ereignissen in Vorfälle zur effizienten Reaktionsverwaltung und -verfolgung
- Ermittlung von Mustern in Ereignissen und Ereignisabfolgen

# Überblick über die Architektur

Das Sentinel-System empfängt Ereignisse vom Wizard Collector Manager. Die Ereignisse werden dann in Echtzeit angezeigt und in einer Datenbank für die Verlaufsanalyse protokolliert.

Das Sentinel-System verwendet eine relationale Datenbank und besteht aus Sentinel-Vorgängen und einer Berichts-Engine. Als Eingabe akzeptiert das System Ereignisse vom Collector Manager. Der Collector Manager dient als Schnittstelle zu Produkten von Drittanbietern und standardisiert die Daten dieser Produkte. Die standardisierten Daten werden dann an die Sentinel-Prozesse und -Datenbank gesendet.

Mithilfe der in Sentinel integrierten Berichts-Engine können Verlaufsanalysen und -berichte erstellt werden. Die Berichts-Engine extrahiert Daten von der Datenbank und integriert die Berichtsanzeigen mit HTML-Dokumenten über eine HTTP-Verbindung in Sentinel Control Center.




Zu den Sentinel-Funktionen gehören:

- Verarbeitung von Ereignissen in Echtzeit, die vom Wizard Collector Manager empfangen werden,
- eine intuitive, flexible und regelbasierte Korrelationssprache,
- auf hohe Leistung ausgelegte Regeln,
- eine skalierbare, verteilbare und erweiterbare Multi-Thread-Architektur.

Die Sentinel-Vorgänge verwenden für die Kommunikation eine Message Oriented Middleware (MOM, meldungsbasierte Middleware).

## iSCALE-Plattform

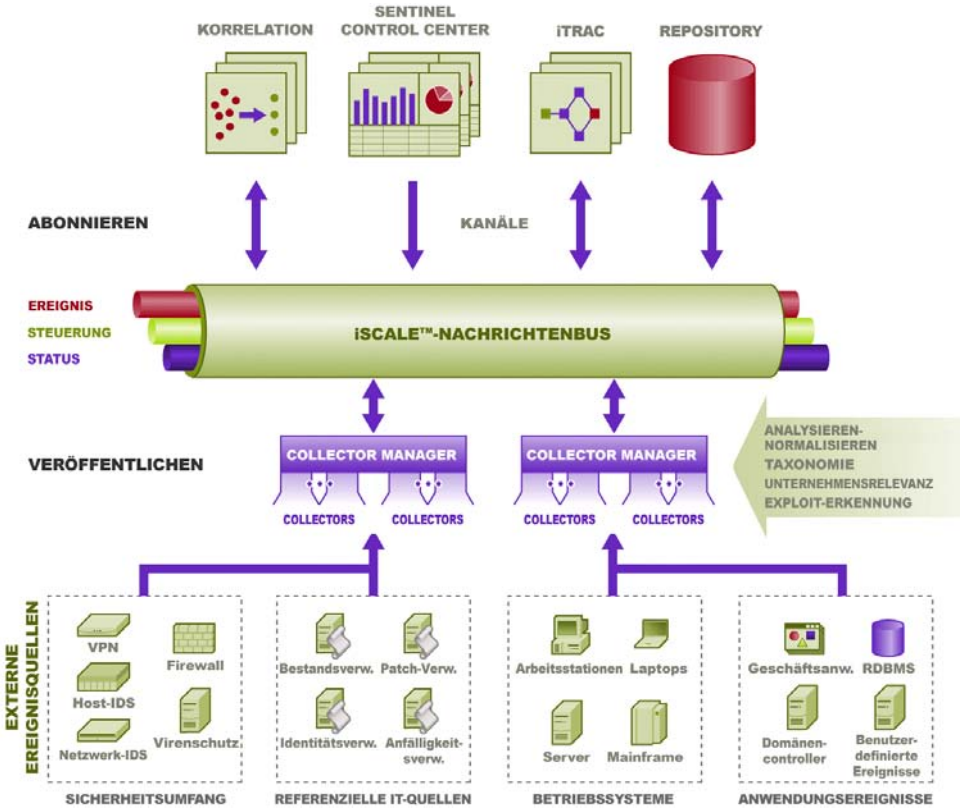
Die iSCALE™-Architektur von Sentinel baut auf einer standardbasierten, serviceorientierten Architektur (Service Oriented Architecture, SOA) auf, die die Vorteile der speicherinternen Verarbeitung und des verteilten Computing in sich vereint. Das Herzstück von iSCALE ist ein spezieller Nachrichtenbus, der große Mengen von Daten verarbeiten kann. Da hinsichtlich der iSCALE-Plattform ausschließlich ein standardbasierter Ansatz mit hochwertigen Komponenten zum Einsatz kommt, kann mit iSCALE die kosteneffiziente Skalierung gewährleistet werden.

### Nachrichtenbus

Der iSCALE-Nachrichtenbus ermöglicht die unabhängige Skalierung einzelner Komponenten sowie die standardbasierte Integration in externe Anwendungen. Der Schlüssel zur Skalierbarkeit liegt darin, dass – im Gegensatz zu anderer verteilter Software – keine zwei Peer-Komponenten direkt miteinander kommunizieren. Sämtliche Komponenten kommunizieren über den Nachrichtenbus, der Tausende Nachrichtenpakete pro Sekunde übermitteln kann.

Durch optimale Nutzung der einzigartigen Funktionen des Nachrichtenbusses kann der Kommunikationskanal mit hohem Durchsatz eine hohe Datendurchsatzrate über unabhängige Komponenten des Systems hinweg erzielen und aufrechterhalten. Ereignisse werden beim Transport komprimiert und verschlüsselt, um die sichere und effiziente Zustellung vom Rand des Netzwerks bzw. von Sammelpunkten zum Hub des Systems zu gewährleisten, wo Echtzeitanalysen vorgenommen werden.

Beim iSCALE-Nachrichtenbus kommen eine Reihe von Warteschlangenservices zum Einsatz, die die Zuverlässigkeit der Kommunikation über die Sicherheits- und Leistungsaspekte der Plattform hinaus erhöhen. Durch eine Vielzahl temporärer und permanenter Warteschlangen bietet das System unübertroffene Zuverlässigkeit und Fehlertoleranz. So werden beispielsweise wichtige Meldungen/Nachrichten, die sich im Transit befinden, für den Fall gespeichert (in eine Warteschlange gestellt), dass es zu einem Ausfall im Kommunikationspfad kommt. Die in die Warteschlange gestellte Nachricht gelangt an ihr Ziel, nachdem das System nach dem Ausfall wiederhergestellt wurde.




## Kanäle

Die iSCALE-Plattform umfasst ein datengesteuertes und ein ereignisgesteuertes Modell, das abhängig von der Arbeitsauslastung die unabhängige Skalierung von Komponenten für das gesamte System ermöglicht. Hieraus ergibt sich ein Modell für die flexible Bereitstellung für die unterschiedlichen Systemumgebungen beim Kunden: An einem Standort sind möglicherweise zahlreiche Geräte mit geringem Ereignisvolumen vorhanden, an einem anderen weniger Geräte mit ausgesprochen hohem Ereignisvolumen. Die Ereignisdichte, also die Ereignisaggregation und das Ereignis-Multiplexing-Muster beim Transport von den Sammelpunkten, ist in diesen Fällen unterschiedlich und der Nachrichtenbus ermöglicht die konsistente Skalierung bei ungleich ausfallender Arbeitsauslastung.

iSCALE nutzt die Vorteile einer unabhängigen Umgebung mit mehreren Kanälen; auf diese Weise werden Konflikte nahezu ausgeschlossen und die Parallelverarbeitung von Ereignissen wird gefördert. Diese Kanäle und Teilkanäle können nicht nur für den Ereignisdatentransport verwendet werden, sie ermöglichen auch die präzise Vorgangssteuerung für Skalierung und Lastenausgleich bei unterschiedlichen Auslastungen. Durch unabhängige Servicekanäle, beispielsweise Steuerkanäle und Statuskanäle, die neben dem Hauptereigniskanal zum Einsatz kommen, kann die ereignisgesteuerte Architektur auf hohem Niveau und kosteneffizient skaliert werden.

## Sentinel-Ereignis

Sentinel erhält Informationen von Geräten, normalisiert diese Informationen in eine als *Sentinel-Ereignis* (kurz: *Ereignis)* bezeichnete Struktur und sendet das Ereignis zu Verarbeitungszwecken. Ereignisse werden in der Echtzeitanzeige, von Correlation Engine sowie dem Back-End-Server verarbeitet.

Ein Ereignis umfasst über 200 Tags. Tags weisen unterschiedliche Typen auf und dienen unterschiedlichen Zwecken. Es gibt einige vordefinierte Tags, beispielsweise zur Angabe des Schweregrads (severity), der Gefährlichkeit (criticality), der Ziel-IP (destination IP) und des Ziel-Ports (destination port). Es gibt zwei Gruppen konfigurierbarer Tags: Reservierte Tags sind für die interne eSecurity-Verwendung (für künftige Erweiterungen) bestimmt, Kunden-Tags sind für Erweiterungen beim Kunden bestimmt.

Tags können durch Umbenennung einen neuen Zweck erfüllen. Die Quelle eines Tags kann entweder *extern* (die Festlegung erfolgt also explizit durch das Gerät oder den entsprechenden Collector) oder *referenziell* sein. Der Wert eines referenziellen Tags wird unter Verwendung des Zuordnungsservice als Funktion eines oder mehrerer weiterer Tags berechnet. Ein Tag kann beispielsweise als Gebäudecode für das Gebäude definiert werden, in dem sich der Bestand befindet (die Angabe erfolgt als Ziel-IP eines Ereignisses). Ein Tag kann beispielsweise vom Zuordnungsservice als kundendefinierte Zuordnung berechnet werden (unter Verwendung der Ziel-IP aus dem Ereignis).

### Zuordnungsservice

Map Service ermöglicht es einem fortschrittlichen Mechanismus, Geschäftsrelevanzdaten im gesamten System zu propagieren. Von dieser Funktion wird die Skalierbarkeit unterstützt; sie ist zudem aufgrund der Erweiterungsfähigkeit vorteilhaft: Sie ermöglicht die intelligente Datenübertragung zwischen unterschiedlichen Knoten des verteilten Systems.

Map Service ist eine Funktion für die Datenpropagierung, mit deren Hilfe Querverweise zwischen Daten des Anfälligkeits-Absuchprogramms und Signaturen des Intrustion Detection-Systems und vielem mehr (z. B. bestandsbezogene Daten, geschäftsrelevante Daten) hergestellt werden können. Auf diese Weise ist die sofortige Benachrichtigung möglich, wenn ein anfälliges System durch einen Angriff ausgenutzt zu werden droht. Diese Funktion wird von drei separaten Komponenten bereitgestellt:

- Erfassen von Echtzeitereignissen von einer Intrusion Detection-Quelle
- Vergleichen dieser Signaturen mit den letzten Anfälligkeits-Absuchvorgängen und
- Erstellen von Querverweisen auf einen Angriffs-Feed über Sentinel Advisor (ein optionales Produktmodul, das Querverweise zwischen Echtzeit-IDS-Angriffssignaturen und den Daten des Anfälligkeits-Absuchprogramms des Benutzers erstellt).

Map Service propagiert Informationen dynamisch im System, ohne sich negativ auf die Systemauslastung auszuwirken. Wenn wichtige Datengruppen („Zuordnungen“ wie Bestandsinformationen oder Informationen zu Patch-Aktualisierungen) im System aktualisiert werden, propagiert Map Service die Aktualisierungen im gesamten System (in vielen Fällen können diese Daten einen Umfang von Hunderten Megabyte aufweisen).

Die Algorithmen von iSCALE Map Service verarbeiten umfangreiche referenzielle Datengruppen in einem Produktionssystem, in dem große Echtzeitdatenvolumen verarbeitet werden. Diese Algorithmen erkennen und analysieren Aktualisierungen und übermitteln per Push-Vorgang gezielt nur die Änderungen bzw. „Deltadatengruppen“ aus dem Repository an den Rand/den Umkreis des Systems.

### Streaming von Zuordnungen

Bei Map Service kommt ein Modell zur dynamischen Aktualisierung zum Einsatz und die Zuordnungen werden per Streaming von einen Punkt an den anderen übertragen. Auf diese Weise wird verhindert, dass sich große statische Zuordnungen im dynamischen Speicher ansammeln. Der Wert dieser Streaming-Funktion erweist sich inbesondere in einem für das Unternehmen essenziellen Echtzeitsystem wie Sentinel, in dem Datenbewegungen zuverlässig, prädiktiv und flexibel erfolgen müssen, unabhängig von einer möglichen temporären Auslastung des Systems.

### Exploit-Erkennung (Zuordnungsservice)

In Sentinel können Querverweise zwischen Ereignisdatensignaturen und Daten von Anfälligkeits-Absuchprogrammen erstellt werden. Benutzer werden automatisch und umgehend benachrichtigt, wenn ein anfälliges System durch einen Angriff ausgenutzt zu werden droht. Hier kommt Folgendes zum Einsatz:

- Advisor-Feed
- Intrusion Detection
- Anfälligkeits-Absuchvorgänge
- Firewalls

Advisor stellt einen Querverweis zwischen Ereignisdatensignaturen und Daten von Anfälligkeits-Absuchprogrammen her. Der Advisor-Feed verfügt über einen Warnungs- und Angriffs-Feed. Der Warnungs-Feed enthält Informationen zu Anfälligkeiten und Bedrohungen. Beim Angriffs-Feed handelt es sich um die normalsierte Form von Ereignissignaturen und Anfälligkeits-Plugins. Informationen zur Advisor-Installation finden Sie im *Sentinel-Installationshandbuch*.

Folgende System werden unterstützt:

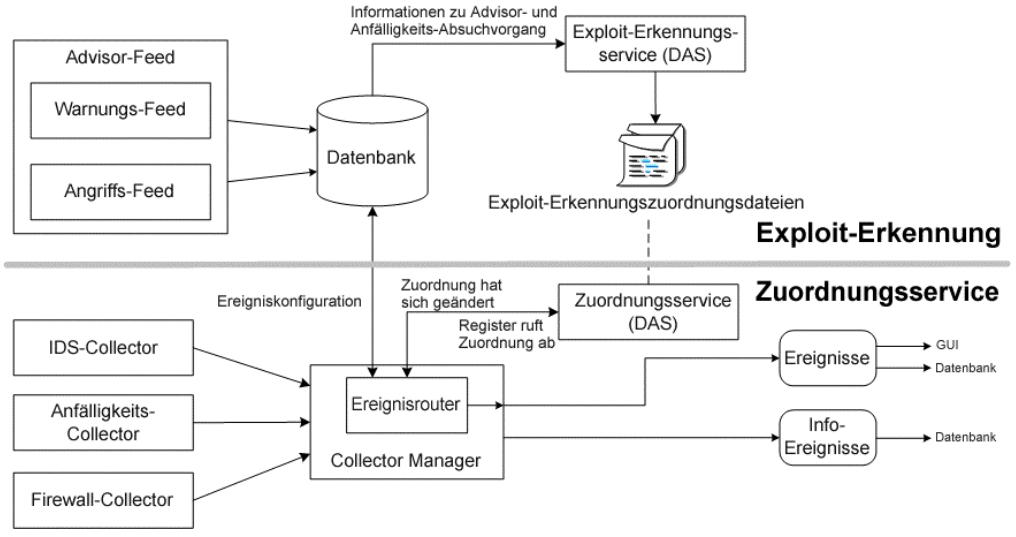
**Intrusion Detection-Systeme**
- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- Intrusion.com (SecureNet_Provider)
- ISS BlackICE
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server
- ISS RealSecure Guard
- Snort
- Symantec Network Security 4.0 (ManHunt)
- Symantec Intruder Alert
- McAfee IntruShield

**Anfälligkeits-Absuchprogramme**
- eEYE Retina
- Foundstone Foundscan
- ISS Database Scanner
- ISS Internet Scanner
- ISS System Scanner
- ISS Wireless Scanner
- Nessus
- nCircle IP360
- Qualys QualysGuard

**Firewalls**
- Cisco IOS Firewall

Sie benötigen mindestens ein Anfälligkeits-Absuchprogramm und entweder ein Intrusion Detection-System (IDS) oder eine Firewall von jeder der obigen Kategorien. Der IDS bzw. Firewall DeviceName (rv31) muss demnach wie oben grau hervorgehoben angezeigt werden. Zudem muss vom IDS bzw. der Firewall das DeviceAttackName (rt1)-Feld vorschriftsmäßig ausgefüllt werden (z. B. WEB-PHP Mambo uploadimage.php access).

Der Advisor-Feed wird an die Datenbank und dann an den Exploit-Erkennungsservice gesendet. Der Exploit-Erkennungsservice erstellt eine oder zwei Dateien, je nachdem, welche Art von Daten aktualisiert wurden.




Die Exploit-Erkennungszuordnungsdateien werden vom Zuordnungsservice verwendet, um Angriffe Ausnutzungsversuchen (Exploits) von Anfälligkeiten zuzuordnen.

Anfälligkeits-Absuchprogramme suchen auf anfällige Bereiche des Systems (Bestands) ab. IDS erkennen etwaige Angriffe auf diese anfälligen Bereiche. Firewalls erkennen, ob Datenverkehr auf diese anfälligen Bereiche ausgerichtet ist. Wenn ein Angriff mit einer Anfälligkeit im Zusammenhang steht, kam es zur Ausnutzung des Bestands.

Der Exploit-Erkennungsservice stellen in folgendem Verzeichnis zwei Dateien:

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

Bei diesen beiden Dateien handelt es sich um attackNormalization.csv und exploitDetection.csv.

Die Datei attackNormalization.csv wird erstellt im Anschluss an:

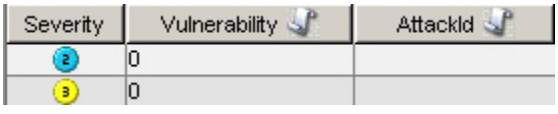
- Advisor-Feed
- DAS-Start (wenn in das_query.xml aktiviert; standardmäßig deaktiviert)

Die Datei exploitDetection.csv wird im Anschluss an einen der nachfolgenden Schritte erstellt:

- Advisor-Feed
- Anfälligkeits-Absuchvorgang
- Sentinel Server-Start (wenn in das_query.xml aktiviert; standardmäßig deaktiviert)

Standardmäßig werden zwei konfigurierte Ereignisspalten für die Exploit-Erkennung verwendet; der Verweis auf sie erfolgt von einer Zuordnung (alle zugeordneten Tags sind mit dem Schriftrollensymbol versehen).

- Vulnerability
- AttackId




Wenn das Feld für die Anfälligkeit (*vul*) 1 entspricht, wird der Bestand bzw. das Zielgerät ausgenutzt. Wenn das Feld für die Anfälligkeit 0 entspricht, wird der Bestand bzw. das Zielgerät nicht ausgenutzt.

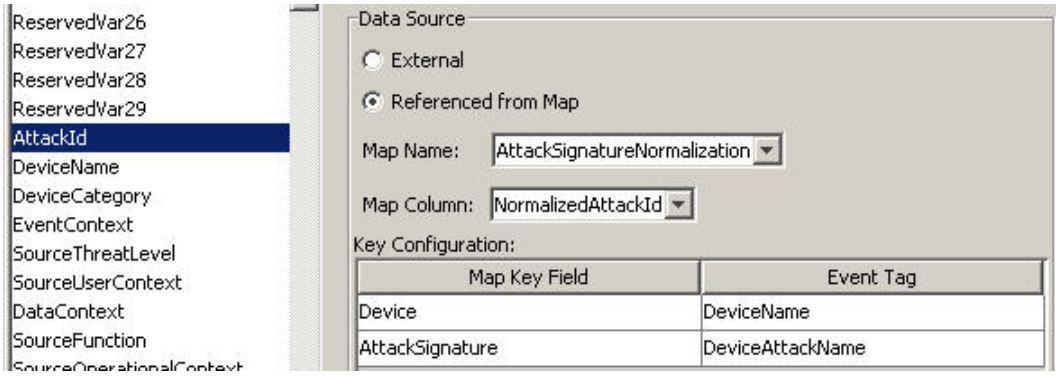
In Sentinel sind die nachfolgend angegebenen Zuordnungsnamen vorkonfiguriert, die mit attackNormalization.csv und exploitDetection.csv verknüpft sind.

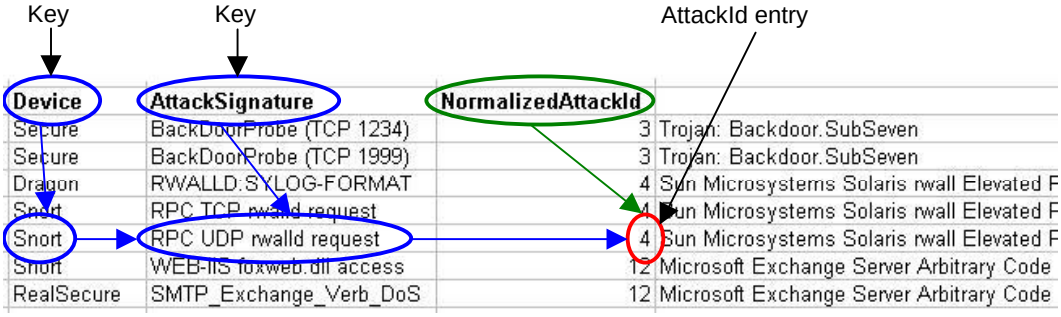
| **Zuordnungsname** | **Name der csv-Datei** |
|---|---|
| ▪ AttackSignatureNormalization | ▪ attackNormalization.csv |
| ▪ IsExploitWatchlist | ▪ exploitDetection.csv |

Es gibt zwei Typen von Datenquellen:

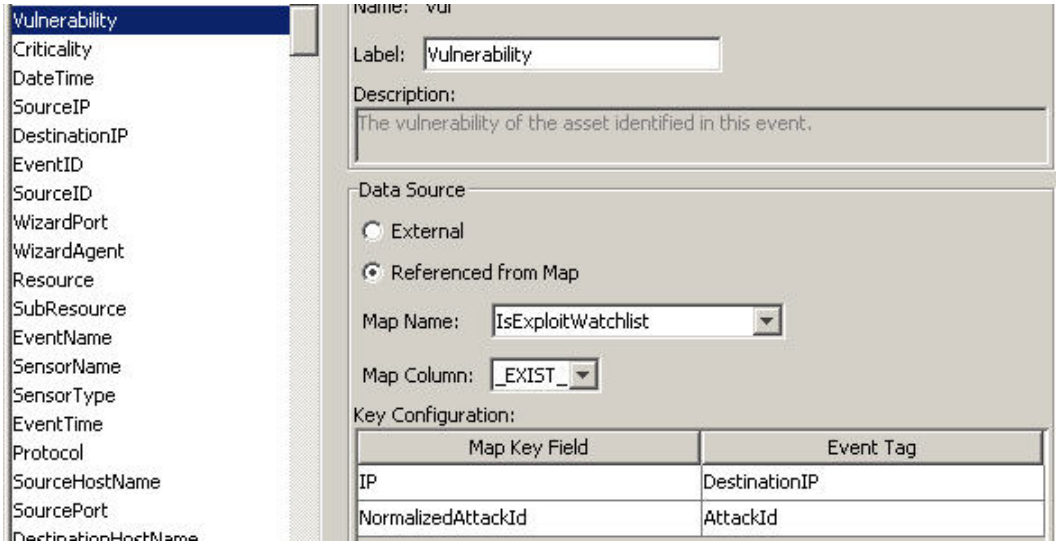
- Extern – Informationen werden vom Collector abgerufen
- Verweis von Zuordnung – Informationen werden aus einer Zuordnung abgerufen und das Tag wird gefüllt.

Für das AttackId-Tags sind die Geräte- (Art des Sicherheitsgeräts, z. B. Snort) und AttackSignature-Spalten als Schlüssel festgelegt und die NormalizedAttackID-Spalte in der Datei attackNormalization.csv wird verwendet. In einer Zeile, in der das DeviceName-Ereignis-Tag (ein IDS-Gerät wie Snort, von Advisor ausgefüllte Informationen sowie Anfälligkeitsinformationen aus der Sentinel-Datenbank) mit dem der Angabe zum Gerät (Device) übereinstimmt und in der das DeviceAttackName-Ereignis-Tag (von Advisor über den Exploit-Erkennungsservice ausgefüllte Angriffsinformationen in der Datenbank) mit AttackSignature übereinstimmt, schneidet diese Zeile beim AttackId-Wert die NormalizedAttackID-Spalte.




Das Anfälligkeits-Tag weist den Spalteneintrag „_EXIST_“ auf; das bedeutet, dass der Zuordnungsergebniswert 1 ist, wenn sich der Schlüssel in „IsExploitWatchlist“ (Datei exploitDetection.csv) befindet; andernfalls ist er 0. Die Schlüsselspalten für das Anfälligkeits-Tag sind „IP“ und „NormalizedAttackId“. Wenn ein eingehendes Ereignis mit einem DestinationIP-Ereignis-Tag , das mit dem Eintrag in der IP-Spalte und ein AttackId-Ereignis-Tag gefunden wird, das mit dem Eintrag in der NormalizedAttackId-Spalte in derselben Zeile übereinstimmt, lautet das Ergebnis „eins“ (1). Wenn keine Übereinstimmung in einer gemeinsamen Zeile gefunden wird. lautet das Ergebnis „null“ (0).



### Data Source Integration

Die Verwendung einer anpassungsfähigen und flexiblen Technologie spielt bei der Data Source Integration-Strategie von Sentinel eine zentrale Rolle; hierfür kommen interpretationsfähige Collectors zum Einsatz, die die Ereignisse im Datenstrom analysieren und normalisieren.

Diese Collectors können nach Bedarf geändert werden und sind an keine spezifische Umgebung gebunden. Erstellung, Änderung, Bereitstellung und Wartung der Collectors gestalten sich als einfach und können von den Benutzern direkt vorgenommen werden. Dank einer integrierten Bereitstellungsumgebung ist die interaktive Erstellung von Collectors über die Ziehen-und-Ablegen-Funktion einer grafischen Benutzeroberfläche möglich. Benutzer ohne Programmierkenntnisse können Collectors erstellen und so sicherstellen, dass sowohl aktuelle als auch künftige Anforderungen in einer sich stets verändernden IT-Umgebung erfüllt werden. Die Steuervorgänge für Collectors (z. B. Starten, Stoppen) werden zentral über Sentinel Control Center durchgeführt.1

### Application Integration

Integration in externe Anwendungen über standardmäßige Anwendungsprogrammierschnittstellen (Application Programming Interfaces, API) spielt in Sentinel eine zentrale Rolle. So ist beispielsweise über eine bidirektionale API für Problemberichtssysteme, einschließlich Remedy® und HP OpenView ServiceDesk®, die einfache Integration in externe Systeme möglich.

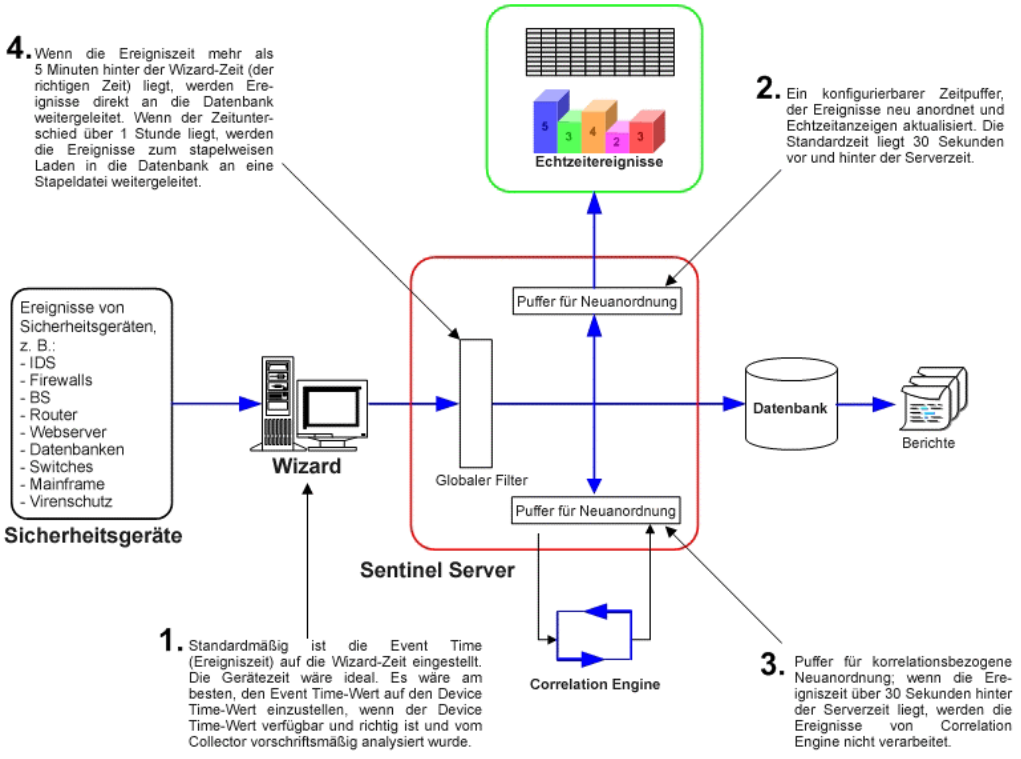
Die API basiert auf Web Services und ermöglicht es folglich sämtlichen SOAP-(Simple Object Access Protocol)-fähigen externen Systemen, von der umfassenden Integration des Sentinel-Systems zu profitieren.

## Time

Die Uhrzeit eines Ereignisses ist für seine Verarbeitung von ausgesprochen großer Bedeutung. Sie spielt für Berichterstellung und Revision sowie für die Echtzeitverarbeitung eine wichtige Rolle. In Correlation Engine werden nach Uhrzeit geordnete Ereignisdatenströme verarbeitet und Muster in Ereignissen sowie Zeitmuster im Datenstrom erkannt. Dem Gerät, das das Ereignis erstellt, ist der Echtzeiterstellungszeitpunkt des Ereignisses möglicherweise nicht bekannt. Aus diesem Grund stehen in Sentinel zwei Optionen für die Verarbeitung von Warnmeldungen von Sicherheitsgeräten zur Verfügung: Entweder wird die vom Gerät gemeldete Uhrzeit übernommen und als Uhrzeit des Ereignisses verwendet oder anstelle der vom Gerät angegebenen Uhrzeit wird das Ereignis bei der erstmaligen Verarbeitung durch Sentinel (den Collector) mit einem Zeitstempel versehen.

Sentinel ist ein verteiltes System und umfasst mehrere Vorgänge, die sich in unterschiedlichen Teilen des Netzwerks befinden können. Zudem kann es durch das Gerät zu einer gewissen Verzögerung kommen. Aus diesem Grund ordnen die Sentinel-Vorgänge die Ereignisse vor der Verarbeitung nach der Uhrzeit neu an.

In der nachfolgenden Abbildung wird das Sentinel-Zeitkonzept erläutert.




1. Standardmäßig ist die Event Time (Ereigniszeit) auf die Wizard-Zeit eingestellt. Die Gerätezeit wäre ideal. Folglich wäre es am besten, den Event Time-Wert auf den Device Time-Wert einzustellen, wenn der Device Time-Wert verfügbar und richtig ist und vom Collector vorschriftsmäßig analysiert wurde.
2. Ein konfigurierbarer Zeitpuffer, der Ereignisse neu anordnet und Echtzeitanzeigen aktualisiert. Die Standardzeit liegt 30 Sekunden vor und hinter der Serverzeit.
3. Puffer für korrelationsbezogene Neuanordnung; wenn die Ereigniszeit über 30 Sekunden hinter der Serverzeit liegt, werden die Ereignisse von Correlation Engine nicht verarbeitet.
4. Wenn die Ereigniszeit mehr als 5 Minuten hinter der Wizard-Zeit (der richtigen Zeit) liegt, werden Ereignisse direkt an die Datenbank weitergeleitet.

## Interne Ereignisse oder Systemereignisse

Interne Ereignisse oder Systemereignisse sollen den Status oder Statusänderungen des Systems melden. Es werden zwei verschiedene Ereignistypen vom internen System generiert:

- Interne Ereignisse
- Leistungsereignisse

Interne Ereignisse haben Informationscharakter und beschreiben einen einzelnen Zustand oder eine Änderung des Systemzustands. Diese Ereignisse melden, wenn sich ein Benutzer anmeldet, ein Fehler bei der Authenifizierung eines Benutzers auftritt, ein Vorgang gestartet oder eine Korrelationsregel aktiviert wird. Leistungsereignisse werden regelmäßig generiert und beschreiben die durchschnittlich von unterschiedlichen Teilen des Systems verwendeten Ressourcen.

Bei allen Systemereignissen werden folgende Attribute ausgefüllt:

- ST-(Sensor Type-)Feld: Für interne Ereignisse ist es auf „I“ eingestellt, für Leistungsereignisse auf „P“’
- Event ID: Eine eindeutige UUID für das Ereignis
- Event Time: Die Uhrzeit, zu der das Ereignis erstellt wurde
- Source: Die UUID des Vorgangs, der das Ereignis erstellt hat
- Sensor Name: Der Name des Vorgangs, der das Ereignis erstellt hat (z. B. DAS_Binary)
- RV32 (Gerätekategorie): Auf „ESEC“ eingestellt
- Collector: „Performance“ für Leistungsereignisse und „Internal“ für interne Ereignisse

Zusätzlich zu den allgemeinen Attributen werden bei jedem Systemereignis Ressource, Teilressource, Schweregrad, Ereignisname sowie Meldungs-Tags festgelegt. Bei internen Ereignissen ist der Ereignisname spezifisch genug, um Aufschluss über die genaue Bedeutung des Ereignisses zu geben (z. B. UserAuthenticationFailed). Durch die Meldungs-Tags werden weitere spezifische Details hinzugefügt; im obigen Beispiel enthält das Meldungs-Tag den Namen des Benutzers, den Namen des Betriebssystems (falls verfügbar) sowie den Namen des Computers. Bei Leistungsereignissen ist der Ereignisname allgemein gehalten und gibt Aufschluss über die Art der Statistikdaten und die Daten selbst befindet sich im Meldungs-Tag.

Leistungsereignisse werden direkt an die Datenbank gesendet. Wenn Sie sie anzeigen möchten, führen Sie eine Schnellabfrage durch.

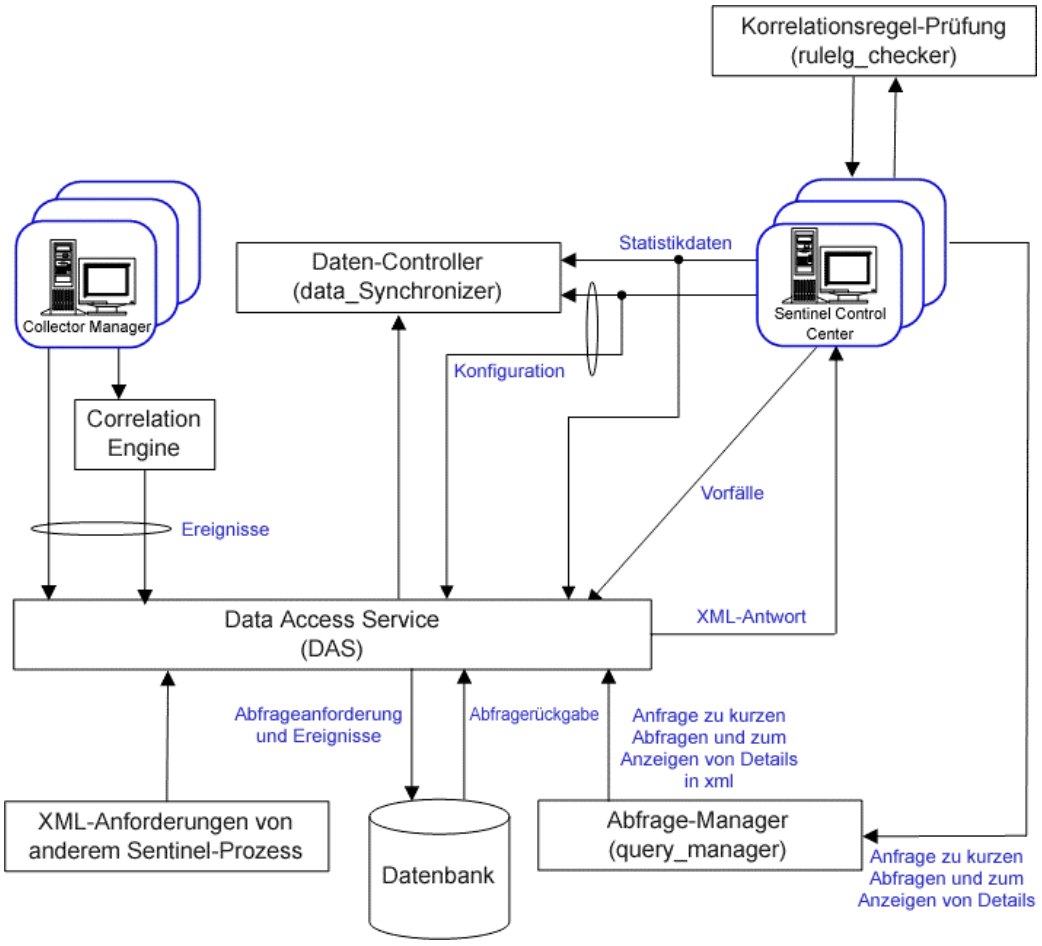
Siehe *Anhang A – Systemereignisse.*

## Vorgänge

Die nachfolgend angegebenen Vorgänge und der Windows-Service kommunizieren über iSCALE – die Message-Oriented Middleware (MOM) – miteinander.

- Watchdog
- Ereignisstatistiken
- Datensynchronisierungsprozess (Data Controller)
- Correlation Engine
- RuleLg Checker (Überprüfung von Korrelationsregeln)
- Data Access Service-Vorgang (DAS) – binär; Abfrage und Active Views™
- Abfrage-Manager
- eSecurity-Service (nur MSSQL) – siehe Watchdog

Nachfolgend ist die Architektur des Sentinel Server erläutert.




## Watchdog-Vorgang

Watchdog ist ein Sentinel-Vorgang, mit dem andere Sentinel-Vorgänge verwaltet werden. Wenn ein anderer Vorgang als Watchdog anhält, gibt Watchdog die entsprechende Meldung aus und startet den Vorgang dann neu.

Unter Windows ist Watchdog ein Service mit der Bezeichnung Sentinel. Wenn dieser Service gestoppt wird, werden sämtliche Sentinel-Vorgänge auf diesem Computer gestoppt.

## Ereignisstatistiken

Die Engine für Ereignisstatistiken ist eine Komponente des das_binary-Vorgangs. Sie verwaltet die von den Active Views-Diagrammen und Ereignistabellen verwendeten Daten in Sentinel Control Center.

Die Engine verwaltet eine Gruppe von Ereignissen und statistischen Daten für jede im Active Views-Assistenten angegebene Kombination aus Filtern und Ereignisattributen. Wenn ein Benutzer erstmals eine aktive Ansicht (Active View) mit einem bestimmten Filter und Ereignisattribut erstellt, wird eine neue Datengruppe erstellt. Diese Datengruppe enthält die Anzahl dieses Attributs in festen Intervallen sowie die aktuellsten Ereignisse für die einzelnen Intervalle. Jede Datengruppe ist für die Verwaltung für die jeweils aktuellsten 24 Stunden an Daten konfiguriert.

Intervalle werden nach kurzer Verzögerung an Sentinel Control Center gesendet, um die Daten zu stabilisieren, die aufgrund von Verzögerungen im Netzwerk und zeitlichen Verschiebungen möglicherweise verspätet eingegangen sind.

Aktive Ansichten werden automatisch für mehrere Benutzer freigegeben, wenn das gewünschte Ereignisattribut und der gewünschte Filter identisch sind. Wenn eine aktive Ansicht von keinem Benutzer mehr verwendet wird, wird sie nach einer Stunde verworfen. Wenn eine aktive Ansicht jedoch in den Benutzereinstellungen gespeichert wird, sammelt sie bis zu 100 Stunden weiter Daten.

### Datensynchronisierungsprozess (Daten-Cotroller)

Der Datensynchronisierungsvorgang (data_synchronizer) verwaltet die Änderung von Konfigurationsdaten durch mehrere Benutzer. Wenn ein Benutzer Daten über das Sentinel Control Center ändern möchte, wird dieser Datensatz vom data_synchronizer gesperrt. Detaillierte Informationen, von wem die Daten gesperrt wurden, werden für die anderen aktiven Sentinel Control Center-Instanzen veröffentlicht und diese Daten können von keinem anderen Benutzer geändert werden. Falls ein Sentinel Control Center geschlossen wird, bevor zuvor gesperrte Daten wieder freigegeben werden, erfolgt eine Zeitüberschreitung für die Sperre.

### Correlation Engine-Vorgang (correlation_engine)

Der Correlation Engine-Vorgang (correlation_engine) empfängt Ereignisse vom Wizard Collector Manager und veröffentlicht korrelierte Ereignisse basierend auf benutzerdefinierten Korrelationsregeln.

### RuleLg Checker-Vorgang (rulelg_checker)

Der RuleLg Checker-Vorgang (rulelg_checker) validiert die Syntax von Filter- und Korrelationsregelausdrücken. Das Sentinel Control Center verwendet diese Ergebnisse, um zu ermitteln, ob ein Filter oder eine Korrelationsregel gespeichert werden kann.

### Data Access Service-Vorgang (DAS)

Beim Data Access Service-(DAS-)Vorgang handelt es sich um den Permanentservice von Sentinel Server, der eine Schnittstelle zur Datenbank zur Verfügung stellt. Er ermöglicht den datengesteuerten Zugriff auf das Datenbank-Back-End.

DAS stellt einen aus fünf Einzelprozessen bestehenden Container dar. Mit jedem Prozess werden unterschiedliche Arten von Datenbankoperationen ausgeführt. Diese Vorgängen (Prozesse) werden mithilfe folgender Konfigurationsdateien gesteuert:

- das_binary.xml: Wird für Einfügevorgänge von Ereignissen und korrelierten Ereignissen verwendet
- das_query.xml: wird für alle anderen Datenbankoperationen verwendet
- activity_container.xml: Wird für die Ausführung und Konfiguration des Aktivitätsservices verwendet
- workflow_container.xml: Wird für die Konfiguration des Workflowservice (iTRAC) verwendet
- das_rt.xml: Wird für die Konfiguration der Active Views-Funktion in der Sentinel-Steuerungskonsole verwendet

DAS empfängt Anforderungen von unterschiedlichen Sentinel-Vorgängen, wandelt sie in eine Abfrage der Datenbank um, verarbeitet das von der Datenbank zurückgegebene Ergebnis und wandelt es wieder in eine Antwort um. Mit diesem Prozess werden Anforderungen unterstützt, um Ereignisse für Quick Query und Event Drill Down abzurufen, die Anfälligkeit von Informationen und Advisor-Informationen abzufragen und Konfigurationsinformationen zu manipulieren. Mithilfe von DAS erfolgt außerdem die Protokollierung aller vom Wizard Collector Manager empfangenen Ereignisse und Anforderungen zum Abrufen und Speichern von Konfigurationsinformationen.

### Abfrage-Manager-Vorgang (query_manager)

Der Abfrage-Manager-Vorgang (query_manager) empfängt von Sentinel Control Center Anforderungen hinsichtlich der Schnellabfrage und dem Anzeigen von Details zu Anforderungen und leitet diese über DAS an die Datenbank weiter. Die Anforderungen von Sentinel Control Center definieren die erforderlichen Ereignisse mithilfe eines Filters. falls ein Filter verwendet wird, empfängt der Abfrage-Manager die Filterdefinition und konvertiert den Filter in ein XML-Kriterium. Der Abfrage-Manager sendet die Anforderung anschließend an DAS. Nicht alle Filter können vollständig in Abfragen umgewandelt werden, die die Datenbank verarbeiten kann. Falls der Filter vollständig konvertiert wurde, weist der Abfrage-Manager DAS an, die Antwort direkt an das Sentinel Control Center zu senden. Wenn der Filter reguläre Ausdrücke enthält, die nicht in SQL (Structured Query Language) umgewandelt werden können, wandelt der Abfrage-Manager den enstprechenden Teil um und erstellt ein konservatives XML-Kriterium, das einen übergeordneten Satz der erforderlichen Ereignisse zurückgibt. In diesem Fall wird DAS vom Abfrage-Manager angewiesen, das Ergebnis an ihn zurückzugeben. Wenn die Antwort an den Abfrage-Manager zurückgegeben wird, wird sie im Arbeitsspeicher gefiltert und die Ereignisse, die den Filter passieren, werden an das Sentinel Control Center gesendet.

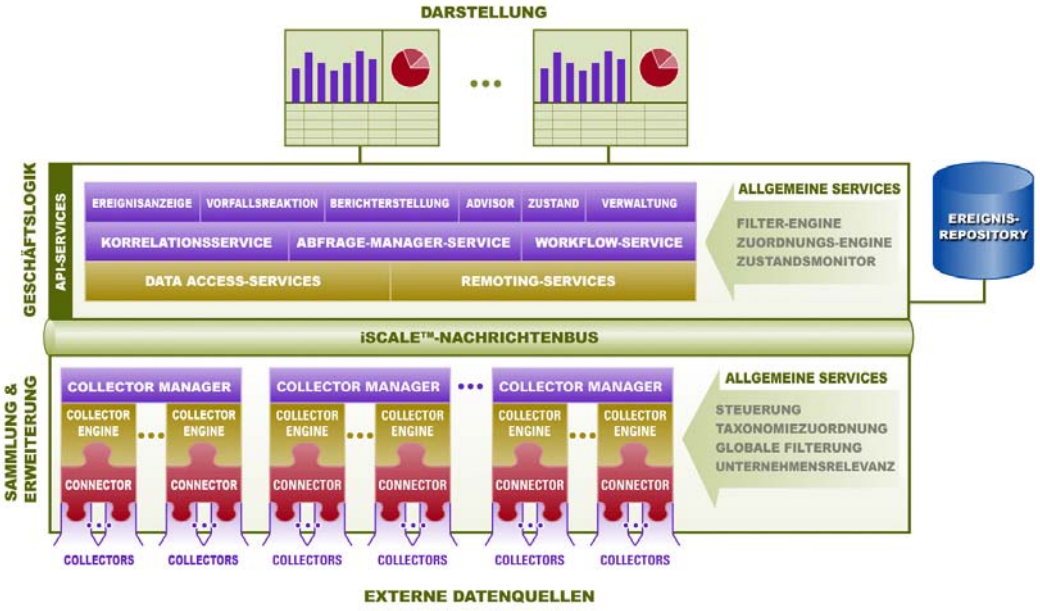
## Logische Architektur

Sentinel 5 besteht aus drei logischen Schichten:

- Sammel- und Erweiterungsschicht
- Geschäftslogikschicht
- Darstellungsschicht

In der Sammel-/Erweiterungsschicht werden die Ereignisse von externen Datenquellen aggregiert, die gerätespezifischen Formate werden in das Sentinel-Format umgewandelt, die native (systemeigene) Ereignisquelle wird um geschäftsrelevante Daten erweitert und die Ereignispakete werden an den Nachrichtenbus übermittelt. Die Schlüsselkomponente, die für die Umsetzung dieser Funktion zuständig ist, ist der Collector, der durch einen Service für Taxonomiezuordnung und globale Filter unterstützt wird.

Die Geschäftslogikschicht umfasst eine Gruppe verteilbarer Komponenten. Bei der Basiskomponente handelt es sich um einen Remoting-Service, der die Datenobjekte und -services mit Nachrichtenfunktionen versieht und so den transparenten Datenzugriff im gesamten Netzwerk gewährleistet, und den Data Access Service, einen Service zur Objektverwaltung, der Benutzern die Definition von Objekten mithilfe von Metadaten ermöglicht. Zudem stehen Korrelations-, Abfrage-Manager-, Workflow-, Ereignisanzeige-, Vorfallsreaktions-, Zustands-, Advisor-, Berichterstellungs- und Verwaltungs-Services zur Verfügung.




Über die Darstellungsschicht wird die Anwendungsoberfläche für den Endbenutzer bereitgestellt. Eine umfassende Konsole mit der Bezeichnung Sentinel Control Center bietet einen integrierten Benutzerarbeitsbereich mit sieben verschiedenen Anwendungen, auf die über ein einziges gemeinsames Framework zugegriffen werden kann. Dieses plattformübergreifende Framework basiert auf Java™ 1.4-Standards und bietet einheitlichen Einblick in unabhängige Geschäftslogikkomponenten – interaktive Echtzeit-Graphen, prozessfähige Vorfallsreaktion, automatisierbarer erzwingbarer Vorfalls-Workflow, Berichterstellung, Vorfallssanierung bei bekannten Ausnutzungsversuchen usw.

Jede dieser Schichten ist in der obigen Abbildung dargestellt und wird in den nachfolgenden Abschnitten detailliert erläutert.

## Sammel- und Erweiterungsschicht

Die Aggregation von Ereignissen erfolgt über eine Gruppe flexibler und konfigurierbarer Collectors, die Daten von einer Vielzahl von Sensoren und anderen Geräten und Quellen sammeln. Benutzer können im Vorfeld erstellte Collectors verwenden, vorhandene Collectors ändern oder eigene Collectors erstellen, um zu gewährleisten, dass das System sämtliche Anforderungen erfüllt.

Die Daten, die von den Collectors in Form von Ereignissen aggregiert werden, werden anschließend normalisiert und in das XML-(eXtensible Markup Language-)Format umgewandelt und durch eine Reihe von Metadaten (also Daten über Daten) erweitert (diese Vorgänge werden über eine Gruppe von Geschäftsrelevanzservices durchgeführt). Dann werden die Daten für die Serverseite propagiert, um die weitere rechnerische Analyse mithilfe der Nachrichtenbusplattform zu ermöglichen. Die Sammel- und Erweiterungsschicht umfasst folgende Komponenten:

- Connectors und Collectors
- Collector Manager und Engine
- Collector Builder

### Connectors und Collectors

Bei einem Connector handelt es sich um einen Konzentrator oder Multiplex-Adapter, der die Verbindung zwischen Collector Engine und den jeweiligen überwachten Ereignissen herstellt.

Bei Collectors handelt es sich um die auf der Komponentenebene agierenden Aggregatoren von Ereignisdaten von einer bestimmten Quelle. Sentinel 5 unterstützt primär „Collector-freie“ Remote-Verbindungen mit Quellen; Collectors können jedoch auf bestimmten Geräten bereitgestellt werden, auf denen der Remote-Ansatz weniger effizient ist.

Collectors werden über Sentinel Control Center gesteuert. Sentinel Control Center sorgt für die Umsetzung der Kommunikation zwischen den Collectors und der Sentinel-Plattform hinsichtlich Echtzeitanalyse, Korrelationsberechnung und Vorfallsreaktion.

### Collector Manager und Engine

Collector Manager verwaltet die Collectors, überwacht Systemsstatusmeldungen und führt die Ereignisfilterung nach Bedarf durch. Zu den Hauptfunktionen 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 Sentinel Server.

Bei einer Collector Engine handelt es sich um die Interpretationskomponente, die den Collector-Code analysiert.

### Collector Builder

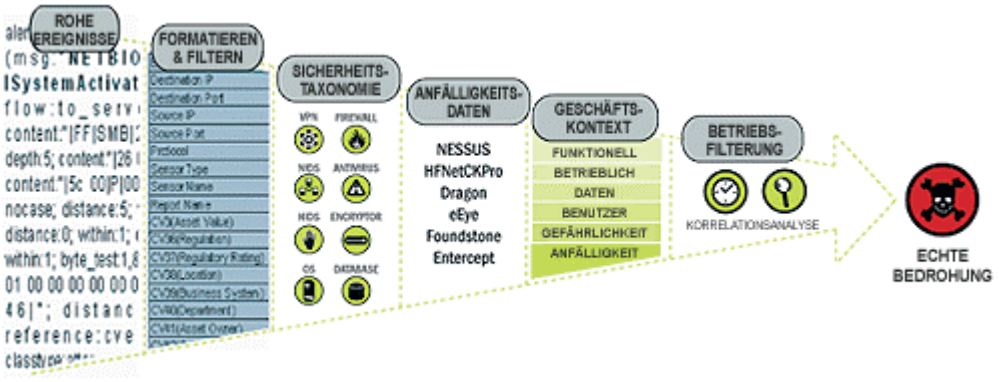
Collector Builder ist eine eigenständige Anwendung, mit der Sie Collectors erstellen und konfigurieren sowie die Fehlersuche für Collectors durchführen können. Diese Anwendung dient als integrierte Entwicklungsumgebung (Integrated Development Environment, IDE), die dem Benutzer das Erstellen neuer Collectors zum Analysieren von Daten von Quellgeräten ermöglicht; hierbei kommt eine Sonderinterpretationssprache zum Verarbeiten von Netzwerk- und Sicherheitsereignissen zum Einsatz.

### Allgemeine Services

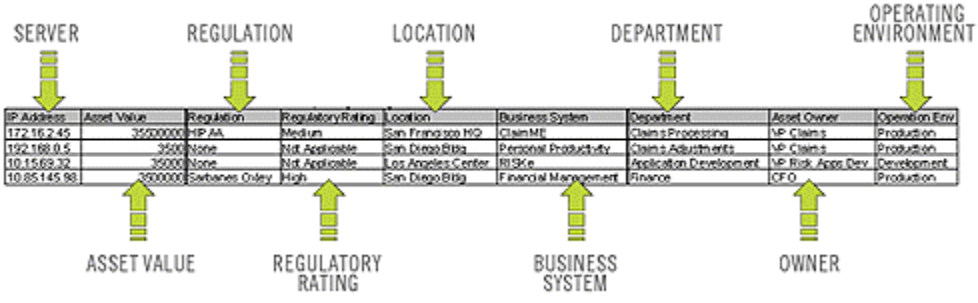
Sämtliche der oben beschriebenen Komponenten dieser Sammel- und Erweiterungsschicht werden von einer Gruppe allgemeiner Services gesteuert. Diese Dienstprogrammservices bilden die Grundlage für Datenerfassung und Datenerweiterung und helfen beim Filtern der störenden Elemente aus den Informationen (über globale Filter). Sie wenden benutzerdefinierte Tags an, um die Ereignisinformationen zu erweitern (über Services für Geschäftsrelevanz und Taxonomiezuordnung) und steuern die Daten-Collectors (über Steuerservices).

**Taxonomie** – Nahezu alle Sicherheitsprodukte generieren Ereignisse in unterschiedlichen Formaten und mit abweichendem Inhalt. Ein Fehler bei der Anmeldung wird unter Windows und Solaris beispielsweise unterschiedlich gemeldet.

Die Taxonomie von Sentinel übersetzt ungleichartige Produktdaten in aussagekräftige Begriffe und ermöglicht so die gleichartige Echtzeitansicht der gesamten Netzwerksicherheit. Die Sentinel-Taxonomie formatiert und filtert unverarbeitete Sicherheitsereignisse, bevor der Datenstrom um Ereigniskontext ergänzt wird. Bei diesem Vorgang werden sämtliche Sicherheitsdaten in die für die Verarbeitung durch Sentinel Correlation Engine optimale Struktur gebracht (siehe nachfolgendes Diagramm).




**Geschäftsrelevanz** – Sentinel 5 fügt geschäftsrelevante kontextbezogene Daten direkt in den Ereignisdatenstrom ein. Es stehen bis zu 135 individuell anpassbare Felder zur Verfügung, über die Benutzer bestandsspezifische Informationen hinzufügen können, beispielsweise Unternehmenseinheit, Eigentümer, Bestandswert und Geografie. Nachdem diese Informationen dem System hinzugefügt wurden, können alle anderen Komponenten von dem zusätzlichen Kontext profitieren.




**Exploit-Erkennung** – Durch die Exploit-Erkennung kann eine sofortige, prozessfähige Benachrichtigung zu Angriffen auf anfällige Systeme erfolgen. Sie stellt eine Echtzeitverknüpfung zwischen IDS-Signaturen und den Ergebnissen von Anfälligkeitsabsuchvorgängen bereit. Auf diese Weise werden Benutzer sofort und automatisch benachrichtigt, wenn versucht wird, ein anfälliges System durch einen Angriff auszunutzen. Hierdurch werden Effizienz und Effektivität der Vorfallsreaktion deutlich gesteigert.

Die Exploit-Erkennung stellt Benutzern Aktualisierungen hinsichtlich von Zuordnungen zwischen dem Intrusion Detection System (IDS) und Signaturen des Anfälligkeitsabsuchprogramms zur Verfügung. Zu den Zuordnungen zählt eine umfassende Liste mit IDS und Anfälligkeitsabsuchprogrammen. Die Benutzer können Ergebnisse der Anfälligkeitsabsuche problemlos in Sentinel heraufladen. Die Exploit-Erkennung analysiert sie automatisch und aktualisiert die entsprechenden IDS-Collectors. Mithilfe eingebetteter Informationen zum Anfälligkeitsstatus wird die Priorität von Reaktionen auf Sicherheitsbedrohungen effizient und effektiv in Echtzeit festgelegt.

Wenn ein Angriff auf einen anfälligen Bestand vorgenommen wird, alarmiert Exploit-Erkennung die Benutzer mit dem entsprechenden Schweregrad der ausgenutzten Anfälligkeit. Auf diese Weise können Benutzer für Ereignisse mit hoher Priorität umgehend Maßnahmen ergreifen. Unsicherheiten bei der Überwachung von Warnmeldungen gehören folglich der Vergangenheit an. Die Vorfallsreaktion wird effizient beschleunigt, da der Schwerpunkt auf bekannten Angriffen auf anfällige Bestände liegt.

Über die Exploit-Erkennung können Benutzer zudem Signaturen und Anfälligkeiten zuordnen und deren Zuordnung aufheben, um falsche Positiv- und Negativ-Meldungen auszublenden und benutzerdefinierte Signaturen bzw. Anfälligkeitsabsuchvorgänge optimal zu nutzen.

## Geschäftslogikschicht

Der Kernel der Sentinel 5-Plattform besteht aus eine Gruppe lose zusammenhängender Services, die in einer Einzelplatzbetriebkonfiguration bzw. in einer verteilten Topologie ausgeführt werden können. Diese serviceorientierte Architektur (Service-Oriented Architecture, SOA) trägt den Namen iSCALE. Die SOA von Sentinel umfasst eine Gruppe von Engines, Services und Anwendungsprogrammierschnittstellen (Application Programming Interfaces, APIs), die gemeinsam für die lineare Skalierung der Lösung bei ansteigender Datenauslastung und/oder Verarbeitungsarbeitsauslastung sorgen.

Sentinel-Services werden in speziellen Containern ausgeführt und ermöglichen unübertroffene Verarbeitung und Skalierung, da sie für meldungsbasierten Transport und meldungsbasierte Berechnung optimiert wurden. Sentinel Server bietet Schlüsselservices für folgende Aspekte:

- Remoting-Service
- Data Access Service
- Abfrage-Manager-Service
- Korrelationsservice
- Workflow-Service
- Ereignisanzeige
- Vorfallsreaktion
- Berichterstellung
- Advisor
- Zustand
- Verwaltung

### Remoting-Service

Der Remoting-Service von Sentinel 5 stellt den Mechanismus für die Kommunikation zwischen Server- und Clientprogrammen bereit. Dieser Mechanismus wird normalerweise als verteilte Objektanwendung bezeichnet.

Der Remoting-Service stellt Folgendes bereit:

- Suche nach Remote-Objekten: Hierfür kommen Metadaten zum Einsatz, die Aufschluss über den Objektnamen bzw. das Registrierungs-Token geben; der tatsächliche Standort ist hierbei nicht erforderlich, da der iSCALE-Nachrichtenbus die Standorttransparenz unterstützt.
- Kommunikation mit Remote-Objekten: Details der Kommunikation zwischen Remote-Objekten werden vom iSCALE-Nachrichtenbus verarbeitet.
- Objekt-Streaming und -Chunking: Wenn große Datenmengen zwischen Client und Server ausgetauscht werden müssen, werden diese Objekte für das Laden von Daten nach Bedarf optimiert.
- Callbacks: Ein weiteres Abstraktionsmuster/eine weitere Abstraktionsschicht in Remoting-Service, die die PTP-Remote-Objektkommunikation ermöglicht.
- Serviceüberwachung und -statistiken: Hier werden Leistungs- und Auslastungsstatistiken hinsichtlich dieser Remote-Services bereitgestellt.

### Data Access Service

Data Access Service (DAS) ist ein Objektverwaltungsservice, der Benutzern die Definition von Objekten über Metadaten ermöglicht. DAS verwaltet das Objekt sowie den Zugriff auf Objekte und automatisiert Übertragungs- und Permanenzaspekte. DAS dient zudem als Schnittstelle für den Zugriff auf Daten von einem beliebigen permanenten Datenspeicher aus, etwa Datenbanken, Verzeichnisservices oder -dateien. Zu den DAS-Vorgängen zählen einheitlicher Datenzugriff über JDBC (Java Database Connectivity) sowie optional Hochleistungs-Ereigniseinfügestrategien mithilfe nativer (systemeigener) Connectors (also OCI (Oracle Call Interfache) für Oracle 9i und ADO (Active Data Object) für Microsoft SQL Server).

### Abfrage-Manager-Service

Der Abfrage-Manager-Service sorgt für die Anzeige von Details sowie die Verarbeitung von Anfragen zum Ereignisverlauf von Sentinel Control Center. Dieser Service ist eine essenzielle Komponente für die Implementierung des Paging-Algorithmus, der in der Funktion zum Durchsuchen des Ereignisverlaufs zum Einsatz kommt. Er wandelt benutzerdefinierte Filter in gültige Kriterien um und fügt Sicherheitsdaten an, bevor Ereignisse abgerufen werden. Von diesem Service wird zudem sichergestellt, dass die Kriterien während einer Paging-Transaktion des Ereignisverlaufs unverändert bleiben.

### Korrelations-Service

Der Korrelationsalgorithmus von Sentinel 5 berechnet korrelierte Ereignisse durch Analyse des Datenstroms in Echtzeit. Er veröffentlicht die korrelierten Ereignisse basierend auf den benutzerdefinierten Regeln, bevor die Ereignisse bei der Datenbank eingehen. Regeln in der Correlation Engine-Instanz können ein Muster in einem einzelnen Ereignis in einem Fenster erkennen, in dem Regeln fortlaufend angezeigt werden. Wird eine Übereinstimmung erkannt, erstellt die Correlation Engine-Instanz ein korreliertes Ereignis, das das erkannte Muster beschreibt. Zudem wird u. U. ein Vorfall erstellt bzw. ein Sanierungs-Workflow über iTRAC ausgelöst. Die Correlation Engine-Instanz arbeitet mit einer Komponente zur Regelüberprüfung zusammen, die die Korrelationsregelausdrücke berechnet und Syntax von Filtern validiert. Correlation Engine von Sentinel stellt nicht nur eine umfassende Gruppe von Korrelationsregeln bereit, sondern bietet auch spezifische Vorteile gegenüber Correlation Engines, deren Herzstück eine Datenbank darstellt.

- Da bei Correlation Engine die Verarbeitung speicherintern erfolgt und keine Einfüge- und Lesevorgänge der Datenbank vorgenommen werden, bietet Correlation Engine bei beständig hoher Auslastung sowie während ereignisbezogenen Spitzenzeiten in Angriffssituationen gute Leistung, also in den Fällen, in denen die Korrelationsleistung am wichtigsten ist.
- Das Korrelationsvolumen hat keinerlei Auswirkung auf die Geschwindigkeit anderer Systemkomponenten, die Benutzeroberfläche reagiert also insbesondere bei großem Ereignisvolumen.
- Verteilte Korrelation – Organisationen können mehrere Correlation Engine-Instanzen (jede auf einem eigenen Server) bereitstellen, ohne dass Konfigurationen repliziert oder Datenbanken hinzugefügt werden müssen. Die unabhängige Skalierung von Komponenten sorgt für kosteneffiziente Skalierbarkeit und Leistung.
- Die Correlation Engine-Instanz kann Vorfällen Ereignisse hinzufügen, nachdem ein Vorfall ermittelt wurde.

Benutzern wird die Verwendung einer Metrik namens Event Rules per Second (ERPS) nahe gelegt. Mit ERPS kann die Anzahl der Ereignisse gemessen werden, die pro Sekunde von einer Korrelationsregel überprüft werden können. Dieser Wert ist ein guter Leistungsindikator, da hiermit die Auswirkung auf die Leistung eingeschätzt wird, wenn es zur Überschneidung zweier Faktoren kommt: Ereignisse pro Sekunden und Anzahl der verwendeten Regeln.

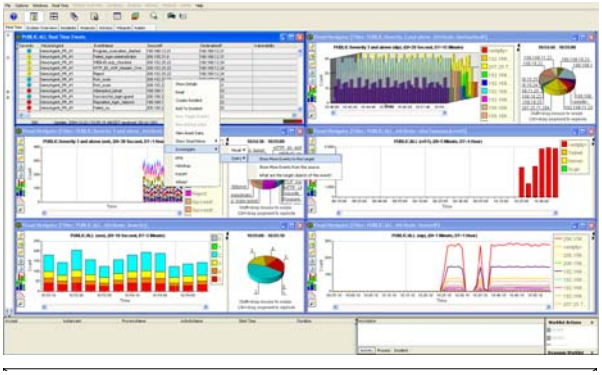
### Workflow-Service (iTRAC)

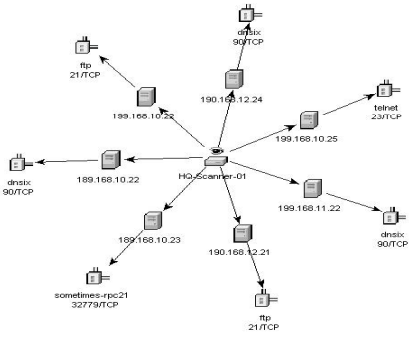
Der Workflow-Service empfängt bei der Vorfallserstellung Auslöser und initiiert basierend auf vordefinierten Workflow-Schablonen Workflow-Vorgänge. Er verwaltet den Lebenszyklus dieser Vorgänge, indem er Arbeitselemente erstellt oder Aktivitäten ausführt. Dieser Service verwaltet zudem einen Verlauf abgeschlossener Vorgänge, der zur Revision von Vorfallsreaktionen herangezogen werden kann.

### Ereignisanzeige

Active Views™, die interaktive grafische Benutzeroberfläche zur Ereignisanzeige, bietet eine integrierte Konsole zur Sicherheitsverwaltung mit einer umfassenden Gruppe von Werkzeugen für die Echtzeitanzeige und die Analyse, mit der Bedrohungen erkannt und analysiert werden können. Benutzer können Ereignisse in Echtzeit überwachen und umgehend Details zu Ereignissen anzeigen, seit denen Sekunden oder Stunden vergangen sind. Zahlreiche Anzeigediagramme und Werkzeuge ermöglichen die Überwachung von Informationen in Form eines 3D-Balkendiagramms, eines gestapelten 2D-Diagramms, eines Liniendiagramms, eines Banddiagramms und andere Formate. Zusätzliche wertvolle Informationen können über die Active Views-Konsole angezeigt werden, beispielsweise Benachrichtigungen zu Ausnutzungsversuchen von Beständen (Exploit-Erkennung). Zudem können Bestandsinformationen sowie grafische Verknüpfungen zwischen entsprechenden Quell-IPs und Ziel-IPs angezeigt werden.

Da in Active Views die iSCALE-Architektur zum Einsatz kommt, können Analytiker zur weiteren Analyse schnell Details anzeigen, da Active Views den direkten Zugriff auf die im Echtzeitspeicher befindlichen Ereignisdaten ermöglicht; dieser Speicher kann problemlos Tausende Ereignisse pro Sekunde verarbeiten, ohne dass es zu Leistungseinbußen kommt. Die Daten verbleiben im Speicher und werden nach Bedarf in die Datenbank geschrieben (bei normaler Ereignisauslastung kann Active Views Daten von bis zu 8 Stunden im Speicher speichern). Diese ununterbrochene leistungsorientierte Echtzeitansicht ist wichtig, wenn das System angegriffen wird bzw. eine gleichmäßige Auslastung vorliegt.

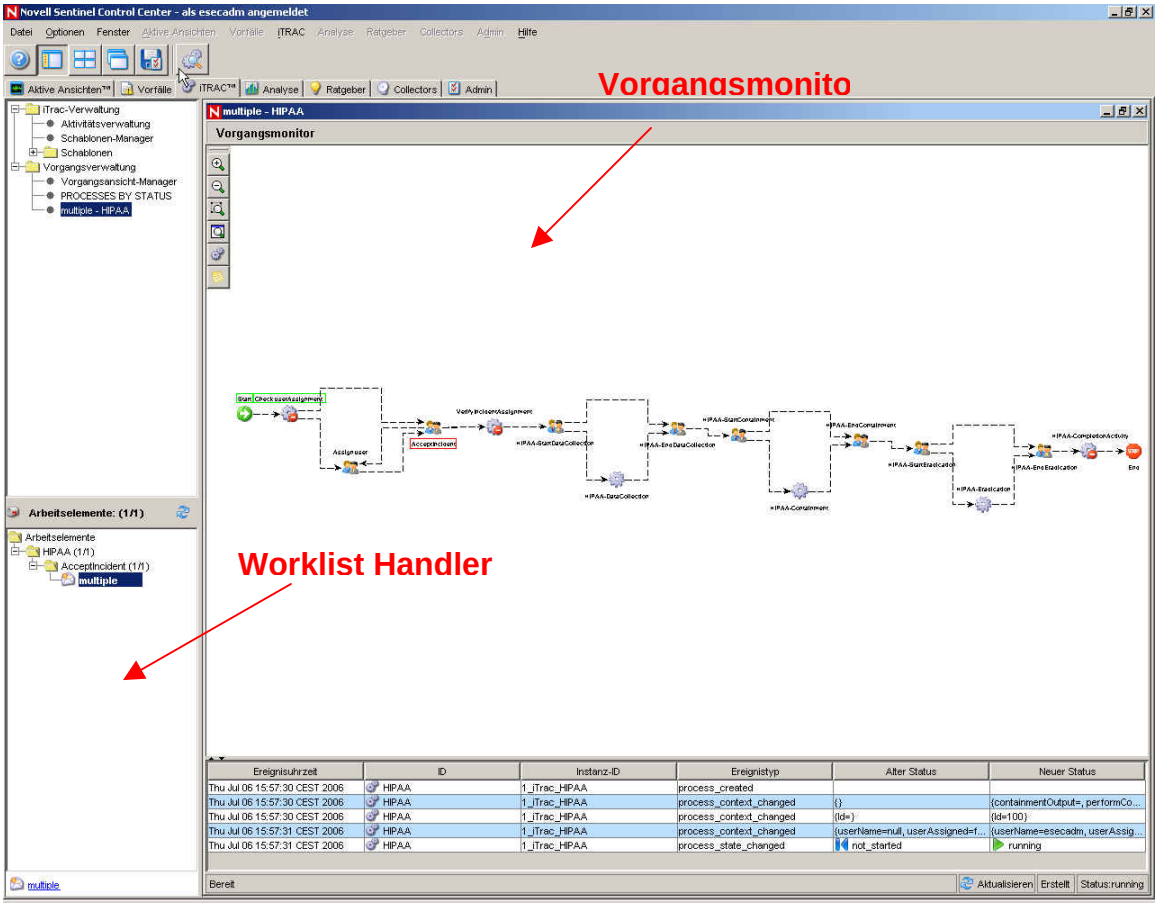




## Vorfallsreaktion über iTRAC

Durch iTRAC findet der Wandel der herkömmlichen Sicherheitsinformationsverwaltung vom passiven „Alarmieren und Anzeigen“ hin zu „prozessfähiger Vorfallsreaktion“ statt, da Organisationen Vorfallslösungsvorgänge definieren und dokumentieren und dann Lösungsvorgänge steuern, umsetzen und verfolgen können, wenn ein Vorfall oder ein Verstoß erkannt wird.

Im Lieferumfang von Sentinel 5 sind sofort einsatzbereite Vorgangsschablonen enthalten, die auf den Vorfallshandhabungsrichtlinien des SANS Institute basieren. Benutzer können mit diesen vordefinierten Vorgängen beginnen und spezifische Aktivitäten konfigurieren, die die optimalen Verfahren der Organisation widerspiegeln. iTRAC-Vorgänge können von der Vorfallserstellung bzw. von den Korrelationsregeln aus automatisch ausgelöst bzw. von einem autorisierten Sicherheits- oder Revisionsexperten manuell gestartet werden. In iTRAC wird eine Revisionsliste sämtlicher Aktionen zur Unterstützung der Konformitätsberichterstellung und der Verlaufsanalyse verwaltet.




In einer Arbeitsliste findet der Benutzer alle Aufgaben, die dem Benutzer zugewiesen wurden, und über eine Vorgangsüberwachung kann der Vorgangsstatus während eines Lösungsvorgangslebenszyklus in Echtzeit angezeigt werden.

Über das iTRAC-Aktivitäts-Framework können Benutzer automatisierte oder manuelle Aufgaben für spezifische Vorfallslösungsvorgänge individuell anpassen. Die iTRAC-Vorgangsschablonen können über das Aktivitäts-Framework so konfiguriert werden, dass sie mit der Schablone für das optimale Verfahren der Organisation übereinstimmen. Die Ausführung von Aktivitäten erfolgt direkt über Sentinel Control Center.

Beim iTRAC-Automatisierungs-Framework kommen zwei Schlüsselkomponenten zum Einsatz – der Aktivitäts-Container und der Workflow-Container. Mit dem ersten wird die Aktivitätsausführung für die angegebene Gruppe von Schritten basierend auf Eingaberegeln automatisiert, mit dem zweiten wird die Workflow-Ausführung baiserend auf Aktitvitäten über eine Arbeitsliste automatisiert. Die Eingaberegeln basieren auf dem XPDL-(XML Processing Description Language-)Standard und stellen ein formales Modell für den Ausdruck von ausführbaren Vorgängen in einem Unternehmen bereit. Mit diesem auf Standards basierenden Ansatz der Implementierung unternehmensspezifischer Regeln und Regelsätze wird gewährleistet, dass Vorgangsdefinitionen für Kunden auch zukünftig verwendet werden können.

### Berichterstellungs-Service

Der Berichterstellungs-Service ermöglicht die Berichterstellung; dies schließt Verlaufsberichte und Berichte zu Anfälligkeiten ein. Im Lieferumfang von Sentinel 5 sind sofort einsatzbereite Berichte enthalten, die Benutzern die Konfiguration eigener Berichte mit Crystal Reports ermöglichen. Hier einige Beispiele der in Sentinel 5 enthaltenen Berichte:

- Trendanalyse
- Sicherheitsstatus von Sparten oder kritischen Beständen
- Angriffstypen
- Ziel-Bestände
- Reaktionszeiten und Lösung
- Verstöße gegen Richtlinienkonformität

### Advisor

Sentinel Advisor, ein optionales Modul, das Querverweise zwischen Echtzeit-Alarmdaten von Sentinel und Informationen über bekannte Anfälligkeiten und Sanierung bietet und so die Lücke zwischen Vorfallserkennung und der entsprechenden Reaktion schließt. Mit Advisor können Organisationen ermitteln, ob bestimmte Anfälligkeiten von Ereignissen ausgenutzt werden und wie sich diese Angriff auf die Bestände der Organisation auswirken. Advisor enthält zudem detaillierte Informationen zu den Anfälligkeiten, deren Ausnutzung Ziel der Angriffe ist, zu den potenziellen Auswirkungen von erfolgreichen Angriffen und die erforderlichen Schritte zur Sanierung. Die empfohlenen Schritte zur Sanierung werden über iTRAC-Vorfallsreaktionsvorgänge umgesetzt und verfolgt.

### Zustand

Über den Zustands-Service können sich Benutzer einen umfassenden Überblick über die verteilte Sentinel 5-Plattform verschaffen. Er aggregiert Zustandsinformationen von unterschiedlichen Vorgängen, die überlicherweise auf mehrere Server verteilt sind. Die Zustandsinformationen werden in Sentinel Control Center in regelmäßigen Abständen für den Endbenutzer angezeigt.

### Verwaltung

Mit der Funktion für die Verwaltung werden die Funktionen zur Benutzerverwaltung sowie zur Einrichtung von Einstellungen bereitgestellt, die Anwendungsadministratoren von Sentinel 5 im Regelfall benötigen.

### Allgemeine Services

Sämtliche der oben beschriebenen Komponenten dieser Geschäftslogikschicht der Architektur werden von einer Gruppe allgemeiner Services gesteuert. Diese Dienstprogrammservices unterstützen bei der präzisen Filterung (über die Filter-Engine) von Ereignissen für Benutzer, bei der laufenden Überwachung von Systemzustandsstatistiken (über den Zustandsmonitor) sowie bei der dynamische Aktualisierung von Daten im gesamten System (über den Zuordnungsservice). Gemeinsam bilden diese Services die Grundlage der lose zusammenhängenden Services, die über das auf dem Nachrichtenbus basierende Transportverfahren die unübertroffene Verarbeitung und Skalierung für Echtzeitanalysen und -berechnungen ermöglichen.

# Darstellungsschicht

Über die Darstellungsschicht wird die Anwendungsoberfläche für den Endbenutzer bereitgestellt. Sentinel Command Center ist eine umfassende Konsole, über die Informationen für den Benutzer angezeigt werden.

# Produktmodule

## Sentinel Control Center

Sentinel Control Center bietet eine integrierte leistungsstarke Konsole zur Sicherheitsverwaltung. Dank der intuitiven Gestaltung können Analytiker schnell neue Trends oder Angriffe erkennen, grafische Informationen in Echtzeit bearbeiten und damit interagieren sowie auf Vorfälle reagieren. Zu den Schlüsselfunktionen zählen:

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

## Sentinel Wizard

Sentinel Wizard sammelt Daten 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. In jeder Konfiguration können ein oder mehrere Instanzen von Wizard bereitgestellt werden, sodass die Kunden die Möglichkeit erhalten, Produktkomponenten auf der Grundlage ihrer Netzwerktopologie in ihrer Infrastruktur bereitzustellen.

## Sentinel Advisor

Sentinel Advisor, ein optionales Modul, erstellt Querverweise zwischen Echtzeit-Alarmdaten von Sentinel und Informationen über bekannte Anfälligkeiten und Sanierungsmaßnahmen.

# Inhalt

Diese Handbuch enthält Folgendes:

- Kapitel 1 – Einführung in Sentinel
- Kapitel 2 – Navigation im Sentinel Control Center
- Kapitel 3 – Registerkarte „Active Views™“
- Kapitel 4 – Registerkarte „Vorfälle“
- Kapitel 5 – Registerkarte „iTRAC™“
- Kapitel 6 – Registerkarte „Analyse“
- Kapitel 7 – Registerkarte „Advisor“
- Kapitel 8 – Registerkarte „Collectors“
- Kapitel 9 – Registerkarte „Admin“
- Kapitel 10 – Sentinel Data Manager
- Kapitel 11 – Dienstprogramme
- Kapitel 12 – Schnellstart
- Anhang A – Systemereignisse

# Verwendete Konventionen

## Hinweise und Warnhinweise

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

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

## Befehle

Befehle sind in Courier-Schriftart angegeben. Beispiel:

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

# Weitere Novell-Referenzen

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

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

# Kontaktaufnahme mit Novell

- Website: http://www.novell.com
- Technischer Support von Novell: http://www.novell.com/support/index.html
- Internationaler technischer Support von Novell: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self-Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Für Support rund um die Uhr: +1800-858-4000

# 2 Navigation im Sentinel Control Center

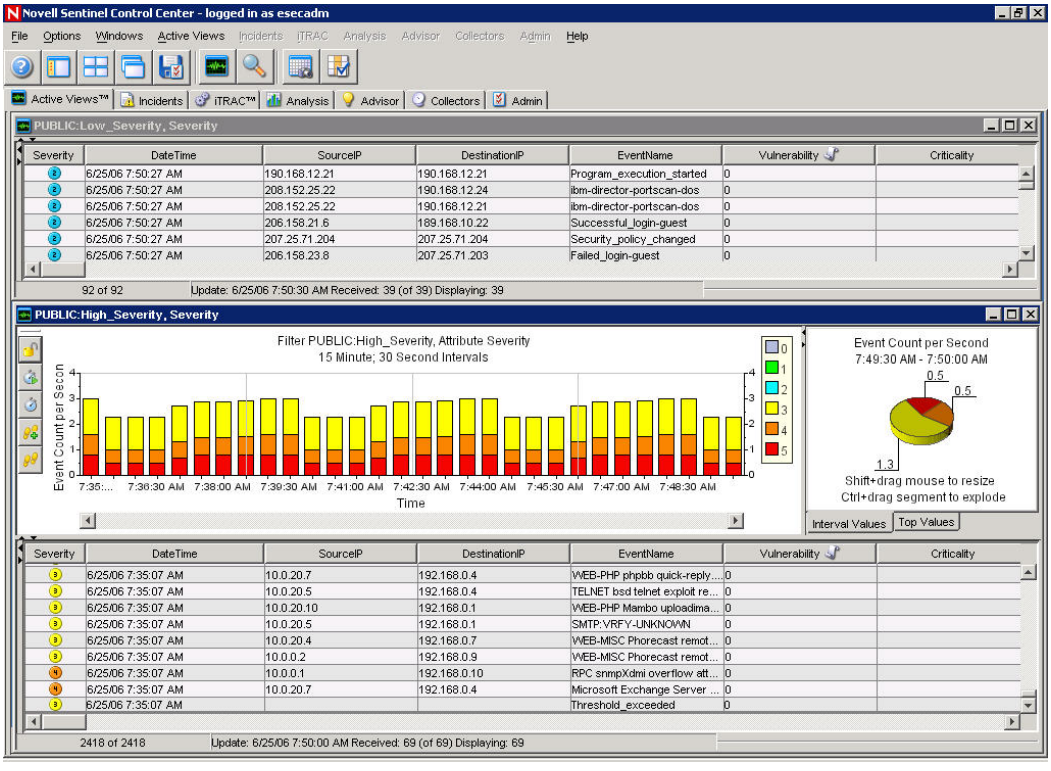
**HINWEIS**: Die Begriffe „Agent“ und „Collector“ sind austauschbar. Im Folgenden werden Agenten als „Collectors“ bezeichnet.

Das Sentinel Control Center setzt sich aus den folgenden Elementen zusammen:

- Menüleiste
- Symbolleiste
- Registerkarten

Zudem werden in diesem Kapitel die folgenden Themen erläutert:

- Starten des Sentinel Control Center
- Ändern des Erscheinungsbilds des Sentinel Control Center
- Speichern von Benutzereinstellungen
- Ändern des Sentinel-Passworts



# Starten des Sentinel Control Center

## Starten des Sentinel Control Center unter Windows

Starten des Sentinel Control Center unter Windows

1. Klicken Sie auf *Start* > *Novell* > *Sentinel Control Center* oder klicken Sie auf dem Desktop auf das *Sentinel Control Center*-Symbol.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf *OK*.

## Starten des Sentinel Control Center unter UNIX

Starten des Sentinel Control Center unter UNIX

1. Wechseln Sie als Benutzer „esecadm“ in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/console
   ```

2. Führen Sie den folgenden Befehl aus:

   ```
   ./run.sh
   ```

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

# Menüleiste

Unterhalb der Titelleiste befinden sich zehn Menüs. Am oberen Rand des Fensters sind von links nach rechts die folgenden Menüs angeordnet: „Datei“, „Optionen“, „Fenster“, „Active Views“, „Vorfälle“, „iTRAC“, „Advisor“, „Collectors“, „Admin“ und „Hilfe“.

Die Menüs „Datei“, „Optionen“, „Fenster“ und „Hilfe“ sind immer verfügbar. Weitere Optionen sind in Abhängigkeit davon verfügbar, welche Registerkarte aktiv ist und welche Berechtigungen Ihnen gewährt wurden.

## Menü „Datei“

- Einstellungen speichern
- Beenden

## Menü „Optionen“

- Passwort ändern
- Position der Registerkarte
  - Oben
  - Unten
- Navigationsfenster andocken
- Navigationsfenster anzeigen

## Menü „Fenster“

- Alle überlappend
- Alle nebeneinander
  - Optimal anpassen
  - Untereinander
  - Nebeneinander
- Alle minimieren
- Alle wieder einblenden
- Alle schließen

## Active Views™

- Eigenschaften
- Aktive Ansicht erstellen
- Ereignisabfrage
- Ereignisechtzeit
  - Snapshot
  - Spalten verwalten

## Vorfälle

- Vorfallsansichts-Manager anzeigen
- Vorfall erstellen
- Konfiguration des Anlage-Viewer

## iTRAC™

- Vorgangs-Manager anzeigen

## Analyse

- Bericht erstellen

## Advisor

- Bericht erstellen

## Collectors

- Collector-Ansichts-Manager anzeigen

## Admin

- Berichtkonfiguration
- Korrelationsregeln
- Correlation Engine-Manager
- Globale Filterkonfiguration
- Menükonfiguration
- Filterkonfiguration
- Benutzerkonfiguration

## Hilfe

- Hilfe
- Info zu Sentinel

# Symbolleiste

Fünf globale Symbolleistenschaltflächen werden immer angezeigt. Weitere Schaltflächen sind in Abhängigkeit davon verfügbar, welche Registerkarte bzw. welches Fenster aktiv ist und welche Benutzerberechtigungen gewährt wurden.

## Globale Symbolleiste

Die folgenden fünf globalen Symbolleistenschaltflächen sind verfügbar:

-  Sentinel-Hilfe anzeigen
-  Navigationsfenster anzeigen/ausblenden
-  Alle Display-Fenster nebeneinander
-  Alle Display-Fenster überlappend
-  Benutzereinstellungen speichern

## Registerkarte „Active Views™“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „ActiveViews™“ aktiv ist:

-  Aktive Ansichten
-  Ereignisabfrage starten

### Fenster „Ereignisanzahl pro Sekunde“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn das Fenster „Ereignisanzahl pro Sekunde“ aktiv ist:

-  Snapshot einer Tabelle für die Ereigniszählung pro Zeitraum
-  Spalten einer Tabelle für die Ereigniszählung pro Zeitraum verwalten

### Diagramm „Ereignisanzahl pro Sekunde“

Folgende Symbolleistenschaltflächen sind im Diagramm verfügbar, wenn das Diagramm „Ereignisanzahl pro Sekunde“ aktiv ist:

- Diagramm sperren/Diagrammsperre aufheben
- Anzeigeintervall vergrößern
- Anzeigeintervall verkleinern
- Anzeigedauer vergrößern
- Anzeigedauer verkleinern

Wenn Sie auf die Schaltfläche zum Sperren klicken, sind die folgenden Schaltflächen verfügbar:

- Diagramm sperren/Diagrammsperre aufheben
- Anzeigeintervall vergrößern
- Anzeigeintervall verkleinern
- Anzeigedauer vergrößern
- Anzeigedauer verkleinern
- Vergrößern
- Verkleinern
- Ereignisse anzeigen
- Als HTML-Datei speichern

### Fenster „Snapshot“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn das Fenster „Snapshot“ aktiv ist:

-  Spalten verwalten

## Registerkarte „Vorfälle“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „Vorfälle“ aktiv ist:

-  Vorfallsansichts-Manager anzeigen
-  Neuen Vorfall erstellen
-  Viewer für Anlagen konfigurieren

### Vorfall

Folgende Symbolleistenschaltflächen sind verfügbar, wenn ein Vorfall geöffnet ist:

-  Spalten mit zugeordneten Ereignissen verwalten

## iTRAC

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „iTRAC“ aktiv ist:

-  Vorgangsansicht-Manager anzeigen

## Registerkarte „Analyse“ und Registerkarte „Advisor“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „Analyse“ bzw. „Advisor“ aktiv ist:

-  Bericht erstellen

## Registerkarte „Collectors“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „Collectors“ aktiv ist:

-  Ansichts-Manager für Collector Manager anzeigen
-  Collector-Ansichts-Manager anzeigen

## Registerkarte „Admin“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn die Registerkarte „Admin“ aktiv ist:

-  Berichtkonfiguration anzeigen
-  Korrelationsregeln anzeigen
-  Correlation Engine-Manager anzeigen
-  Globale Filterkonfiguration anzeigen
-  Menükonfiguration anzeigen
-  Filter-Manager anzeigen
-  Benutzer-Manager anzeigen
-  Serveransichts-Manager anzeigen

### Fenster „Filter-Manager“

Folgende Symbolleistenschaltflächen sind verfügbar, wenn das Fenster „Filter-Manager“ aktiv ist:

-  Neuen Filter erstellen
-  Ausgewählten Filter löschen (Schaltfläche ist aktiv, wenn ein Filter ausgewählt ist)

### Fenster „Menükonfiguration“

Die folgenden Symbolleistenschaltflächen sind verfügbar, wenn das Fenster „Menükonfiguration“ aktiv und im Bearbeitungsmodus ist:

-  Neues Menüelement erstellen
-  Menüelement löschen
-  Menüelement aktivieren
-  Menüelement deaktivieren

# Registerkarten

In Abhängigkeit von Ihren Benutzerberechtigungen werden im Sentinel Control Center die folgenden Registerkarten angezeigt. Sie müssen über die entsprechenden Berechtigungen verfügen, um die einzelnen Registerkarten anzeigen zu können.

- Active Views™
- Vorfälle
- iTRAC™
- Analyse
- Advisor
- Collectors
- Admin

Weitere Informationen zu Registerkarten finden Sie in den jeweiligen Kapiteln zu den einzelnen Registerkarten.

# Ändern des Erscheinungsbilds des Sentinel Control Center

Sie können das Erscheinungsbild des Sentinel Control Center wie folgt ändern:

- Festlegen der Registerkartenposition
- Einblenden oder Ausblenden des Navigationsfensters
- Andocken oder Aufheben der Verankerung des Navigationsfensters
- Anordnen von Fenstern
- Anordnen von Fenstern nebeneinander
- Minimieren und Wiederherstellen aller Fenster
- Schließen aller geöffneten Fenster

## Festlegen der Registerkartenposition

So legen Sie die Registerkartenposition fest

1. Klicken Sie auf *Optionen* > *Position der Registerkarte*.
2. Wählen Sie entweder „Oben“ oder „Unten“ aus.

## Einblenden oder Ausblenden des Navigationsfensters

So blenden Sie das Navigationsfenster ein bzw. aus

1. Klicken Sie auf *Optionen* > aktivieren bzw. deaktivieren Sie *Navigationsfenster anzeigen*.

## Andocken oder Aufheben der Verankerung des Navigationsfensters

So docken Sie das Navigationsfenster an bzw. so heben Sie dessen Verankerung auf

1. Klicken Sie auf *Optionen* > aktivieren bzw. deaktivieren Sie *Navigationsfenster andocken*.

## Überlappendes Anordnen von Fenstern

So ordnen Sie Fenster überlappend an

1. Klicken Sie auf *Fenster* > *Alle überlappend.* Alle geöffneten Fenster im rechten Bereich werden überlappend angeordnet.

## Anordnen von Fenstern nebeneinander

So ordnen Sie Fenster nebeneinander an

1. Klicken Sie auf *Fenster* > *Alle nebeneinander*.
2. Zeigen Sie auf eine der folgenden Optionen:
   - „Optimal anpassen“
   - „Nebeneinander“
   - „Untereinander“

## Minimieren und Wiederherstellen aller Fenster

So minimieren Sie alle Fenster

1. Klicken Sie auf *Fenster* > *Alle minimieren*. Alle geöffneten Fenster im rechten Bereich werden minimiert.

## So stellen Sie alle Fenster in der ursprünglichen Größe wieder her

So stellen Sie alle Fenster in der ursprünglichen Größe wieder her

1. Klicken Sie auf *Fenster* > *Alle wieder einblenden*. Alle geöffneten Fenster im rechten Bereich werden in ihrer ursprünglichen Größe wiederhergestellt.

## So stellen Sie ein einzelnes Fenster wieder her

So stellen Sie ein einzelnes Fenster wieder her

1. Klicken Sie auf das minimierte Fenster. Das Fenster wird in der ursprünglichen Größe wiederhergestellt.

### Gleichzeitiges Schließen aller geöffneten Fenster

So schließen Sie alle Fenster

1. Klicken Sie auf *Fenster* > *Alle schließen*.

## Speichern von Benutzereinstellungen

Sie müssen über die Benutzerberechtigung „Arbeitsbereich speichern“ verfügen.

Die folgenden Einstellungen können gespeichert werden:

- Dauerhaft verfügbare Fenster, die wiederhergestellt werden können, weil sie nicht von Daten abhängen, die zum Zeitpunkt ihrer Erstellung verfügbar waren. Zusammenfassungsanzeigen und Active Views können beispielsweise gespeichert werden. Temporäre Fenster hingegen können nicht gespeichert werden, beispielsweise Snapshots und Schnellabfragen. Alle im Admin-Navigationsfenster aufgelisteten Fenster werden gespeichert. Sekundäre Fenster, die durch Doppelklicken auf eine Auswahl in einem dieser Fenster geöffnet werden, werden jedoch nicht gespeichert.
- Fensterpositionen
- Fenstergrößen, einschließlich der Größe des Anwendungsfensters
- Registerkartenpositionen
- Angedocktes bzw. nicht verankertes und eingeblendetes bzw. ausgeblendetes Navigatorfenster

So speichern Sie Ihre Einstellungen

1. Klicken Sie auf *Datei* > *Einstellungen* speichern oder klicken Sie auf *Einstellungen speichern*.

# Ändern des Sentinel Control Center-Passworts

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

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

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

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

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

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

So ändern Sie Ihr Sentinel Control Center-Passwort

1. Klicken Sie auf *Optionen* > *Passwort ändern*.
2. Geben Sie das alte Passwort ein.
3. Geben Sie das neue Passwort ein und bestätigen Sie dieses, indem Sie es noch einmal eingeben.

   **HINWEIS**: Novell empfiehlt als optimales Verfahren eine Passwort-Mindestlänge von 8 Zeichen, wobei das Passwort alphanumerische Zeichen enthalten sollte.

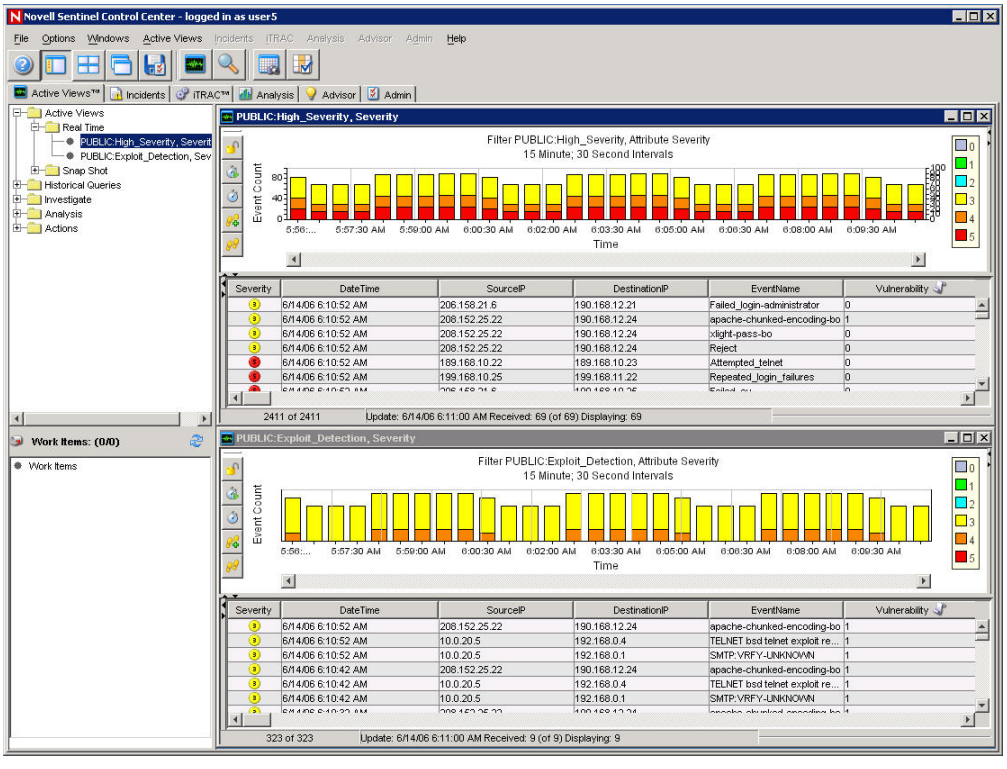
4. Klicken Sie auf *OK*.

# 3 Registerkarte „Active Views™“

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

Sie müssen über die entsprechende Berechtigung verfügen, um die Registerkarte „Active Views™“ verwenden zu können. Wenn Ihnen diese Berechtigung nicht erteilt wurde, verfügen Sie auch nicht über die Berechtigungen zur Durchführung von Aktionen mithilfe dieser Registerkarte.

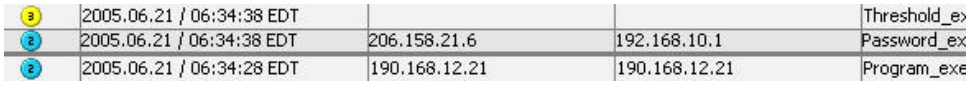
Auf der Registerkarte „Active Views“ können Sie Ereignisse fast in Echtzeit überwachen, wenn sie eintreten, und Abfragen an diese Ereignisse senden. Die Ereignisse können im Tabellenformat oder in Form eines 3D-Balkendiagramms, eines gestapelten 2D-Balkendiagramms, eines Liniendiagramms oder eines Banddiagramms überwacht werden.



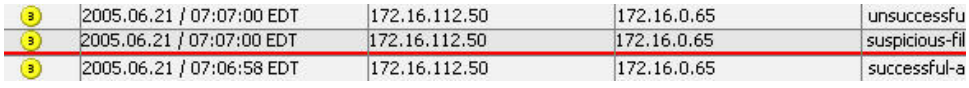
# Registerkarte „Active Views“ – Beschreibung

Ereignisansichten sind als Tabellen formatiert. Die Active View-Konfiguration wird durch die Datei das_rt.xml festgelegt. Eine Ereignistabelle fast in Echtzeit mit einer grafischen Darstellung und ein Snapshot sind die beiden verfügbaren Typen von aktiven Ansichten.

- Ereignistabelle fast in Echtzeit
  - Enthält bis zu 750 Ereignisse für einen Zeitraum von 30 Sekunden.
  - Der Client behält Ereignisse standardmäßig 24 Stunden lang im Cache. Diese Funktion kann über Eigenschaften der aktiven Ansicht konfiguriert werden.
  - In der Ereignistabelle werden standardmäßig maximal 30.000 Ereignisse angezeigt. Diese Funktion kann über Eigenschaften der aktiven Ansicht konfiguriert werden.
  - Die Ereignistabelle wird standardmäßig alle 30 Sekunden aktualisiert (Sendezeitverzögerung). Dies wird durch eine graue Linie in der Ereignistabelle dargestellt.




    Falls in einem Zeitraum von 30 Sekunden mehr als 750 Ereignisse auftreten, wird eine rote Trennlinie angezeigt, die darauf hinweist, dass mehr Ereignisse vorhanden sind als angezeigt werden.




  - Wenn Benutzereinstellungen gespeichert werden, werden 4 Tage lang weiterhin Daten gesammelt. Wenn Sie beispielsweise Ihre Einstellungen speichern, sich abmelden und sich dann am folgenden Tag wieder anmelden, zeigt Ihre aktive Ansicht alle Daten an, als ob Sie sich nie abgemeldet hätten.
  - Wenn eine aktive Ansicht erstellt, aber nicht gespeichert wird, fährt sie eine Stunde lang mit dem Sammeln von Daten fort. Wenn innerhalb dieses Zeitraums von einer Stunde eine identische aktive Ansicht erstellt wird, zeigt die aktive Ansicht Daten für die letzte Stunde an.
- Snapshot – Mit Zeitstempel versehene Ansichten einer Ereignisansichtstabelle in Echtzeit.

Die folgenden Punkte machen eine aktive Ansicht einzigartig.

- der Filter, der einer aktiven Ansicht zugewiesen ist
- das z-Achsenattribut
- der Sicherheitsfilter, der einem Benutzer zugewiesen wurde

Auf der Registerkarte „Active Views“ können Sie:

- Aktive Ansichten neu konfigurieren
- Einem Vorfall Ereignisse hinzufügen
- Einen Snapshot oder ein visuelles Navigatorfenster schließen
- Einen Vorfall erstellen
- Benutzerdefinierte Menüoptionen mit Ereignissen verwenden
- Einen Snapshot oder ein visuelles Navigatorfenster löschen
- Eine Ereignisabfrage durchführen
- Diagrammzuordnungen vornehmen
- Advisor-Daten anzeigen
- Spalten verwalten
- Nachrichten über Ereignisse per Email versenden
- Ereignisdetails ein- oder ausblenden
- Einen Snapshot eines visuellen Navigatorfensters erstellen
- Ereignisse anzeigen, die ein korreliertes Ereignis ausgelöst haben
- Eine Anfälligkeitsvisualisierung anzeigen
- Bestandsdaten anzeigen
- HP-OpenView-Operationen und Service Desk ausführen
- Remedy-Operationen ausführen

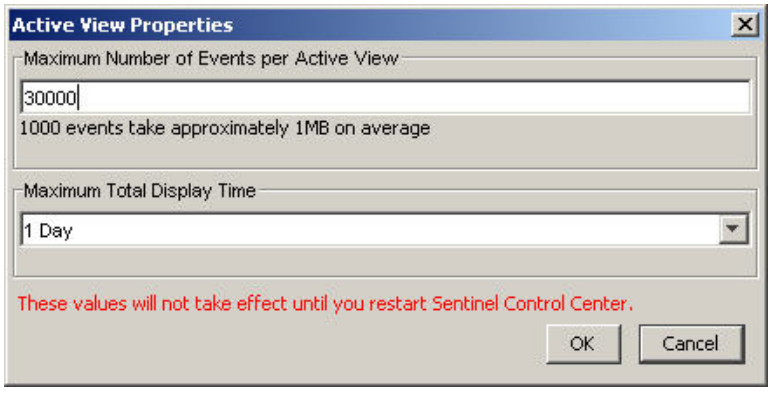
Als Benutzer können Sie Werte (Spaltennamen) ändern, um logische Namen anzuzeigen und diese im gesamten System zu verwenden. Sie können auf den Ereignisstrom Attribute anwenden, die für Ihr Unternehmen von Relevanz sind. Weitere Informationen finden Sie in *Kapitel 10 – Sentinel Data Manager*, im *Wizard-Benutzerhandbuch* und im *Sentinel-Referenzhandbuch für Benutzer*.

# Neukonfigurieren der maximalen Anzahl von Ereignissen und des Cache-Werts in aktiven Ansichten

„Eigenschaften der aktiven Ansicht“ ermöglicht Ihnen das Konfigurieren der maximalen Anzahl von Ereignissen, die in einer aktiven Ansicht angezeigt werden können, sowie der Zeit im Cache auf jedem Client. Die standardmäßige maximale Anzahl von Ereignissen in einer aktiven Ansicht ist 30.000. Der Standardwert für die Zeit im Cache in einer aktiven Ansicht ist 24 Stunden.

So konfigurieren Sie die maximale Anzahl von Ereignissen und die Caching-Dauer in aktiven Ansichten neu

1. Klicken Sie auf die Registerkarte *Active Views*.
2. Klicken Sie auf *Aktive Ansichten* > *Eigenschaften*.
3. Nehmen Sie die gewünschten Änderungen vor.




Die neuen Werte werden erst übernommen, wenn Sie das Sentinel Control Center neu starten.

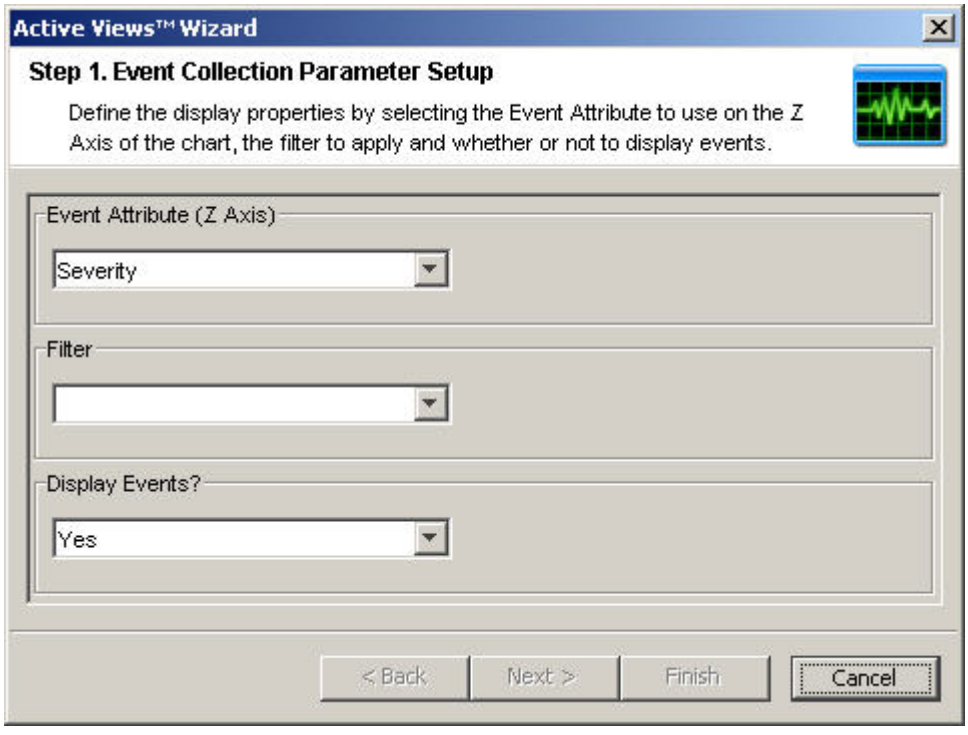
# So zeigen Sie Echtzeitereignisse an

So zeigen Sie Echtzeitereignisse an

1. Klicken Sie auf die Registerkarte *Active Views*.
2. Klicken Sie auf *Aktive Ansichten* > *Aktive Ansicht erstellen* oder klicken Sie auf *Aktive Ansicht erstellen*.

3. Klicken Sie im Fenster „Assistent für Active Views“ auf die Abwärtspfeile, um eine Z-Achse und einen Filter auszuwählen und um anzugeben, ob Ereignisse angezeigt werden sollen („Ja“ oder „Nein“).

**HINWEIS**: Im Fenster für die Filterauswahl können Sie einen eigenen Filter erstellen oder einen bereits erstellten Filter auswählen. Durch Auswahl des Filters *Alle* werden alle Ereignisse im Fenster angezeigt. Wenn bei der Erstellung einer aktiven Ansicht der Filter, der der aktiven Ansicht zugewiesen ist, nach dem Erstellen der aktiven Ansicht geändert oder gelöscht wird, wird die aktive Ansicht davon nicht beeinflusst.




Nachdem Sie Ihre Auswahl vorgenommen haben, können Sie auf *Weiter* oder *Fertig stellen* klicken. Wenn Sie *Fertig stellen* wählen, werden die folgenden Standardwerte ausgewählt:

- eine Anzeige- und Aktualisierungsrate von 30 Sekunden
- eine Anzeigedauer von 15 Minuten
- die Y-Achse als Ereignisanzahl
- der Diagrammtyp „Gestapeltes 2D-Balkendiagramm“

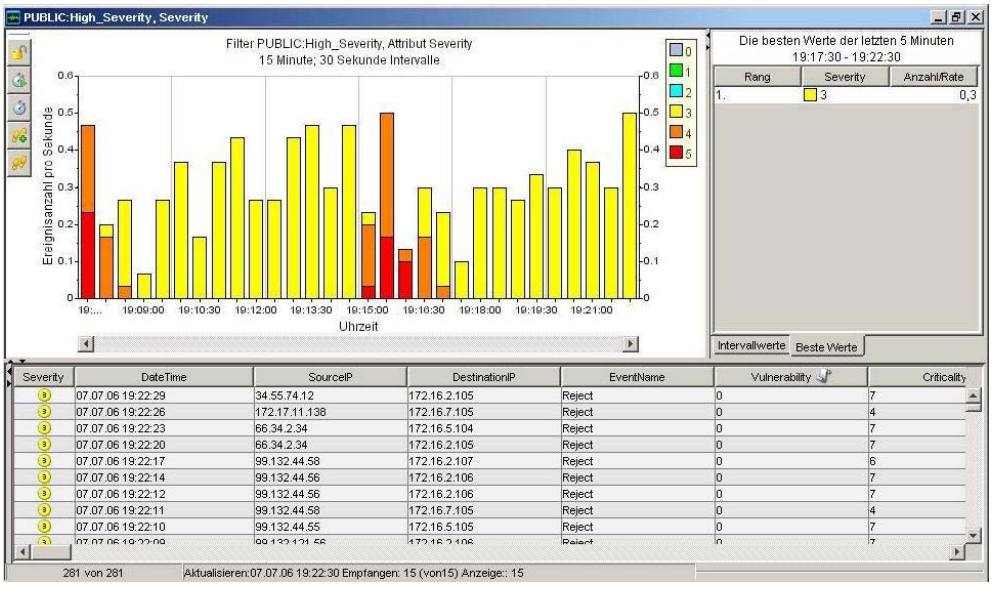
4. Wenn Sie auf *Weiter* klicken, können Sie mithilfe der Abwärtspfeile Folgendes auswählen:
   - Anzeige- und Aktualisierungsrate – die Anzahl von Sekunden, nach der die Ereignisse aktualisiert werden
   - Anzeigedauer – die Dauer, während der das Diagramm angezeigt wird
   - Y-Achse – entweder „Ereignisanzahl“ oder „Ereignisanzahl pro Sekunde“

   Klicken Sie auf *Next* (Weiter).
5. Wählen Sie den Diagrammtyp aus. Klicken Sie auf *Next* (Weiter).
   - Diagrammtyp – 3D-Balkendiagramm, Gestapeltes 2D-Balkendiagramm, Liniendiagramm oder Banddiagramm
6. Zusätzlich zur Auswahl eines Filters können Sie Ihre Ereignistabelle überarbeiten. Folgende Filterbedingungen stehen zur Auswahl:
   - Keine
   - ist genau
   - ist nicht
   - ist < (ist kleiner als)
   - ist <= (ist kleiner oder gleich)
   - ist > (ist größer als)
   - ist >= (ist größer oder gleich)
   - enthält
   - enthält nicht
   - ist leer
   - ist nicht leer

   Klicken Sie nach dem Erstellen der Kriterien auf *Zu Liste hinzufügen*. Klicken Sie auf *Finish*.

**HINWEIS**: Nachdem Sie Ihre Ansicht erstellt haben, können Sie diese Überarbeitung der Ereignistabelle ändern oder entfernen, indem Sie mit der rechten Maustaste auf den Diagrammbereich klicken und Eigenschaften auswählen. Weitere Informationen finden Sie unter So setzen Sie die Parameter, den Diagrammtyp oder die Ereignistabelle einer aktiven Ansicht zurück.

Ihr Diagramm wird ungefähr so aussehen:




**HINWEIS**: Eigenschaften der aktiven Ansicht – „Ereignistabelle überarbeiten“ hat keine Auswirkungen auf die grafische Darstellung.

Die fünf Schaltflächen auf der linken Seite des Diagramms führen die folgenden Funktionen aus:

- Diagramm sperren/Diagrammsperre aufheben – Wird beim Durchführen eines Drilldown, beim Vergrößern und Verkleinern des Diagramms, beim Vergrößern einer Auswahl und beim Speichern eines Diagramms als HTML-Datei verwendet.

- Anzeigeintervall vergrößern – Vergrößert das Anzeigeintervall für eingehende Ereignisse.

- Anzeigeintervall verkleinern – Verkleinert das Anzeigeintervall für eingehende Ereignisse.

- Anzeigedauer vergrößern – Vergrößert das Zeitintervall entlang der x-Achse.

- Anzeigedauer verkleinern – Verkleinert das Zeitintervall entlang der x-Achse.

Wenn Sie auf die Schaltfläche *Sperre* klicken, sind zusätzlich die folgenden Schaltflächen verfügbar:

- Diagramm sperren/Diagrammsperre aufheben – Wird beim Durchführen eines Drilldown, beim Vergrößern und Verkleinern des Diagramms, beim Vergrößern einer Auswahl und beim Speichern eines Diagramms als HTML-Datei verwendet.

- Vergrößern – Vergrößert das Diagramm, ohne die Zeiteinstellungen des Diagramms zu verändern.

- Verkleinern – Verkleinert das Diagramm, ohne die Zeiteinstellungen des Diagramms zu verändern.

- Auswahl vergrößern – Vergrößert eine Auswahl von Zeitintervallen mit Ereignissen.

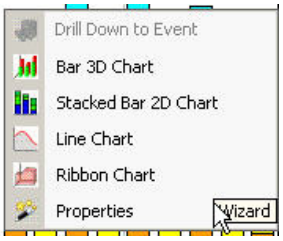
- Speichert die Navigatordetails als HTML-Datei mit dem Diagramm als Bild und den Ereignissen im Tabellenformat.

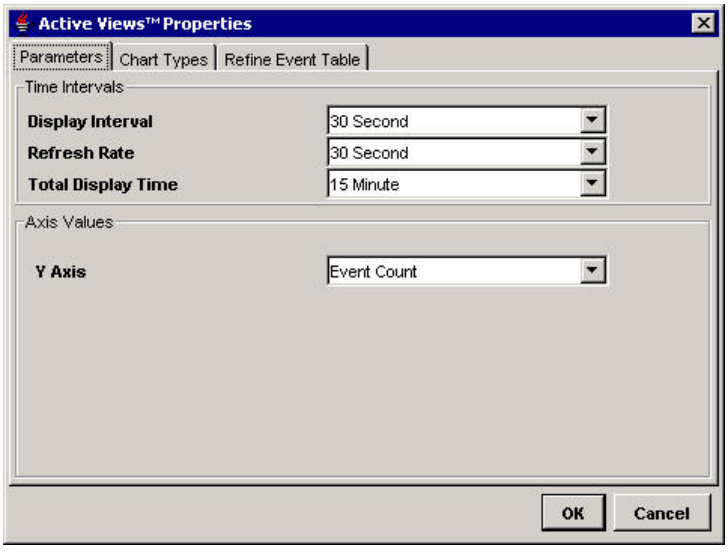
## So setzen Sie die Parameter, den Diagrammtyp oder die Ereignistabelle einer aktiven Ansicht zurück

Beim Anzeigen einer aktiven Ansicht können Sie die Diagrammparameter zurücksetzen und den Diagrammtyp ändern. Wenn interessante Ereignisse vorhanden sind, können Sie zudem andere Ereignisse herausfiltern, anstatt eine neue aktive Ansicht und einen neuen Filter zu erstellen.

So setzen Sie die Parameter, den Diagrammtyp oder die Ereignistabelle einer aktiven Ansicht zurück

1. Klicken Sie mit der rechten Maustaste auf eine aktive Ansicht, in der ein Diagramm angezeigt wird, und wählen Sie *Eigenschaften*.



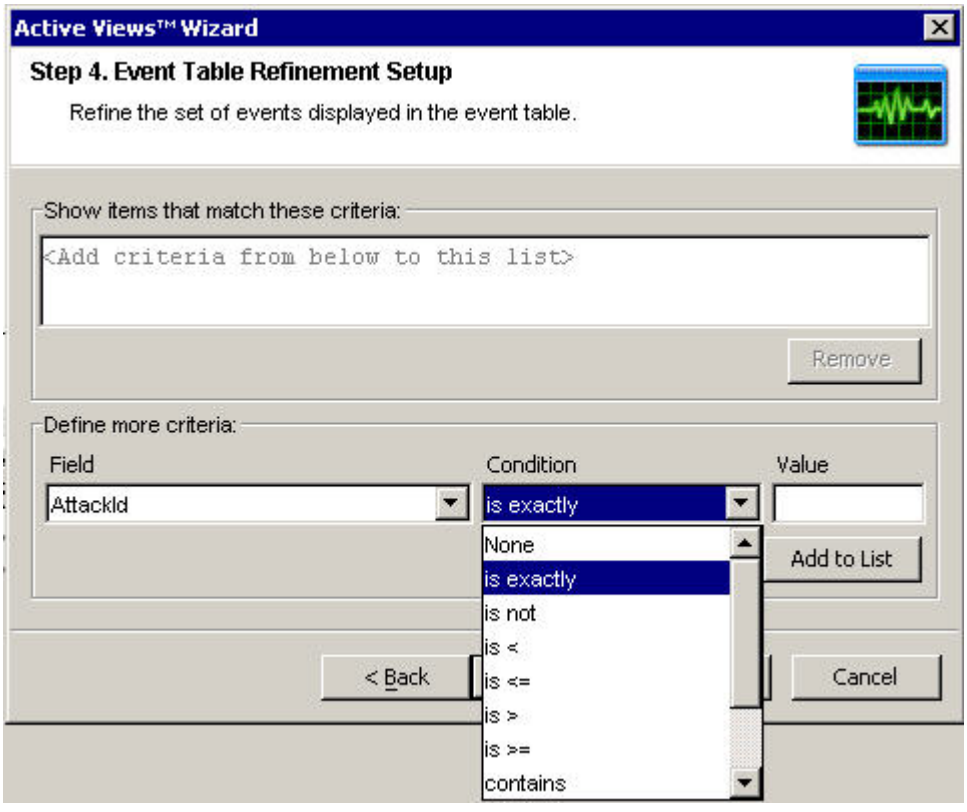




Auf der Registerkarte „Parameter“ können Sie Folgendes festlegen:

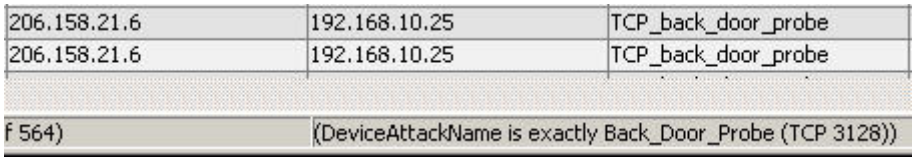
- Anzeigeintervall – die Zeit zwischen den einzelnen Intervallen
- Aktualisierungsrate – die Anzahl von Sekunden, nach der die Ereignisrate aktualisiert wird
- Gesamtanzeigedauer – die Dauer, während der das Diagramm angezeigt wird
- Y-Achse – entweder „Ereignisanzahl“ oder „Ereignisanzahl pro Sekunde“

Auf der Registerkarte „Diagrammtypen“ können Sie den Typ Ihres Diagramms auf „3D-Balkendiagramm“, „Gestapeltes 2D-Balkendiagramm“, „Liniendiagramm“ oder „Banddiagramm“ einstellen.


Auf der Registerkarte „Ereignistabelle überarbeiten“ können Sie einen Filter für das Ereignisfeld in Ihrer aktiven Ansicht festlegen.




So können Sie beispielsweise alle Ereignisse mit einem bestimmten Eintrag in einem Feld filtern, wie z. B. DeviceAttackName ist genau Back_Door_Probe (TCP 3128). Dieser Filter ergibt eine Ereignistabelle mit Ereignissen, bei denen der DeviceAttackName ausschließlich Back_Door_Probe (TCP 3128) lautet.




Beim Überarbeiten einer Ereignistabelle werden die Filterkriterien rechts unten in der Ereignistabelle angezeigt.

## Rotieren eines 3D-Balkendiagramms oder eines Banddiagramms

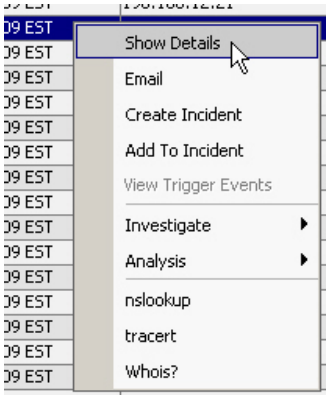
So rotieren Sie ein 3D-Balkendiagramm oder ein Banddiagramm

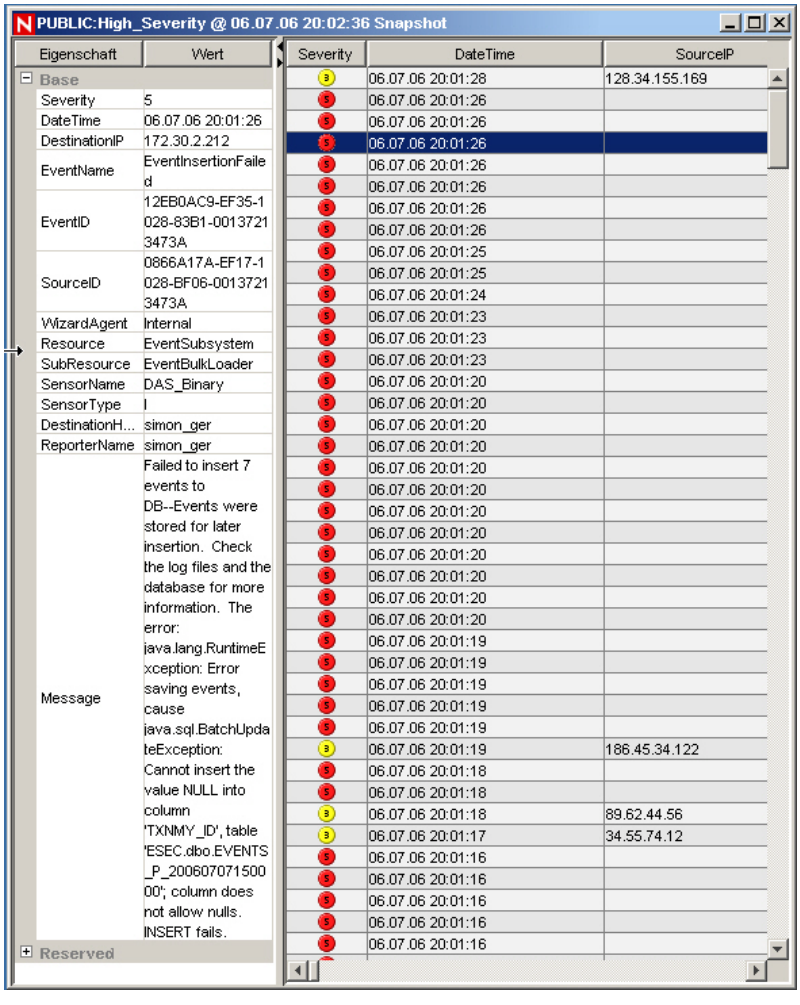
1. Klicken Sie auf das Diagramm und halten Sie die Maustaste gedrückt.
2. Positionieren Sie das Diagramm nach Ihren Wünschen, indem Sie die Maus bewegen, während Sie die Maustaste gedrückt halten.

# Ein- und Ausblenden von Ereignisdetails

So blenden Sie Ereignisdetails ein

1. Doppelklicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot auf ein Ereignis (oder klicken Sie mit der rechten Maustaste darauf) und klicken Sie dann auf *Details anzeigen*. Im linken Feld der Ereignistabelle in Echtzeit werden Ereignisdetails angezeigt.



2. Falls Details angezeigt werden sollen, wenn Sie das Sentinel Control Center das nächste Mal öffnen, klicken Sie auf *Datei* > *Einstellungen speichern* oder klicken Sie auf *Benutzereinstellungen speichern.*

So blenden Sie Ereignisdetails aus

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot, in der im linken Feld Ereignisdetails angezeigt werden, mit der rechten Maustaste auf ein Ereignis und klicken Sie dann auf *Details anzeigen*. Das Ereignisdetailfenster wird geschlossen.
2. Falls keine Details angezeigt werden sollen, wenn Sie das Sentinel Control Center das nächste Mal öffnen, klicken Sie auf *Datei* > *Einstellungen speichern* oder klicken Sie auf *Benutzereinstellungen speichern*.

# Senden von Nachrichten über Ereignisse und Vorfälle per Email

Die Funktion zum Senden von Emails wird während der Installation in der Datei execution.properties eingerichtet. Diese Datei kann nach der Installation bearbeitet werden. Sie befindet sich im folgenden Verzeichnis:

Für Windows:

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

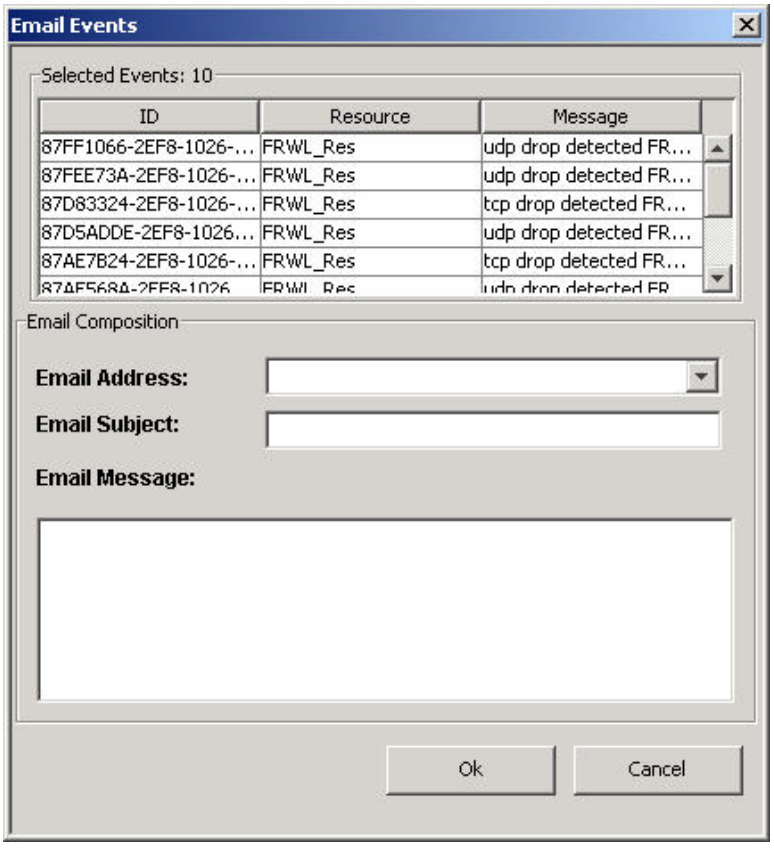
Für UNIX:

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

Weitere Informationen finden Sie in Kapitel 11 – *Dienstprogramme* unter *Konfigurieren von Email-Einstellungen unter Sentinel*.

So senden Sie eine Ereignisnachricht per Email

1. Wählen Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot ein Ereignis oder eine Gruppe von Ereignissen aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie *Email*.




2. Füllen Sie die folgenden Felder aus:
   - Email-Adresse
   - Email-Betreff
   - Email-Nachricht
3. Klicken Sie auf *OK*.

### So senden Sie eine Vorfallsnachricht per Email

1. Klicken Sie nach dem Speichern des Vorfalls auf die Registerkarte „Vorfälle“ und dann auf *Vorfälle > Vorfallsansichts-Manager anzeigen*.
2. Doppelklicken Sie auf *Alle Vorfälle*.
3. Doppelklicken Sie auf einen Vorfall.
4. Klicken Sie auf *Vorfall mailen*  .
5. Geben Sie Folgendes ein:
   - Email-Adresse
   - Email-Betreff
   - Email-Nachricht
6. Klicken Sie auf *OK*. Die Email-Nachricht verfügt über HTML-Anlagen mit Informationen zu den Vorfallsdetails, zu Ereignissen, Beständen, Anfälligkeiten, Advisor-Informationen und zum Vorfallsverlauf.

# Erstellen eines Vorfalls

Zum Ausführen dieser Funktion müssen Sie über die Benutzerberechtigung zum Erstellen von Vorfällen verfügen.

Dies ist hilfreich beim Zusammenfassen eines Satzes von Ereignissen, die von Interesse sein können (ähnliche Ereignisse oder einen Satz unterschiedlicher Ereignisse gruppieren, die ein Interessenmuster, z. B. einen Angriff, angeben).

**HINWEIS**: Wenn in einem neu erstellten Vorfall zu Beginn keine Ereignisse angezeigt werden, liegt dies wahrscheinlich an einer Zeitverzögerung zwischen dem Anzeigen im Fenster für Echtzeitereignisse und dem Einfügen in die Datenbank. In diesem Fall kann es einige Minuten dauern, bis die ursprünglichen Ereignisse in die Datenbank eingefügt und im Vorfall angezeigt werden.

So erstellen Sie einen Vorfall

1. Wählen Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot ein Ereignis oder eine Gruppe von Ereignissen aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie *Vorfall erstellen*.


   Das Fenster „Neuer Vorfall“ enthält die folgenden Registerkarten:

   - Ereignisse – Zeigt, aus welchen Ereignissen der Vorfall besteht.
   - Bestände – Zeigt betroffene Bestände an.
   - Anfälligkeit – Zeigt verwandte Bestandsanfälligkeiten an.
   - Advisor – Enthält Informationen zu Bestandsangriffen und Warnmeldungen.
   - Workflow – Auf dieser Registerkarte können Sie einen WorkFlow (iTrac) zuweisen.
   - Verlauf – Zeigt den Vorfallsverlauf an.
   - Anlagen – Sie können jedes Dokument oder jede Textdatei mit Informationen über diesen Vorfall beifügen.

   Geben Sie in das Dialogfeld „Vorfall erstellen“ Folgendes ein:

   - Titel
   - Status
   - Schweregrad
   - Priorität
   - Kategorie
   - Zuständig – Das Benutzerkonto, das dem Fall zugewiesen ist.
   - Beschreibung
   - Lösung

2. Klicken Sie auf *Speichern*. Der Vorfall wird auf der Registerkarte „Vorfälle“ im Sentinel Control Center hinzugefügt.

# Anzeigen von Ereignissen, die ein korreliertes Ereignis ausgelöst haben

Sie müssen mit der rechten Maustaste auf ein korreliertes Ereignis klicken, um die Ereignisse anzuzeigen, die das korrelierte Ereignis ausgelöst haben. Suchen Sie in der Zusammenfassungsansicht auf der rechten Seite der Ereignistabelle, aus der Sie das Ereignis auswählen, nach einem Ereignis mit einer SensorType-Eigenschaft mit dem Wert C (C: korreliertes Ereignis) oder W (W: Beobachtungsliste).

So zeigen Sie Ereignisse an, die ein korreliertes Ereignis ausgelöst haben

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot oder in einer Ereignisabfragetabelle mit der rechten Maustaste auf ein korreliertes Ereignis und wählen Sie „Auslöseereignisse anzeigen“. Die Ereignisse, die die Regel ausgelöst haben, und der Name der Korrelationsregel werden in einem neuen Fenster angezeigt.


# Untersuchen eines Ereignisses oder von Ereignissen

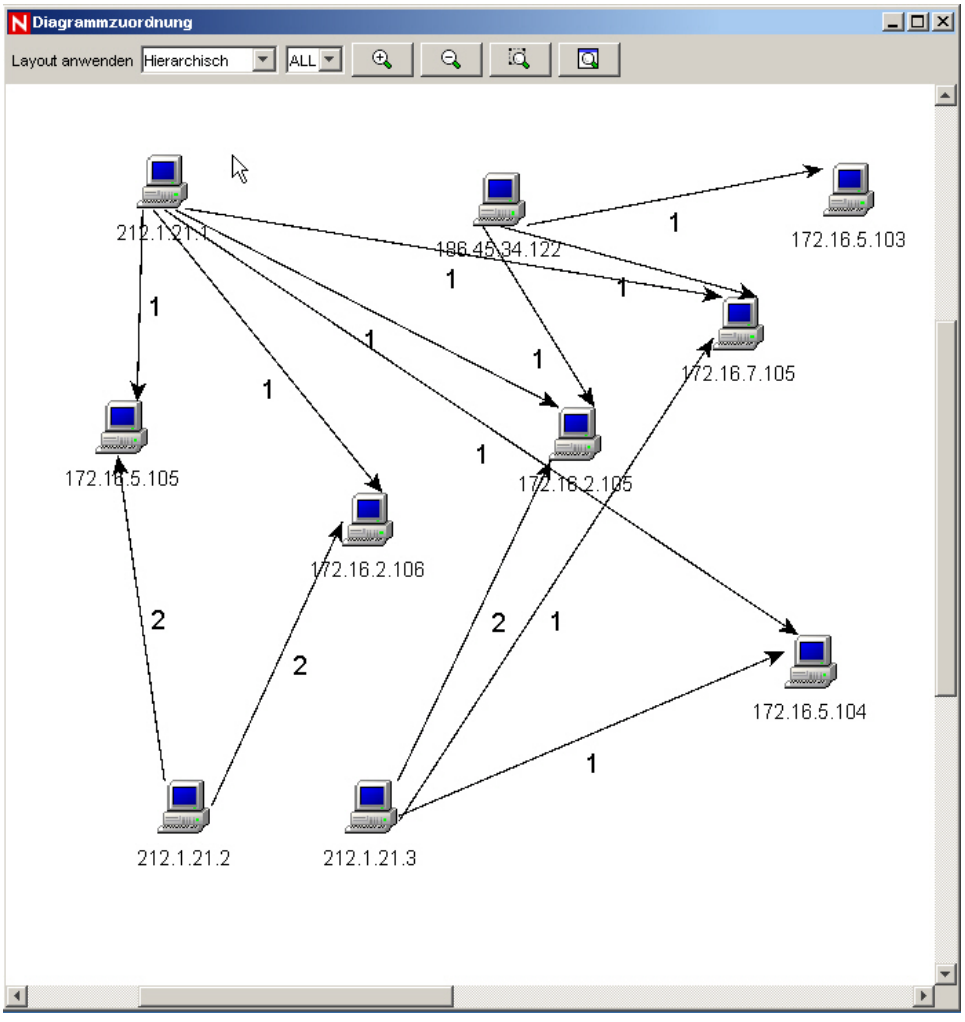
Mithilfe dieser Funktion können Sie:

- Die Quellenfelder (IP, Port, Ereignis, Sensortyp, Collector-Name, ...) grafisch anzeigen, die Zielfeldern (IP, Port, Ereignis, Sensortyp, Collector-Name, ...) ausgewählter Ereignisse zugeordnet sind.
- Eine Ereignisabfrage für die letzte Stunde eines einzelnen Ereignisses durchführen für:

  **HINWEIS**: Sie können keine Abfrage für ein Feld mit dem Wert Null (leer) durchführen.

  - Ziel-IP-Adressen
  - Quellen-IP-Adressen
  - Ereignisname

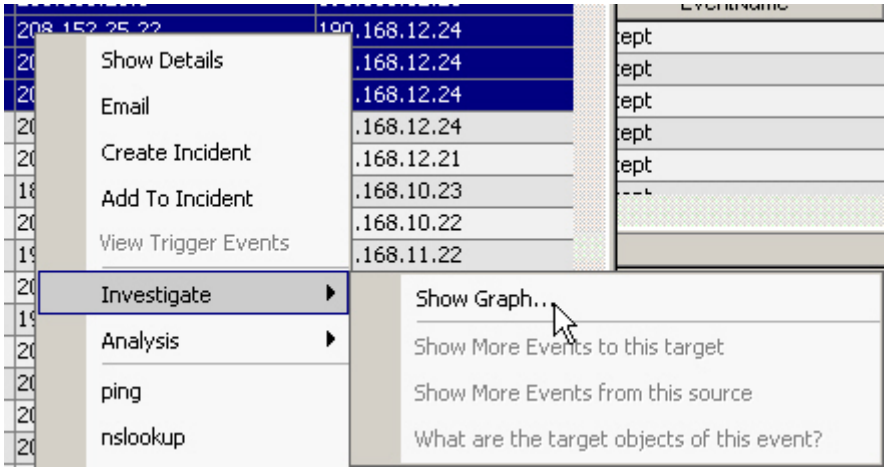
Nachfolgend sehen Sie eine Illustration der Zuordnung von Quellen-IP-Adressen zu Ziel-IP-Adressen.




## Untersuchen – Diagrammzuordnung

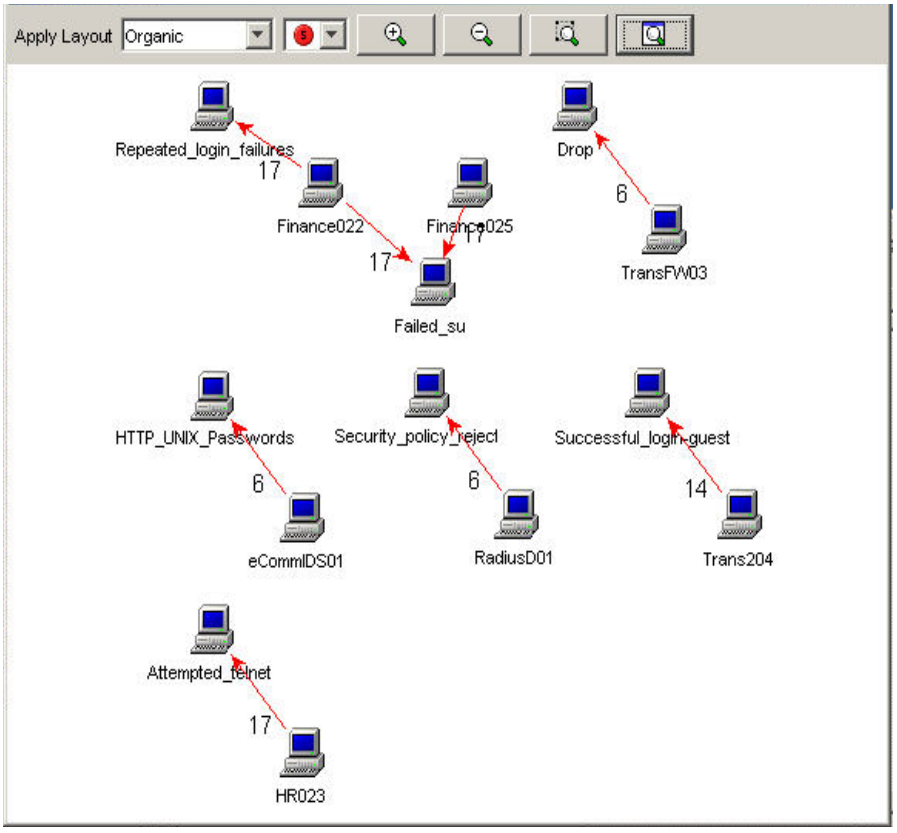
So erstellen Sie eine Diagrammzuordnung

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot mit der rechten Maustaste auf ein oder mehrere Ereignisse und klicken Sie dann auf *Untersuchen > Visuell > Diagramm anzeigen.*




Nachfolgend sehen Sie eine grafische Darstellung der Zuordnung von Sensornamen zu Ereignisnamen mit einem Schweregrad von 5 in einem organischen Format. Eine grafische Zuordnung kann in den folgenden Formaten angezeigt werden:

- Rund
- Hierarchisch
- Organisch
- Rechtwinklig



## Untersuchen – Ereignisabfrage

Diese Funktion ermöglicht Ihnen das Abfragen von Ereignissen der letzten Stunde.

So führen Sie eine Ereignisabfrage mithilfe der Funktion „Untersuchen“ durch

1. Klicken Sie in einem visuellen Navigator oder in einem Snapshot-Fenster mit der rechten Maustaste auf ein Ereignis, dann auf *Untersuchen* und schließlich auf eine der drei unten genannten Optionen.

| Option | Funktion |
|---|---|
| Mehr Ereignisse an diesem Ziel anzeigen | Ziel-IP-Adresse |
| Mehr Ereignisse von dieser Quelle anzeigen | Quellen-IP-Adresse |
| Wie lauten die Zielobjekte dieses Ereignisses? | Ereignisname |

# Analyse – Anzeigen von Advisor-Daten

Advisor bietet einen Querverweis zwischen Echtzeit-IDS-Angriffssignaturen und der Advisor Knowledge Base für Anfälligkeiten. Der Advisor-Feed verfügt über einen Warnungs- und Angriffs-Feed. Der Warnungs-Feed enthält Informationen zu Anfälligkeiten und Viren. Der Angriffs-Feed listet die mit den Anfälligkeiten verknüpften Exploits auf.

Die unterstützten Intrusion Detection-Systeme sind:

- Cisco Secure IDS
- Enterasys Dragon Host Sensor
- Enterasys Dragon Network Sensor
- ISS BlackICE PC Protection
- ISS RealSecure Desktop
- ISS RealSecure Network
- ISS RealSecure Server Sensor
- ISS RealSecure Guard
- Snort/Sourcefire
- Symantec ManHunt
- Symantec Intruder Alert
- McAfee IntruShield

Der IDS-Collector füllt das Feld DeviceAttackName (rt1) eines Ereignisses. Advisor verwendet diese Informationen zum Generieren von Angriffs- und Anfälligkeitsinformationen. Beispiele für Anfälligkeiten sind:

- FINGER: Cfinger Search Probe
- SMTP: SmartServer3 MAIL FROM Buffer Overflow
- HTTP: Dragon Fire IDS Web Interface Remote Execution
- FTP:MKDIR-DOS
- hp-printer-flood
- wh00t-backdoor
- nt-telnet
- FINGER / execution attempt
- tellurian-tftpdnt-filename-bo
- FTP MKD Stack Overflow

So zeigen Sie Advisor-Daten an

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot mit der rechten Maustaste auf ein Ereignis oder auf eine Reihe ausgewählter Ereignisse und klicken Sie dann auf *Analyse* > *Advisor-Daten*. Wenn das Feld DeviceAttackName ordnungsgemäß ausgefüllt wird, wird ein ähnlicher Bericht wie unten aufgeführt angezeigt. Dies ist ein Beispiel für einen WEB-MISC Amazon 1-Click Cookie-Diebstahl.


# Analyse – Anzeigen von Bestandsdaten

Diese Funktion ermöglicht Ihnen das Anzeigen und Speichern Ihrer Ansicht als HTML-Datei Ihres Bestandsberichts. Zum Anzeigen dieser Daten müssen Sie Ihren Bestandsverwaltungs-Collector ausführen. Die folgenden Daten können angezeigt werden:

**Hardware**
- MAC-Adresse
- Name
- Typ
- Hersteller
- Produkt
- Version
- Wert
- Gefährlichkeit
- Vertraulichkeit
- Umgebung
- Standort

**Netzwerk**
- IP-Adresse
- Hostname

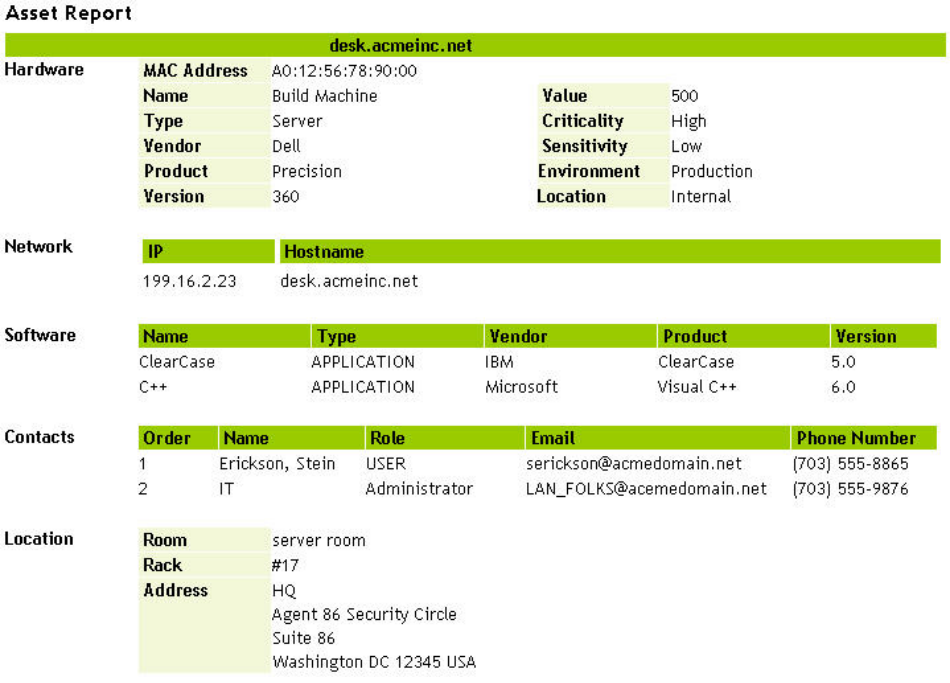
**Software**
- Name
- Typ
- Hersteller
- Produkt
- Version

**Kontaktinformationen**
- Reihenfolge
- Name
- Funktion
- Email
- Telefonnummer

**Standort**
- Raum
- Regal
- Adresse

So zeigen Sie Bestandsdaten an

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot-Fenster mit der rechten Maustaste auf ein oder mehrere Ereignisse und klicken Sie dann auf *Analyse* > *Inventardaten*. Ein ähnliches Fenster wie unten zu sehen ist, wird eingeblendet.



**Asset Report**

| desk.acmeinc.net | | | | |
|---|---|---|---|---|
| **Hardware** | **MAC Address** | A0:12:56:78:90:00 | | |
| | **Name** | Build Machine | **Value** | 500 |
| | **Type** | Server | **Criticality** | High |
| | **Vendor** | Dell | **Sensitivity** | Low |
| | **Product** | Precision | **Environment** | Production |
| | **Version** | 360 | **Location** | Internal |

**Network**

| IP | Hostname |
|---|---|
| 199.16.2.23 | desk.acmeinc.net |

**Software**

| Name | Type | Vendor | Product | Version |
|---|---|---|---|---|
| ClearCase | APPLICATION | IBM | ClearCase | 5.0 |
| C++ | APPLICATION | Microsoft | Visual C++ | 6.0 |

**Contacts**

| Order | Name | Role | Email | Phone Number |
|---|---|---|---|---|
| 1 | Erickson, Stein | USER | serickson@acmedomain.net | (703) 555-8865 |
| 2 | IT | Administrator | LAN_FOLKS@acemedomain.net | (703) 555-9876 |

**Location**

| | |
|---|---|
| **Room** | server room |
| **Rack** | #17 |
| **Address** | HQ<br>Agent 86 Security Circle<br>Suite 86<br>Washington DC 12345 USA |

# Analyse – Anfälligkeitsvisualisierung

Novell verfügt über Collectors, die Anfälligkeitsprüfungen aus Nessus-, ISS-, Foundstone-, eEye- und Qualys-Absuchvorgängen verarbeiten. Die Anfälligkeitsvisualisierung bietet eine grafische Darstellung von Echtzeitereignisdaten in anfälligen Systemen und ist für ein Ereignis zur Darstellung der aktuellen Anfälligkeit oder der Ereigniszeitanfälligkeit verfügbar.

Diese Funktion ruft die Anfälligkeitsdaten für die Ziel-IPs ausgewählter Ereignisse ab und zeigt diese an. Weitere Informationen finden Sie in der PDF-Dokumentation für den jeweiligen Collector unter %ESEC_HOME%\wizard\elements\<Collector-Name>\doc. Damit Anfälligkeitsdaten angezeigt werden, muss einer der Scanner-Collectors hochgeladen sein und ausgeführt werden.

**HINWEIS**: Der Anfälligkeits-Collector ist ein Informations-Collector und kein Ereignis-Collector.

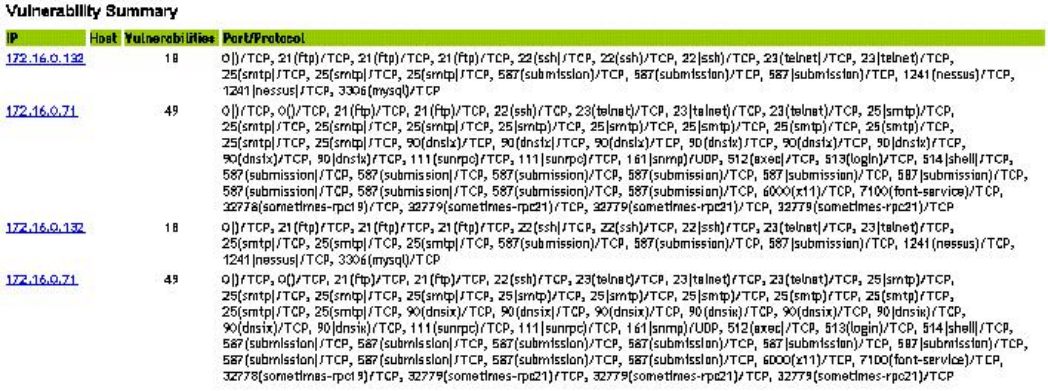
Sie können Ihre Anfälligkeitsvisualisierung auf verschiedene Weisen anzeigen:

- in HTML
- grafisch
  - rund (organisch)
  - hierarchisch
  - alle
  - Ereigniszuordnungsknoten
  - rechtwinklig

Die HTML-Ansicht ist eine berichtartige Ansicht, die Folgendes auflistet:

- IP
- Host
- Anfälligkeit
- Port/Protokoll

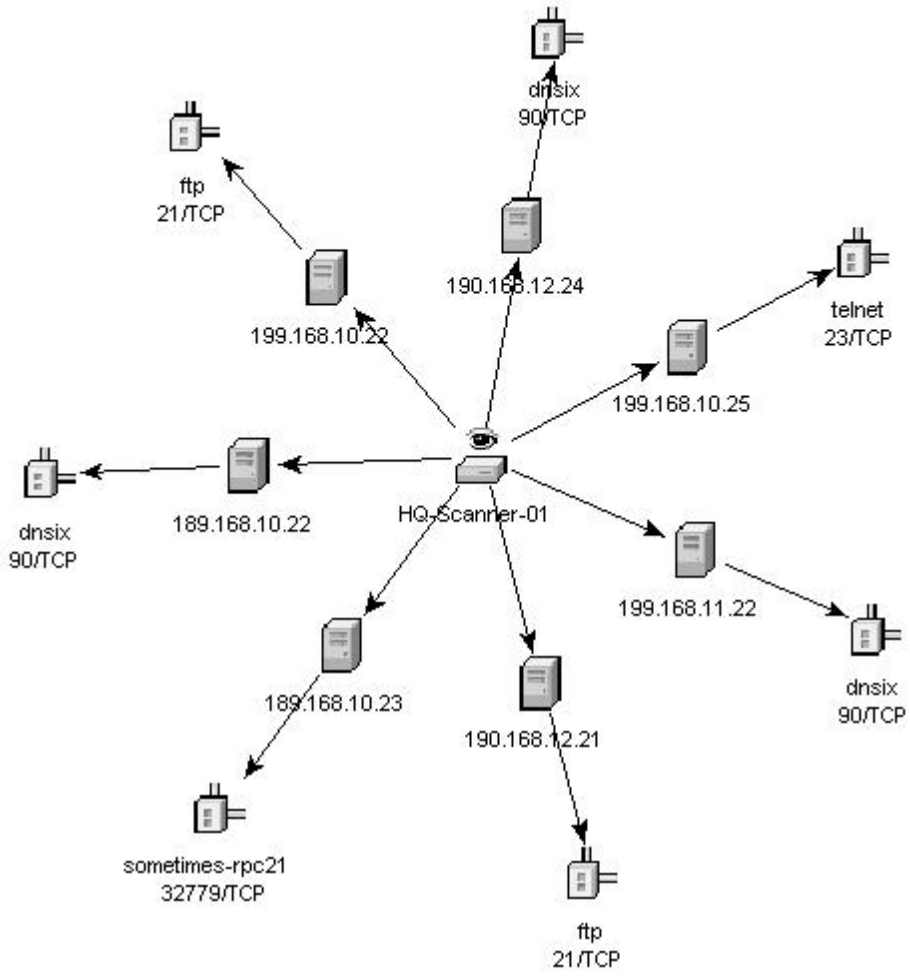
Nachfolgend sehen Sie ein Beispiel für einen Nessus-Absuchvorgang.



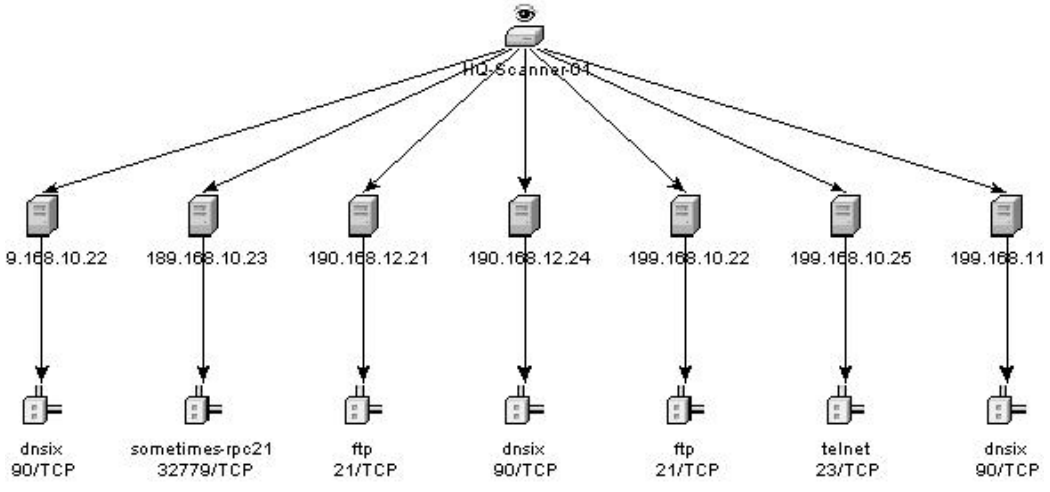
**Vulnerability Summary**

| IP | Host | Vulnerabilities | Port/Protocol |
|---|---|---|---|
| 172.16.0.132 | | 18 | 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 22(ssh)/TCP, 22\|ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 1241(nessus)/TCP, 1241\|nessus\|/TCP, 3306(mysql)/TCP |
| 172.16.0.71 | | 49 | 0()/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 23(telnet)/TCP, 25\|smtp)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 90(dnsix)/TCP, 90(dnsix\|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 111(sunrpc)/TCP, 111\|sunrpc)/TCP, 161\|snmp)/UDP, 512(exec\|/TCP, 513(login)/TCP, 514\|shell\|/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 587\|submission)/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP |
| 172.16.0.132 | | 18 | 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 22(ssh)/TCP, 22\|ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 1241(nessus)/TCP, 1241\|nessus\|/TCP, 3306(mysql)/TCP |
| 172.16.0.71 | | 49 | 0()/TCP, 0()/TCP, 21(ftp)/TCP, 21(ftp)/TCP, 22(ssh)/TCP, 23(telnet)/TCP, 23\|telnet)/TCP, 23(telnet)/TCP, 25\|smtp)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 25\|smtp)/TCP, 25\|smtp)/TCP, 25(smtp)/TCP, 25(smtp)/TCP, 25(smtp\|/TCP, 25(smtp\|/TCP, 90(dnsix)/TCP, 90(dnsix\|/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 90(dnsix)/TCP, 90\|dnsix)/TCP, 111(sunrpc)/TCP, 111\|sunrpc)/TCP, 161\|snmp)/UDP, 512(exec\|/TCP, 513(login)/TCP, 514\|shell\|/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 587\|submission)/TCP, 587\|submission)/TCP, 587(submission\|/TCP, 587(submission\|/TCP, 587(submission)/TCP, 587(submission)/TCP, 6000(x11)/TCP, 7100(font-service)/TCP, 32778(sometimes-rpc19)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP, 32779(sometimes-rpc21)/TCP |

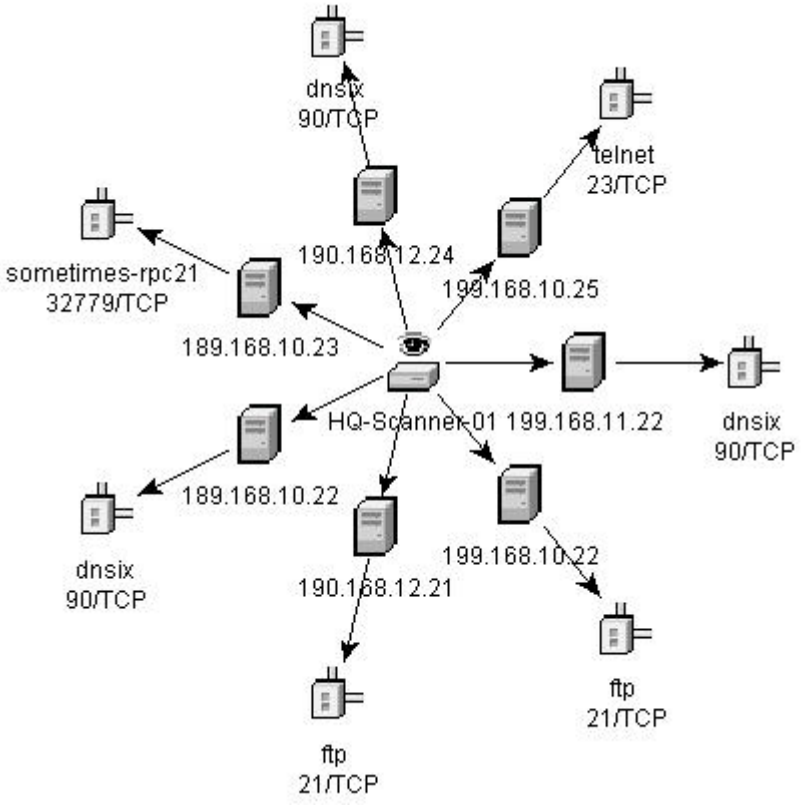
Die grafische Anzeige ist eine Darstellung der Anfälligkeiten, die diese über allgemeine Ports mit einem Ereignis verbinden. Nachfolgend sehen Sie vier Beispiele für verfügbare Ansichten.


dnsix
90/TCP
ftp
21/TCP
190.168.12.24
199.168.10.22
telnet
23/TCP
199.168.10.25
dnsix
90/TCP
189.168.10.22
HQ-Scanner-01
199.168.11.22
dnsix
90/TCP
189.168.10.23
190.168.12.21
sometimes-rpc21
32779/TCP
ftp
21/TCP

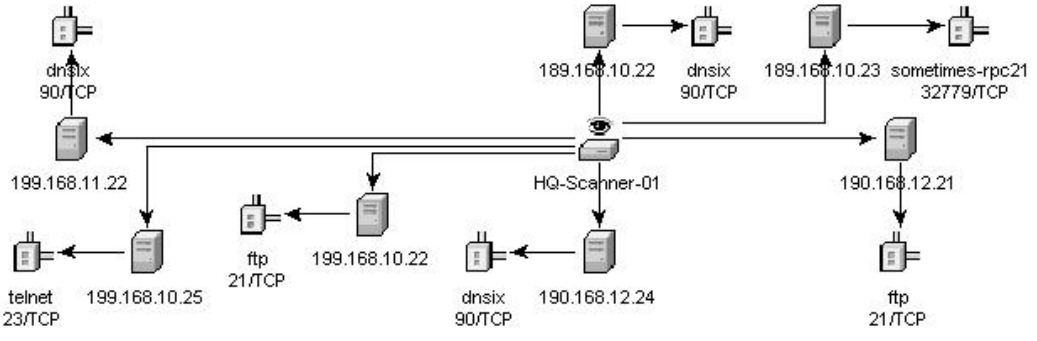
**Organisch**


HQ-Scanner-01
9.168.10.22
189.168.10.23
190.168.12.21
190.168.12.24
199.168.10.22
199.168.10.25
199.168.11
dnsix
90/TCP
sometimes-rpc21
32779/TCP
ftp
21/TCP
dnsix
90/TCP
ftp
21/TCP
telnet
23/TCP
dnsix
90/TCP

**Hierarchisch**




**Rund**




**Rechtwinklig**

Die grafische Anzeige enthält vier Felder. Hierbei handelt es sich um:

- das Diagrammfeld
- das Baumfeld
- die Systemsteuerung
- das Detail-/Ereignisfeld

Die Diagrammfeldanzeige verknüpft Anfälligkeiten mit einer Port/Protokoll-Kombination einer Ressource (IP-Adresse). Wenn eine Ressource beispielsweise über fünf eindeutige Port/Protokoll-Kombinationen verfügt, die anfällig sind, werden fünf Knoten mit dieser Ressource verbunden. Die Ressourcen werden unter dem Scanner gruppiert, der die Ressourcen abgesucht und die Anfälligkeiten gemeldet hat. Wenn zwei unterschiedliche Scanner verwendet werden (ISS und Nessus), gibt es zwei unabhängige Scanner-Knoten, mit denen Anfälligkeiten verknüpft sind.

**HINWEIS**: Die Ereigniszuordnung erfolgt nur zwischen den ausgewählten Ereignissen und den zurückgegebenen Anfälligkeitsdaten.

Das Baumfeld organisiert die Daten in derselben Hierarchie wie das Diagramm. Das Baumfeld ermöglicht den Benutzern zudem das Ein- bzw. Ausblenden von Knoten auf jeder Hierarchieebene.

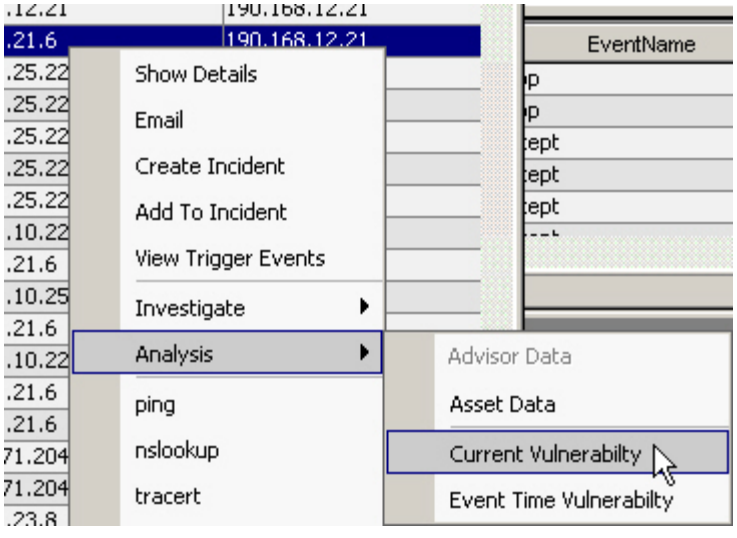
Die Systemsteuerung offenbart die gesamte Funktionalität der Anzeige. Diese umfasst:

- vier verschiedene Algorithmen, die angezeigt werden können
- die Möglichkeit, alle oder ausgewählte Knoten anzuzeigen, denen Ereignisse zugeordnet sind
- das Vergrößern und Verkleinern ausgewählter Bereiche des Diagramms

Das Feld „Details/Ereignisse“ verfügt über zwei Registerkarten. Wenn Sie auf der Registerkarte „Details“ auf einen Knoten klicken, werden die Knotendetails angezeigt. Wenn Sie auf der Registerkarte „Ereignisse“ auf ein Ereignis klicken, das mit einem Knoten verknüpft ist, wird der Knoten wie in einem Echtzeit- oder Ereignisabfragefenster in Tabellenform angezeigt.

### So führen Sie eine Anfälligkeitsvisualisierung aus

1. Klicken Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot mit der rechten Maustaste auf ein Ereignis oder auf eine Reihe ausgewählter Ereignisse und klicken Sie dann auf:
   - Analyse
     - Aktuelle Anfälligkeit – Fragt die Datenbank nach Anfälligkeiten ab, die zum aktuellen Zeitpunkt aktiv (wirksam) sind.
     - Ereigniszeitanfälligkeit – Fragt die Datenbank nach Anfälligkeiten ab, die zum Zeitpunkt des ausgewählten Ereignisses aktiv (wirksam) waren.



2. Klicken Sie am unteren Rand des Fensters „Anfälligkeitsergebnisse“ auf eine der folgenden Optionen:
   - Diagramm Ereignis/Anfälligkeit
   - Anfälligkeitsbericht
3. (Für „Diagramm Ereignis/Anfälligkeit“) Innerhalb der Anzeige können Sie:
   - Knoten und ihre Kennungen verschieben
   - einen von vier verschiedenen Layoutalgorithmen zum Anzeigen des Diagramms verwenden
   - alle Knoten oder nur jene Knoten anzeigen, denen Ereignisse zugeordnet sind
   - eine Filterung im Baum durchführen, wenn eine große Anzahl von Ressourcen als anfällig zurückgegeben wurde
   - ausgewählte Bereiche vergrößern und verkleinern

# Drittanbieter-Integration

Die Drittanbieter-Integration ermöglicht Ihnen das Senden von Ereignissen aus jeder beliebigen Anzeige, einschließlich Vorfällen und der zugehörigen Objekte, an eines der folgenden Programme:

- HP Service Desk
- Remedy

So senden Sie einzelne oder mehrere Ereignisse für Drittanbieter-Software

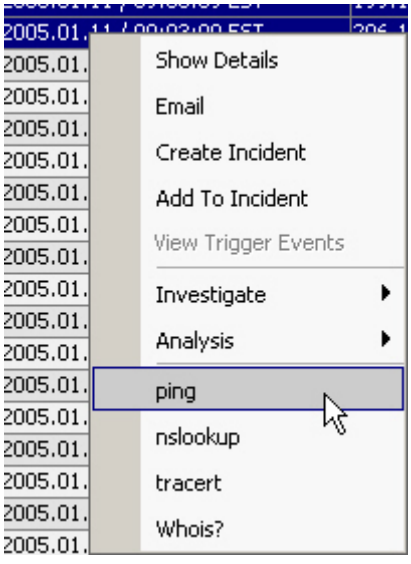
1. Klicken Sie, je nachdem, welche Drittanbieter-Integrationssoftware Sie installiert haben, in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot-Fenster mit der rechten Maustaste auf ein Ereignis und klicken Sie dann auf eine der Optionen zum Senden des Ereignisses an:
   - HP Service Desk
   - Remedy

# Verwenden von benutzerdefinierten Menüoptionen mit Ereignissen

So verwenden Sie eine benutzerdefinierte Menüoption mit einem Ereignis

1. Wählen Sie in einer vorhandenen Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot ein Ereignis oder eine Gruppe von Ereignissen aus, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf eine Option. Im eingeblendeten Dialogfeld werden die Informationen angezeigt, für die die Menüoption konfiguriert ist, oder Sie erhalten darin die Möglichkeit zum Angeben der Informationen, die zum Ausführen einer Aktion erforderlich sind. Die standardmäßigen benutzerdefinierten Menüoptionen sind:
   - ping
   - nslookup
   - traceroute
   - Whois?

Darüber hinaus können Sie Benutzerberechtigungen zum Anzeigen der Anfälligkeit und zum Durchführen von HP-Aktionen zuweisen. Im Fenster „Menükonfiguration“, das über die Registerkarte „Admin“ verfügbar ist, können Sie Optionen hinzufügen.



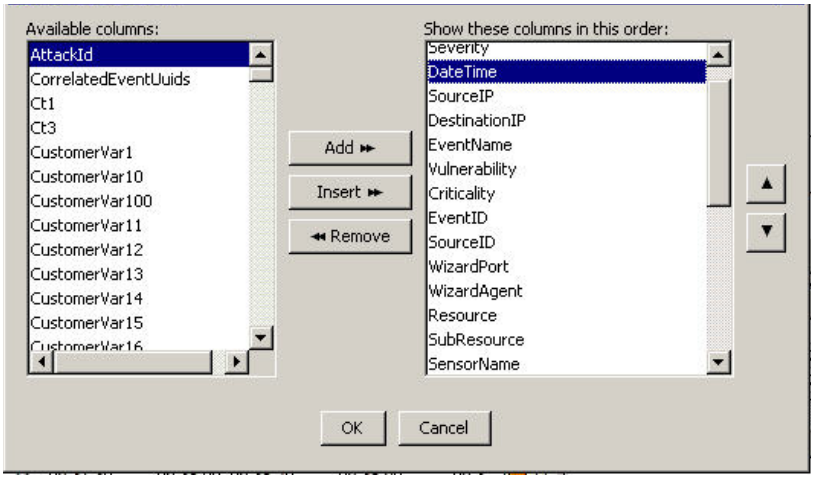

# Verwalten der Spalten in einem Snapshot- oder visuellen Navigatorfenster

So können Sie die Spalten in einem Snapshot oder visuellen Navigator auswählen und anordnen

1. Klicken Sie bei geöffnetem Snapshot- oder visuellen Navigatorfenster auf *Aktive Ansicht* > *Ereignisechtzeit* > *Spalten verwalten* oder klicken Sie auf die Schaltfläche *Spalten verwalten* der Echtzeitereignistabelle.

2. Verwenden Sie die Schaltflächen *Hinzufügen* und *Entfernen*, um die Spaltentitel zwischen der Liste „Verfügbare Spalten“ und der Liste „Spalten in dieser Reihenfolge anzeigen“ zu verschieben. Mit „Einfügen“ können Sie einen verfügbaren Spalteneintrag an einer bestimmten Position einfügen. Wenn beispielsweise in der folgenden Abbildung auf die Schaltfläche *Einfügen* geklickt wird, wird AttackId vor DateTime eingefügt.




Verwenden Sie die Auf- und Abwärtspfeile, um die Anzeigereihenfolge der Spalten in der Echtzeitereignistabelle anzupassen. Die Reihenfolge der Spaltentitel im Dialogfeld „Spalten verwalten“ von oben nach unten bestimmt die Reihenfolge der Spalten in der Echtzeitereignistabelle von links nach rechts.

3. Klicken Sie im Dialogfeld „Spalten verwalten“ auf *OK*.
4. Falls die Spaltenreihenfolge beibehalten werden soll, wenn Sie das Sentinel Control Center das nächste Mal öffnen, klicken Sie auf *Datei > Einstellungen speichern* oder klicken Sie auf *Benutzereinstellungen speichern*.

# Erstellen eines Snapshot eines visuellen Navigatorfensters

Zum Ausführen dieser Funktion müssen Sie über die Snapshot-Benutzerberechtigung verfügen.

Dies ist hilfreich, um Ereignisse von Interesse zu untersuchen, da der visuelle Navigator automatisch aktualisiert wird und die Warnung oder Warnungen von Interesse nach einiger Zeit nicht mehr angezeigt werden. Innerhalb eines Snapshot können Sie auch eine Sortierung nach Spalten vornehmen.

### So erstellen Sie einen Snapshot einer Echtzeitereignistabelle

1. Klicken Sie bei geöffnetem visuellen Navigatorfenster auf *Aktive Ansicht > Ereignisechtzeit > Snapshot* oder klicken Sie in der Menüleiste auf *Snapshot-Ereignistabelle in Echtzeit*.

Ein Snapshot-Fenster wird geöffnet und im Navigator unter „Ereignisanzeigen“ der Ordnerliste „Snapshots“ hinzugefügt. Die grafische Anzeige ist im Snapshot nicht enthalten.

## Sortieren der Spalten in einem Snapshot

So sortieren Sie die Spalten in einem Snapshot

1. Klicken Sie einmal auf eine Spaltenüberschrift, um die Spalte in aufsteigender Reihenfolge zu sortieren, und zweimal, um sie in absteigender Reihenfolge zu sortieren.

## Schließen eines Snapshot oder visuellen Navigatorfensters

So schließen Sie einen Snapshot oder eine Echtzeitereignistabelle

1. Klicken Sie bei geöffnetem Snapshot oder visuellen Navigatorfenster auf *Datei > Einstellungen speichern*, falls die Tabelle verfügbar sein soll, wenn Sie das Sentinel Control Center das nächste Mal starten.
2. Schließen Sie die Tabelle über die Schaltfläche „Schließen“ (in der rechten oberen Ecke unter Windows oder in der linken unteren Ecke unter UNIX).

## Löschen eines Snapshot oder visuellen Navigatorfensters

So löschen Sie einen Snapshot oder ein visuelles Navigatorfenster

1. Schließen Sie einen geöffneten Snapshot oder visuellen Navigator über die Schaltfläche „Schließen" (in der rechten oberen Ecke unter Windows oder in der linken unteren Ecke unter UNIX).
2. Klicken Sie auf *Datei > Einstellungen* speichern oder klicken Sie auf *Benutzereinstellungen speichern.*

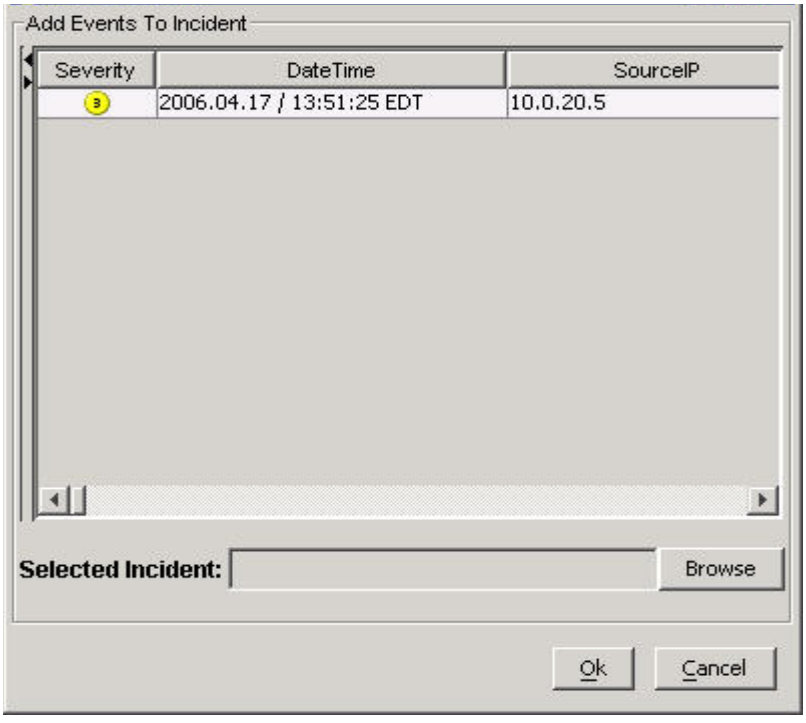
   Die Ansicht oder der Snapshot werden nicht wieder angezeigt, wenn Sie das Sentinel Control Center schließen und wieder öffnen.

## Hinzufügen von Ereignissen zu einem Vorfall

Zum Ausführen dieser Funktion müssen Sie über die Benutzerberechtigung zum Ändern und Zuweisen von Vorfällen verfügen.

So fügen Sie einem Vorfall Ereignisse hinzu

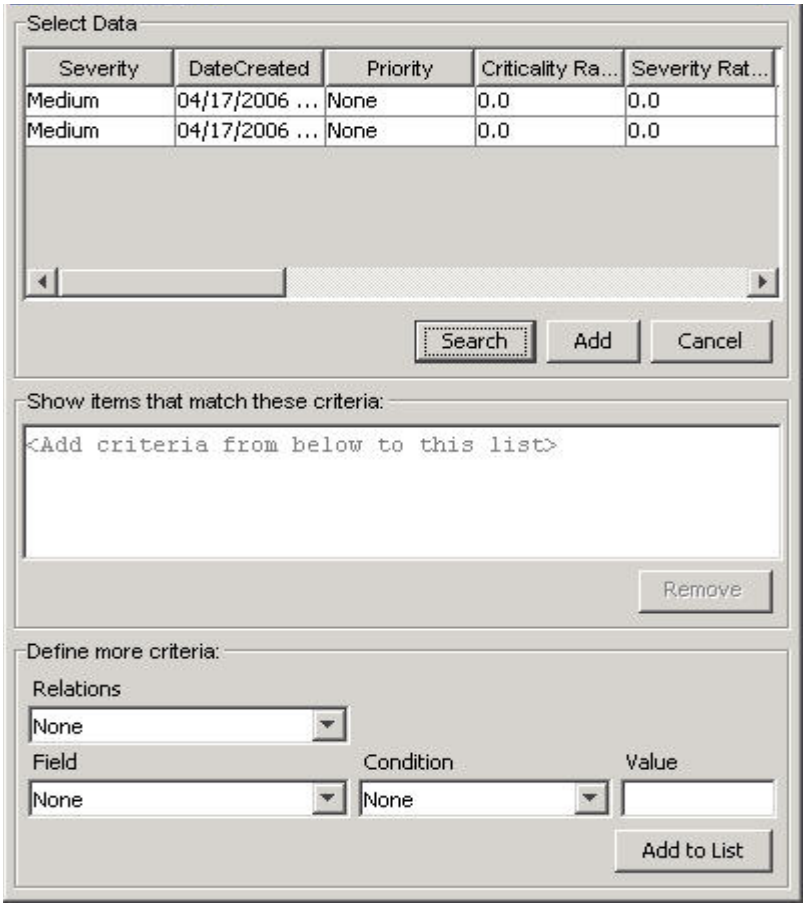
1. Wählen Sie in einer Echtzeitereignistabelle im visuellen Navigator oder in einem Snapshot ein Ereignis oder eine Gruppe von Ereignissen aus, klicken Sie mit der rechten Maustaste darauf und klicken Sie dann auf *Zum Vorfall hinzufügen*.
2. Klicken Sie im Dialogfeld *Zum Vorfall hinzufügen* auf die Schaltfläche „Durchsuchen“.




3. Klicken Sie auf *Durchsuchen*, um die verfügbaren Vorfälle aufzulisten.

**HINWEIS**: Sie können eigene Kriterien definieren, um besser nach einem bestimmten Vorfall oder mehreren Vorfällen zu suchen.

4. Klicken Sie auf *Suchen*, um eine Liste mit Vorfällen anzuzeigen.




5. Markieren Sie einen Vorfall und klicken Sie auf *Hinzufügen*.
6. Klicken Sie auf *OK* (Hinzufügen). Das bzw. die ausgewählten Ereignisse werden im Vorfallsnavigator zum Vorfall hinzugefügt.

**HINWEIS**: Wenn in einem neu erstellten Vorfall zu Beginn keine Ereignisse angezeigt werden, liegt dies wahrscheinlich an einer Zeitverzögerung zwischen dem Anzeigen im Fenster für Echtzeitereignisse und dem Einfügen in die Datenbank. In diesem Fall kann es einige Minuten dauern, bis die ursprünglichen Ereignisse in die Datenbank eingefügt und im Vorfall angezeigt werden.

# 4 Registerkarte „Vorfälle“

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

Sie müssen über die entsprechende Berechtigung verfügen, um die Registerkarte „Vorfälle“ verwenden zu können. Wenn Ihnen diese Berechtigung nicht erteilt wurde, verfügen Sie auch nicht über die anderen Berechtigungen zur Durchführung von Aktionen mithilfe dieser Registerkarte.

In diesem Kapitel werden Vorfälle behandelt. Vorfälle sind Gruppierungen von ein oder mehreren Ereignissen, die von Interesse sind.

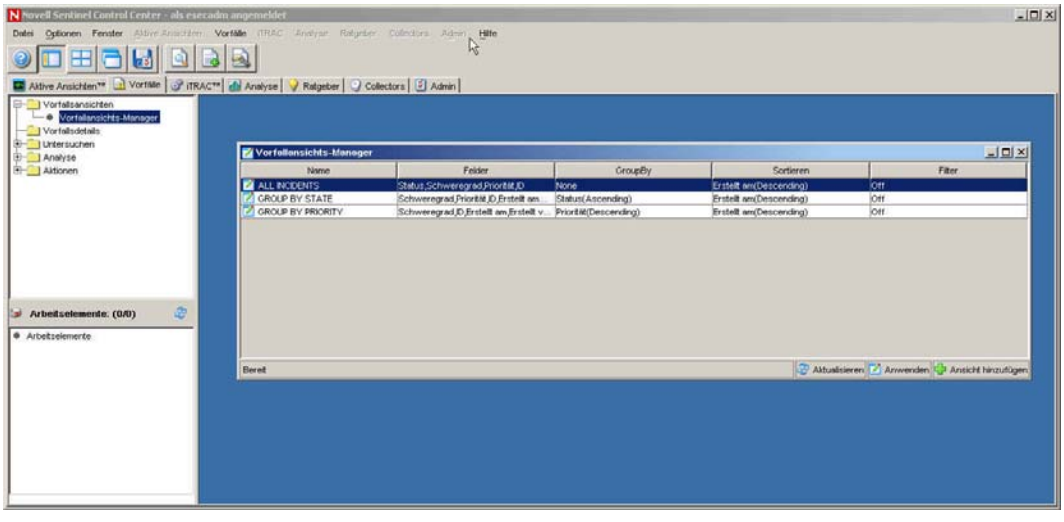
Vorfälle können folgendermaßen erstellt werden:

- Im Echtzeitfenster können Sie Ereignisse einzeln auswählen, um einen neuen Vorfall zu erstellen oder um sie einem bestehenden Vorfall hinzuzufügen.
- Durch Korrelationsregeln, die ausgelöst werden, können Vorfälle auch automatisch erstellt werden.

## Registerkarte „Vorfall“ – Beschreibung

Auf der Registerkarte „Vorfälle“ können Sie:

- Senden eines Vorfalls per Email
- Ändern eines Vorfalls
- Anzeigen eines Vorfalls
- Löschen eines Vorfalls
- Hinzufügen einer Vorfallsansicht



## Beziehung zwischen Ereignissen und Vorfällen

Ein Ereignis ist eine Aktion oder ein Vorgang, die bzw. der von einem Sicherheitsgerät oder -programm entdeckt wurde. Ereignisse gelten als „statuslos“.

Ein Vorfall ist die Gruppierung von einem oder mehreren Ereignissen, die als wichtig erachtet werden (ein möglicher Angriff). Vorfälle weisen „Status“ auf, die eine Antwort und Schließung erforderlich machen.

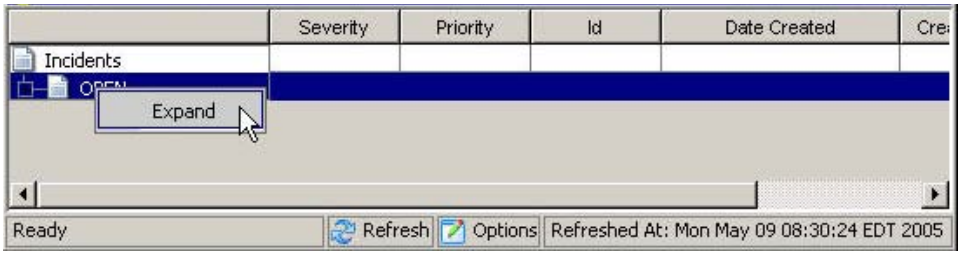
## Anzeigen eines Vorfalls

Sie müssen über die Benutzerberechtigung zum Anzeigen von Vorfällen verfügen.

### So zeigen Sie einen Vorfall an

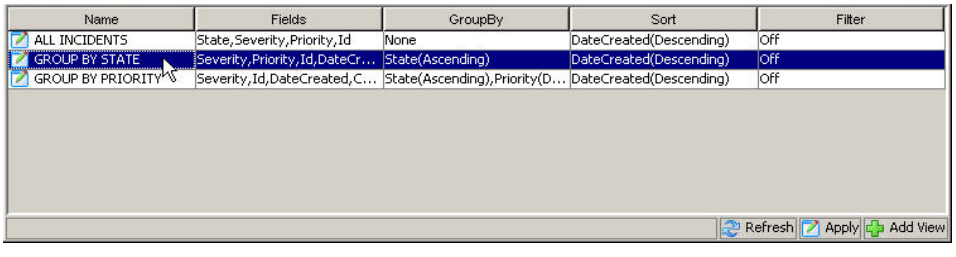
1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Klicken Sie auf *Vorfälle* > *Vorfallsansichts-Manager anzeigen* oder klicken Sie auf die Schaltfläche *Vorfallsansichts-Manager anzeigen*.  .
3. Im Fenster „Vorfallsansichts-Manager“ stehen die folgenden Ansichten zur Auswahl:
   - Alle Vorfälle
   - Nach Status gruppieren
   - Nach Priorität gruppieren

   Doppelklicken Sie auf den Namen einer Ansicht.
4. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Erweitern*, um die Vorfälle anzuzeigen.

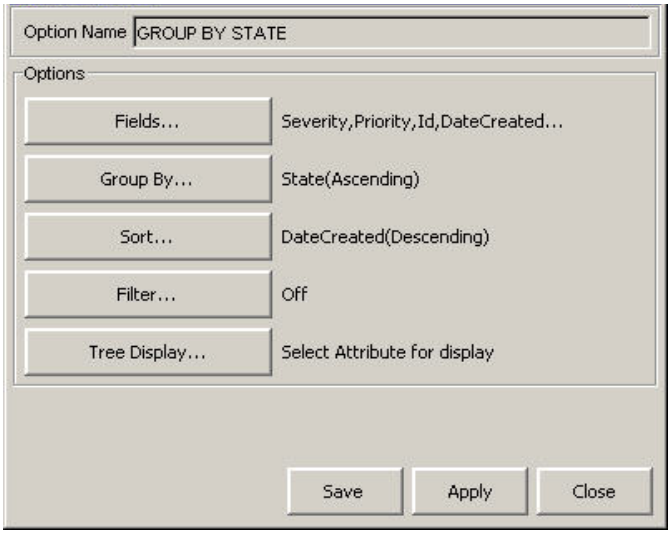



### So legen Sie eine Vorfallsansichtsoption fest

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Klicken Sie auf *Vorfälle* > *Vorfallsansichts-Manager anzeigen* oder klicken Sie auf die Schaltfläche *Vorfallsansichts-Manager anzeigen*.  .
3. Doppelklicken Sie im Fenster „Vorfallsansichts-Manager“ auf den Namen einer Ansicht.



4. Klicken Sie auf *Optionen*.

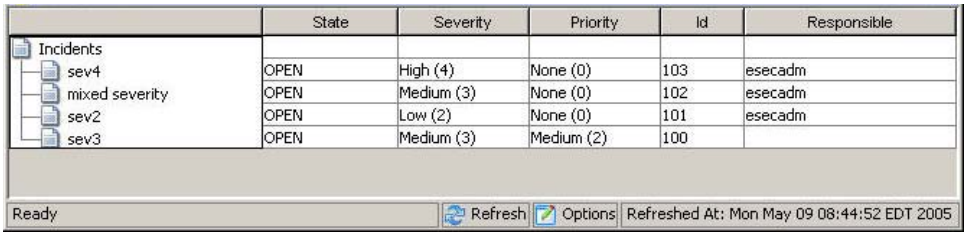

In diesem Fenster können Sie auch Folgendes festlegen:

- Felder...
- Gruppieren nach...
- Sortieren...
- Filter...
- Baumansicht

Klicken Sie auf *Anwenden* und dann auf *Speichern*.

5. Doppelklicken Sie im Fenster „Vorfallsansichts-Manager“ auf den Namen einer Ansicht.

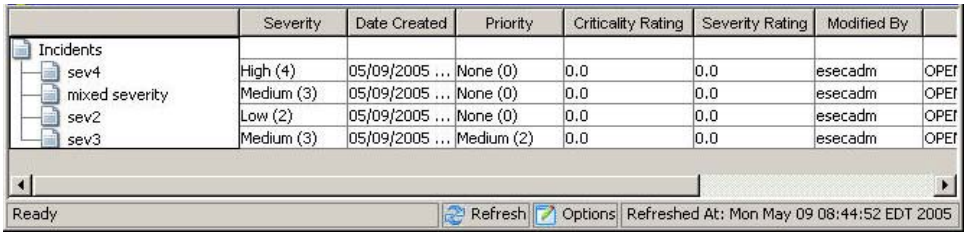
Nachfolgend sehen Sie eine Standardansicht des Fensters „Ansicht aller Vorfälle“.



| | State | Severity | Priority | Id | Responsible |
|---|---|---|---|---|---|
| Incidents | | | | | |
| sev4 | OPEN | High (4) | None (0) | 103 | esecadm |
| mixed severity | OPEN | Medium (3) | None (0) | 102 | esecadm |
| sev2 | OPEN | Low (2) | None (0) | 101 | esecadm |
| sev3 | OPEN | Medium (3) | Medium (2) | 100 | |

Ready | Refresh | Options | Refreshed At: Mon May 09 08:44:52 EDT 2005

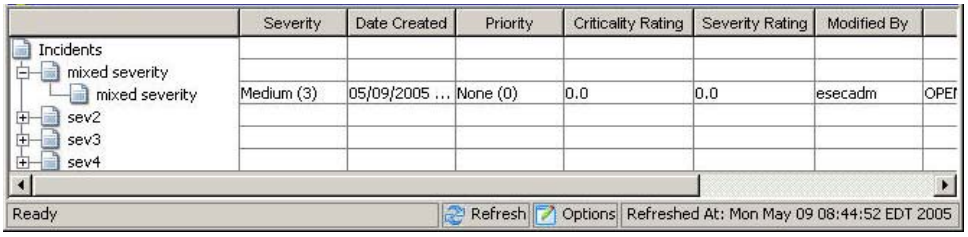
Nachfolgend sehen Sie eine Ansicht, die nach Schweregrad sortiert ist und deren Felder (Spaltenverwaltung) für die ersten vier Spalten auf „Schweregrad“, „Erstellt am“, „Priorität“ und „Gefährlichkeits-Rating“ eingestellt sind.



| | Severity | Date Created | Priority | Criticality Rating | Severity Rating | Modified By | |
|---|---|---|---|---|---|---|---|
| Incidents | | | | | | | |
| sev4 | High (4) | 05/09/2005 ... | None (0) | 0.0 | 0.0 | esecadm | OPEI |
| mixed severity | Medium (3) | 05/09/2005 ... | None (0) | 0.0 | 0.0 | esecadm | OPEI |
| sev2 | Low (2) | 05/09/2005 ... | None (0) | 0.0 | 0.0 | esecadm | OPEI |
| sev3 | Medium (3) | 05/09/2005 ... | Medium (2) | 0.0 | 0.0 | esecadm | OPEI |

Ready | Refresh | Options | Refreshed At: Mon May 09 08:44:52 EDT 2005

Nachfolgend sehen Sie eine Ansicht, die nach Titel gruppiert ist.




Nachfolgend sehen Sie einen Ansichtsbaum nach Erstellungsdatum (Erstellt am).

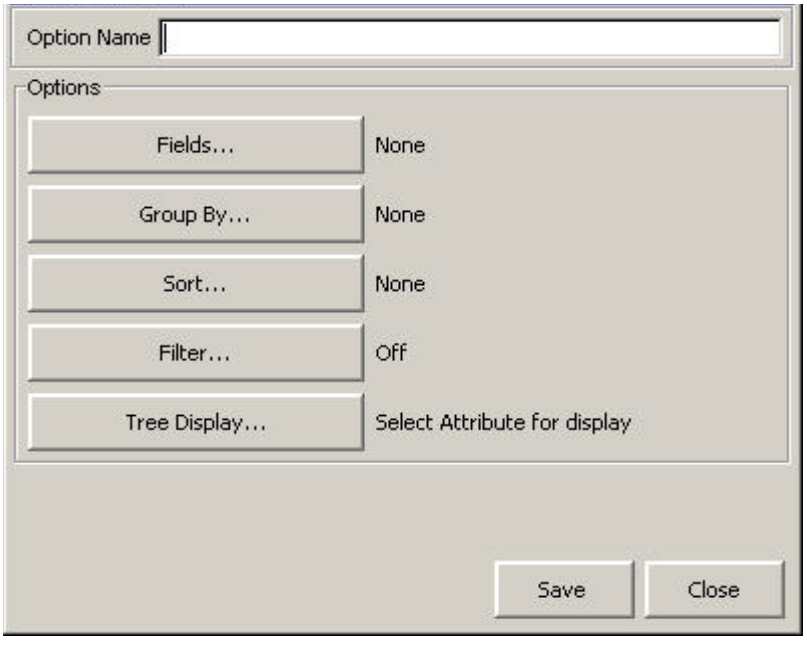

## Hinzufügen einer Vorfallsansicht

Beim Hinzufügen einer Vorfallsansicht stehen folgende Optionen zur Verfügung:

- Felder...
- Gruppieren nach...
- Sortieren...
- Filter...
- Baumansicht

So fügen Sie eine Vorfallsansicht hinzu

1. Klicken Sie im „Vorfallsansichts-Manager“ auf *Ansicht hinzufügen*.




2. Geben Sie einen Optionsnamen ein, wählen Sie die gewünschten Optionen aus und klicken Sie dann auf *Speichern*.

## Vorfallsfelder und -details

### Vorfallsfelder

- Titel – der Name des Vorfalls
- Status
  - Offen
  - Bestätigt
  - Zugewiesen
  - Wird untersucht
  - Falsch positiv
  - Überprüft
  - Genehmigt
  - Geschlossen
- Schweregrad
  - Keine (0)
  - Geringfügig (1)
  - Niedrig (2)
  - Mittel (3)
  - Hoch (4)
  - Schwer (5)
- Priorität
  - Niedrig (1)
  - Mittel (2)
  - Hoch (3)
  - Dringend (4)
  - Höchste (5)
- Kategorie – (optional); Texteintrag, der zur weiteren Identifizierung des Vorfalls verwendet werden kann.
- Zuständig – Das Benutzerkonto, das dem Fall zugewiesen ist.
- Beschreibung – Texteintrag
- Lösung – Texteintrag

### Vorfallsdetails

- Ereignisse – Ereignisse, die mit dem Vorfall in Verbindung stehen
- Bestände – Liste aller Bestände, die mit dem Vorfall in Verbindung stehen
- Anfälligkeit – Zeigt Anfälligkeiten in Verbindung mit dem Vorfall an
- Advisor – Zeigt Angriffsinformationen in Verbindung mit dem Vorfall an
- Workflow – Zeigt den Workflow in Verbindung mit dem Vorfall an. Auf dieser Registerkarte können Sie folgende Zuweisungen vornehmen:
  - Keine
  - HIPAA-Konformitätsprozess
  - SANS-Vorfallsreaktionsprozess
  - Sarbanes Oxley FTP-Konformitätsprozess
  - Automatische Reaktion
- Verlauf – Vorfallsverlauf (Listet alle Aktionen auf, die in Verbindung mit dem Vorfall ausgeführt wurden; dazu gehören auch Datum/Zeit-Benutzeraktionen und kurze Informationen.)
- Anlagen – Sie können beliebige Informationen (Textdateien oder Dokumente) über diesen Vorfall beifügen.
- Externe Daten

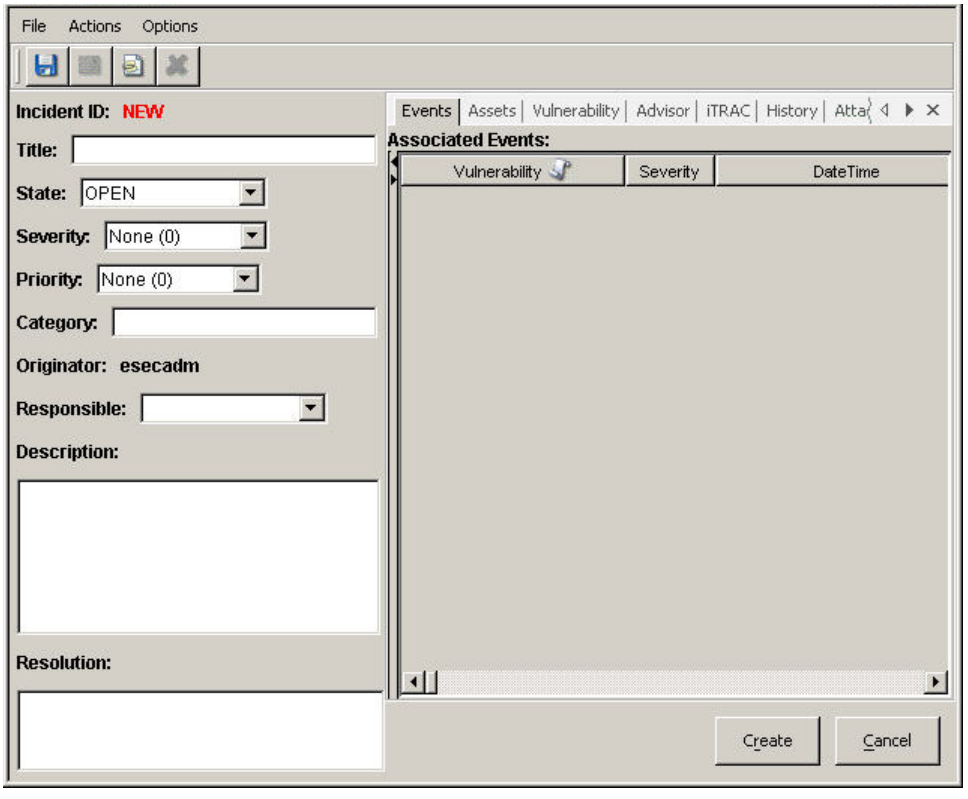
**HINWEIS**: Wenn einem Vorfall Ereignisse hinzugefügt werden, werden die Registerkarten „Bestände“, „Anfälligkeit“ und „Advisor“ durch eine Liste aller Bestands-, Anfälligkeits- oder Advisor-Daten zu den DIP/Destination Host-Namen der zugehörigen Ereignisse ergänzt.

**HINWEIS**: Die Schaltflächen *Hinzufügen* und *Entfernen* auf den Registerkarten „Bestände“, „Anfälligkeit“ und „Advisor“ ermöglichen den Benutzern das manuelle Hinzufügen oder Entfernen von Bestands-, Anfälligkeits- oder Advisor-Daten.

## Erstellen eines Vorfalls

Erstellen eines Vorfalls

1. Klicken Sie auf die Registerkarte *Vorfall*.
2. Klicken Sie auf *Vorfälle* > *Vorfall erstellen* oder klicken Sie auf die Schaltfläche *Neuen Vorfall erstellen*.




Geben Sie Ihre Informationen in die leeren Felder im Dialogfeld „Vorfall erstellen“ ein.

3. Klicken Sie auf *Speichern*.

## Anzeigen und Speichern von Anlagen

So zeigen Sie eine Anlage an

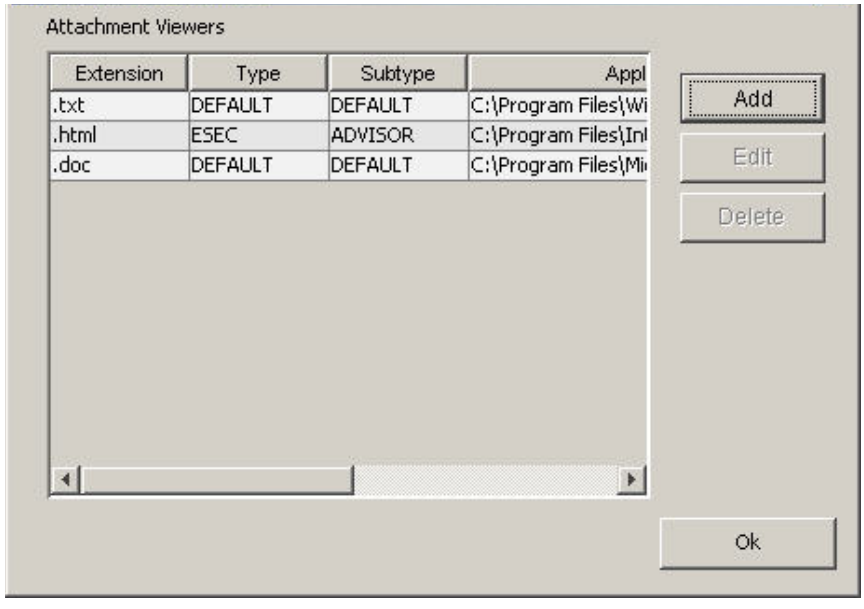
1. Klicken Sie mit der rechten Maustaste auf eine Anlage und dann auf *Anzeigen* oder *Speichern*.

**HINWEIS**: Zum Anzeigen einer Anlage muss ein Anlage-Viewer konfiguriert werden. Wenn eine Anlage nicht zum Öffnen einer Datei konfiguriert ist, wird eine Eingabeaufforderung zur Auswahl des Programms eingeblendet, das zum Öffnen der Datei verwendet werden soll. Anlagedateien werden in der Sentinel-Datenbank gespeichert.

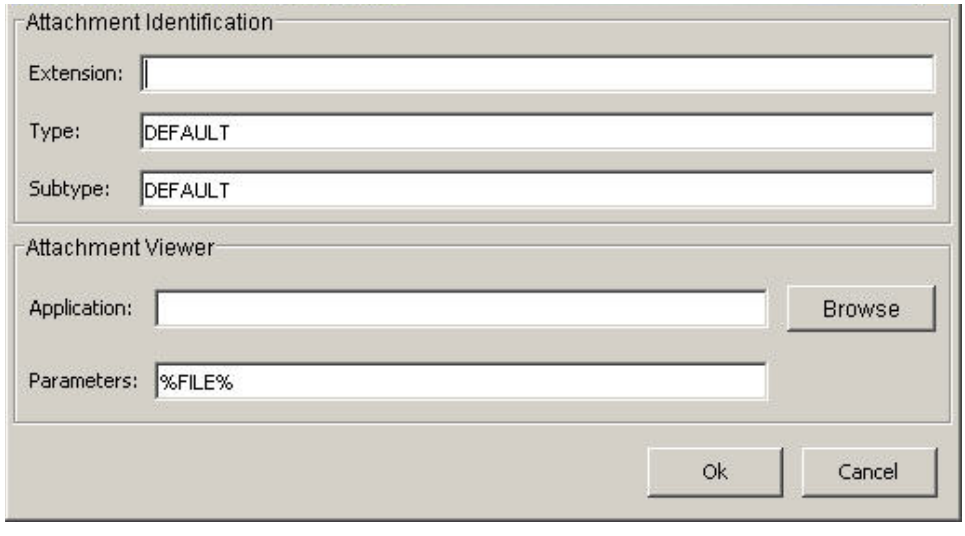
## Konfigurieren des Anlage-Viewer

Konfigurieren des Anlage-Viewer

1. Klicken Sie auf die Registerkarte *Vorfall*.
2. Klicken Sie auf *Vorfälle > Konfiguration des Anlage-Viewer* oder klicken Sie auf die Schaltfläche *Viewer für Anlagen konfigurieren.*




3. Klicken Sie auf *Add* (Hinzufügen).




Geben Sie den Erweiterungstyp ein (z. B. .doc, .xls, .txt, .html usw.) und klicken Sie auf *Durchsuchen* oder geben Sie das Anwendungsprogramm zum Starten dieses Dateityps ein (z. B. notepad.exe für Notepad).

4. Klicken Sie auf *OK*.

## Senden eines Vorfalls per Email

Die Funktion zum Senden von Emails wird während der Installation in der Datei execution.properties eingerichtet. Informationen zum Konfigurieren dieser Datei finden Sie in *Kapitel 11 – Dienstprogramme*.

Senden eines Vorfalls per Email

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Erweitern Sie den Ordner „Vorfälle“ im Navigator, falls verfügbar, oder klicken Sie auf *Vorfälle > Vorfallsliste anzeigen* oder klicken Sie auf die Schaltfläche *Vorfallsliste anzeigen*.

    .
3. Doppelklicken Sie auf den Namen einer *Vorfallsansicht*.
4. Doppelklicken Sie auf einen Vorfall.
5. Klicken Sie auf *Vorfall mailen*  .
6. Geben Sie Folgendes ein:
   - Email-Adresse
   - Email-Betreff
   - Email-Nachricht
7. Klicken Sie auf *OK*. Die Email-Nachricht verfügt über HTML-Anlagen mit Informationen zu den Vorfallsdetails, zu Ereignissen, Beständen, Anfälligkeiten, Advisor-Informationen und zum Vorfallsverlauf.

## Ändern eines Vorfalls

So ändern Sie einen Vorfall

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Klicken Sie auf *Vorfälle > Vorfallsansichts-Manager anzeigen* oder klicken Sie auf die Schaltfläche *Vorfallsansichts-Manager anzeigen.*  .
3. Doppelklicken Sie auf eine Vorfallsansicht.
4. Doppelklicken Sie auf einen Vorfall.
5. Das Fenster „Vorfallsdetails“ wird angezeigt.
6. Sie können die folgenden Felder in einem Vorfall bearbeiten (optional):
   - Titel
   - Status
   - Schweregrad
   - Priorität
   - Kategorie
   - Zuständig
   - Beschreibung
   - Lösung
7. Auf der Registerkarte „Anlagen“ können Sie Anlagen hinzufügen oder entfernen.
8. Klicken Sie auf *Speichern*.

## Löschen eines Vorfalls

**HINWEIS**: Zum Löschen eines Vorfalls, der einem WorkFlow (iTRAC) beigefügt wurde, müssen Sie den iTRAC-Prozess beenden.

So löschen Sie einen Vorfall

1. Klicken Sie auf die Registerkarte *Vorfälle*.
2. Klicken Sie auf *Vorfälle* > *Vorfallsansichts-Manager anzeigen* oder klicken Sie auf die Schaltfläche *Vorfallsansichts-Manager anzeigen*.  .
3. Doppelklicken Sie auf eine Vorfallsansicht.
4. Doppelklicken Sie im Fenster „Vorfallsansicht“ mit der rechten Maustaste auf einen Vorfall und dann auf *Löschen*.

**HINWEIS**: Zum Löschen eines Vorfalls, der einem WorkFlow (iTRAC) beigefügt wurde, müssen Sie den iTRAC-Prozess beenden. Ein iTRAC-Prozess kann mithilfe des Vorgangsansichts-Managers auf der Registerkarte „iTRAC“ beendet werden. Weitere Informationen finden Sie in *Kapitel 5 – Registerkarte „iTRAC“*.

5. Klicken Sie im Bestätigungsfenster auf *Ja*.

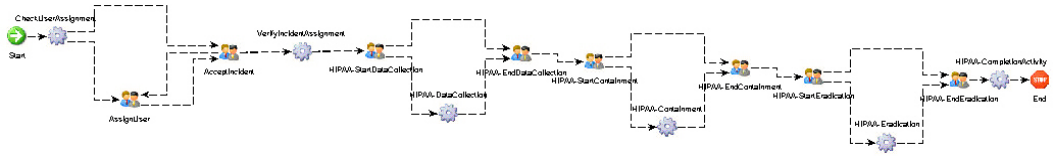
# 5 Registerkarte „iTRAC™“

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

iTRAC (Workflow) umfasst die Automatisierung von Prozeduren und die Möglichkeit, auf Vorfälle zu reagieren. Sentinel stellt ein iTRAC-Management-System bereit, das die Automatisierung von Prozeduren umfasst. An iTRAC ist das Aktivitäts-Framework von Sentinel gebunden. Das Aktivitäts-Framework stellt die Aktivitäten bereit, die in den einzelnen Phasen des iTRAC-Vorgangs automatisch ausgeführt werden können.

Schablonen (Vorgangsdefinitionen) und die Vorgangsausführung ergeben zusammen das Workflow-Management-System.

## Schablonen (Vorgangsdefinition)




Die Schablone ist der Entwurf, der den Ausführungsfluss in iTRAC steuert. Die Schablone umfasst ein Netzwerk von Aktivitäten und deren Beziehungen, Kriterien für den Übergang zwischen den Aktivitäten sowie Informationen zu einzelnen Aktivitäten. Schablonen verfügen über Attribute, die vom Benutzer geändert werden können.

iTRAC ermöglicht den Benutzern das Festlegen von Zeitüberschreitungsattributen für eine iTRAC-Schablone.

Eine Aktivität ist eine logische, unabhängige Arbeitseinheit innerhalb des iTRAC-Vorgangs. Eine Aktivität repräsentiert Arbeit, die entweder von Benutzern/Funktionen (manuelle Aktivität) oder von Computeranwendungen (automatische Aktivitäten) verarbeitet wird.

Aktivitäten verfügen auch über Zeitüberschreitungen. Die Benutzer können die Zeitüberschreitungen für alle manuellen oder automatischen Aktivitäten aktivieren bzw. deaktivieren.

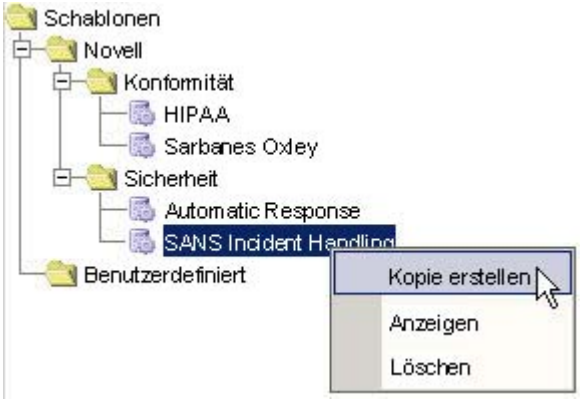
Neben den Zeitüberschreitungsattributen können die Benutzer bei manuellen Aktivitäten auch das Ressourcenattribut konfigurieren, das den Benutzer/die Funktion bestimmt, der bzw. die diese Aktivität ausführt.

Bei automatischen Aktivitäten können die Benutzer neben den Zeitüberschreitungsattributen über das Sentinel-Aktivitäts-Framework auch die automatische Aktivität konfigurieren.

## Schablonen-Manager

iTRAC ermöglicht den Benutzern das Erstellen neuer Schablonen, das Bearbeiten der Vorgangs- und Aktivitätsattribute einer bestehenden Schablone sowie das Löschen von Schablonen über das Schablonen-Manager-Fenster auf der Registerkarte „iTRAC“.

Der Schablonen-Manager kann durch Klicken auf den Schablonen-Manager-Knoten im Navigationsbaum auf der Registerkarte „iTRAC“ geöffnet werden.




## Standardschablonen

iTRAC wird mit vier Standardschablonen bereitgestellt, die automatische und manuelle Aktivitäten umfassen. Die Vorgangs- und Aktivitätsattribute für diese Schablonen wurden auf vordefinierte Werte eingestellt, die von den Benutzern nach Bedarf angepasst werden können. Die Standardschablonen sind:

- HIPAA
- Sarbanes Oxley
- SANS-Vorfallbehandlung
- Automatische Reaktion

### Erstellen neuer Schablonen

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Schablonen-Manager*.
3. Markieren Sie einen vorhandenen Vorgang (HIPAA, Sarbanes-Oxley, SANS oder einen benutzerdefinierten Vorgang), klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Kopie erstellen.*
4. Geben Sie einen Namen ein.
5. Wenn Sie eine Zeitüberschreitung auswählen, müssen Sie eine Email-Adresse und eine Zeit eingeben. Die Zeit wird in Ganzzahlen angegeben. Sie können Minuten, Sekunden, Stunden oder Tage auswählen.
6. Geben Sie eine Beschreibung ein. Unter „Ändern vorhandener Schablonen“ finden Sie Informationen zum Ändern von Vorgangs- und Aktivitätsattributen. Klicken Sie auf *OK* (Hinzufügen).
7. Klicken Sie in der Schablonenanpassung auf *Speichern*.

## Ändern vorhandener Schablonen

Wenn Sie einen Vorgang ändern, können Sie auch die Vorgangsattribute oder die Attribute der Aktivitäten innerhalb des Vorgangs ändern:

Die folgenden Vorgangsattribute können geändert werden:

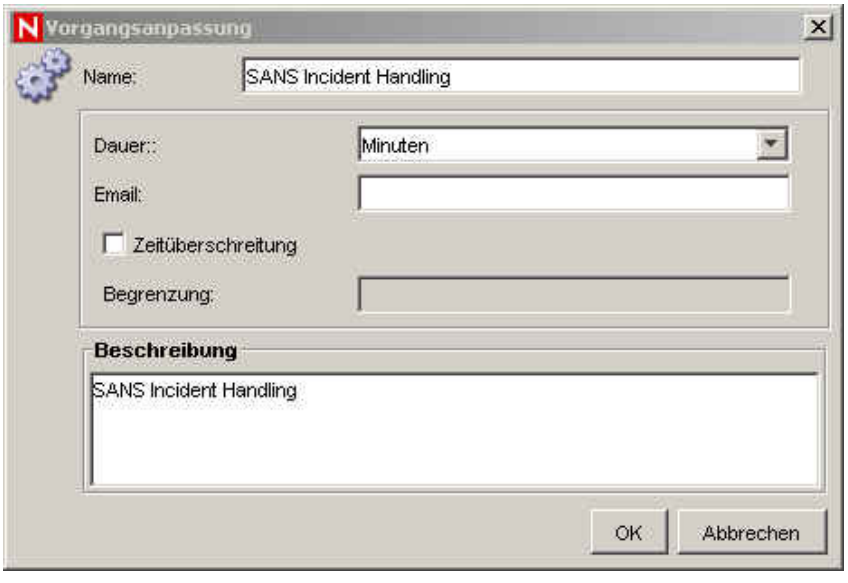
- der Name
- der Zeitraum für die Zeitüberschreitung bzw. ihre Aktivierung/Deaktivierung
- die Beschreibung

## Ändern von Vorgangsattributen

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Schablonen-Manager*.
3. Markieren Sie eine vorhandene Schablone, klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Anzeigen*.

   Klicken Sie im Schablonenfenster auf die Schaltfläche „Vorgangsdetails“.

   
4. Im Dialogfeld „Vorgangsanpassung“ können Sie Folgendes bearbeiten:
   - Name
   - Dauer (Minuten, Sekunden, Stunden oder Tage)
   - Zeitüberschreitung (Ist diese Option aktiviert, müssen Sie eine Email-Adresse und eine Zeit eingeben.)
   - Beschreibung




## Ändern manueller Aktivitäten

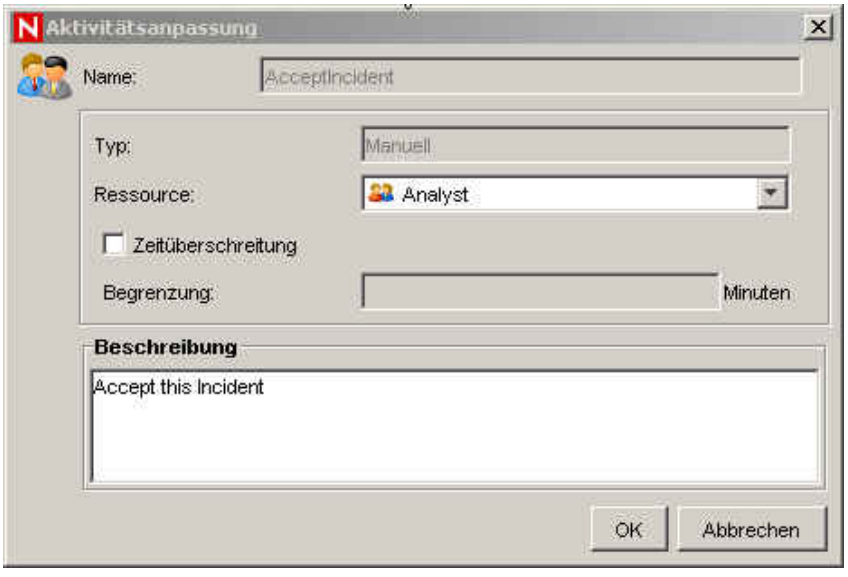
Sie können die Ressource (Benutzer/Funktion), die Zeitüberschreitung und die Beschreibung manueller Aktivitäten bearbeiten.

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Schablonen-Manager*.

3. Markieren Sie eine vorhandene Schablone, klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Anzeigen*.
4. Die Schablone wird in einem separaten Fenster angezeigt.
5. Zum Bearbeiten doppelklicken Sie auf eines der Symbole für eine manuelle Aktivität in der Schablone und nehmen Sie die gewünschten Änderungen vor.

**HINWEIS**: Die folgenden manuellen Aktivitäten in der vorhandenen Schablone können auf diese Weise geändert werden.

- AssignUser
- AcceptIncident
- ConfirmStartDataCollection
- ConfirmEndDataCollection
- ConfirmStartContainment
- ConfirmEndContainment
- ConfirmStartEradication
- ConfirmEndEradication



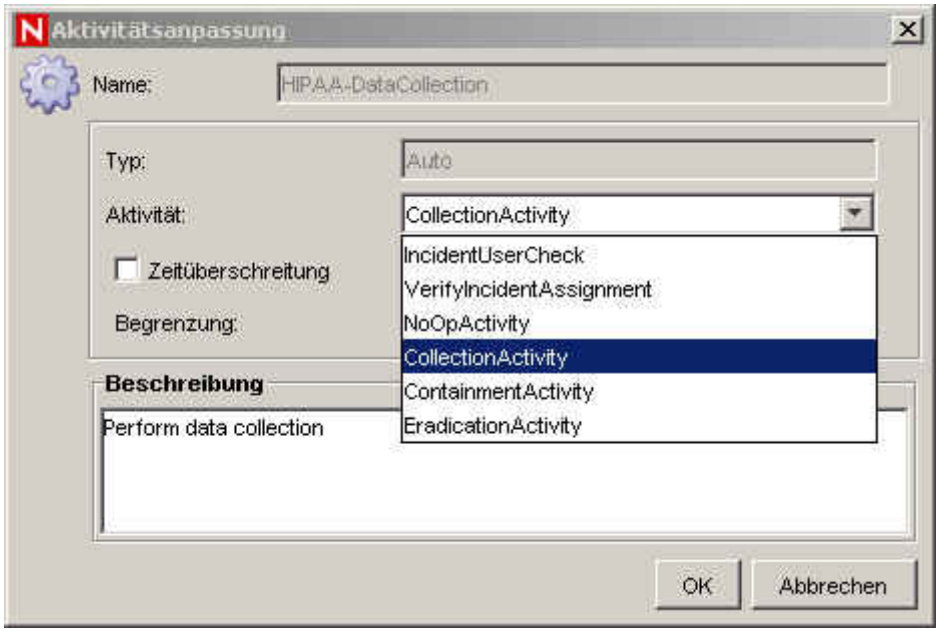

## Ändern automatischer Aktivitäten

Sie können die Aktivität, die Zeitüberschreitung und die Beschreibung einer automatischen Aktivität bearbeiten.

1. Zum Bearbeiten doppelklicken Sie auf eines der Symbole für eine automatische Aktivität in der Schablone und nehmen Sie die gewünschten Änderungen vor.
2. Die Dropdown-Liste im Dialogfeld „Aktivitätsanpassung“ zeigt die Aktivitäten an, die als automatische Aktivitäten verwendet werden können. Die Aktivitäten in der Liste sind Aktivitäten, die unter Verwendung des Aktivitäts-Framework erstellt wurden.

**HINWEIS**: Die folgenden automatischen Aktivitäten in den vorhandenen Schablonen können auf diese Weise geändert werden.

- DataCollection
- Containment
- Eradication




Löschen von Schablonen

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Schablonen-Manager*.
3. Markieren Sie eine vorhandene Schablone, klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Löschen*.
4. Klicken Sie im Popup-Fenster zum Löschen der Schablone auf *Ja*.

# Vorgangsausführung

Bei der Vorgangsausführung handelt es sich um den Zeitraum, während dem der Vorgang ausgeführt wird und Vorgangsinstanzen erstellt und verwaltet werden.

Wenn ein iTRAC-Vorgang auf dem iTRAC-Server ausgeführt oder instanziiert wird, wird vom iTRAC-Server in Übereinstimmung mit der Vorgangsdefinition eine Vorgangsinstanz erstellt, verwaltet und schließlich beendet. Während der Vorgang abläuft und sich seinem Abschluss oder Ende nähert, führt er auf der Grundlage der Kriterien für die Übergänge zwischen den einzelnen Aktivitäten verschiedene Aktivitäten aus, die in der Workflow-Schablone definiert sind. Der iTRAC-Workflow-Server verarbeitet manuelle und automatische Aktivitäten auf unterschiedliche Weise.

Ein iTRAC-Vorgang ist von einem Sentinel-Vorfall abhängig. Eine Vorgangsinstanz kann daher nur vorhanden sein, wenn ein Bezug zu einem Vorfall besteht. Im Gegensatz dazu können auch Vorfälle vorhanden sein, die keinen Bezug zum Workflow-Server aufweisen. Mit einer iTRAC-Vorgangsinstanz kann stets nur ein Vorfall verknüpft sein.

## Instanziieren eines Vorgangs

Ein iTRAC-Vorgang kann durch Verknüpfen eines Vorfalls mit einem iTRAC-Vorgang auf dem iTRAC-Server instanziiert werden. Dies ist auf drei verschiedene Weisen möglich:

- Verknüpfung eines iTRAC-Vorgangs mit einem Vorfall zum Zeitpunkt der Vorfallerstellung
- Verknüpfung eines iTRAC-Vorgangs mit einem Vorfall nach der Vorfallerstellung
- Verknüpfung eines iTRAC-Vorgangs mit einem Vorfall durch Korrelation

Detaillierte Informationen zum Verknüpfen eines Vorgangs mit einem Vorfall finden Sie im Kapitel über die Registerkarte „Vorfälle“.

## Ausführung automatischer Aktivitäten

Wenn die Vorgangsinstanz eine automatische Aktivität ausführt, wird die in der Schablone definierte verknüpfte Aktivität ausgeführt. Die verknüpfte Aktivität ist eine Aktivität, die unter Verwendung des Aktivitäts-Framework erstellt wurde. Der iTRAC-Server führt die Aktivität aus, speichert das Ergebnis in Vorgangsvariablen und geht dann zur nächsten Aktivität in der iTRAC-Schablone über.

Die Aktivität aus dem Aktivitäts-Framework kann beispielsweise darin bestehen, ein Ping an einen Server zu senden und die Ergebnisse dem verknüpften Vorfall beizufügen.

## Ausführung manueller Aktivitäten

Wenn der iTRAC-Server auf eine manuelle Aktivität trifft, sendet er Benachrichtigungen in Form von Arbeitselementen an die zugewiesene Ressource. Wenn es sich bei der zugewiesenen Ressource um einen Benutzer handelt, wird das Arbeitselement nur an diesen Benutzer gesendet. Wenn die Aktivität hingegen einer Funktion zugewiesen wurde, wird an alle Benutzer dieser Funktion ein Arbeitselement gesendet. Der iTRAC-Server wartet dann, bis der Benutzer das Arbeitselement abgeschlossen hat, bevor er mit der nächsten Aktivität fortfährt.

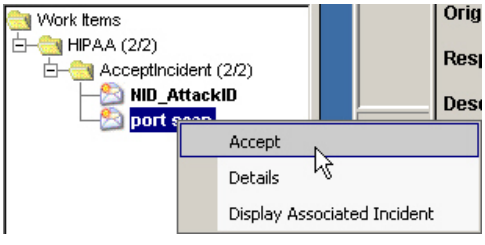
## Arbeitslisten

Die Arbeitselemente werden dem Benutzer über eine Arbeitsliste angezeigt, die Details zu allen Arbeitselementen enthält, die diesem Benutzer zugewiesen sind. Dies ist die Aufgabenliste für den Benutzer.


Die Arbeitsliste kann über jede Registerkarte der Sentinel-Benutzeroberfläche angezeigt werden. Die Arbeitselemente sind nach Vorgang und Aktivität gruppiert. Fett formatierte Arbeitselemente sind jene Arbeitselemente, die noch nicht vom Benutzer akzeptiert wurden.

Die Arbeitsliste ermöglicht den Benutzern die Interaktion mit den einzelnen Arbeitselementen.

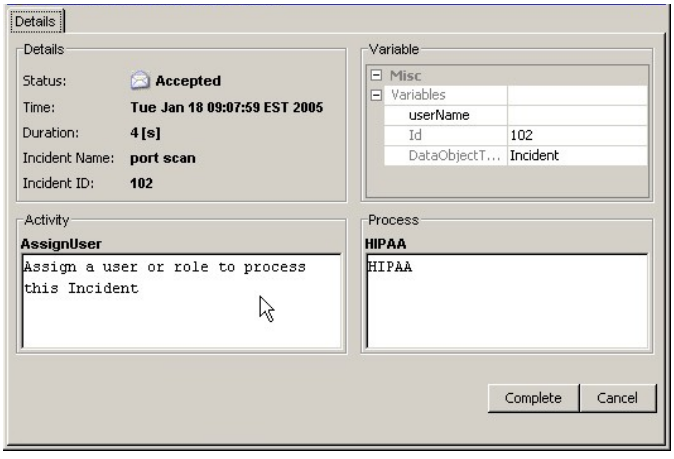
- Die Benutzer können doppelklicken oder mit der rechten Maustaste klicken und dann *Details* wählen, um Arbeitselementdetails anzuzeigen.
- Die Benutzer können mit der rechten Maustaste klicken und dann nicht akzeptierte Arbeitselemente *akzeptieren*.
- Die Benutzer können mit der rechten Maustaste klicken und dann Details zum verknüpften Vorfall *anzeigen*.




## Arbeitselemente

Ein Arbeitselement stellt die Aufgabe dar, die der Benutzer für die aktuell ausgeführte manuelle Aktivität in einem iTRAC-Vorgang ausführen muss. Für die Kontrolle und den Fortschritt des Arbeitselements ist der Benutzer verantwortlich.

Der iTRAC-Server wartet, bis der Benutzer die Aufgabe abgeschlossen hat, bevor er mit der nächsten Aktivität in der Vorgangsinstanz fortfährt.




Das oben abgebildete Dialogfeld mit Arbeitselementdetails enthält die folgenden Informationen:

- Arbeitselementdetails
- Arbeitselementvariablen
- Aktivitätsbeschreibung
- Vorgangsbeschreibung

Die Interaktion mit einem Arbeitselement umfasst drei Schritte:

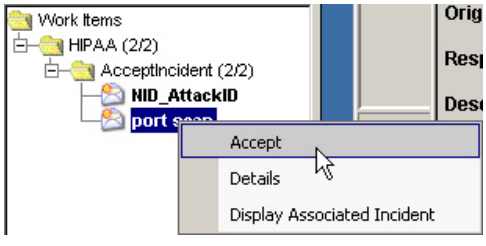
- Akzeptieren eines Arbeitselements
- Aktualisieren der Variablen im Arbeitselement
- Abschließen des Arbeitselements

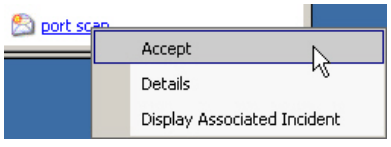
## Akzeptieren eines Arbeitselements

Ein Arbeitselement kann allen Benutzern einer Funktion oder auch nur einem einzelnen Benutzer zugewiesen werden. Ein Arbeitselement muss vom Benutzer akzeptiert werden, bevor dieser eine andere Aktion für das Arbeitselement ausführen kann. Durch das Akzeptieren des Arbeitselements wird der Benutzer zum Eigentümer des Arbeitselements und das Arbeitselement wird aus der Arbeitsliste aller anderen zugewiesenen Benutzer entfernt.

### Akzeptieren von Arbeitselementen

1. Sie können mit der rechten Maustaste auf ein Arbeitselement in der Arbeitsliste klicken und dann die folgenden Aktionen ausführen:



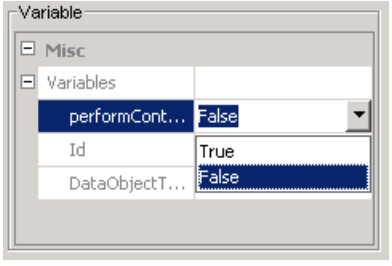

   - Akzeptieren (wenn der Vorgang noch akzeptiert werden muss)
   - Sie können auch das Detailfenster öffnen und darin auf die Schaltfläche „Akzeptieren“ klicken.

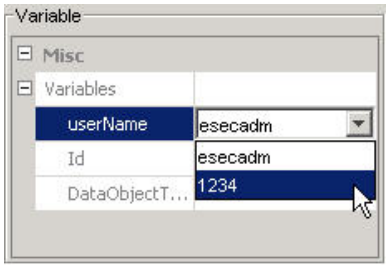
## Aktualisieren der Variablen im Arbeitselement

Der iTRAC-Server verwendet Arbeitselemente, um in Form von Arbeitselementvariablen Informationen von den Benutzern zu erhalten, auf deren Grundlage die nächste Aktivität innerhalb eines Vorgangs bestimmt wird. Der Benutzer kann erst auf die Variablen zugreifen, nachdem er das Arbeitselement akzeptiert hat.

iTRAC unterstützt schreibgeschützte Variablen und aktualisierbare Variablen. Schreibgeschützte Variablen dienen zur Information des Benutzers, beispielsweise über den Status einer Aktivität, die ID eines Vorfalls usw.

Aktualisierbare Variablen dienen zur Annahme von Benutzereingaben. Zurzeit gibt es in iTRAC zwei Arten von aktualisierbaren Variablen: Benutzervariablen und Boolesche Variablen.




Aktualisieren von Variablen

1. Doppelklicken oder klicken Sie mit der rechten Maustaste auf das Arbeitselement, um das Dialogfeld „Details“ anzuzeigen.
2. Nur aktualisierbare Variablen befinden sich im Bearbeitungsmodus. Schreibgeschützte Variablen können nicht bearbeitet werden.
3. Klicken Sie auf das Kombinationsfeld und wählen Sie den passenden Wert aus.

## Abschließen des Arbeitselements

Durch Abschließen des Arbeitselements signalisieren Sie dem iTRAC-Server, dass die Aufgabe ausgeführt wurde. Die aktualisierbaren Variablen aus dem Arbeitselement werden vom Server verarbeitet, um auf der Grundlage bestimmter Kriterien zur nächsten Aktivität zu wechseln. Das Arbeitselement wird aus der Arbeitsliste des Benutzers entfernt. Ein Arbeitselement muss akzeptiert werden, bevor es abgeschlossen werden kann.

Abschließen von Arbeitselementen

1. Klicken Sie mit der rechten Maustaste oder doppelklicken Sie auf das Arbeitselement, das im Dialogfeld „Details“ angezeigt werden soll.

2. Klicken Sie im Dialogfeld auf *Abgeschlossen*.

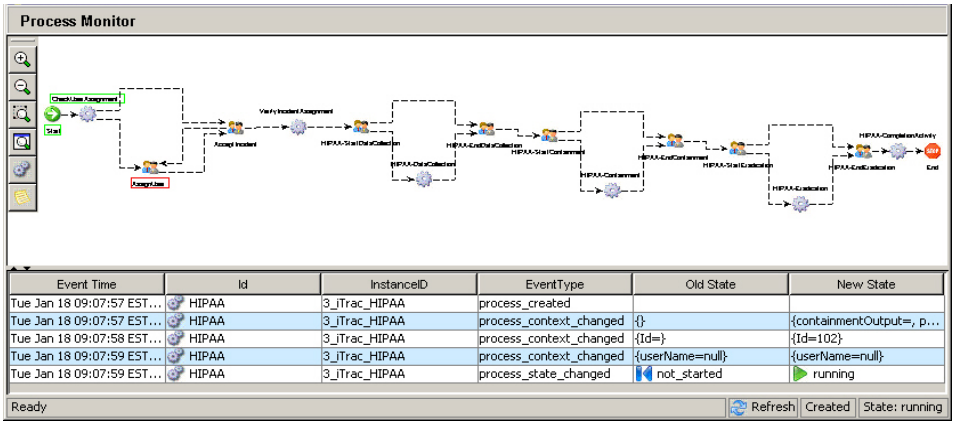
# Vorgangsverwaltung

Die Vorgangsverwaltung ermöglicht Ihnen Folgendes:

- Anzeigen des Status Ihres Vorgangs (Vorgangsmonitor)
- Starten des Vorgangs
- Abschließen des Vorgangs

## Vorgangsmonitor

Die Funktion „Vorgangsmonitor“ dient zur Überwachung des Fortschritts eines Vorgangs. Während die Vorgangsinstanz eine Aktivität nach der anderen ausführt, kann der Benutzer den Fortschritt durch Klicken auf die Schaltfläche „Aktualisieren“ anzeigen. Der Vorgangsmonitor stellt zudem eine Revisionsliste aller Aktionen bereit, die vom iTRAC-Server während der Vorgangsausführung ausgeführt wurden.

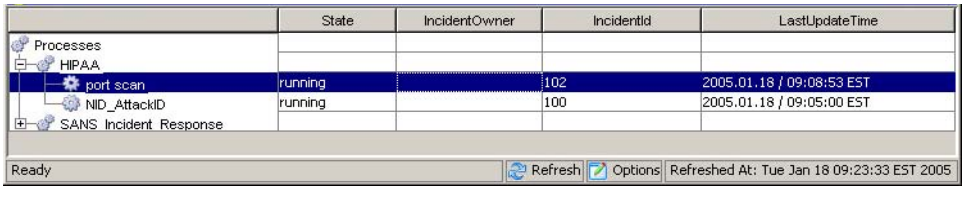


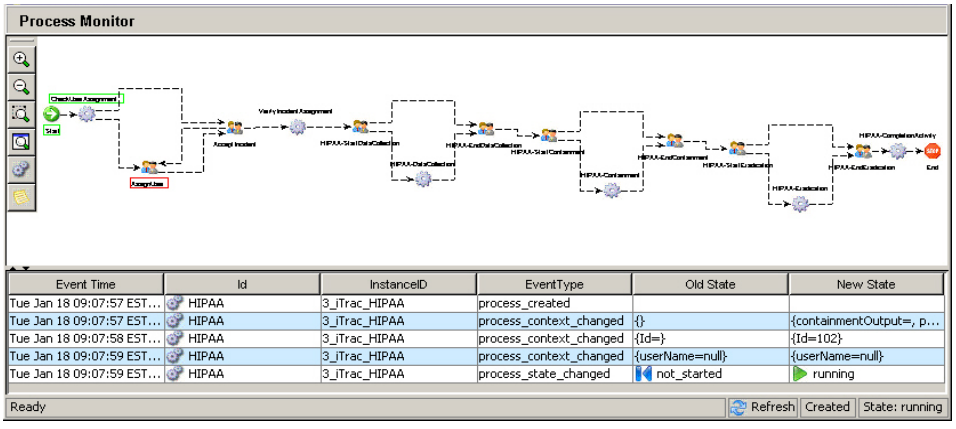

Aktivitäten, die vom Vorgang abgeschlossen wurden, sind durch einen grünen Rahmen gekennzeichnet, während die aktuell ausgeführte Aktivität einen roten Rahmen aufweist.

### Zugriff auf die Vorgangsüberwachung

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie auf die Schaltfläche *Ansichtsoptions-Manager*.

   
3. Doppelklicken Sie auf eine der Standardansichten oder erstellen Sie eine neue Ansicht. Die Standardansichten sind:
   - Alle Vorgänge
   - Vorgänge nach Vorfall
   - Vorgänge nach Status
4. Markieren Sie im aktiven Vorgangs-Manager einen Vorgang und doppelklicken Sie darauf.

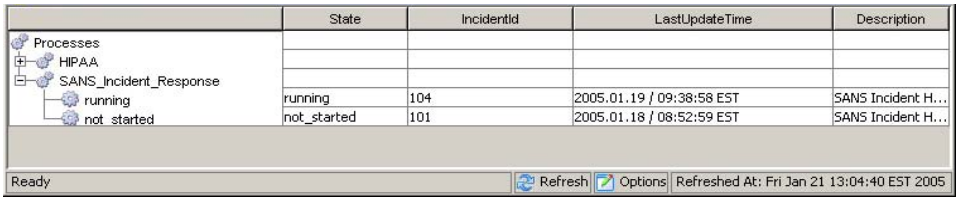





So legen Sie eine Vorgangs-Manager-Option fest

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Doppelklicken Sie auf einen der Vorgänge.
3. Klicken Sie auf die Schaltfläche „Optionen“. In diesem Fenster können Sie auch Folgendes festlegen:
   - Felder...
   - Gruppieren nach...
   - Sortieren...
   - Filter...
   - Baumansicht
4. Klicken Sie auf *Anwenden* und dann auf *Speichern*.

   Nachfolgend sehen Sie eine Ansicht, für die „Baumansicht" auf „Status" eingestellt ist („läuft“ und „nicht gestartet“).




## Starten oder Beenden eines Vorgangs

Starten oder Beenden eines Vorgangs

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie auf die Schaltfläche *Ansichtsoptions-Manager*.

3. Doppelklicken Sie auf eine der Standardansichten oder erstellen Sie eine neue Ansicht. Die Standardansichten sind:
   - Alle Vorgänge
   - Vorgänge nach Vorfall
   - Vorgänge nach Status

4. Markieren Sie im Ansichtsoptions-Manager einen Vorgang, klicken Sie mit der rechten Maustaste und wählen Sie *Vorgang starten* oder *Vorgang beenden*.

# Erstellen einer Aktivität unter Verwendung des Aktivitäts-Framework

## Erstellen einer Aktivität

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung > Aktivitätsverwaltung*.
3. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Neue Aktivität*.
4. Wählen Sie eine der folgenden Optionen:

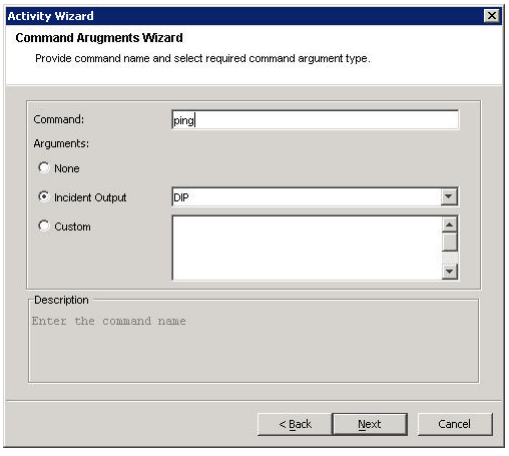

- Befehlsaktivität bei Vorfall – Startet einen bestimmten Befehl mit oder ohne Argumente.

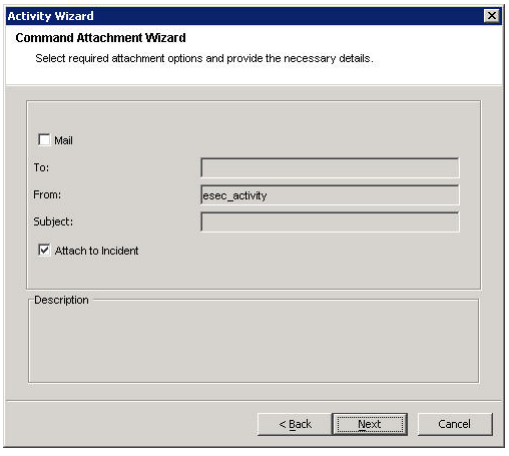
  „Vorfallsausgabe“ gibt die folgenden Argumente aus:

  - DIP
  - DIP:Port
  - Vorfall
  - RT1 (DeviceAttackName)
  - SIP
  - SIP:Port
  - Text

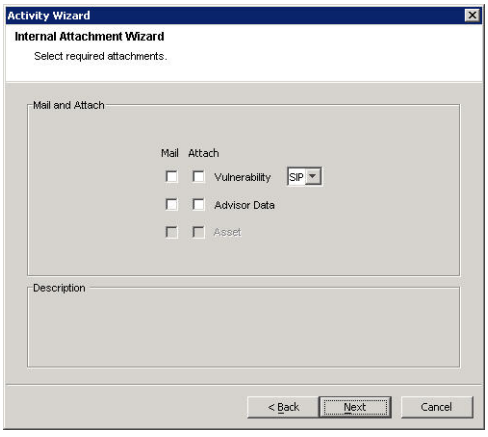
  „Benutzerdefiniert“ ermöglicht Ihnen die Eingabe eigener benutzerdefinierter Argumente.

  Für diese Aktivität können Sie auch festlegen, dass die Ausgabe per Email versendet und/oder dem Vorfall beigefügt wird.

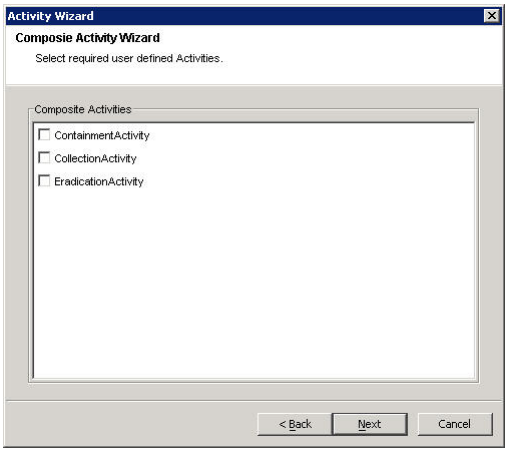


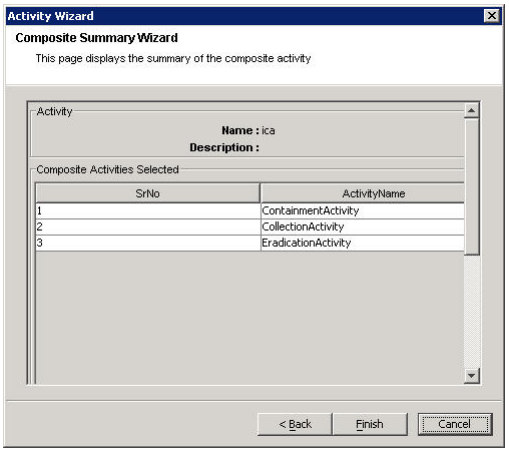



- Interne Aktivität bei Vorfall – Ermöglicht Ihnen das Mailen und/oder Beifügen von Informationen über:
  - Anfälligkeit für (SIP oder DIP)
  - Advisor-Daten
  - Bestand




- Zusammengesetzte Aktivität bei Vorfall – Ermöglicht Ihnen das Erstellen einer Aktivität durch das Kombinieren einer oder mehrerer bestehender Aktivitäten.




## Ändern einer Aktivität

Ändern einer Aktivität

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Aktivitätsverwaltung* > *iTRAC-Aktivitäten*.
3. Doppelklicken Sie auf eine iTRAC-Aktivität. Bearbeiten Sie die Aktivität und klicken Sie auf *OK*.

## Importieren/Exportieren einer Aktivität

Aktivitäten werden als XML-Dateien exportiert. Diese Dateien können aus einem System in ein anderes importiert werden.

### Exportieren einer Aktivität

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Aktivitätsverwaltung*.
3. Klicken Sie mit der rechten Maustaste auf *iTRAC-Aktivitäten* > *Import/Export-Aktivität.*
4. Wählen Sie „Aktivität exportieren“ und klicken Sie auf die Schaltfläche *Durchsuchen*.
5. Wechseln Sie zum Verzeichnis, in dem Sie die exportierte Datei speichern möchten.
6. Benennen Sie die Datei und klicken Sie auf *Exportieren.*
7. Klicken Sie auf *Next* (Weiter).
8. Wählen Sie ein oder mehrere Aktivitäten zum Exportieren aus.
9. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

### Importieren einer Aktivität

1. Klicken Sie auf die Registerkarte *iTRAC*.
2. Klicken Sie im Navigator auf *iTRAC-Verwaltung* > *Aktivitätsverwaltung*.
3. Klicken Sie mit der rechten Maustaste auf *iTRAC-Aktivitäten* > *Import/Export-Aktivität.*
4. Wählen Sie „Aktivität importieren“ und klicken Sie auf die Schaltfläche „Durchsuchen“.
5. Wechseln Sie zu Ihrer Importdatei. Klicken Sie auf *Importieren*.
6. Klicken Sie auf *Next* (Weiter).
7. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.

# 6 Registerkarte „Analyse“

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

Sie müssen über die entsprechende Berechtigung verfügen, um die Registerkarte „Analyse“ verwenden zu können. Wenn Ihnen diese Berechtigung nicht erteilt wurde, verfügen Sie auch nicht über die anderen Berechtigungen zur Durchführung von Aktionen mithilfe dieser Registerkarte.

## Beschreibung

Die Registerkarte „Analyse“ ermöglicht Ihnen das Erstellen von Verlaufsberichten. Verlaufs- und Anfälligkeitsberichte werden auf einem Webserver veröffentlicht. Diese werden direkt mit der Datenbank ausgeführt und auf den Registerkarten „Analyse“ und „Advisor“ in der Navigationsleiste angezeigt.

**HINWEIS**: Crystal Reports® wurde für die Erstellung und Anzeige von Berichten in Sentinel integriert. Der Administrator muss den Standort des Crystal Enterprise Servers konfigurieren, der Berichte im Fenster „Allgemeine Optionen“ auf der Registerkarte „Admin“ veröffentlicht. Im Navigatorfenster befindet sich eine Liste der verfügbaren Berichte.

Zum Ausführen der Berichtsschablonen muss die Crystal Reports Enterprise Edition installiert und das Sentinel Control Center für den Zugrif auf diesen Server konfiguriert sein. Weitere Informationen finden Sie im *Installationshandbuch für Sentinel™ 5*.

Außerdem stehen Beispielberichte im pdf-Format zur Verfügung.

### Top 10-Berichte

Zur Ausführung von Top 10-Berichten muss die Aggregation aktiviert und EventFileRedirectService (in DAS_Binary.xml) muss eingeschaltet sein. Informationen zur Aktivierung der Aggregation finden Sie im *Sentinel-Benutzerhandbuch, Kapitel 10 – Sentinel Data Manager*, im Abschnitt zur Registerkarte „Bericht für Daten“.

#### Aktivieren von EventFileRedirectService für Sentinel Top 10-Berichte

Aktivieren von EventFileRedirectService

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

   Für UNIX:

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

   Für Windows:

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

2. Ändern Sie den Status von EventFileRedirectService auf „on“ (ein).

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

3. Starten Sie unter Windows den Sentinel-Service neu. Starten Sie unter UNIX den DAS-Computer neu.

## Ausführen eines Berichts aus Crystal Reports

So erstellen Sie einen Bericht aus einer Crystal Reports-Schablone

1. Klicken Sie auf die Registerkarte *Analyse*.
2. Klicken Sie im *Analysennavigator* auf einen der verfügbaren Berichte.

**HINWEIS**: Zur Ausführung von Top 10-Berichten muss die Aggregationaktiviert und EventFileRedirectService (in DAS_Binary.xml) muss eingeschaltet sein. Informationen zur Aktivierung der Aggregation finden Sie im *Sentinel-Benutzerhandbuch, Kapitel 10 – Sentinel Data Manager*, im Abschnitt zur Registerkarte „Bericht für Daten“.

3. Klicken Sie auf *Analyse* > *Bericht erstellen* oder klicken Sie auf *Bericht erstellen*.

4. Geben Sie die Informationen in die Schablone ein und klicken Sie auf *Bericht anzeigen*. Der Bericht wird angezeigt.

## Ausführen eines Ereignisabfrageberichts

So erstellen Sie einen Ereignisabfragebericht

1. Klicken Sie auf die Registerkarte *Analyse*.
2. Öffnen Sie den Ordner „Verlaufsberichte“ im Analysennavigator.
3. Klicken Sie auf *Ereignisabfrage*.
4. Klicken Sie auf *Analyse* > *Bericht erstellen* oder klicken Sie auf *Bericht erstellen*.

Ein Ereignisabfragefenster wird geöffnet.

5. Legen Sie Folgendes fest:
   - Zeitrahmen
   - Filter
   - Schweregrad
   - Stapelgröße (Dies ist die Anzahl der angezeigten Ereignisse – ältere Ereignisse werden vor neueren Ereignissen angezeigt.)
6. Klicken Sie auf *Abfrage aktualisieren*.
7. Klicken Sie zum Anzeigen des nächsten Ereignisstapels auf *Weitere Optionen*.
8. Ordnen Sie die Spalten neu an, indem Sie diese ziehen und ablegen, und ändern Sie die Sortierreihenfolge, indem Sie auf die Spaltenüberschrift klicken.
9. Wenn Ihre Abfrage fertig ist, wird sie im Navigator der Liste der Schnellabfragen hinzugefügt.

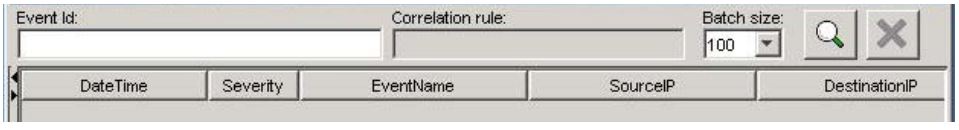
## Ausführen eines in Korrelation stehenden Ereignisberichts

So erstellen Sie einen in Korrelation stehenden Ereignisbericht

1. Klicken Sie auf die Registerkarte *Analyse*.
2. Öffnen Sie den Ordner „Verlaufsberichte“ im Analysennavigator.
3. Klicken Sie auf *In Korrelation stehende Ereignisse*.
4. Klicken Sie auf *Analyse* > *Bericht erstellen* oder klicken Sie auf *Bericht erstellen*.

   Ein in Korrelation stehender Ereignisbericht wird geöffnet.

5. Geben Sie in das Feld „Korrelations-ID“ eine der folgenden Optionen ein:
   - Ereignis-ID-Nummer
   - CorrelatedEventUUID

   **HINWEIS**: CorrelatedEventUUID ist nur in einer Echtzeitereignistabelle verfügbar.

6. Klicken Sie zum Anzeigen des nächsten Ereignisstapels auf *Weitere Optionen*.

# 7 Registerkarte „Advisor“

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

Sie müssen über die entsprechende Berechtigung verfügen, um die Registerkarte „Advisor“ verwenden zu können. Wenn Ihnen diese Berechtigung nicht erteilt wurde, verfügen Sie auch nicht über die anderen Berechtigungen zur Durchführung von Aktionen mithilfe dieser Registerkarte.

Advisor ist ein optionales Modul. Wenn Sie über keine Lizenz für Advisor verfügen und auf die Registerkarte „Advisor“ klicken, werden Sie in einem Benachrichtigungsfenster darauf hingewiesen.

Sentinel Advisor basiert auf SecurityNexus. Advisor bietet Echtzeitintelligenz für Anfälligkeiten von Unternehmen, Expertenrat sowie empfohlene Schritte für die Sanierung. Advisor bietet einen Querverweis zwischen Echtzeit-IDS-Angriffssignaturen und der Advisor Knowledge Base für Anfälligkeiten. Weitere Informationen finden Sie unter http://www.esecurity.net/Software/Products/Advisor.asp.

Der Advisor-Datenfeed umfasst zwei Teile:

- Warnungsdaten: Informationen zu bekannten Sicherheitsanfälligkeiten und Bedrohungen
- Angriffsdaten: Normalisierung von Intrusion Detection-Signaturen und Plugins für Anfälligkeits-Absuchvorgänge

**HINWEIS**: Während der Installation und bis zum ersten Datenfeed von SecurityNexus ist die Kontextmenüfunktion bei Ereignissen (mit ausgefülltem rt1-Feld) für Advisor-Daten nicht voll funktionsfähig.

## Ausführen von Advisor-Berichten

So erstellen Sie einen Advisor-Bericht

1. Klicken Sie auf die Registerkarte „Advisor“.
2. Klicken Sie im Advisor-Navigator auf eine Berichtsschablone.
3. Klicken Sie auf *Advisor > Bericht erstellen.*
4. Geben Sie die Informationen in die Schablone ein und klicken Sie auf *Bericht anzeigen*.

# Eigenständige Installation – Manuelle Aktualisierung von Advisor

Manuelle Aktualisierung des Advisor-Feed

1. Wechseln Sie zur URL //advisor.esecurityinc.com/advisordata/.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
3. Wechseln Sie in den Ordnern „attack“ und „alert“ jeweils zum neuesten Monat und laden Sie die ZIP-Dateien herunter.
4. Speichern Sie die neuen Warnungs- und Attacke-Datenfeed-Dateien (im ZIP-Format) auf Ihrem Computer.

   **HINWEIS**: Speichern Sie die ZIP-Dateien nicht in den Verzeichnissen „attack“ und „alert“.

5. Entpacken Sie die ZIP-Dateien für den Attacke-Datenfeed in das folgende Verzeichnis:

   Für Windows:

   ```
   <Bei der Installation festgelegtes Verzeichnis für
      Advisor-Datendateien>\attack
   ```

   oder

   Für UNIX:

   ```
   <Bei der Installation festgelegtes Verzeichnis für
      Advisor-Datendateien>/attack
   ```

6. Entpacken Sie die ZIP-Dateien für den Warnungs-Datenfeed in das folgende Verzeichnis:

   Für Windows:

   ```
   <Bei der Installation festgelegtes Verzeichnis für
      Advisor-Datendateien>\alert
   ```

   oder

   Für UNIX:

   ```
   <Bei der Installation festgelegtes Verzeichnis für
      Advisor-Datendateien>/alert
   ```

7. Wechseln Sie zu folgendem Verzeichnis:

   Für Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Für UNIX:

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

8. Führen Sie den folgenden Befehl aus:

   Für Windows:

   ```
   advisor.bat
   ```

   Für UNIX:

   ```
   ./advisor.sh
   ```

**HINWEIS:** Die Dateien advisor.sh und advisor.bat aktualisieren die Datenbank und löschen dann die Attacke- und Warnungsdateien, die in die Verzeichnisse „attack“ und „alert“ entpackt wurden.

# Direktes Herunterladen vom Internet – Manuelle Aktualisierung von Advisor

Manuelle Aktualisierung des Advisor-Feed

1. Wechseln Sie zu folgendem Verzeichnis:

   Für Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   Für UNIX:

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

2. Führen Sie den folgenden Befehl aus:

   Für Windows:

   ```
   advisor.bat
   ```

   Für UNIX:

   ```
   ./advisor.sh
   ```

**HINWEIS:** Die Dateien advisor.sh und advisor.bat aktualisieren die Datenbank und löschen dann die Attacke- und Warnungsdateien, die in die Verzeichnisse „attack“ und „alert“ entpackt wurden.

# Ändern des Passworts und der Email-Konfiguration Ihres Advisor-Servers

## Ändern des Passworts Ihres Advisor-Servers (Einzelplatzbetrieb)

Dieses Verfahren gilt nicht für Einzelplatzbetrieb-Konfigurationen.

## Ändern des Passworts Ihres Advisor-Servers (Direktes Herunterladen)

So ändern Sie das Passwort Ihres Advisor-Servers (Direktes Herunterladen)

1. Übermitteln Sie eine Passwortänderung an Novell Technical Support.

2. Nachdem Sie von Novell über die erfolgte Passwortänderung unterrichtet wurden, melden Sie sich unter UNIX als esecadm bzw. unter Windows mit Administratorrechten an.
3. Wechseln Sie in das folgende Verzeichnis:

   Für UNIX:

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

   Für Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

4. Geben Sie die folgenden Befehle ein:

   Für UNIX:

   ```
   ./adv_change_passwd.sh <altespasswort> <neuespasswort>
   ```

   Für Windows:

   ```
   adv_change_passwd.bat <altespasswort> <neuespasswort>
   ```

## Ändern der Email-Konfiguration Ihres Advisor-Servers

So ändern Sie die Email-Konfiguration Ihres Advisor-Servers

1. Melden Sie sich unter UNIX als esecadm bzw. unter Windows mit Administratorrechten an.
2. Wechseln Sie in das folgende Verzeichnis:

   Für UNIX:

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

   Für Windows:

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

3. Öffnen Sie die Dateien alertcontainer.xml und alertcontainer.xml mithilfe eines Texteditors. Nehmen Sie Änderungen am grau markierten Bereich vor.

   ```
   <property
      name="advisor.mail.from">fromNAME@domain.com</prope
      rty>

   <property
      name="advisor.mailto.list">toNAME@domain.com</prope
      rty>
   ```

**HINWEIS**: Wenn Sie mehr als eine Email-Adresse angeben möchten, geben Sie die Email-Adressen durch Kommas getrennt ohne Leerschritte ein.

# Ändern der Datenfeed-Zeit

Die standardmäßigen Datenfeed-Zeiten sind:

- Sechs Stunden: 01:00, 07:00, 13:00 und 19:00 Uhr
- Zwölf Stunden: 02:00 und 14:00 Uhr

So ändern Sie die Datenfeed-Zeiten

1. Melden Sie sich bei Ihrem Advisor-Computer an (unter UNIX als esecadm).
2. So bearbeiten Sie die Datenfeed-Zeiten:

   Für UNIX: Verwenden Sie den Befehl „crontab“.

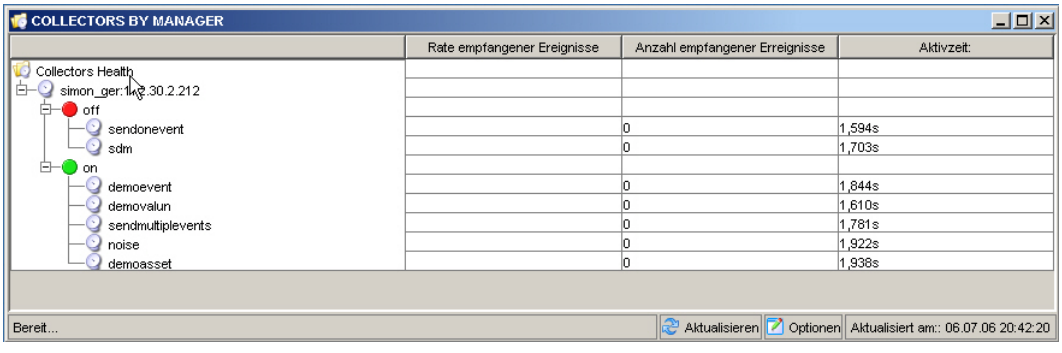
   Für Windows: Verwenden Sie den Befehl „at“.

# 8 Registerkarte „Collectors“

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

Sie müssen über die entsprechende Berechtigung verfügen, um die Registerkarte „Collectors“ verwenden zu können. Auf der Registerkarte „Collectors“ ist die Funktionalität des Wizard nur eingeschränkt verfügbar. Verwenden Sie zur Nutzung der vollen Wizard-Funktionalität den Collector Builder. Auf der Registerkarte „Collectors“ können Sie:

- einen Assistenten-Host überwachen
- einen Collector überwachen
- Collectors starten und stoppen (Collector Manager) für einen ausgewählten Host




## Layout

Das linke Feld auf der Registerkarte „Collectors“ enthält einen Baum mit verschiedenen Ansichten. Im Stamm des Baums befinden sich standardmäßig zwei untergeordnete Objekte: Collector Manager-Ansichten und Collector-Ansicht. Im rechten Feld werden die Ansichten in Tabellenform angezeigt. Jede Ansicht im rechten Feld verfügt über einen Eintrag im Baum auf der linken Seite.

Im rechten Feld werden vier Ansichten angezeigt.

- Collector-Ansicht
  - Collector-Ansichts-Manager
- Collector Manager-Ansicht
  - Ansichts-Manager für Collector Manager

Die Collector-Ansicht zeigt Informationen zu Collectors und die Collector Manager-Ansicht zeigt Informationen zu Collector-Managern an. Jede Ansicht wird als Baumtabelle angezeigt: die Objekte sind anhand eines oder mehrerer Attribute gruppiert. Die Konfiguration der Ansicht kann angepasst werden. Die Optionen einer Ansicht können geändert und neue Ansichtstypen hinzugefügt werden. Die Ansichtskonfiguration wird in einem Ansichts-Manager (Collector-Ansichts-Manager oder Ansichts-Manager für Collector Manager) angezeigt.

Wenn die Registerkarte angezeigt wird, enthält der Baum im linken Feld zunächst die beiden Ansichts-Manager und der Collector-Ansichts-Manager wird im rechten Feld angezeigt.

Der Collector-Ansichts-Manager verfügt standardmäßig über drei vorkonfigurierte Ansichtsoptionen und Sie können neue Optionen erstellen. Die drei Ansichtsoptionen sind: „Alle Collectors“, „Collectors nach Manager“ und „Collectors nach Status“.

Die Ansicht „Alle Collectors“ zeigt alle Collectors gruppiert nach dem Manager, in dem sie ausgeführt werden, an.

Der Ansichts-Manager von Collector Manager gruppiert alle Collectors nach ihrem Manager und zudem nach ihrem Status („Ein“ oder „Aus“) innerhalb der einzelnen Manager.

Die Ansicht „Collectors nach Status“ gruppiert alle Collectors nach ihrem Status („Ein“ oder „Aus“) und zudem innerhalb der einzelnen Status nach ihrem Manager.

Zum Anzeigen von Collector Managern gibt es eine Standardansicht, die Ansicht „Alle Manager“. Sie zeigt alle aktiven Collector Manager im System ohne Gruppierung an.

# Überwachen eines Collectors

Im Fenster „Wizard-Hosts“ können Sie standardmäßig Folgendes überwachen:

**Ansichts-Manager für Collector Manager**

- StartTime — Zeitpunkt, zu dem der Collector Manager gestartet wurde, angegeben in mm/tt/jj hh:mm:ss und Zeitzone
- UpTime — Dauer der Ausführung des Collector Managers, angegeben in Tagen, Stunden, Minuten und Sekunden
- EventReceivedCount — Anzahl der Ereignisse, die der Collector Manager seit seinem Start von allen Collectors erhalten hat
- EventReceivedRate — Durchschnittliche Ereignisrate pro Sekunde, die der Collector Manager in der letzten Minute erhalten hat

**Collector-Ansichts-Manager**

- Status — „Ein“ oder „Aus“
- EventsReceivedRate — Durchschnittliche Ereignisrate pro Sekunde, die der Collector-Port in der letzten Minute erhalten hat
- EventsReceivedCount — Anzahl der Ereignisse, die der Collector-Port seit seinem Start erhalten hat
- UpTime — Dauer der Ausführung des Collector-Ports, angegeben in Stunden, Minuten und Sekunden

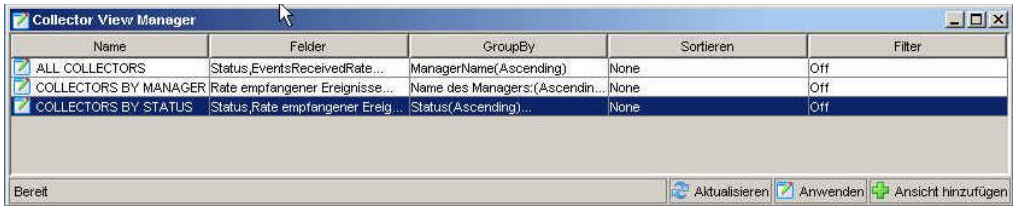
Sie können eigene Ansichten erstellen, die zusätzliche oder weniger Felder aufweisen.

## Überwachen eines Wizard-Host

Überwachen eines Wizard-Hostt

1. Klicken Sie auf die Registerkarte „Collectors“.
2. Klicken Sie auf *Ansichts-Manager für Collector Manager*.

3. Wählen Sie eine Ansichtsoption durch Doppelklicken auf eine Ansicht aus oder erstellen Sie eine neue Ansicht. Ein Wizard-Host-Fenster wird angezeigt.




## Erstellen einer Collector-Ansicht

Erstellen einer Collector-Ansicht

1. Klicken Sie auf die Registerkarte *Collectors*.
2. Klicken Sie auf *Ansichts-Manager für Collector Manager*.

3. Klicken Sie auf *Ansicht hinzufügen*, um eine neue Ansicht zu erstellen.
   - Geben Sie Ihren Optionsnamen ein.
   - Klicken Sie auf *Felder*, um festzulegen, welche Felder angezeigt werden sollen.
   - Klicken Sie auf die Schaltfläche *Gruppieren nach*, um verschiedene Titel zu gruppieren.
   - Klicken Sie auf *Sortieren*, um eine Sortierung nach Titeln vorzunehmen.
   - Klicken Sie auf die Schaltfläche *Filter*, um einen Filter anzuwenden.

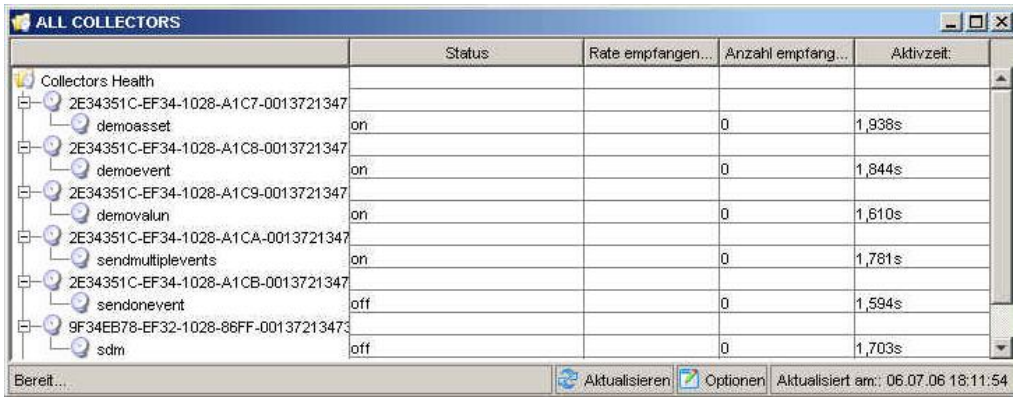
   Nachfolgend sehen Sie eine Ansicht, für die „Gruppieren nach“ auf „ManagerUUID“ eingestellt ist und die nach Version sortiert ist.

## Ändern einer Collector-Ansicht

Ändern einer Collector-Ansicht

1. Öffnen Sie den Collector-Ansichts-Manager.
2. Doppelklicken Sie auf einen der Namen.
3. Klicken Sie auf *Optionen*. In diesem Fenster können Sie auch Folgendes festlegen:
   - Felder...
   - Gruppieren nach...
   - Sortieren...
   - Filter...
   - Baumansicht
4. Klicken Sie auf *Anwenden* und dann auf *Speichern*.

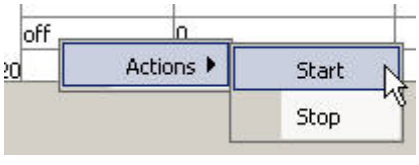
   Nachfolgend sehen Sie eine Ansicht, für die „Baumansicht“ auf „Manager-UUID“ eingestellt ist.




## Stoppen und Starten von Collectors sowie Anzeigen von Details

Stoppen und Starten von Collectors sowie Anzeigen von Details

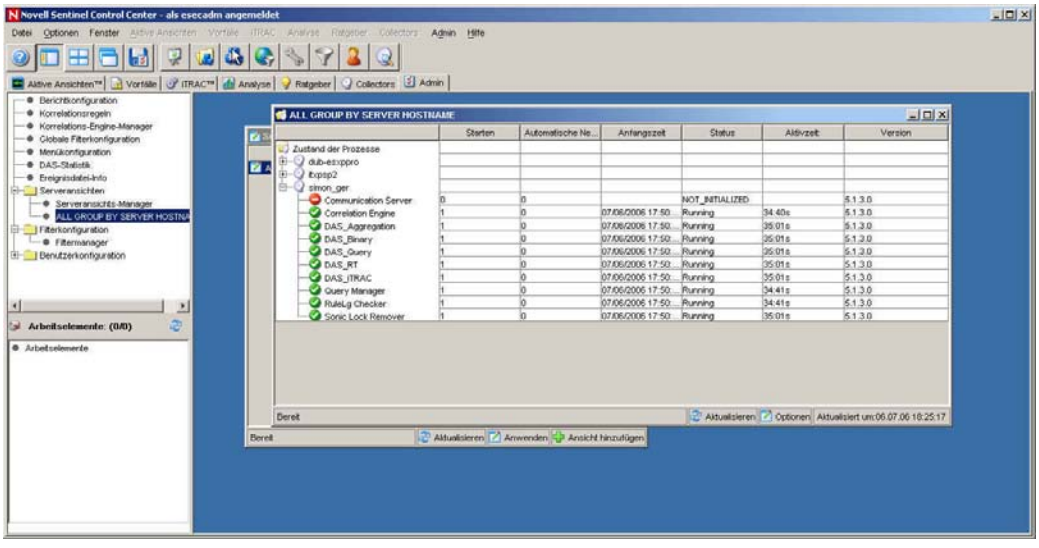
1. Klicken Sie auf die Registerkarte *Collectors*.
2. Öffnen Sie einen Collector-Ansichts-Manager.
3. Zum Stoppen und Starten eines Collectors sowie zum Anzeigen von Details klicken Sie mit der rechten Maustaste auf einen *Collector* und dann auf *Aktionen* > *Starten* oder *Stoppen*.



# 9 Registerkarte „Admin“

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

Zur Verwendung dieser Funktion müssen Sie über die entsprechende Berechtigung verfügen. Wenn Ihnen diese Berechtigung nicht erteilt wurde, verfügen Sie auch nicht über die anderen Berechtigungen zur Durchführung von Aktionen mithilfe dieser Registerkarte.




## Registerkarte „Admin“ – Beschreibung

Über die Registerkarte „Admin“ erhalten Sie Zugriff auf:

- die Berichtkonfiguration für Analysen- und Advisor-Berichte
- Filter verwalten
- das Arbeiten mit Korrelationsregeln von Sentinel
- das Menü zum Konfigurieren der Menükonfiguration
- DAS-Statistiken
- Ereignisdatei-Informationen
- Serveransichten
- die Benutzerkontenkonfiguration

# Berichtkonfigurationsoptionen für Analysen- und Advisor-Berichte

So konfigurieren Sie die URL für Analysen- und Advisor-Berichte

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie im *Admin-Navigator* auf *Berichtkonfiguration*.
3. Klicken Sie im Fenster *Berichtkonfiguration* auf *Bearbeiten*.
   - Geben Sie in das Feld „Analyse-URL“ die URL für den Crystal Enterprise Server ein und klicken Sie auf *Aktualisieren*.

     ```
     http://<IP>/GetReports.asp?APS=<IP>&user=Guest&passwor
        d=&tab=Analysis
     ```

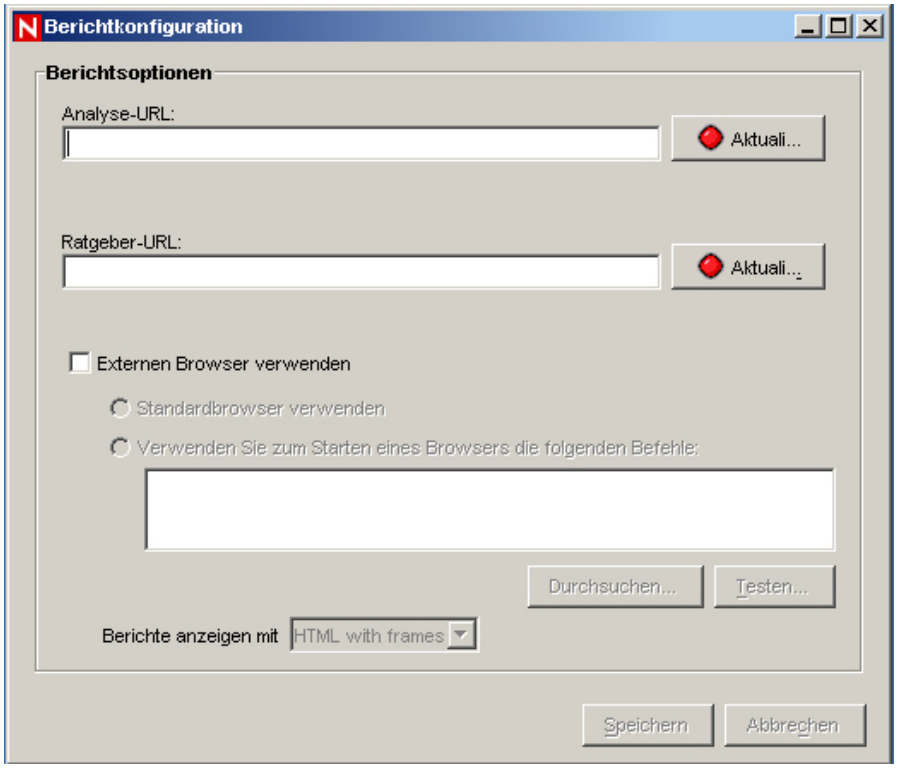
**HINWEIS**: <IP> ist die IP-Adresse des Crystal Enterprise Servers.

   - Geben Sie in das Feld „Advisor-URL“ die URL für den Crystal Enterprise Server ein und klicken Sie auf *Aktualisieren*.

     ```
     http://<IP>/GetReports.asp?ASP=<IP>&user=Guest&passwor
        d=&tab=Advisor
     ```

**HINWEIS**: <IP> ist die IP-Adresse des Crystal Enterprise Servers.

Weitere Informationen finden Sie im *Installationshandbuch*.



Die Option für externe Browser ermöglicht Ihnen die Verwendung Ihres Standardbrowsers oder eines anderen Browsers. Wenn Sie anstelle des Standardbrowsers einen anderen Browser verwenden, muss Ihre Befehlszeile mit %URL% enden. Beispiel:

```
C:\Programme\Internet Explorer\IEXPLORE.EXE %URL%
```

4. Warten Sie, bis die Schaltfläche „Aktualisieren“ grün wird, und klicken Sie dann auf *Speichern*. Sie müssen sich vom Sentinel Control Center ab- und dann wieder anmelden.

# Sentinel-Korrelationsregeln

Die Korrelation bietet mehr Intelligenz bei der Verwaltung von Sicherheitsereignissen, indem sie es Ihnen ermöglicht, die Analyse des eingehenden Ereignisstreams zu automatisieren, um Muster von Interesse zu entdecken. 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.

Regelordner sind eine logische Gruppierung von Korrelationsregeln. Das Gruppieren von Korrelationsregeln in Regelordnern ermöglicht Ihnen zudem die Verwendung eines Satzes von Regeln, die an Werktagen ausgeführt werden, oder eines Satzes, der nachts ausgeführt wird, und eines weiteren Satzes, der am Wochenende ausgeführt wird. Dies bedeutet im Wesentlichen, dass Sie je nach Tageszeit verschiedene Aktivitäten überwachen können.

Sie können beispielsweise alle Korrelationsregeln, die tagsüber ausgeführt werden sollen, von Montag bis Freitag um 8 Uhr starten und gleichzeitig die Korrelationsregeln, die nachts ausgeführt werden, deaktivieren. Wenn es nicht nötig ist, dass die Korrelationsregeln in Regelordnern gruppiert werden, können Sie auch nur einen Regelordner erstellen und dann alle Korrelationsregeln in diesem Ordner erstellen.

Die Anzahl der Benutzer, die auf Korrelationsregeln zugreifen können, ist nicht beschränkt. Wenn mehrere Benutzer dieselbe Regel gleichzeitig bearbeiten, werden alle vorherigen Änderungen durch die Änderung des zuletzt speichernden Benutzers überschrieben.

In diesem Abschnitt werden folgende Themen behandelt:



**HINWEIS**: Null-Werte (leere Werte) können nicht korreliert werden.

## Regelordner und Regeln

Die Beziehung zwischen Regelordnern und Regeln ist, wie nachfolgend beschrieben, definiert. Regelordner und Regeln werden im Fenster „Korrelationsregeln“ hierarchisch angezeigt.

- Ein Regelordner kann leer sein oder mehrere Regeln enthalten.
- Die Anzahl der Regelordner und Regeln ist nur durch den verfügbaren Speicherplatz beschränkt.

- Durch Doppelklicken auf einen Regelordner wird der Regeleditor für diesen Korrelationsregeltyp angezeigt.
- Für Regelordnernamen gilt eine Längenbeschränkung von 255 Zeichen für den Pfad und 255 Zeichen für den Regelnamen.
- Regelordner- und Regelbeschreibungen können bis zu 1024 Zeichen lang sein.

## Korrelationsregeltypen

Beim Definieren von Regeln stehen Ihnen vier Korrelationsregeltypen zur Auswahl. Hierbei handelt es sich um:

- Beobachtungsliste
- Grundlegende Korrelation
- Erweiterte Korrelation
- FreeForm RuleLg

---

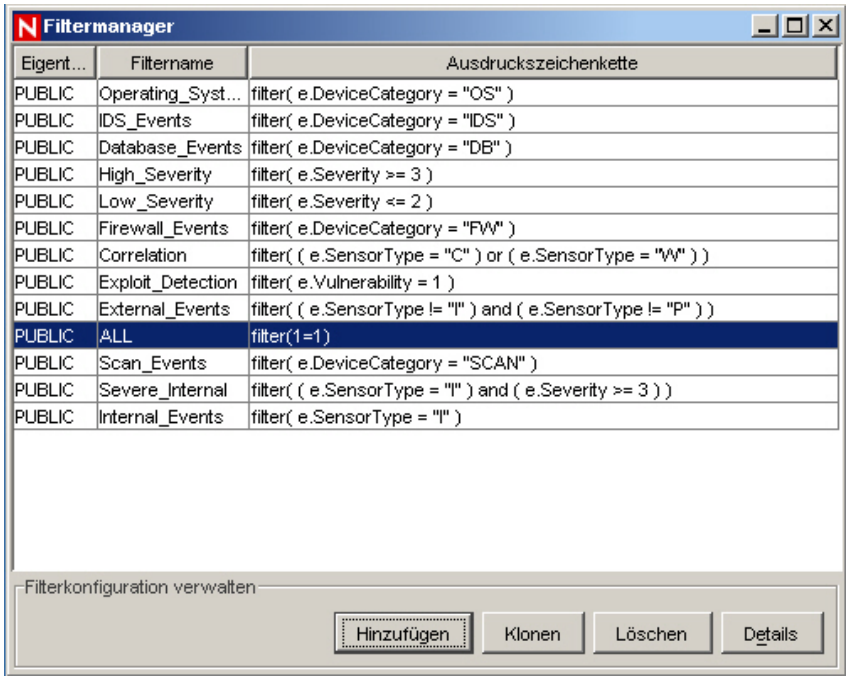
**ACHTUNG:** Sie sollten mit der RuleLg-Sprache für die Definition von Korrelationsregeln vertraut sein, bevor Sie diesen Korrelationsregeltyp verwenden. Falls Sie ein Tag umbenannt haben, sollte darüber hinaus zum Erstellen einer Korrelationsregel nicht der ursprüngliche Name verwendet werden.

---

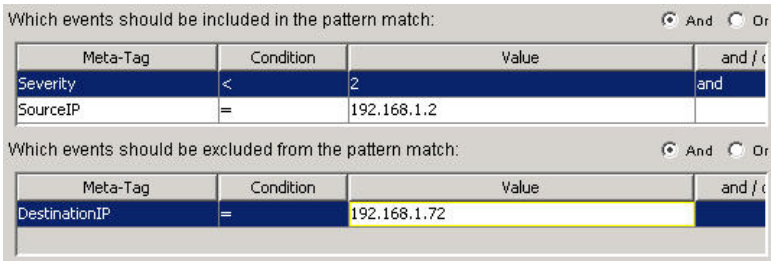
### Beobachtungsliste

Es kann aus vier unterschiedlichen Filtertypen ausgewählt werden. Hierbei handelt es sich um:

- Alle zulassen – Lässt alle Ereignisse durch.
- Muster – Alle regulären Ausdrücke mit einer Grep-Syntax.
- Filter-Manager – Eine Dropdown-Liste, die den Filter-Manager anzeigt, um einen neuen Filter auszuwählen oder zu erstellen.



- Editor – Erstellen von Kriterien zum Einschließen oder Ausschließen von Ereignissen auf Grundlage boolescher Algebra. Es sind zwei Bereiche verfügbar (zum Einschließen und zum Ausschließen). Geben Sie Ihre Werte hier ein. Beispiel:




## Grundlegende Korrelation

Es kann aus vier unterschiedlichen Filtertypen ausgewählt werden. Hierbei handelt es sich um:

- Alle zulassen – Lässt alle Ereignisse durch.
- Muster – Alle regulären Ausdrücke mit einer Grep-Syntax.
- Filter-Manager – Eine Dropdown-Liste, die den Filter-Manager anzeigt, um einen neuen Filter auszuwählen oder zu erstellen.
- Editor – Erstellen von Kriterien zum Einschließen oder Ausschließen von Ereignissen auf Grundlage boolescher Algebra.

Mithilfe dieser Regel können Sie zählen, wie häufig bestimmte Bedingungen innerhalb eines bestimmten Zeitrahmens erfüllt werden.

Beispielsweise kann mit einer grundlegenden Korrelationsregel nach derselben Quellen-IP-Adresse gesucht werden, die innerhalb von 5 Minuten fünfmal gemeldet wurde, auch wenn die Ereignisse über verschiedene Geräte (z. B. IDS (Intrusion Detection System) und Firewall) gemeldet werden.

## Erweiterte Korrelation

Es kann aus vier unterschiedlichen Filtertypen ausgewählt werden. Hierbei handelt es sich um:

- Alle zulassen – Lässt alle Ereignisse durch.
- Muster – Alle regulären Ausdrücke mit einer Grep-Syntax.
- Filter-Manager – Eine Dropdown-Liste, die den Filter-Manager anzeigt, um einen neuen Filter auszuwählen oder zu erstellen.
- Editor – Erstellen von Kriterien zum Einschließen oder Ausschließen von Ereignissen auf Grundlage boolescher Algebra.

Diese Regel ermöglicht Ihnen Folgendes:

- Zählen, wie häufig bestimmte Bedingungen innerhalb eines bestimmten Zeitrahmens erfüllt werden.
- Alle Funktionen einer einfachen Korrelationsregel einbeziehen und Ereignisse mit früheren Ereignissen abgleichen.

Beispielsweise kann mit einer erweiterten Korrelationsregel nach Ereignissen gesucht werden, die von derselben Quellen-IP-Adresse zu derselben Ziel-IP-Adresse erfolgten, denselben Ereignisnamen aufweisen und innerhalb und außerhalb der Firewall aufgetreten sind. (Dies bedeutet, dass möglicherweise ein Angriff durch die Firewall gelangen konnte.)

### FreeForm RuleLg-Korrelation

Mit der RuleLg-Sprache für die Definition von Korrelationsregeln können Sie die Definition von Korrelationsregeln selbstständig steuern. Sie sollten mit der RuleLg-Sprache für die Definition der Korrelationsregel vertraut sein, bevor Sie diesen Korrelationsregeltyp verwenden.

## Correlation Engine-Regelbereitstellung

Zur Verwendung dieser Funktion müssen Sie über die Berechtigung zum Starten/Stoppen der Correlation Engine verfügen. Die Correlation Engine befindet sich stets in einem von zwei möglichen Status: „Aktiviert“ oder „Deaktiviert“. Das Symbol spiegelt den aktuellen Status wider.

- Aktiviert – 
- Deaktiviert – 

Wenn die Correlation Engine aktiviert ist, verarbeitet sie aktive Korrelationsregelordner.

Wenn die Correlation Engine deaktiviert ist, bleiben all ihre Daten aus dem Arbeitsspeicher erhalten und es werden keine neuen korrelierten Ereignisse generiert. Dieser Status entspricht der Deaktivierung aller Regelordner. Die Deaktivierung der Correlation Engine hat keinerlei Auswirkungen auf die anderen Teile des Systems. Eingehende Ereignisse werden weiterhin empfangen und in der Sentinel-Datenbank gespeichert.

## Importieren und Exportieren von Korrelationsregeln

Die Exportfunktion ermöglicht Sentinel das Erstellen und Exportieren von Korrelationsregeln für den Import in Ihr System. Diese XML-Dokumente sind speziell für die Correlation Engine formatiert. Diese vorgefertigten Regeln werden von Sentinel erstellt und sind im Kundenportal unter http://www.esecurityinc.com verfügbar.

Die Funktion zum Exportieren von Regeln als XML-Dokumente ist hilfreich, wenn Sie Novell zur Fehlersuche in Ihren Korrelationsregeln einsetzen möchten. Das Exportieren ist zudem von Vorteil, wenn Sie über einen Sentinel für die Produktion und über einen Sentinel für die Entwicklung verfügen. Korrelationsregeln können in einer Entwicklungsumgebung entwickelt und getestet und dann in eine Produktionsumgebung exportiert werden. Die Dateierweiterung für exportierte Korrelationsregeln ist .crf.

## Funktion der Datenbank beim Speichern von Korrelationsregeln

Wenn Sie die Correlation Engine (einen Sentinel Server-Vorgang) im Sentinel Control Center aktivieren, ruft diese die Bereitstellungsinformationen und -regeln von der Datenbank ab. Wenn Sie Korrelationsregeln ändern und dann speichern, werden sie zur Speicherung an die Datenbank gesendet. Die Correlation Engine spiegelt die Änderungen an der Regel nur wider, wenn eine der folgenden Bedingungen erfüllt wird:

- die bereitgestellte Regel wird deaktiviert und dann wieder aktiviert
- die Regel wird neu bereitgestellt

Wenn Sie Bereitstellungsregeln ändern und dann speichern, werden sie zur Speicherung an die Datenbank gesendet und an die Correlation Engine übermittelt, wo sie angewendet werden.

## Logische Bedingungen für Korrelationsregeln

Die folgenden logischen Bedingungen werden bei der Erstellung von Korrelationsregeln verwendet. Weitere Informationen zu META-Tags finden Sie im *Sentinel-Referenzhandbuch für Benutzer*.

| Bedingung | Feldtyp | Beschreibung |
|---|---|---|
| = | Numerisch Zeichenkette | Der Inhalt des ausgewählten META-Tag ist gleich dem eingegebenen Wert. |
| != | Numerisch Zeichenkette | Der Inhalt des ausgewählten META-Tag ist nicht gleich dem eingegebenen Wert. |
| < | Numerisch | Der Inhalt der ausgewählten Eigenschaft ist kleiner als der eingegebene Wert. |
| > | Numerisch | Der Inhalt des ausgewählten META-Tag ist größer als der eingegebene Wert. |
| <= | Numerisch | Der Inhalt des ausgewählten META-Tag ist kleiner als oder gleich dem eingegebenen Wert. |
| >= | Numerisch | Der Inhalt des ausgewählten META-Tag ist größer als oder gleich dem eingegebenen Wert. |
| =META-Tag | Numerisch Zeichenkette | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist gleich dem Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| !=META-Tag | Numerisch Zeichenkette | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist nicht gleich dem Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| <META-Tag | Numerisch | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist kleiner als der Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| >META-Tag | Numerisch | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist größer als der Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| <=META-Tag | Numerisch | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist kleiner als oder gleich dem Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| >=META-Tag | Numerisch | Der Inhalt des in der Dropdown-Liste auf der linken Seite ausgewählten META-Tag ist größer als oder gleich dem Inhalt des auf der rechten Seite des Ausdrucks ausgewählten META-Tag. |
| =regex | Numerisch Zeichenkette | Verwendet einen Punkt (.) und ein Sternchen (*) mit der Zeichenkette für den Wert. |
| subnet | Numerisch Zeichenkette | Eine „match subnet“-Operation ergibt eine Übereinstimmung, wenn sich die verglichene IP-Adresse in jenem Teilnetz befindet, das in der „match subnet“-Operation angegeben ist. |

## Öffnen des Fensters „Korrelationsregeln“

Das Fenster „Korrelationsregeln“ bietet Ihnen folgende Optionen:

- Neuer Ordner – Dient zum Erstellen eines neuen Regelordners.
- Neue Regel – Dient zum Erstellen einer Regel für einen Regelordner.
- Regelordner kopieren – Ermöglicht Ihnen das Ändern von kopierten Regelordnern oder Regeln während der Speicherung des ursprünglichen Regelordners oder der ursprünglichen Regel.
- Regelordner oder Regel löschen – Gelöschte Regelordner oder Regeln können nach Bestätigung des Löschvorgangs nicht wiederhergestellt werden.
- Umbenennen – Dient zum Umbenennen einer Regel oder eines Regelordners.
- Regelordner importieren – Öffnet ein Browserfenster.
- Regelordner exportieren – Öffnet ein Browserfenster zum Exportieren des Regelordners als XML-Datei.
- Bearbeiten – Ermöglicht das Bearbeiten der Regel- und Ordnereigenschaften sowie das Anzeigen in einer Vorschau.

Öffnen des Fensters „Korrelationsregeln“

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie im *Admin-Navigator* auf *Korrelationsregeln*.

## Kopieren und Erstellen eines Regelordners oder einer Regel

Erstellen eines Regelordners

1. Öffnen Sie das Fenster „Korrelationsregeln“.
2. Wählen Sie den übergeordneten Ordner aus, in dem der neue Ordner erstellt werden soll.
3. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Neuer Ordner*.
4. Geben Sie für den Regelordner einen Namen mit maximal 255 Zeichen und ohne Punkte ein. Die Groß- und Kleinschreibung muss beachtet werden.
5. (Optional) Geben Sie für die Regel eine Beschreibung mit maximal 1024 Zeichen ein.
6. Klicken Sie auf *OK*.

Erstellen einer Regel

1. Wählen Sie den übergeordneten Ordner aus, in dem die neue Regel erstellt werden soll.
2. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Neue Regel*.

3. Der Regelassistent wird geöffnet. Wählen Sie einen der folgenden Regeltypen aus:
   - Beobachtungsliste
   - Grundlegende Korrelation
   - Erweiterte Korrelation
   - Ohne Formatvorgabe

   **HINWEIS:** Beschreibungen der Regeltypen finden Sie im Abschnitt Korrelationsregeltypen.
4. Klicken Sie auf *Fertig stellen*.

## Löschen eines Korrelationsregelordners oder einer Regel

Löschen eines Korrelationsregelordners oder einer Regel

1. Öffnen Sie das Fenster „Korrelationsregeln“.
2. Wählen Sie den Regelordner oder die Regel aus, den bzw. die Sie löschen möchten.
3. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Löschen*.
4. Ein Bestätigungsfenster wird angezeigt:
   - Ja – Beim Löschen eines Regelordners werden die Regeln in diesem Regelordner ebenfalls gelöscht. Eine gelöschte Regel kann nicht wiederhergestellt werden, nachdem Sie auf *OK* geklickt haben.
   - Nein – Sie kehren zum Fenster „Korrelationsregeln“ zurück.

## Importieren oder Exportieren eines Korrelationsregelordners

Importieren oder Exportieren eines Korrelationsregelordners

1. Öffnen Sie das Fenster „Korrelationsregeln“.
2. Wählen Sie einen Regelordner aus.
3. Klicken Sie mit der rechten Maustaste und wählen Sie *Regelordner importieren* oder *Regelordner exportieren*.
   - Importieren – Ein Dateibrowser wird geöffnet. Wechseln Sie zum Regelordner, den Sie importieren möchten, und klicken Sie auf *OK*.
   - Exportieren – Ein Dateibrowser wird geöffnet. Wechseln Sie zum Zielgerät, auf dem der Regelordner gespeichert werden soll, und klicken Sie auf *OK*. Der Regelordner wird als CRF-Datei exportiert.

## Bearbeitung im Fenster „Korrelationsregeln“

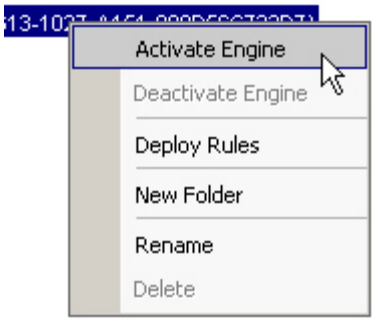
Bearbeitung im Fenster „Korrelationsregeln“

1. Öffnen Sie das Fenster „Korrelationsregeln“.
2. Klicken Sie mit der rechten Maustaste und klicken Sie dann auf *Bearbeiten*.
3. Bearbeiten Sie die Regel und klicken Sie auf *Fertig stellen*.

## Aktivieren oder Deaktivieren einer Correlation Engine

Aktivieren oder Deaktivieren einer Correlation Engine

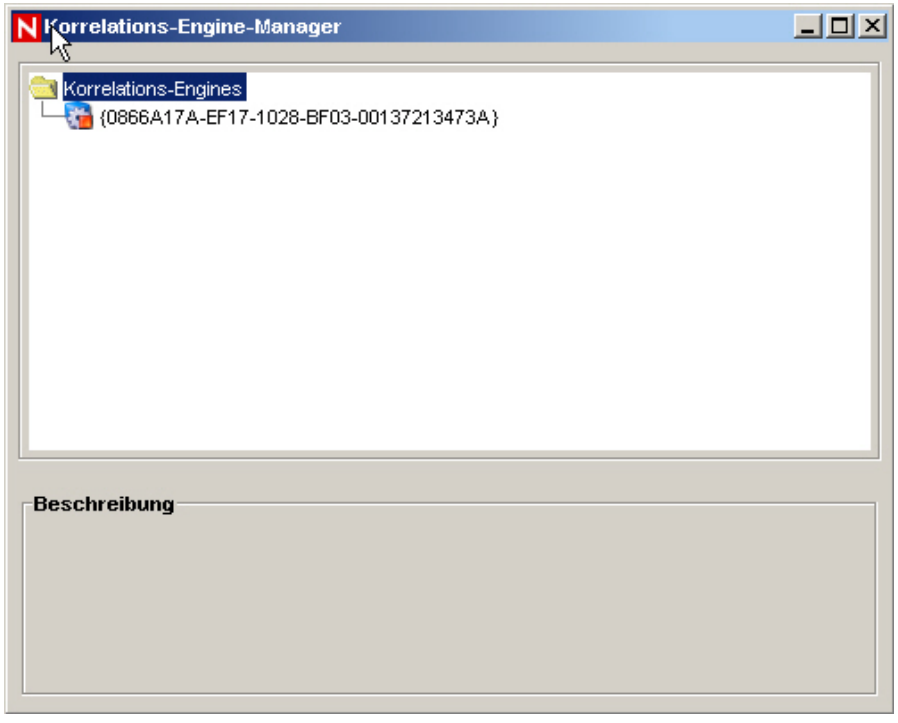
1. Öffnen Sie das Fenster „Correlation Engine-Manager“.
2. Markieren und klicken Sie mit der rechten Maustaste auf eine Correlation Engine und klicken Sie dann auf *Engine aktivieren* oder *Engine deaktivieren*.



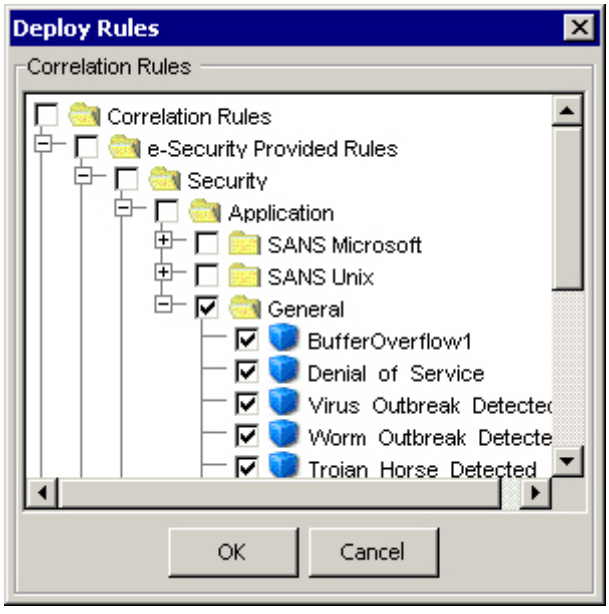

## Bereitstellen von Korrelationsregeln

Bereitstellen von Korrelationsregeln

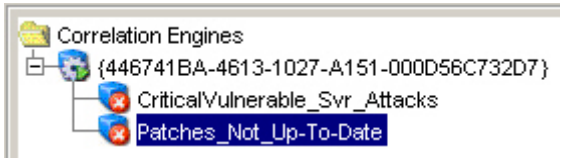
1. Öffnen Sie das Fenster „Correlation Engine-Manager“.




2. Klicken Sie mit der rechten Maustaste (auf einen beliebigen Ordner im Fenster oder markieren Sie die Engine, um die Regel dort bereitzustellen) und klicken Sie dann auf *Bereitstellungsregeln*.
3. Platzieren Sie ein Häkchen neben den Regeln, die Sie bereitstellen möchten. Klicken Sie auf *OK*.

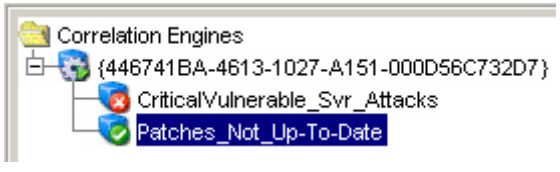



4. Zum Starten der Regel müssen Sie die Regel unter eine Correlation Engine verschieben.




**HINWEIS**: Regeln werden aktiviert bereitgestellt.

5. Markieren Sie Ihre Regel unter der Correlation Engine und klicken Sie mit der rechten Maustaste auf *Regel aktivieren*.



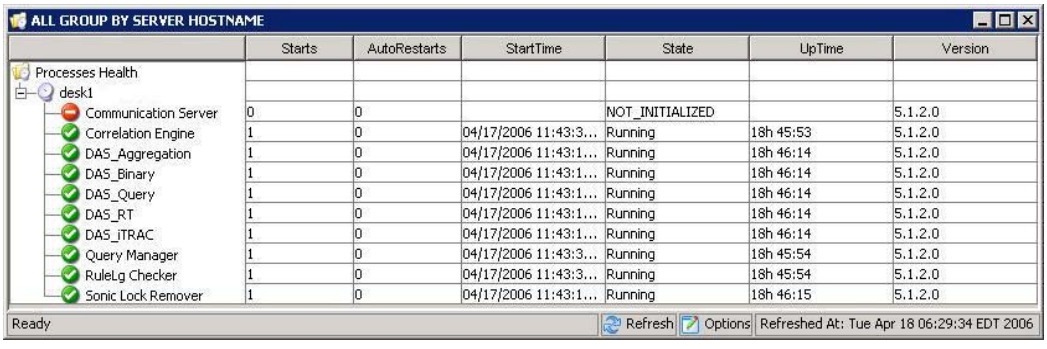

# Serveransichten

Mithilfe der Serveransichten können Sie:

- den Status sämtlicher Sentinel Server-Vorgänge im System überwachen
  - Communication Server
  - Correlation Engine
  - DAS_Binary
  - DAS_iTrac
  - DAS_Query
  - DAS_RT
  - Query Manager
  - RuleLg Checker
  - Sonic Lock Remover

**HINWEIS**: Unter Windows wird der Communication Server-Prozess (für den Kommunikationsserver) als Windows-Service ausgeführt und kann folglich über die Serveransicht nicht überwacht werden. Wenn Sie den Communication Server-Vorgang unter Windows überwachen möchten, verwenden Sie den Windows-Dienst-Manager.

Der Sonic Lock Remover-Prozess ist nur unter Windows aktiviert. Wenn ein Prozess auf einem bestimmten Server nicht aktiviert ist, enthält die zugehörige Aktiviert-Spalte den Wert 0 und in der zugehörigen Status-Spalte wird NOT_INITIALIZED angezeigt.




- Prozesse starten, stoppen oder neu starten – Wenn Sie diese Aktion für einen Prozess ausführen möchten, klicken Sie mit der rechten Maustaste auf den Prozesseintrag.

**HINWEIS**: Die durch Klicken mit der rechten Maustaste zu aktivierenden Aktionen für den Communication Server-Prozess sind nicht aktiviert, da durch das Stoppen des Communication Server-Prozesses (also des Kommunikationsservers) der Kontakt mit allen Prozessen unterbrochen würde.

Im Kontext der *Serveransicht* sind die Begriffe *Starten* und *Automatische Neustarts* wie folgt definiert:

- Starten – Gibt an, wie oft der Vorgang gestartet wurde (unabhängig vom Grund). Diese Zahl umfasst sowohl Starts, die vom Benutzer über die Benutzeroberfläche initialisiert wurden, als auch automatische Starts.
- Automatische Neustarts – Gibt an, wie oft der Vorgang automatisch neu gestartet wurde. Da diese Zahl nur völlig automatische Neustart-Szenarios umfasst, werden von einem Benutzer initialisierte Neustarts nicht berücksichtigt. Dieses Feld ist hilfreich, um zu ermitteln, ob der Vorgang beendet (z. B. aufgrund eines Fehlers) und von Sentinel Watchdog automatisch neu gestartet wurde.

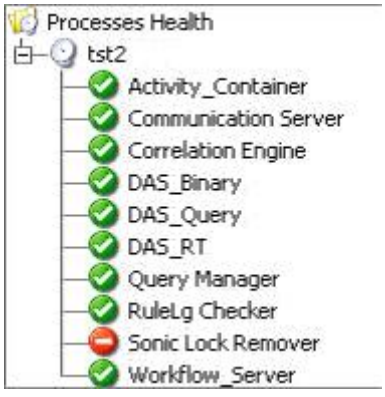
## Überwachen eines Vorgangs

Überwachen eines Vorgangs

6. Klicken Sie auf die Registerkarte *Admin*.
7. Klicken Sie auf *Serveransichten*.

8. Doppelklicken Sie auf eine Ansicht. Eine Ansicht wird angezeigt.

9. Erweitern Sie die Serveransicht. Es werden alle Prozesse aufgelistet.




## Erstellen einer Serveransicht

Erstellen einer Serveransicht

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie auf *Serveransichten*.

3. Klicken Sie auf *Ansicht hinzufügen*, um eine neue Ansicht zu erstellen.
   - Geben Sie Ihren Optionsnamen ein.
   - Klicken Sie auf *Felder*, um festzulegen, welche Felder angezeigt werden sollen.
   - Klicken Sie auf die Schaltfläche *Gruppieren nach*, um verschiedene Titel zu gruppieren.
   - Klicken Sie auf *Sortieren*, um eine Sortierung nach Titeln vorzunehmen.
   - Klicken Sie auf die Schaltfläche *Filter*, um einen Filter anzuwenden.
4. Klicken Sie auf *OK* und dann auf *Speichern*.

## Starten, Stoppen und Neustarten von Vorgängen

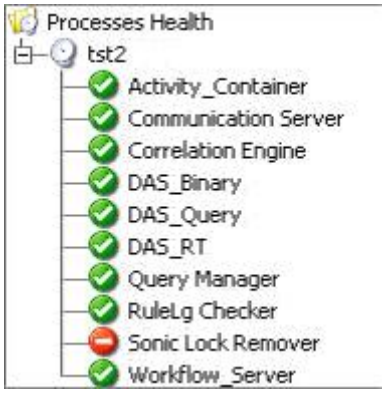
Der Kommunikationsserver kann nicht über diese Funktion gestoppt werden.

Starten, Stoppen und Neustarten von Vorgängen

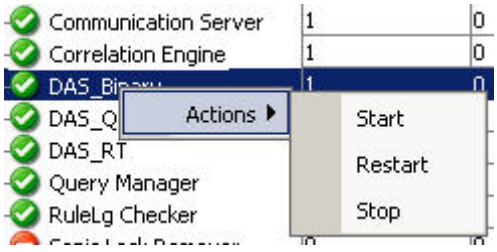
1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie auf *Serveransichten*.

3. Doppelklicken Sie auf eine Ansicht. Eine Ansicht wird angezeigt.

4. Erweitern Sie die Serveransicht. Es werden alle Prozesse aufgelistet.




5. Wählen Sie einen Prozess aus, klicken Sie mit der rechten Maustaste, klicken Sie auf *Aktionen* und wählen Sie eine Funktion aus (*Starten*, *Neu starten* oder *Stoppen*).




# Filter

Mithilfe von Filtern können Daten auf der Grundlage spezifischer Kriterien verarbeitet werden. Dies gilt für Ereignisse in Echtzeit sowie für Benutzer des Systems. Filter ermöglichen Ihnen die Verwaltung von Daten aus dem Sentinel Control Center. Die Filter-Engine steuert die Fenster für Echtzeitereignisse durch Beibehaltung der Datenstruktur für jeden Sicherheitsfilter. Filter verhindern, dass Benutzer unautorisierte Ereignisse anzeigen, und sortieren Ereignisse aus, die die Benutzer nicht anzeigen möchten. Filter werden auf der Registerkarte „Admin“ im Sentinel Control Center erstellt.

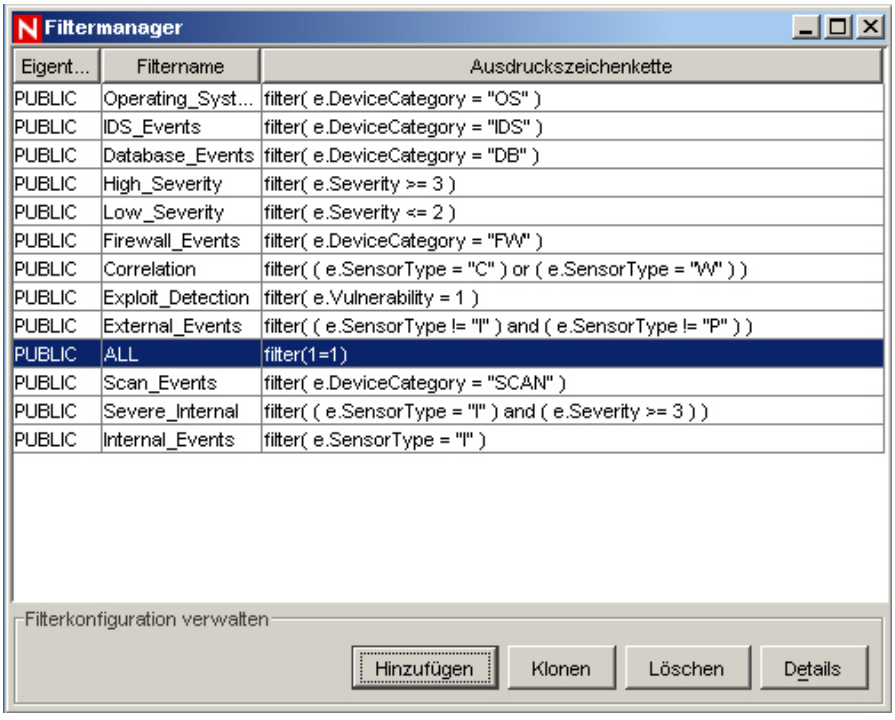
**HINWEIS**: Die folgenden Zeichen sind in Filternamen nicht zulässig:
$ # . * & : < >.

Es gibt drei Filtertypen:

- Öffentliche Filter
- Private Filter
- Globale Filter

## Öffentliche Filter

Öffentliche Filter sind systemeigen. Öffentliche Filter können als Sicherheits- oder als Anzeigefilter verwendet werden. Sicherheitsfilter richten sich nach den Benutzerberechtigungen. Anzeigefilter bestimmen, welche Ereignisse in den Echtzeit-Tabellen, Grafiken und Diagrammen dargestellt werden.




## Private Filter

Private Filter sind im Besitz des jeweiligen Benutzers. Private Filter sind Anzeigefilter. Sie können diese Filter freigeben, wenn Sie über die Berechtigung zum Anzeigen privater Filter verfügen.

## Globale Filter

Globale Filter gehören zur Klasse der öffentlichen Filter. Globale Filter werden im Collector Manager für jedes Ereignis sequenziell verarbeitet, bis eine Übereinstimmung gefunden wird. Die Auswertung der globalen Filter wird für dieses Ereignis gestoppt und die übereinstimmende globale Filteraktion wird für dieses Ereignis verwendet. Die Auswertung der globalen Filter erfolgt von oben nach unten, wie in der Console dargestellt. Sie können nach Bedarf aktiviert oder deaktiviert werden.

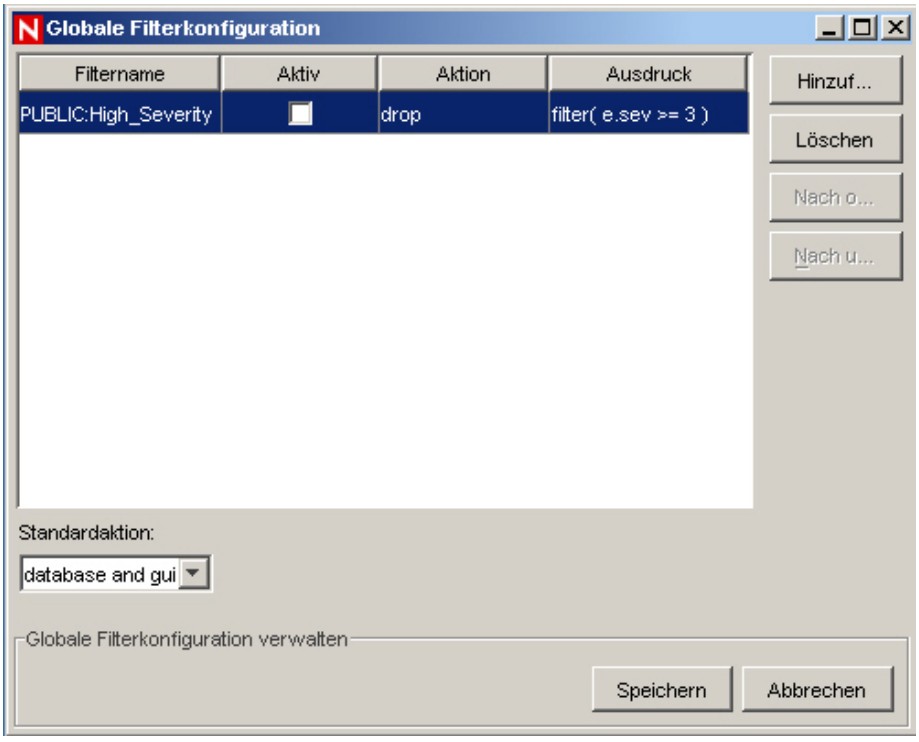
Globale Filter bewirken Folgendes:

- Sie aktivieren eine globale Aktion für Ereignisse, wie beispielsweise das Verwerfen von Ereignissen, die Weiterleitung von Ereignissen ausschließlich an die Datenbank oder die Weiterleitung von Ereignissen an die Datenbank und an das Sentinel Control Center.
- Sie werden vom Collector Manager des Assistenten verarbeitet.
- Sie werden auf der Registerkarte „Admin“ unter der Option „Globale Filterkonfiguration“ konfiguriert. Dort können sie aktiviert und deaktiviert werden.
- Sie verwerfen Ereignisse.

- Sie können Ereignisse ausschließlich an die Datenbank weiterleiten.
- Sie können Ereignisse an die Datenbank und an das Sentinel Control Center weiterleiten.

Über das Fenster „Globale Filterkonfiguration“ können Sie:

- Erstellen eines globalen Filters
- Neuanordnen globaler Filter
- Löschen eines globalen Filters




## Erstellen eines globalen Filters

Erstellen eines globalen Filters

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie auf *Admin* > *Globale Filterkonfiguration* oder wählen Sie *Globale Filterkonfiguration* im Navigationsbaum.
3. Klicken Sie im Fenster „Globale Filterkonfiguration“ auf *Bearbeiten* und dann auf *Hinzufügen*.
4. Klicken Sie in der neuen leeren Zeile auf die Spalte *Filtername*.
5. Wählen Sie einen Filter aus und klicken Sie auf *Auswählen* oder *Hinzufügen* (wenn Sie einen Filter erstellen möchten).
6. Klicken Sie in der Spalte „Aktiv“ auf das Feld *Aktiv*.
7. Wählen Sie in der Spalte „Aktion“ die Aktion aus, die der globale Filter bei Ereignissen ausführen soll, die diesem globalen Filter entsprechen. Wenn ein Ereignis keinem der aktiven globalen Filter entspricht, bestimmt die Standardaktion, wie mit dem Ereignis verfahren wird.

   Das Feld „Standardaktion“ kann die folgenden Einstellungen aufweisen:

   - Verwerfen – Die Ereignisse werden nicht an das Sentinel Control Center oder die Sentinel Server-Datenbank weitergeleitet.

- Datenbank – Die Ereignisse werden direkt an die Datenbank gesendet. Das Sentinel Control Center wird umgangen.
- Datenbank und GUI – Die Ereignisse werden an das Sentinel Control Center und die Sentinel Server-Datenbank gesendet.

8. Fahren Sie mit dem Hinzufügen von Filtern fort, bis Sie fertig sind.
9. Klicken Sie auf *Speichern*.

### Neuanordnen globaler Filter

Neuanordnen globaler Filter

1. Klicken Sie im Fenster „Globale Filterkonfiguration“ auf *Bearbeiten*.
2. Wählen Sie einen Filter aus und klicken Sie auf *Nach oben* oder *Nach unten*, um ihn in der Liste an eine andere Position zu verschieben.
3. Klicken Sie auf *Speichern*.

### Löschen eines globalen Filters

**HINWEIS:** Beim Löschen eines globalen Filters wird keine Bestätigungsmeldung angezeigt.

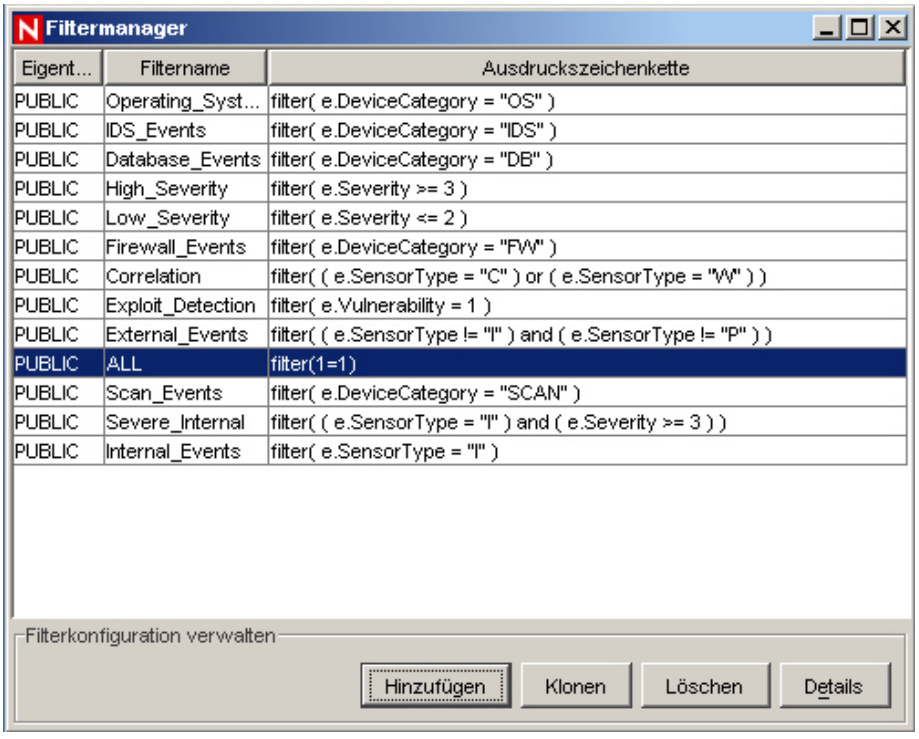
So löschen Sie einen globalen Filter

1. Klicken Sie im Fenster *Globale Filterkonfiguration* auf *Bearbeiten*.
2. Wählen Sie einen Filter aus der Liste und klicken Sie auf *Löschen*.
3. Klicken Sie auf *Speichern*.

## Konfigurieren öffentlicher und privater Filter

Beim Konfigurieren öffentlicher und privater Filter können Sie:

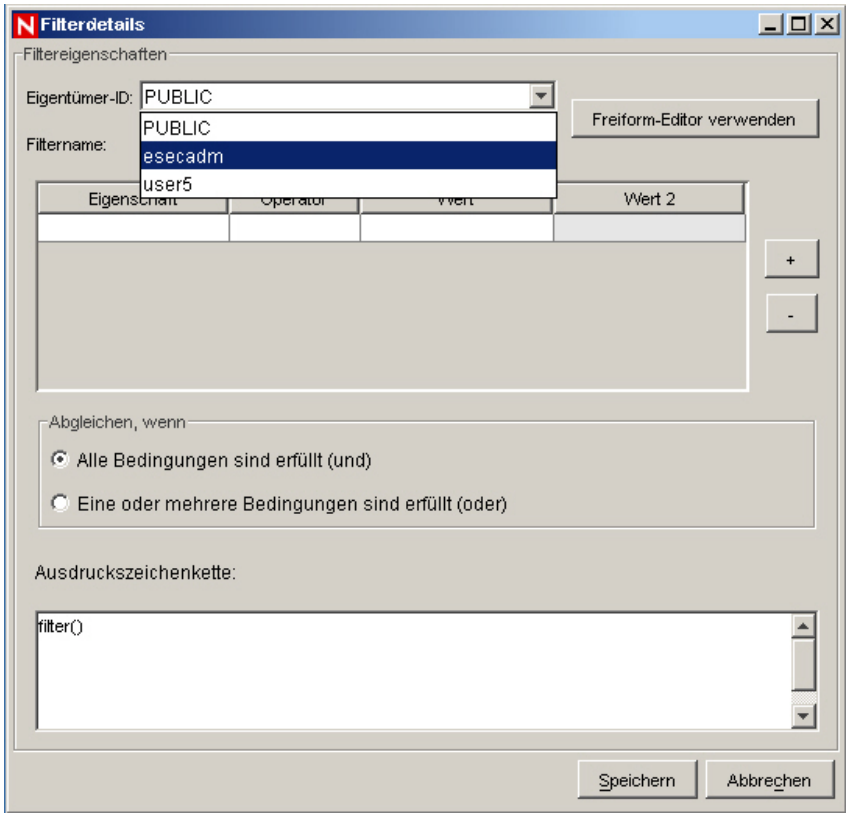
- Einen Filter hinzufügen
- Einen Filter klonen
- Einen Filter ändern
- Filterdetails anzeigen
- Einen Filter löschen




## Hinzufügen eines Filters

So fügen Sie einen öffentlichen oder privaten Filter hinzu

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie auf *Admin* > *Filter-Manager* oder wählen Sie *Filter-Manager*“ unter dem Ordner „*Filterkonfiguration*“ im Navigator.
3. Klicken Sie auf *Hinzufügen*.
4. Wählen Sie eine Eigentümer-ID (öffentlich oder privat [im Besitz des Benutzers]).




5. Geben Sie einen Filternamen ein.
6. Der Tabellen-Editor ist die Standardauswahl für das Bearbeiten von Inhalten.

---

**HINWEIS**: (Optional) Sie können auch auf „Freiform-Editor verwenden“ klicken, um einen Freiform-Editor anzuzeigen. Der Freiform-Editor ermöglicht Ihnen das Erstellen komplexer Ausdrücke, die im Tabellen-Editor nicht erstellt werden können. Nachdem der Ausdruck mit dem Freiform-Editor geändert wurde, kann der Tabellen-Editor jedoch nicht mehr dafür verwendet werden.

---

7. Wählen Sie die Kriterien für die folgenden Spalten aus:
   - Eigenschaft
   - Operator
   - Wertspalten

   Ihre Auswahl wird im Feld „Ausdruckszeichenkette“ angezeigt.
8. Klicken Sie im Feld „Abgleichen, wenn“ auf eine der folgenden Optionen:
   - Alle Bedingungen sind erfüllt (und)
   - Eine oder mehrere Bedingungen sind erfüllt (oder)
9. Zum Erstellen eines anderen Filterausdrucks klicken Sie auf *Neuen Filterausdruck erstellen* (+), um der Filterausdruckstabelle eine neue Zeile hinzuzufügen.
10. Zum Entfernen eines Filterausdrucks wählen Sie einen Filterausdruck aus der Tabelle und klicken Sie auf *Ausgewählten Ausdruck entfernen* (-).
11. Klicken Sie auf *Speichern*.

### So klonen Sie einen öffentlichen oder privaten Filter

Das Klonen ist eine praktische Möglichkeit zum Duplizieren eines Filters, um die Konsistenz der Kriterien innerhalb einer Gruppe von Filtern oder Benutzern sicherzustellen.

So klonen Sie einen öffentlichen oder privaten Filter

1. Öffnen Sie das Fenster „Filter-Manager“.
2. Klicken Sie auf *Klonen*.
3. Geben Sie einen neuen Filternamen ein.
4. Ändern Sie die Kriterien des ursprünglichen Filters.
5. Klicken Sie auf *Speichern*.

### Ändern eines öffentlichen oder privaten Filters

So ändern Sie einen öffentlichen oder privaten Filter

1. Öffnen Sie den Filter-Manager.
2. Wählen Sie einen Filter aus und klicken Sie auf *Details*.
3. Ändern Sie die Kriterien nach Bedarf. Eigentümer-ID und *Filtername* können nicht geändert werden.
4. Klicken Sie auf *Speichern*.

### Anzeigen der Details eines öffentlichen oder privaten Filters

So zeigen Sie einen öffentlichen oder privaten Filter an

1. Öffnen Sie das Fenster „Filter-Manager“.
2. Wählen Sie einen Filter aus und klicken Sie auf *Details*.

### Löschen eines öffentlichen oder privaten Filters

So löschen Sie einen öffentlichen oder privaten Filter

1. Öffnen Sie das Fenster *Filter-Manager*.
2. Wählen Sie einen Filter aus und klicken Sie auf *Löschen*.
3. Ein Bestätigungsfenster wird geöffnet.

## Konfigurieren der Menükonfiguration

Zur Verwendung dieser Funktion müssen Sie über die Benutzerberechtigung „Menükonfiguration“ verfügen.

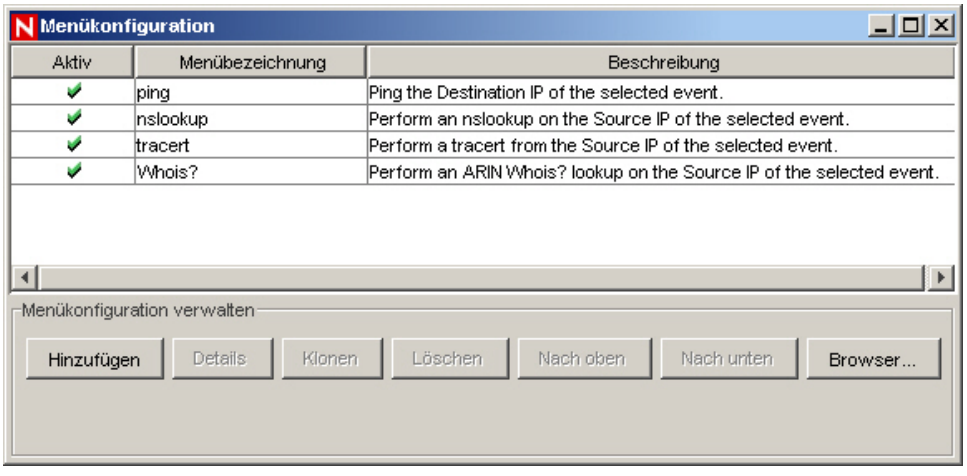
Verwenden Sie das Fenster „Menükonfiguration“, um die Menüelemente zu erstellen, die im Menü „Ereignis“ angezeigt werden sollen, das in jeder Tabelle mit einem Ereignis angezeigt wird (z. B. in den Fenstern „Ereignisechtzeit“, „Snapshot“, „Vorfallereignisse“ usw.), wenn Sie eines oder mehrere Ereignisse auswählen oder mit der rechten Maustaste klicken. Sentinel verfügt über die folgenden standardmäßigen Menükonfigurationselemente, die Sie klonen, aktivieren oder deaktivieren können:

- ping – Sendet ein Ping-Signal an die Ziel-IP des ausgewählten Ereignisses.
- nslookup – Führt eine Namenserversuche für die Quellen-IP des ausgewählten Ereignisses durch.
- traceroute (tracert in MS SQL) – Ermittelt die Route von der Quellen-IP des ausgewählten Ereignisses zum Sentinel Server.

- Whois? – Führt eine ARIN Whois?-Suche für die Quellen-IP des ausgewählten Ereignisses durch.

Das Fenster „Menükonfiguration“ ermöglicht Ihnen Folgendes:

- Hinzufügen einer Option zum Menü für die Menükonfiguration
- Klonen einer Menüoption für die Menükonfiguration
- Ändern einer Menüoption für die Menükonfiguration
- Anzeigen der Optionsparameter für eine Menükonfiguration
- Aktivieren oder Deaktivieren einer Menüoption für die Menükonfiguration
- Neuanordnen von Ereignismenüoptionen
- Löschen einer Menüoption für die Menükonfiguration
- Hinzufügen einer Browserfunktion zur Menükonfigurationsoption




## Hinzufügen einer Option zum Menü für die Menükonfiguration

**HINWEIS**: Wenn Sie einen Tag umbenannt haben, beispielsweise CustomerVar24 in PolicyName, müssen Sie beim Einstellen der Parameter den neuen Namen verwenden.

So fügen Sie dem Menü für die Menükonfiguration eine Option hinzu

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie im Admin-Navigator auf *Admin* > *Menükonfiguration*.
3. Geben Sie im Dialogfeld „Menükonfiguration“ Folgendes ein:
   - Name
   - Beschreibung
   - Aktion – entweder das Ausführen eines Befehls oder das Starten eines Browsers
   - Browser verwenden – Wenn Sie die Aktion „Befehl ausführen“ ausgewählt haben und Ihre Browsereinstellungen auf „Externen Browser verwenden“ eingestellt sind (siehe Bearbeiten der Browsereinstellungen für die Menükonfiguration zur Bearbeitung der Browsereinstellungen), können Sie die Option „Browser verwenden“ auswählen. Bei Auswahl dieser Option wird die Ausgabe Ihres Befehls unter Verwendung der Menükonfigurations-Browsereinstellungen für das Sentinel Control Center angezeigt.

- Dateityp – Wenn Sie die Aktion „Befehl ausführen“ ausgewählt haben, Ihre Browsereinstellungen auf „Externen Browser verwenden“ eingestellt sind und Sie die Option „Browser verwenden“ ausgewählt haben, können Sie den Dateityp für die Ausgabe dieses Befehls festlegen.
- Befehlszeile/URL

**HINWEIS**: Unter UNIX muss sich das Skript/die Anwendung oder der symbolische Link zum Skript/zur Anwendung im Verzeichnis $ESEC_HOME\sentinel\exec befinden. Geben Sie für Skripts, Anwendungen oder symbolische Links nur den Befehl ein. Eingegebene Pfade werden ignoriert.

**HINWEIS**: Unter Windows (Korrelation) muss sich das Skript/die Anwendung in einem der Verzeichnisse befinden, die in den Windows-Umgebungsvariablen aufgeführt sind. Eingegebene Pfade werden ignoriert.

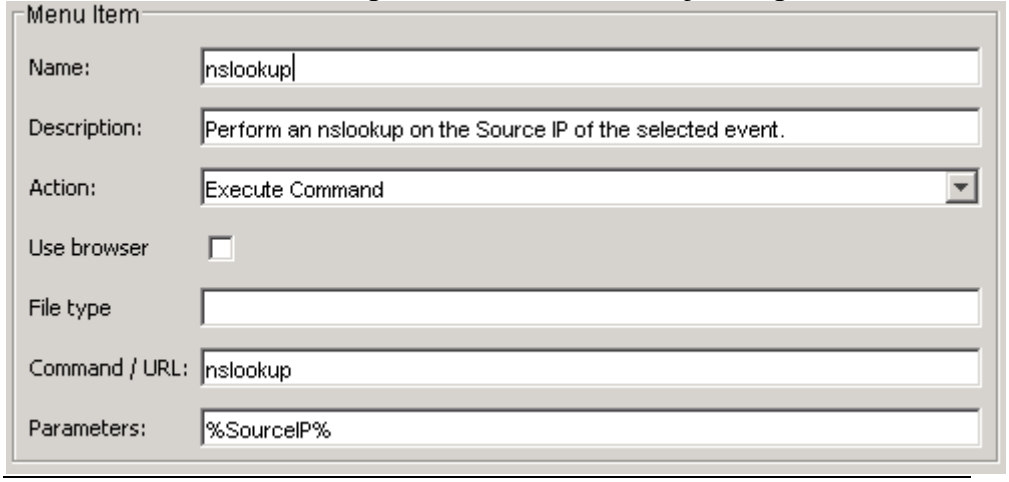
**HINWEIS**: Unter Windows (ohne Korrelation) ist die Pfadeingabe optional. Bei Eingabe eines Befehls ohne Pfad werden standardmäßig das Verzeichnis %ESEC_HOME%\sentinel\bin und alle anderen Pfade, die in den Umgebungsvariablen festgelegt sind, verwendet.

- Parameter – müssen in Prozentzeichen eingeschlossen sein (z. B. %EventName%)

**HINWEIS:** Eine Liste der verfügbaren Tags, die Sie bei der Angabe von Parametern verwenden können, erhalten Sie, wenn Sie im Dialogfeld „Menükonfiguration“ auf „Hilfe“ klicken oder im *Sentinel-Referenzhandbuch für Benutzer* im Kapitel „META-Tag“ nachschlagen.

4. Klicken Sie auf *OK*. Die neue Option wird der Liste der Menüelemente im Fenster „Menükonfiguration“ hinzugefügt.

**HINWEIS:** Markieren Sie beispielsweise eines der Standardmenüelemente und klicken Sie auf *Details*. Nachfolgend sehen Sie eine nslookup-Konfiguration:



## Klonen einer Menüoption für die Menükonfiguration

So klonen Sie eine Menüoption für die Menükonfiguration

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Wählen Sie ein Menüelement aus der Tabelle und klicken Sie auf *Klonen*.
3. Bearbeiten Sie im Dialogfeld „Menükonfiguration“ die folgenden Elemente:
   - Name
   - Beschreibung
   - Aktion
   - Geben Sie an, ob ein Browser verwendet werden soll. Informationen hierzu finden Sie unter Hinzufügen einer Browserfunktion zur Menükonfigurationsoption.
   - Befehlszeile/URL
   - Parameter
   - Wählen Sie eine Aktion:
     - Befehl ausführen
     - Webbrowser starten

   **HINWEIS:** Eine Liste der verfügbaren Tags, die Sie bei der Angabe von Paramtern verwenden können, erhalten Sie, wenn Sie im Dialogfeld „Menükonfiguration“ auf „Hilfe“ klicken oder im *Sentinel-Referenzhandbuch für Benutzer* im Kapitel „META-Tag“ nachschlagen.
4. Klicken Sie auf *OK*. Die neue Option wird der Liste der Menüelemente im Fenster „Menükonfiguration“ hinzugefügt.

## Ändern einer Menüoption für die Menükonfiguration

So ändern Sie eine Menüoption für die Menükonfiguration

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Doppelklicken Sie auf eine Menüoption.
3. Geben Sie die gewünschten Änderungen ein und klicken Sie auf *OK*.

## Anzeigen der Optionsparameter für eine Menükonfiguration

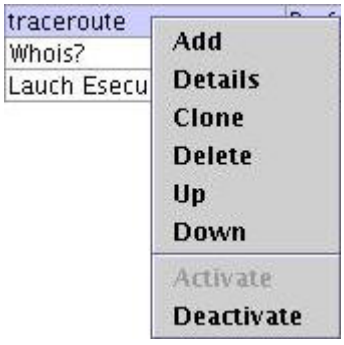
So zeigen Sie die Optionsparameter für eine Menükonfiguration an

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Markieren Sie ein Menüelement und klicken Sie auf *Details*.

## Aktivieren oder Deaktivieren einer Menüoption für die Menükonfiguration

So aktivieren oder deaktivieren Sie eine Menüoption für die Menükonfiguration

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Wählen Sie eine Menüoption, klicken Sie mit der rechten Maustaste und wählen Sie *Aktivieren* oder *Deaktivieren*.




## Neuanordnen von Ereignismenüoptionen

So verschieben Sie eine Ereignismenüoption nach oben oder unten

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Wählen Sie eine Menüoption und klicken Sie auf *Nach oben* oder *Nach unten*.

## Löschen einer Menüoption für die Menükonfiguration

So löschen Sie eine Menüoption für die Menükonfiguration

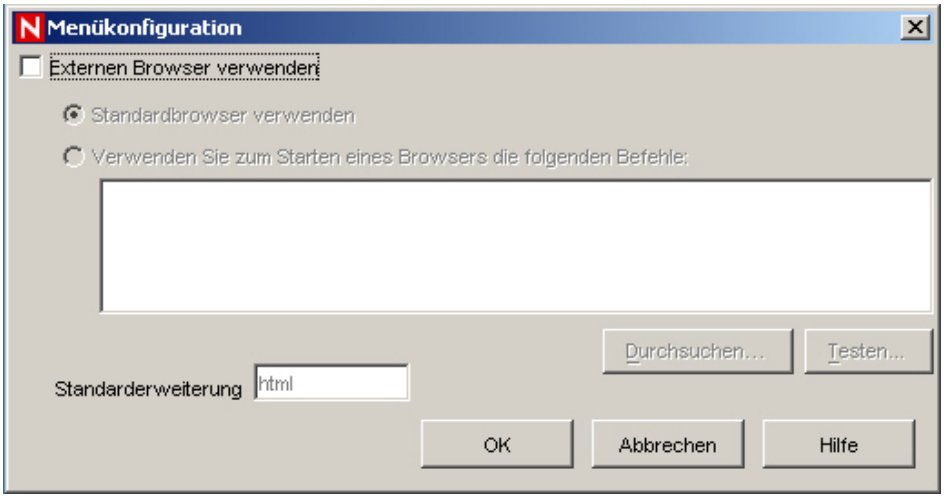
1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Wählen Sie eine Menüoption aus und klicken Sie auf *Löschen*.
   - Klicken Sie auf *Ja*, um die Menüoption zu löschen.
   - Klicken Sie auf *Nein*, um die Menüoption beizubehalten.

## Bearbeiten der Browsereinstellungen für die Menükonfiguration

Diese Option ermöglicht Ihnen das Senden der Ausgabe Ihrer Menükonfigurationsoption an einen externen Browser. Der externe Browser kann eine beliebige Anwendung sein. Es können nicht nur Internetbrowser verwendet werden. Durch Änderung der Dateierweiterung können Sie jede beliebige Anwendung starten, die mit dieser Erweiterung verknüpft ist. Die Erweiterung TXT beispielsweise ist in der Regel mit dem Editor verknüpft. Sie können jedoch auch angeben, dass ein bestimmtes Programm gestartet werden soll. Beispielsweise können Sie TXT-Dateien von Wordpad oder einem anderen Texteditor öffnen lassen.

Bearbeiten der Browsereinstellungen für die Menükonfiguration

1. Öffnen Sie das Fenster „Menükonfiguration“.
2. Klicken Sie auf *Browser*.



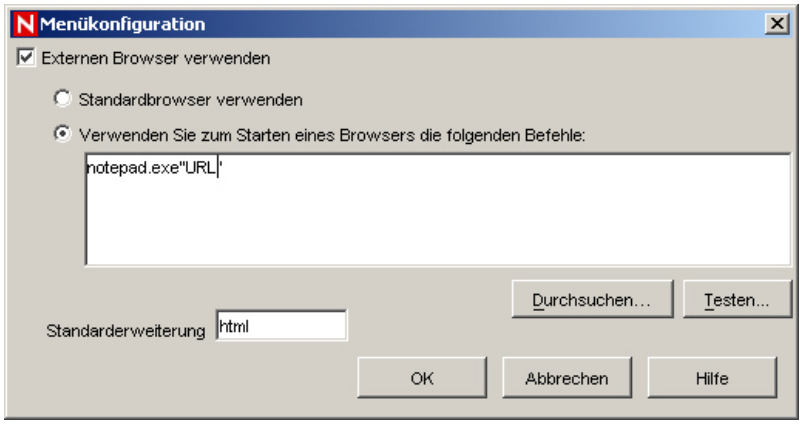

Wenn Sie beim Einrichten einer Menükonfigurationsoption „Browser verwenden“ wählen und die Browserfunktion auf die Standardeinstellung eingestellt ist (wie oben), reagiert die Menükonfigurationsoption so, als ob das Feld „Browser verwenden“ nicht aktiviert wäre.

Wenn Sie das Kontrollkästchen „Externen Browser verwenden“ aktivieren, können Sie eine der folgenden Optionen wählen:

- Standardbrowser verwenden – Verwendet den Standardbrowser (Anwendung), der mit der Dateierweiterung verknüpft ist, die im Feld „Dateierweiterung“ festgelegt ist.
- Verwenden Sie zum Starten eines Browsers die folgenden Befehle – Ermöglicht Ihnen das Angeben einer bestimmten Anwendung, die gestartet werden soll. Wenn Sie anstelle des Standardbrowsers einen anderen Browser verwenden, muss Ihre Befehlszeile mit %URL% enden. Beispiel:

  ```
  C:\Programme\Internet Explorer\IEXPLORE.EXE %URL%
  ```

Nachfolgend sehen Sie ein Beispiel, bei dem die Ausgabe der Menüoption im Editor (notepad.exe) erfolgt.




3. Klicken Sie nach dem Festlegen der Konfiguration auf *OK*.

# DAS-Statistik

Diese Funktion dient zur internen Überwachung Ihres Systems. Sie ist nicht für den durchschnittlichen Benutzer gedacht. DAS-Statistik überwacht Folgendes:

- DAS_Binary
- DAS_Query
- DAS_rt

Die Statistik ist wie folgt unterteilt:

- Service – Name des Dienstes, wie z. B: DAS_Query
- Uhrzeit – Vergangene Zeit seit der letzten Aktualisierung
- Num – Anzahl der Anforderungen, die für diesen Eintrag verarbeitet wurden
- WaitTime – Durchschnittliche Wartezeit einer Anforderung in Sekunden, bevor ihre Verarbeitung beginnt
- Laufzeit – Durchschnittliche Dauer der Verarbeitung einer Anforderung (in Sekunden)
- #Wartet – Durchschnittliche Größe der Wartet-Warteschlange
- #Läuft – Durchschnittliche Größe der Läuft-Warteschlange

Die Informationen sind in drei Abschnitte eingeteilt:

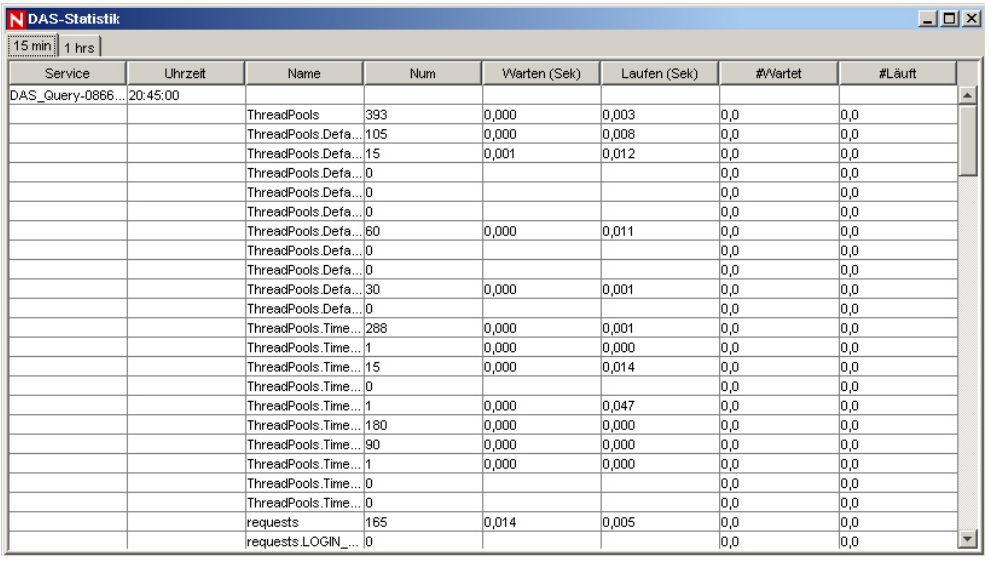
- Anforderungen
- Services
- ThreadPools

Unter „Anforderungen“ werden alle Anforderungen nach Kanal aufgeführt (z. B. services.CorrelationService). Unter „Services“ erfolgt die Auflistung nach Service. Manchmal erfolgt eine Aufschlüsselung durch Hinzufügen von „<Kategorie>“ unter dem Namen, wie z. B. Services.CorrelationService oder Services.RemoteObjectService.EMap.getMapPK.

Unter „Services“ werden alle Remote-Methodenaufrufe durch benutzerdefinierte Services (Ihre XML-Services) unterhalb von services.RemoteObjectService aufgeführt. Darunter steht der Name des Service (EMap im oben genannten Beispiel) und, falls angefordert, der Name der Methode (getMapPK im oben genannten Beispiel).

Wenn ein Server eine Anforderung empfängt, wie z. B. DAS Query, wird ein Task erstellt und geplant. Der Task wird dann einem Thread-Pool zur Ausführung zugewiesen. Es können mehrere Thread-Pools vorhanden sein und ein Thread-Pool kann mehrere Services bedienen. Aus diesem Grund muss eine Anforderung möglicherweise auf einen verfügbaren Thread warten, selbst wenn der Service nicht stark ausgelastet ist. Wenn die Statistik erkennen lässt, dass die Wartezeit einer Anforderung lang und die Anzahl der Anforderungen für diesen Service niedrig ist, sollten Sie die Informationen zu den Thread-Pools überprüfen.

Die Zahl neben einem Eintrag stellt die Summe seiner untergeordneten Elemente dar. Daher bedeutet „requests 15“, dass 15 Anforderungen für alle Anforderungsmethodenaufrufe vorhanden sind. Der Eintrag „requests.configurations 1“ darunter bedeutet, dass eine der 15 Anforderungen eine Konfigurationsanforderung ist. „requests.esecurity.correlation.config 2“ bedeutet, dass 2 der 15 Anforderungen für esecurity.correlation.config eingegangen sind usw.



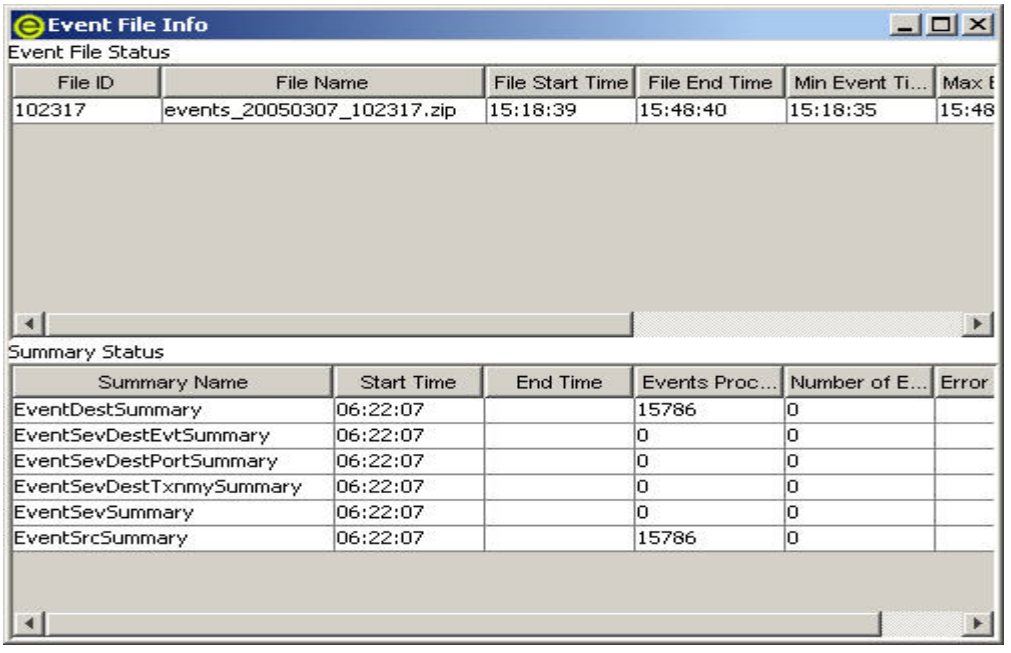

| Service | Uhrzeit | Name | Num | Warten (Sek) | Laufen (Sek) | #Wartet | #Läuft |
|---|---|---|---|---|---|---|---|
| DAS_Query-0866... | 20:45:00 | | | | | | |
| | | ThreadPools | 393 | 0,000 | 0,003 | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 105 | 0,000 | 0,008 | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 15 | 0,001 | 0,012 | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 60 | 0,000 | 0,011 | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 30 | 0,000 | 0,001 | 0,0 | 0,0 |
| | | ThreadPools.Defa... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Time... | 288 | 0,000 | 0,001 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 1 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 15 | 0,000 | 0,014 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Time... | 1 | 0,000 | 0,047 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 180 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 90 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 1 | 0,000 | 0,000 | 0,0 | 0,0 |
| | | ThreadPools.Time... | 0 | | | 0,0 | 0,0 |
| | | ThreadPools.Time... | 0 | | | 0,0 | 0,0 |
| | | requests | 165 | 0,014 | 0,005 | 0,0 | 0,0 |
| | | requests.LOGIN_... | 0 | | | 0,0 | 0,0 |

Diese Informationen können hilfreich sein, da sie aufzeigen, was vor sich geht. Die Anzahl der Anforderungen ist besonders hilfreich, da Sie daraus ersehen können, wohin die Anforderungen gehen oder worauf sie sich konzentrieren. Die Zahl unter „#Wartet“ ist hilfreich, da sie zeigt, wie beschäftigt der Server ist. Diese Zahl sollte möglichst klein sein. Wenn sie groß ist, müssen neue Anforderungen (selbst für einfache Tasks) auf potenziell langsamere warten. Dies ist nicht gut. Die durchschnittliche Laufzeit ist sehr wichtig, da sie zeigt, welche Anforderungen die gesamte Zeit tatsächlich in Anspruch nehmen und nicht nur auf andere warten.

# Ereignisdatei-Info

Im oberen Bereich werden die Statusinformationen für die einzelnen Ereignisdateien angezeigt. Der Status der Ereignisdateien wird beim Öffnen des Fensters erfasst. Statusinformationen zu früheren Ereignissen werden nicht angezeigt. Die angezeigten Informationen umfassen die Datei-ID (entspricht der arch_id in der Ereignistabelle), der Dateiname sowie Statistiken zur Datei (ob sie abgeschlossen ist, die Start- und Endzeit des Schreibvorgangs, die minimale und maximale Dauer der Ereignisse in der Datei usw.).

Wenn Sie im oberen Bereich eine Datei markieren, wird im unteren Bereich der Zusammenfassungsstatus für diese Ereignisdatei angezeigt. Im unteren Bereich werden der Zusammenfassungsname, die Start- und Endzeit der Verarbeitung sowie die Anzahl der verarbeiteten Ereignisse angezeigt und ob Fehler gemeldet wurden.




# Benutzerkonfigurationen

Zur Verwendung dieser Funktion und zum Arbeiten im Fenster „Benutzerkonfiguration“ müssen Sie über die Benutzerberechtigung „Benutzerkonfiguration“ verfügen.

Das Fenster „Benutzerkonfiguration“ ermöglicht Ihnen Folgendes:

- Erstellen eines Benutzerkontos
- Ändern eines Benutzerkontos
- Anzeigen von Benutzerkontodetails
- Klonen eines Benutzerkontos
- Löschen eines Benutzerkontos
- Beenden einer aktiven Sitzung
- Hinzufügen einer iTRAC-Funktion
- Löschen einer iTRAC-Funktion
- Details einer iTRAC-Funktion

Das Installationsprogramm erstellt folgende Standardbenutzer in Sentinel Server:

### Oracle- und MS SQL-Authentifizierung:

- esecdba – Schemaeigentümer (zum Zeitpunkt der Installation zu konfigurieren).
- esecadm – Sentinel-Administratorbenutzer (zum Zeitpunkt der Installation zu konfigurieren).

  **HINWEIS:** Unter UNIX erstellt das Installationsprogramm zudem den Betriebssystembenutzer mit demselben Benutzernamen und Passwort.

- esecrpt – Reporter-Benutzer, Passwort wie admin-Benutzer.
- ESEC_CORR – Correlation Engine-Benutzer, Verwendung zur Erstellung von Vorfällen.
- esecapp – Sentinel-Anwendungsbenutzername zum Herstellen der Datenbankverbindung.

### Windows-Authentifizierung:

- Sentinel-DB-Administrator – Schemaeigentümer (zum Zeitpunkt der Installation zu konfigurieren).
- Sentinel-Administrator – Sentinel-Administratorbenutzer (zum Zeitpunkt der Installation zu konfigurieren).
- Sentinel Report-Benutzer – Reporter-Benutzer, Passwort wie admin-Benutzer.

- Sentinel-DB-Anwendungsbenutzer – Sentinel-Anwendungsbenutzername zum Herstellen der Datenbankverbindung.

## Öffnen des Fensters „Benutzer-Manager“

So öffnen Sie das Fenster „Benutzer-Manager“

1. Klicken Sie auf die Registerkarte *Admin*.
2. Klicken Sie auf *Admin* > *Benutzerkonfiguration*.

## Erstellen eines Benutzerkontos

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

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

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

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

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

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

Zur Verwendung dieser Funktion müssen Sie über die Benutzerberechtigung zum Erstellen von Benutzerkonten verfügen. Benutzerberechtigungen sind ziemlich detailliert. Informationen hierzu finden Sie im *Sentinel-Referenzhandbuch für Benutzer* unter *Benutzerberechtigungen*.

**HINWEIS**: Das esecrpt-Benutzerpasswort muss direkt in der Datenbank geändert werden. Enterprise Manager kann hierfür verwendet werden.

So erstellen Sie ein Benutzerkonto

1. Öffnen Sie das Fenster „Benutzer-Manager“.
2. Klicken Sie auf *Neuen Benutzer hinzufügen*


oder markieren Sie einen Benutzer, klicken Sie mit der rechten Maustaste und wählen Sie *Benutzer hinzufügen*.


3. Geben Sie unter „Autorisierung“ Folgendes ein:
   - Benutzername
   - Passwort
   - Passwort bestätigen
   - Sicherheitsfilter – Klicken Sie auf den Abwärtspfeil, um einen Filter auszuwählen. Das Fenster „Filterauswahl“ wird geöffnet. Markieren Sie einen Filter oder klicken Sie auf *Hinzufügen*, um einen Filter für dieses Benutzerkonto zu erstellen.

---

**HINWEIS**: Wenn Sie einem Benutzer einen Sicherheitsfilter zugewiesen haben, können Sie diesen Filter nicht löschen.

---

   - Klicken Sie auf *Auswählen*.

---

**HINWEIS**: Als optimales Verfahren wird eine Passwort-Mindestlänge von 8 Zeichen dringend empfohlen, wobei das Passwort alphanumerische Zeichen enthalten sollte.

---

   (Optional) Geben Sie unter „Details“ Folgendes ein:
   - Vorname
   - Nachname
   - Department
   - Telefon
   - Email
4. Klicken Sie auf die Registerkarte *Berechtigungen* und weisen Sie Benutzerberechtigungen zu.
5. Klicken Sie auf die Registerkarte *Funktionen* und wählen Sie die Funktion für den Benutzer aus.
6. Klicken Sie auf *OK*.

---

**HINWEIS:** Oracle gestattet nicht die Verwendung von Benutzernamen, die gleich lauten wie die von Oracle reservierten Wörter. Diese Namen werden von Sentinel ebenfalls abgelehnt.

---

## Ändern eines Benutzerkontos

Zur Verwendung dieser Funktion müssen Sie über die Benutzerberechtigung zum Ändern von bestehenden Benutzerkonten verfügen.

**HINWEIS**: Das esecrpt-Benutzerpasswort muss direkt in der Datenbank geändert werden. Enterprise Manager kann hierfür verwendet werden.

So ändern Sie ein Benutzerkonto

1. Öffnen Sie das Fenster „Benutzer-Manager“.
2. Doppelklicken Sie auf ein Benutzerkonto oder klicken Sie mit der rechten Maustaste auf *Benutzerdetails*.
3. Ändern Sie das Konto.
4. Klicken Sie auf *OK*.

## Anzeigen von Benutzerkontodetails

Zur Verwendung dieser Funktion müssen Sie über die Benutzerberechtigung zum Verwenden/Anzeigen von Benutzerkonten verfügen.

So zeigen Sie Benutzerkontodetails an

1. Öffnen Sie das Fenster „Benutzer-Manager“.
2. Doppelklicken Sie auf ein Benutzerkonto oder klicken Sie mit der rechten Maustaste auf *Benutzerdetails*.
3. Überprüfen Sie die Details des Benutzerkontos und schließen Sie das Fenster.

## Klonen eines Benutzerkontos

So klonen Sie ein Benutzerkonto

1. Öffnen Sie das Fenster „Benutzer-Manager“.
2. Wählen Sie eine Benutzerkonto-ID aus, klicken Sie mit der rechten Maustaste und wählen Sie *Benutzer klonen*.
3. Ändern Sie die Benutzerinformationen und die Benutzerberechtigungen.
4. Klicken Sie auf *Speichern*.

## Löschen eines Benutzerkontos

Zur Verwendung dieser Funktion müssen Sie über die Benutzerberechtigung zum Löschen von Benutzerkonten verfügen.

**HINWEIS**: Wenn ein Benutzer gelöscht wird, kann der Benutzer nicht wieder erstellt werden. Wenn Sie beispielsweise einen Benutzer namens Johann erstellen und Johann später löschen, können Sie nicht wieder einen Benutzer namens Johann erstellen.

So löschen Sie ein Benutzerkonto

1. Öffnen Sie das Fenster „Benutzer-Manager“.
2. Wählen Sie eine Benutzerkonto-ID aus, klicken Sie mit der rechten Maustaste und wählen Sie *Benutzer löschen*.

## Beenden einer aktiven Sitzung

Beenden einer aktiven Sitzung

1. Öffnen Sie das Fenster „Aktive Benutzersitzungen“.
2. Markieren Sie eine aktive Sitzung, die Sie beenden möchten.
3. Klicken Sie mit der rechten Maustaste und wählen Sie *Sitzung terminieren*.
4. Sie werden zur Eingabe einer Beendigungsnachricht aufgefordert: Sie dient dazu, den Benutzer darüber zu informieren, warum Sie die Sitzung beenden.

## Hinzufügen einer iTRAC-Funktion

So fügen Sie eine iTRAC-Funktion hinzu

1. Öffnen Sie das Fenster „Funktions-Manager“.
2. Klicken Sie auf *Neue Funktion hinzufügen*


oder klicken Sie mit der rechten Maustaste und wählen Sie *Neue Funktion hinzufügen*.

## Löschen einer iTRAC-Funktion

So löschen Sie eine iTRAC-Funktion

1. Öffnen Sie das Fenster „Funktions-Manager“.
2. Wählen Sie eine Funktion aus, klicken Sie mit der rechten Maustaste und wählen Sie *Funktion löschen.*

## Anzeigen von Funktionsdetails

So zeigen Sie Funktionsdetails an

1. Öffnen Sie das Fenster „Funktions-Manager“.
2. Wählen Sie eine Funktion aus, klicken Sie mit der rechten Maustaste und wählen Sie *Funktionsdetails*.

# 10 Sentinel Data Manager

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

Der Sentinel Data Manager (SDM) ist ein Tool, mit dessen Hilfe Benutzer die Sentinel-Datenbank verwalten können. Mit dem SDM können Benutzer die folgenden Vorgänge ausführen:

- Überwachen der Datenbank-Speicherplatzauslastung
- Anzeigen und Verwalten von Datenbankpartitionen
- Verwalten von Datenbankarchiven
- Importieren von Daten in die Datenbank
- Konfigurieren der Datenzuordnung
- Konfigurieren der Namen von Ereignistags
- Konfigurieren von Einstellungen für Zusammenfassungsberichte

## Installieren des SDM

Der SDM kann direkt über den Sentinel 5 InstallShield Wizard installiert werden. Wählen Sie dazu im Bildschirm zum Auswählen von Sentinel 5-Funktionen die Komponente *Sentinel Data Manager* aus.


(Nur für Oracle) Beachten Sie, dass Sie für die Kommunikation des SDM mit Oracle-Datenbanken den Oracle JDBC-Treiber 9.2.0.4 bzw. 9.2.0.5 manuell herunterladen und die heruntergeladene JAR-Datei in das Verzeichnis „$ESEC_HOME/lib“ am selben Speicherort kopieren müssen, an dem der SDM bzw. „%ESEC_HOME%\lib“ installiert ist, wenn eine Installation des SDM unter Windows ausgeführt wird. Der JDBC-Treiber kann unter der folgenden URL heruntergeladen werden:

**HINWEIS:** Auf einem UNIX-Computer mit installierter DAS-Komponente wird der JDBC-Treiber automatisch vom Installationsprogramm am richtigen Speicherort abgelegt. Daher ist in diesem Fall kein manuelles Herunterladen erforderlich.

http://otn.oracle.com/software/tech/java/sqlj_jdbc/index.html

Diese JAR-Datei heißt i. d. R. „ojdbc14.jar“.

**HINWEIS:** Zum Zeitpunkt der Veröffentlichung des vorliegenden Handbuchs war der oben aufgeführte Link zur Website korrekt.

**HINWEIS**: SDM für Oracle erfordert, dass Oracle Enterprise mit Partitionierung installiert ist.

# Starten der SDM-GUI

**HINWEIS**: Damit Sie die SDM-GUI verwenden können, muss die Datei „configuration.xml“ auf einen Kommunikationsserver verweisen, mit dem DAS_Binary und DAS_Query ebenfalls verbunden sind. Dies ist in der Standardeinstellung der Fall, sofern der Kommunikationsserver und DAS-Prozesse ausgeführt werden.

Für UNIX: Starten der SDM-GUI

1. Melden Sie sich bei der UNIX-Box als Mitglied der Gruppe „esec“ an (Beispiel: „esecadm“).
2. Wechseln Sie in das Verzeichnis „$ESEC_HOME/sdm“.
3. Geben Sie an der Befehlszeile Folgendes ein:

```
./sdm
```

Für Windows: Starten der SDM-GUI

1. Klicken Sie auf *Start* > *Programme* > *Sentinel* > *Sentinel Data Manager*.

**HINWEIS**: Informationen zum Ausführen des SDM von der Befehlszeile finden Sie im Abschnitt SDM-Befehlszeile in diesem Dokument.

## Herstellen einer Verbindung mit der Datenbank

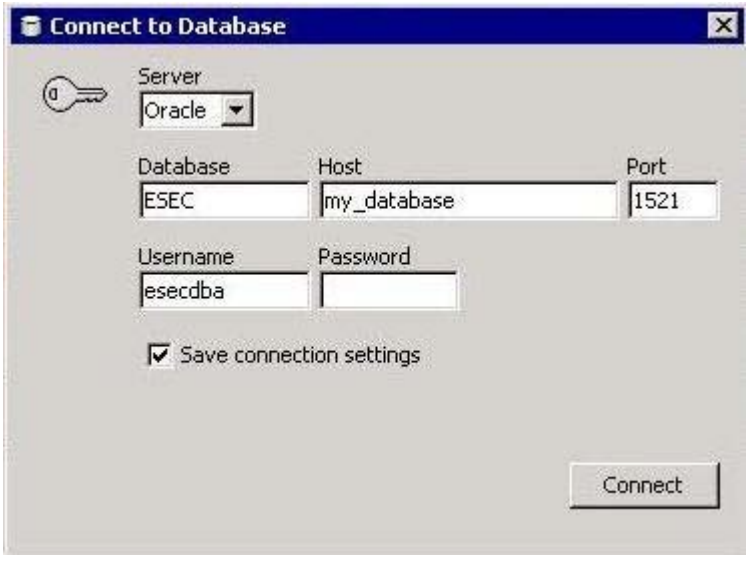
Beim Starten des SDM müssen Sie eine Verbindung mit der Datenbank herstellen. Geben Sie im Dialogfeld *Verbindung mit Datenbank* die entsprechenden Werte in den einzelnen Feldern ein.

Herstellen einer Verbindung mit der Datenbank

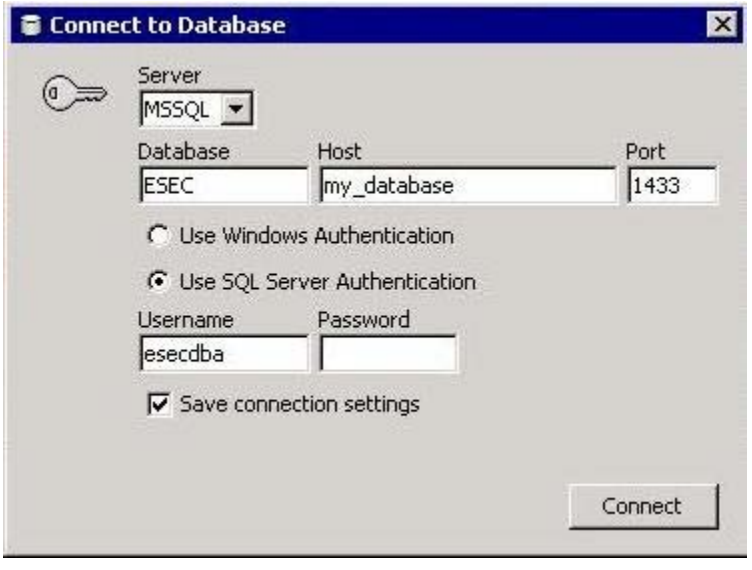
1. Starten Sie die SDM-GUI.
2. Wählen Sie den Datenbanktyp aus („Oracle“ bzw. „MSSQL“).
3. Geben Sie den Datenbankinstanznamen ein (z. B. „ESEC“).
4. Geben Sie den Datenbankhost an (verwenden Sie den Hostnamen oder die IP-Adresse).
5. Legen Sie als Port den Standardport 1521 für Oracle bzw. den Standardport 1433 für MSSQL fest.
6. Geben Sie als Benutzernamen und Passwort Ihren Benutzernamen und Ihr Passwort eines Sentinel-Datenbankadministrators ein. (Verwenden Sie beispielsweise „esecdba“.)

**HINWEIS**: Wenn Sie unter MS SQL und Windows MS SQL im gemischten Modus installiert haben, können Sie sich mithilfe der Windows-Authentifizierung ODER der SQL Server-Authentifizierung anmelden. Bei der Installation von MS SQL in einem Modus, in dem nur die Windows-Authentifizierung zulässig ist, müssen Sie sich mithilfe der Windows-Authentifizierung anmelden. Wenn Sie sich für die Verwendung der Windows-Authentifizierung entscheiden, werden Sie bei der MS - Datenbank als der Benutzer authentifiziert, der zurzeit bei Windows angemeldet ist (d. h. Einzelanmeldung).

Für Oracle:




Für Windows:




**HINWEIS:** Wenn Sie Ihre Verbindungseinstellungen speichern, werden diese in der lokalen Datei „sdm.connect“ gespeichert. Wenn Sie die GUI das nächste Mal starten, werden die Verbindungseinstellungen aus der Datei „sdm.connect“ neu gefüllt. Diese Datei kann beim Ausführen des SDM von der Befehlszeile verwendet werden.

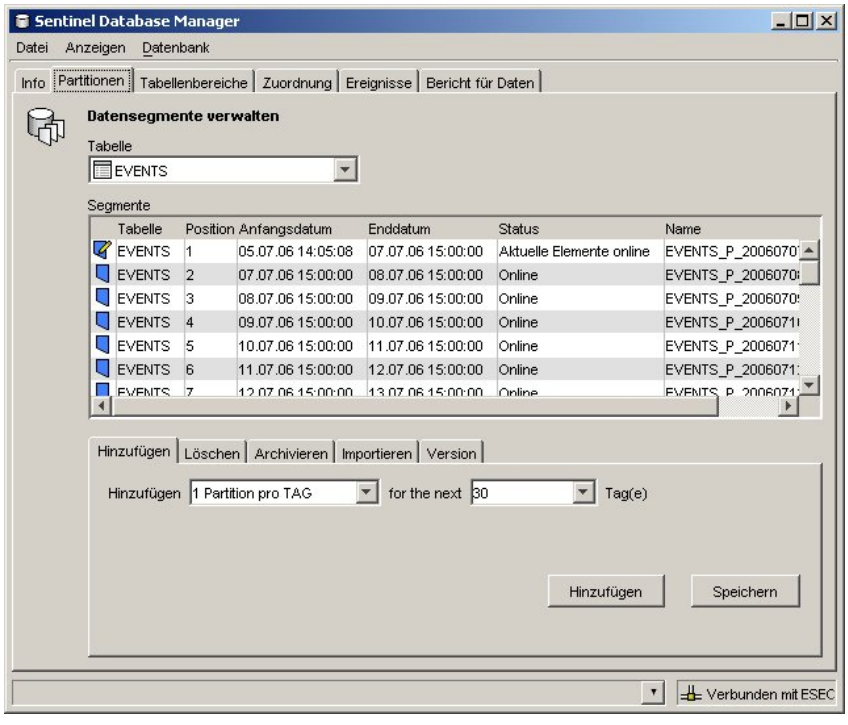
7. Klicken Sie auf *Verbinden*.

## Partitionen

Mithilfe der Registerkarte „Partitionen“ im SDM können Benutzer Datenbankpartitionen anzeigen und verwalten.

So zeigen Sie Partitionen in der GUI an

1. Klicken Sie auf die Registerkarte *Partitionen.*
2. Wählen Sie die anzuzeigende Tabelle in der Dropdown-Liste aus.




In der Tabelle „Segmente“ werden die Partitionen der zurzeit ausgewählten Datenbanktabelle angezeigt.

In jeder Zeile der Tabelle „Segmente“ werden die zugehörige Datenbanktabelle, der Zeitraum, der Status und der Name der jeweiligen Partition aufgeführt.

Als Status der einzelnen in der Tabelle „Segmente“ aufgeführten Tabellen können die Folgenden vorhanden sein:

| | |
|---|---|
| Online | Auf die Daten auf einer Online-Partition kann zugegriffen werden. |
| Aktuelle Elemente online | Dabei handelt es sich um eine Online-Partition, in deren Zeilen zurzeit Daten eingefügt werden. |
| Archivierte Elemente online | Dabei handelt es sich um eine Partition, deren Daten archiviert sind. Auf die Daten kann aus einem der folgenden Gründe jedoch noch zugegriffen werden:<br>▪ Die Partition wurde noch nicht verworfen.<br>▪ Die Partition wird zurückimportiert. |
| Offline | Auf Daten auf einer Offline-Partition kann nicht zugegriffen werden, da die Partition verworfen und nicht importiert wurde. |
| Offline archiviert | Dieser Status kennzeichnet eine Partition, die archiviert und verworfen wurde. |

### So verwalten Sie Partitionen

1. Klicken Sie auf die Registerkarte *Partitionen.*
2. Wählen Sie die Tabelle in der Dropdown-Liste aus.
3. Wählen Sie die Registerkarte am unteren Rand des Fensters aus, die sich auf den gewünschten Vorgang bezieht – „Hinzufügen“, „Löschen“, „Archivieren“, „Importieren“ oder „Release“.

### So fügen Sie Partitionen hinzu

1. Wählen Sie die Registerkarte *Hinzufügen* für Partitionen aus.
2. Geben Sie die Anzahl der hinzuzufügenden Partitionen sowie die Anzahl der Tage an, für die die Partitionen hinzugefügt werden sollen.
3. Klicken Sie auf *Hinzufügen*.

### So löschen Sie Partitionen

1. Wählen Sie die Registerkarte *Löschen* für Partitionen aus.
2. Geben Sie die Anzahl der Tage an, für die ältere Partitionen gelöscht werden sollen.
3. Klicken Sie auf *Löschen*.

### So archivieren Sie Partitionen

**HINWEIS**: Aggregationstabellen werden nicht archiviert.

1. Wählen Sie die Registerkarte *Archivieren* für Partitionen aus.
2. Geben Sie die Anzahl der Tage an, für die ältere Partitionen archiviert werden sollen, sowie das Verzeichnis, in dem das Archiv gespeichert werden soll.

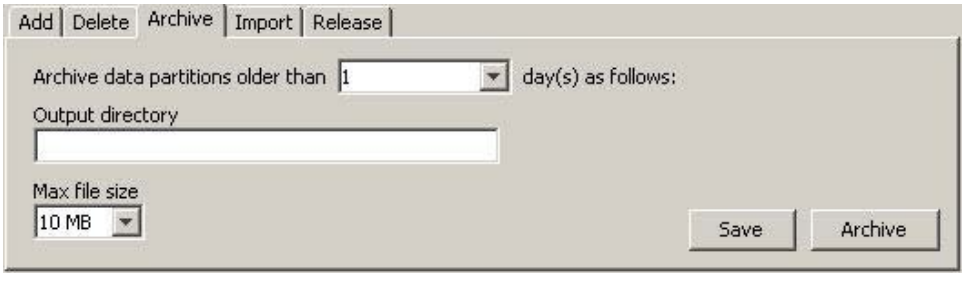
**HINWEIS**: Unter UNIX können Partitionen nicht in „/root“ archiviert werden.

3. Klicken Sie auf *Archivieren*.

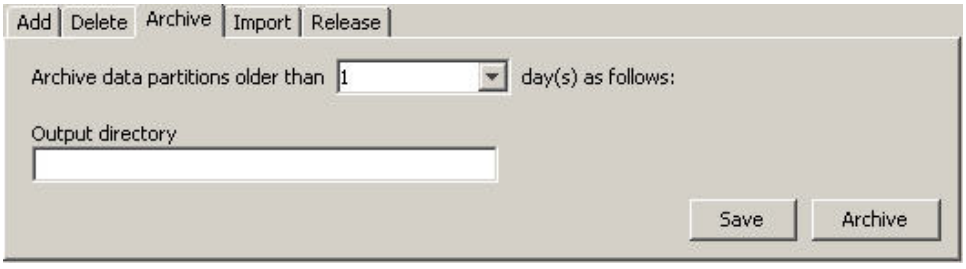
**HINWEIS**: Achten Sie beim Archivieren darauf, dass Sie einen gültigen Pfad auf dem Datenbankserver mit den entsprechenden Berechtigungen eingeben.

**HINWEIS**: Die Registerkarte „Archivieren“ unterscheidet sich für MSSQL und Oracle. Unter Oracle können Sie die maximal zulässige Größe für die Archivdatei festlegen.

Registerkarte „Archivieren“ für Partitionen unter Oracle:



Registerkarte „Archivieren“ für Partitionen unter MSSQL:




So importieren Sie Partitionen

1. Wählen Sie die Registerkarte *Importieren* für Partitionen aus.
2. Wählen Sie in der Tabelle „Segmente“ die Partition aus, in die die Daten importiert werden sollen.
3. Geben Sie das Eingabeverzeichnis an, aus dem die archivierten Daten gelesen werden.
4. Klicken Sie auf *Importieren*.

So geben Sie importierte Partitionen frei

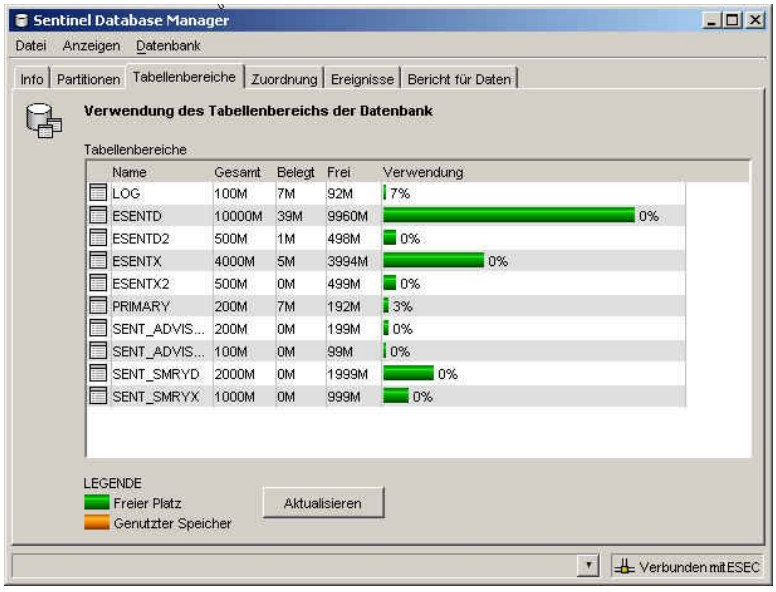
1. Wählen Sie die Registerkarte *Release* für Partitionen aus.
2. Wählen Sie in der Tabelle „Segmente“ die Partition aus, die freigegeben werden soll.
3. Klicken Sie auf *Release.*

## Tabellenbereiche

Mithilfe der Registerkarte „Tabellenbereiche“ im SDM können Benutzer die aktuelle Datenbank-Speicherplatzauslastung anzeigen lassen.

So zeigen Sie die Tabellenbereiche in der GUI an

1. Klicken Sie auf die Registerkarte *Tabellenbereiche*.



In der Tabelle „Verwendung des Tabellenbereichs der Datenbank“ wird der Gesamtspeicherplatz angezeigt, der den einzelnen Tabellenbereichen zugewiesen ist. Zudem wird aufgeführt, welche Menge an Speicherplatz von den einzelnen Tabellenbereichen verwendet wird und welche Menge an Speicherplatz für die einzelnen Tabellenbereiche noch verfügbar (frei) ist. In Balkendiagrammen mit Farbcodierung wird der Gesamtspeicherplatz grafisch veranschaulicht, der den einzelnen Tabellenbereichen zugewiesen ist, sowie der Prozentsatz an Speicherplatz, der von den einzelnen Tabellenbereichen verwendet wird.

**HINWEIS**: Unter MS SQL ist das Konzept der Tabellenbereiche nicht vorhanden, daher werden Dateigruppen verwendet.

## Registerkarte „Zuordnung“

**HINWEIS**: Damit Sie die Registerkarte „Zuordnung“ verwenden können, muss die Datei „configuration.xml“ auf einen Kommunikationsserver verweisen, mit dem DAS_Binary und DAS_Query ebenfalls verbunden sind. Dies ist in der Standardeinstellung der Fall, sofern der Kommunikationsserver und DAS-Prozesse ausgeführt werden.

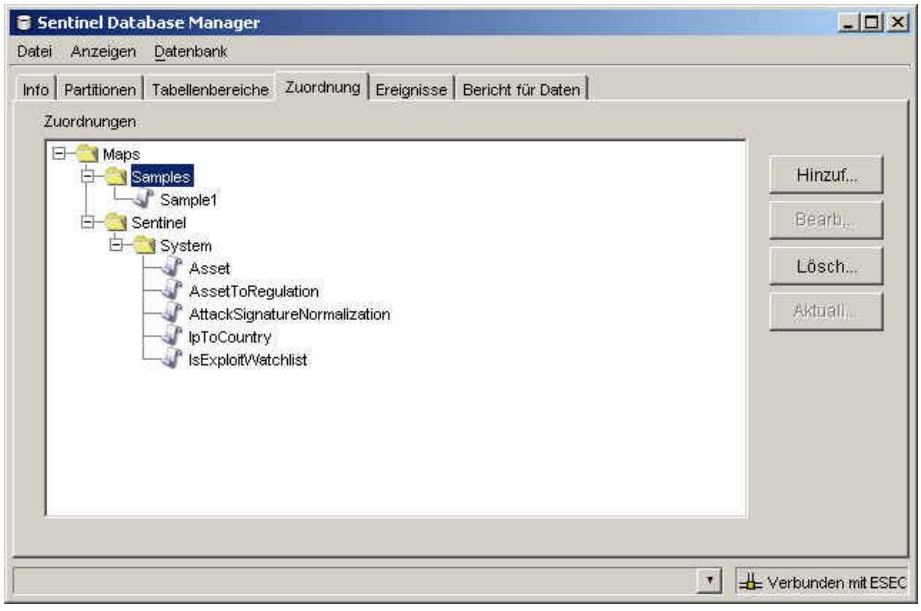
Mithilfe der Registerkarte „Zuordnung“ können Sie folgende Vorgänge ausführen:

- Hinzufügen neuer Zuordnungsdefinitionen
- Bearbeiten von Zuordnungsdefinitionen
- Löschen von Zuordnungsdefinitionen
- Aktualisieren von Zuordnungsdaten

Zuordnungen wirken mit der Datenquellen-Option *Verweis von Zuordnung* auf der Registerkarte „Ereignisse“ zusammen. Eine Zuordung kann mithilfe einer Zeichenkette oder eines Zahlenbereichs durchgeführt werden.

So zeigen Sie Zuordnungen in der GUI an

1. Klicken Sie auf die Registerkarte *Zuordnung*.



In der Haupt-GUI von „Zuordnung“ wird eine Auflistung aller Zuordnungen angezeigt, die für das System definiert wurden.

**HINWEIS**: Zuordnungen unter dem Systemordner können nicht bearbeitet oder gelöscht werden.

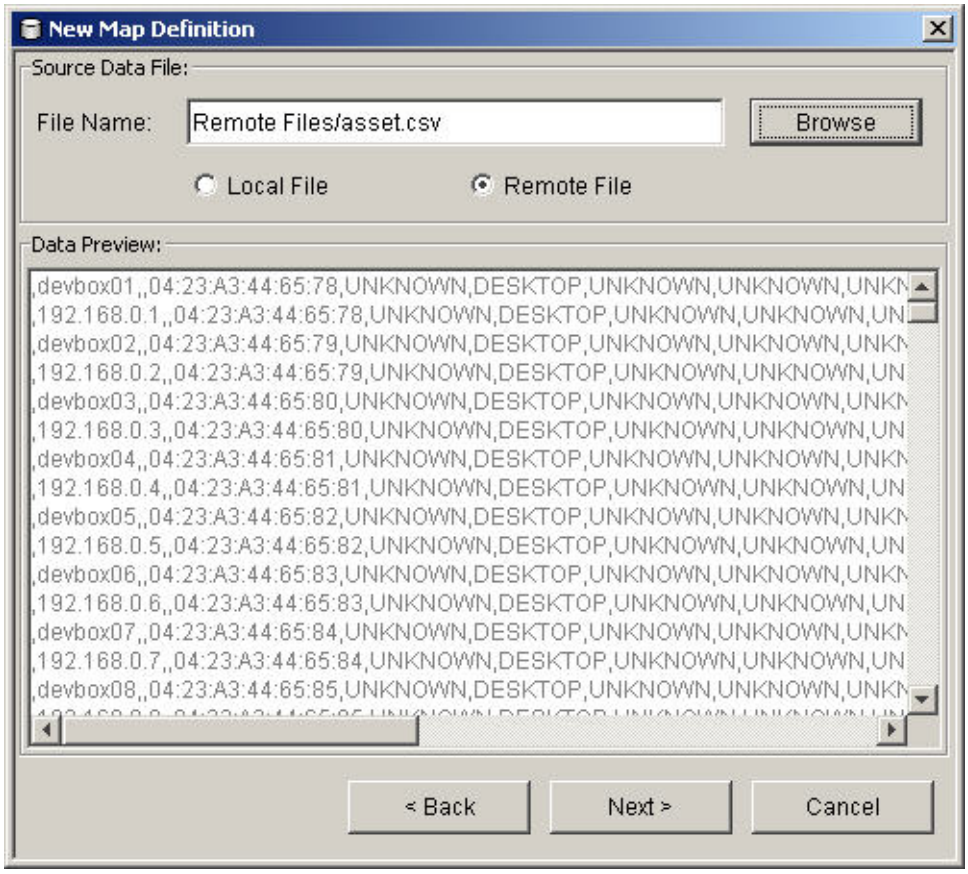
## Hinzufügen von Zuordnungsdefinitionen

So fügen Sie eine Zuordnungsdefinition hinzu

1. Klicken Sie auf die Registerkarte *Zuordnung*.
2. Klicken Sie auf *Hinzufügen*.
3. Wenn Sie einen neuen Zuordnungsordner erstellen möchten, klicken Sie auf die Schaltfläche *Neu*... Geben Sie einen Namen für den Ordner ein.

   **HINWEIS**: Wenn es sich hierbei um die erste Zuordnungsdefinition handelt, wird empfohlen, dass Sie einen neuen Ordner für Zuordnungsdefinitionen erstellen. Wenn Sie eine Zuordnungsdefinition unter dem Systemordner erstellen, können Sie diese nicht bearbeiten oder löschen.
4. Vergewissern Sie sich, dass der Ordner ausgewählt ist, in den die Zuordnungsdefinition eingegeben werden soll. (Das heißt, dieser Ordner wird als geöffnet angezeigt.)
5. Geben Sie einen Namen für die Zuordnung ein.
6. Klicken Sie auf *Weiter*.

   **HINWEIS**: Das Feld „Zuordnungstyp“ ist deaktiviert.
7. Wählen Sie entweder „Lokale Datei“ oder „Ferndatei“ aus.
   - „Lokale Datei“ – Hiermit können Sie nach einer Datei im lokalen Dateisystem suchen (auf dem Computer, auf dem SDM gestartet wurde).
   - „Ferndatei“ – Hiermit können Sie aus vorhandenen Quelldateien mit Zuordnungsdaten auf dem Server auswählen, auf dem DAS ausgeführt wird. Möglicherweise sind bereits zwei Dateien auf dem Server vorhanden (wenn Advisor installiert ist und Vulnerability-Daten heraufgeladen wurden): „attackNormalization.csv“ und „exploitDetection.csv“. Die Ferndatei verweist auf „%ESEC_HOME%\sentinel\bin\map_data“ (Windows) oder auf „$ESEC_HOME/sentinel/bin/map_data“ (UNIX)




Wählen Sie die Zuordnungsdefinitionsdatei aus. Klicken Sie auf *Weiter*.

**HINWEIS**: Bei Zuordnungsdateien mit mehr als 500 Zeilen werden nicht alle Zeilen im SDM angezeigt.

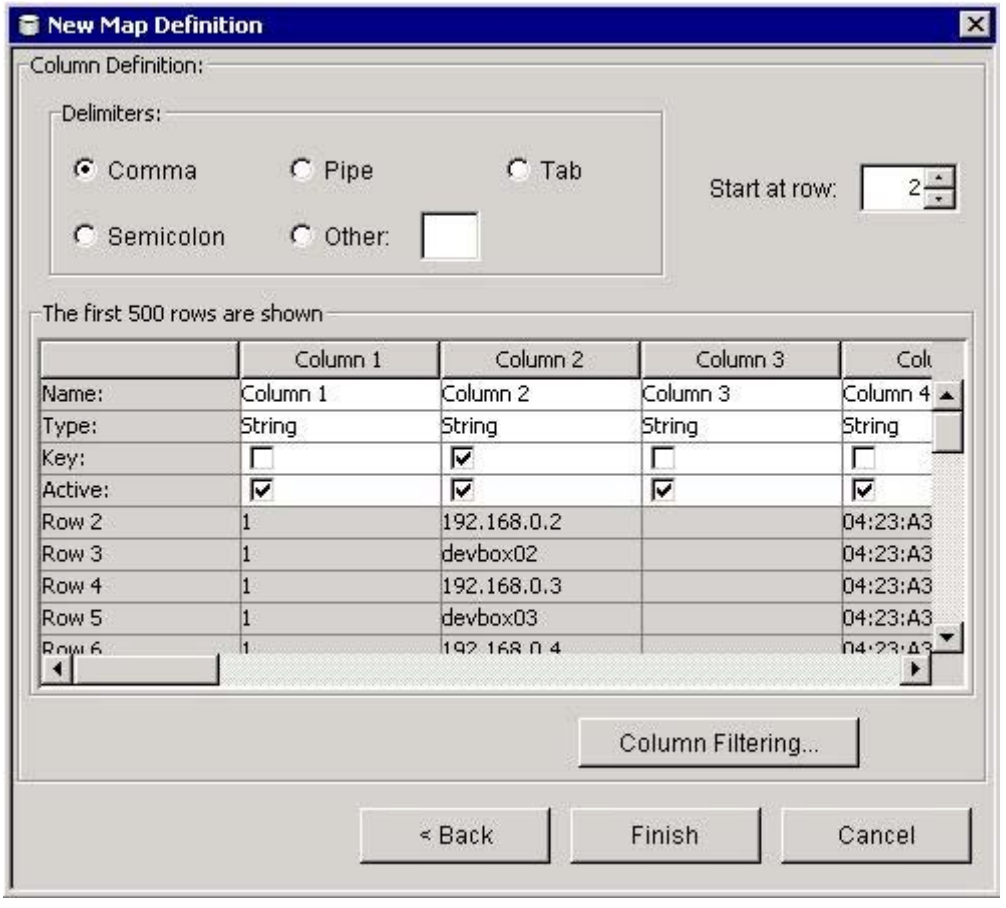
8. Legen Sie im Fenster „Neue Zuordnungsdefinition“ Folgendes fest:
   - Trennzeichen (Pipe, Komma, Semikolon usw.) für Daten in den Zeilen der Quelldatei mit Zuordnungsdaten
   - „Starten bei Reihe“ – Hiermit legen Sie die Anzahl der Zeilen fest, die vom Anfang der Quelldatei mit Zuordnungsdaten übersprungen werden sollen.
   - Spaltennamen
   - Spaltentypen – Zurzeit werden folgende Spaltentypen unterstützt:

     *Zeichenkette* – Eine Zeichenkette ist eine Menge von Zeichen, die von einem Computer als ein einzelnes Objekt verwendet wird. Eine Zeichenkette kann aus einem einzelnen Buchstaben, einem einzelnen Wort oder einer einzelnen Zahl bestehen. Bei dem Wort FINANZEN oder der IP-Adresse 192.168.2.40 kann es sich um eine Zeichenkette handeln. Außerdem können Zeichenketten aus einer Kombinantion von Wörtern, Leerzeichen und Zahlen bestehen. Die Anschrift HEINRICH-HEINE-STR. 133 kann eine Zeichenkette sein.

*Zahlenbereich* – Ein Zahlenbereich (NumberRange) ist ein Bereich von Zahlen. Der Bereich 10 bis 200 beispielsweise würde als „10-200“ angegeben. Zur Verwendung der Bereichszuordungsfunktion muss eine Bereichsdefinition genau eine Schlüsselspalte enthalten, die den Typ NumberRange aufweist. Wenn andere Schlüsselspalten vorhanden sind oder die Schlüsselspalte einen anderen Typ aufweist, wird die Zuordnung vom Zuordnungsservice nicht als Bereichszuordnung angesehen.

- Aktive Spalten – Wenn eine Spalte als aktiv gekennzeichnet ist, werden die Daten in der betreffenden Spalte mithilfe von Zuordnungen auf Prozesse verteilt. Alle Schlüsselspalten müssen aktiv sein. Alle aktiven Nicht-Schlüsselspalten können als *Zuordnungsspalte* auf der Registerkarte „Ereignisse“ ausgewählt werden.
- Schlüsselspalten – Ein Schlüssel ist ein eindeutiger Bezeichner für die Datenzeile in den Zuordnungsdaten. Wenn mehrere Spalten als Schlüsselspalten ausgewählt wurden, enthält der Gesamtschlüssel der Zuordnung alle Spalten, die als Schlüsselspalten ausgewählt wurden.
- „Spaltenfilter“ – Eine Zeile kann explizit anhand von Suchkriterien für eine bestimmte Spalte einbezogen bzw. ausgeschlossen werden. Damit können Zeilen aus den Zuordnungsquelldaten ausgeschlossen werden, die nicht benötigt werden oder die Zuordnung beeinträchtigen.

Beim Konfigurieren der einzelnen Einstellungen und Filter wird die Datentabelle automatisch aktualisiert, sodass Sie eine Vorschau der Daten erhalten und sich vergewissern können, dass die Daten erwartungsgemäß ausgewertet werden.



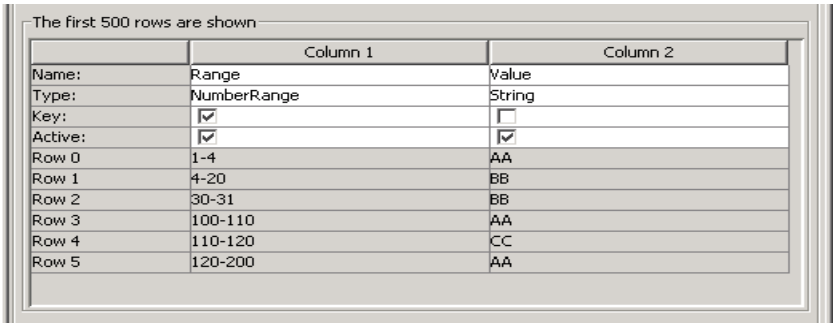

9. Wenn Sie alle Parameter und Filter für die Definition konfiguriert haben, klicken Sie auf *Fertig stellen*.
10. Wenn Sie oben in Schritt 7 „Lokale Datei“ ausgewählt haben, werden Sie aufgefordert, die Datei in den virtuellen Ordner für Ferndateien heraufzuladen, der sich an folgendem Speicherort befindet: %ESEC_HOME%\sentinel\bin\map_data. Geben Sie einen Dateinamen ein und klicken Sie auf *OK*.

### Hinzufügen einer Zuordnungsdefinition für einen Zahlenbereich

Damit Bereichszuordnungen verwendet werden können, muss eine Zuordnungsdefinition über genau eine Schlüsselspalte verfügen und die Schlüsselspalte muss den Typ „NumberRange“ aufweisen. Wenn andere Schlüsselspalten vorhanden sind oder die Schlüsselspalte einen anderen Typ aufweist, wird die Zuordnung vom Zuordnungsservice nicht als Bereichszuordnung angesehen.

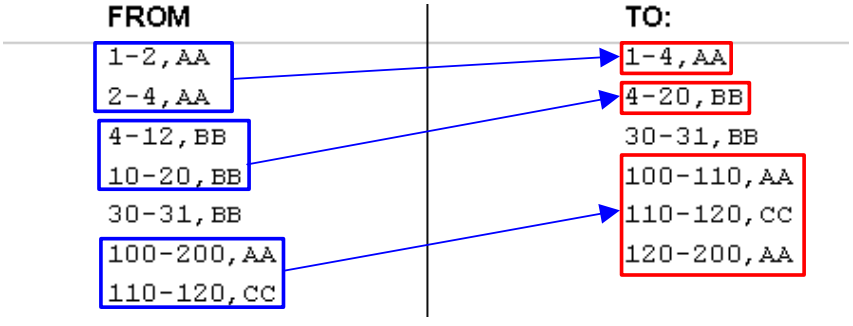
Wählen Sie zum Erstellen einer Bereichszuordnung eine einzige Spalte aus, die den Schlüssel der Zuordnung darstellen soll, und wählen Sie *NumberRange* als Typ der Spalte aus. Das Format der Daten in einer Spalte vom Typ *NumberRange* muss „m-n“ sein. Dabei ist „m“ die kleinste Zahl im Bereich und „n“ die größte Zahl im Bereich (z. B. 10-200). Die größte Zahl im Bereich gehört nicht zum Bereich (d. h. [m,n)). Das heißt, ein Bereich von 10-200 enthält nur Schlüsselzahlen von 10 bis 199. In den Beispieldaten stellt die erste Spalte den Schlüssel dar:

```
1-2,AA
2-4,AA
4-12,BB
10-20,BB
30-31,BB
100-200,AA
110-120,CC
```

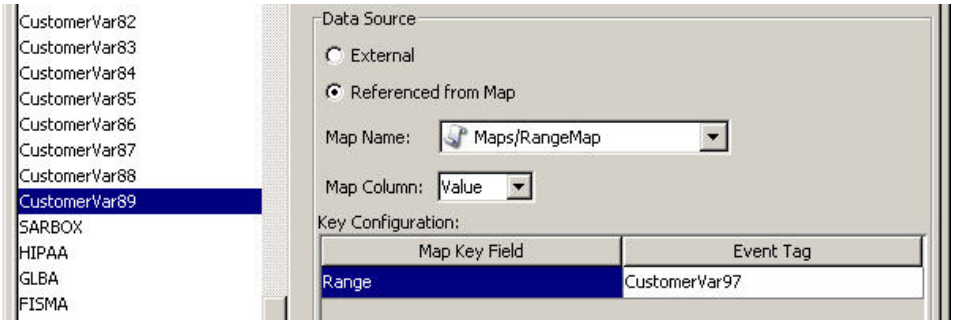

The first 500 rows are shown

| | Column 1 | Column 2 |
|---|---|---|
| Name: | Range | Value |
| Type: | NumberRange | String |
| Key: | ☑ | ☐ |
| Active: | ☑ | ☑ |
| Row 0 | 1-4 | AA |
| Row 1 | 4-20 | BB |
| Row 2 | 30-31 | BB |
| Row 3 | 100-110 | AA |
| Row 4 | 110-120 | CC |
| Row 5 | 120-200 | AA |

Beachten Sie, wie die Beispieltabelle transformiert wird.




Ein Beispiel für eine Ereigniskonfiguration für die obige Zuordnung kann wie folgt aussehen:



Dabei wird für „CustomerVar97“ erwartet, dass ein numerischer Wert enthalten ist (oder dass ein Typ vorliegt, der in einen numerischen Wert konvertiert werden kann, z. B. eine IP-Adresse oder ein Datum).

Beim Ausführen von Suchvorgängen in der Beispielbereichszuordnung erfasst der Wert in „CustomerVar97“ die Bereichszuordnung und sucht nach dem Bereich, zu dem der Wert gehört (sofern vorhanden). Im Folgenden sind einige Beispiele und die zugehörigen Ergebnisse aufgeführt:

```
CustomerVar97 = 1; CustomerVar89 will be set to AA
CustomerVar97 = 4; CustomerVar89 will be set to BB
CustomerVar97 = 300; CustomerVar89 will not be set
```

Intern konvertiert Sentinel IP-Adressen und Datumsangaben für Tags vom Typ „IPv4“ und „Datum“ in eine Ganzzahl.

IPv4-Tags:

- DestinationIP (dip)
- SourceIP (sip)

Date-Tags:

- CustomerVar11 bis CustomerVar20 (cv11 bis cv20)
- DateTime (dt)
- ReservedVar11 bis ReservedVar20 (rv11 bis rv20)

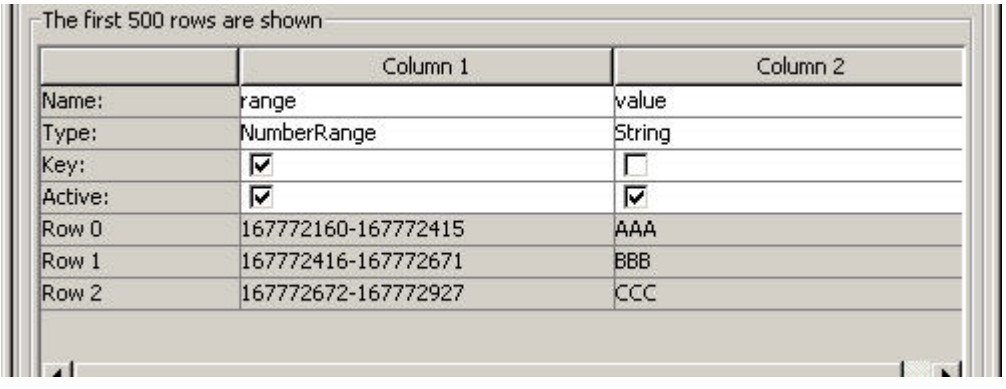
Weitere Informationen zu META-Tags finden Sie im Sentinel-Referenzhandbuch in Kapitel 5 „META-Tags für Wizard und Sentinel“.

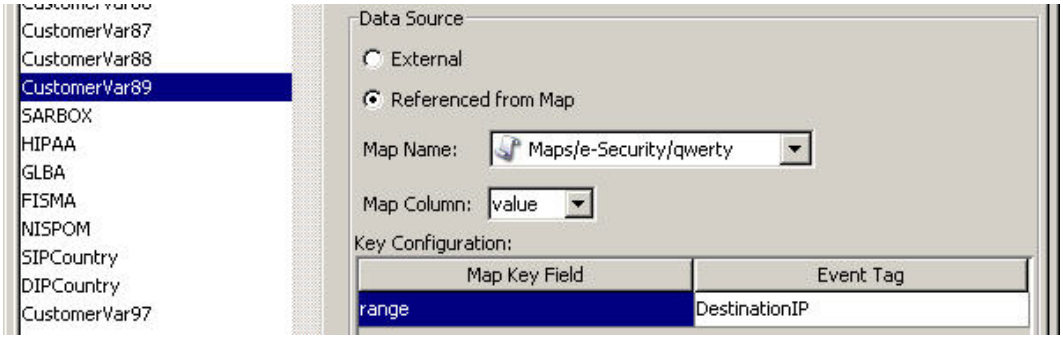
Für die unten stehende Tabelle ist Spalte 1 beispielsweise ein numerisches Bereichsäquivalent eines IP-Bereichs von 10.0.0.0 bis 10.0.2.255.

```
167772160-167772415,AAA
167772416-167772671,BBB
167772672-167772927,CCC
```

Verwenden Sie dieselben Einstellungen wie für das vorherige Beispiel, wenn Folgendes gilt:

- Die Ereigniskennung ist auf „DestinationIP“, und die Schlüsselspalte ist auf Spalte 1 („range“) festgelegt.
- Zuordnungsspalte ist Spalte 2 („value“). Die Ausgabewerte sind für „CustomerVar89“.






Wenn ein Ereignis eine Ziel-IP von 10.0.1.14 (entspricht einem numerischen Wert von 167772430) enthält, ist die Ausgabe für Spalte „CustomerVar89“ im Ereignis BBB.

Sentinel unterstützt die folgenden Zahlenbereiche:

- Bereich von negativer Zahl zu negativer Zahl (z. B. „-234--34“)
- Bereich von negativer Zahl zu positiver Zahl (z. B. „-234-34“)
- Bereich von positiver Zahl zu positiver Zahl (z. B. „234-236“)
- Bereich mit einer einzigen Zahl (negativ) (z. B. „-234“). In diesem Fall ist sowohl das Minimum als auch das Maximum -234.
- Bereich mit einer einzigen Zahl (positiv) (z. B. „234“). In diesem Fall ist sowohl das Minimum als auch das Maximum 234.
- Bereich von negativer Zahl zu maximaler Zahl (z. B. „-234-“) In diesem Fall ist das Minimum -234 und das Maximum ist (2^63 - 1).
- Bereich von positiver Zahl zu maximaler Zahl (z. B. „234-“) In diesem Fall ist das Minimum 234 und das Maximum ist (2^63 - 1).

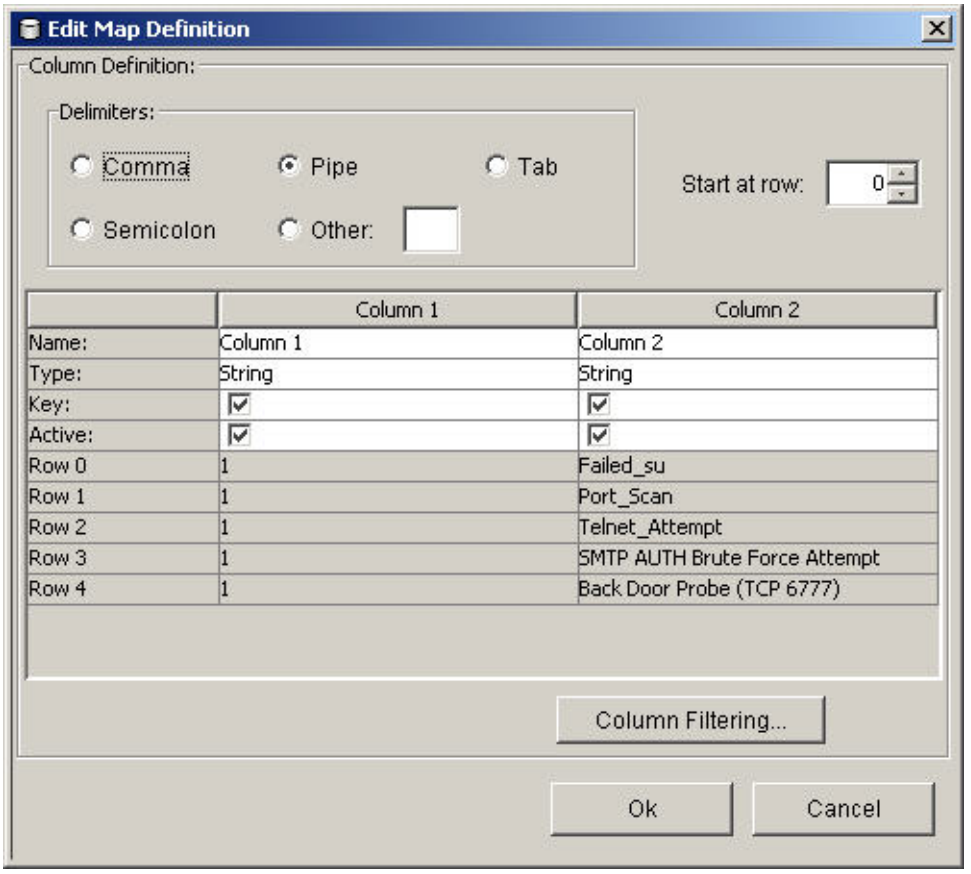
**HINWEIS**: In allen Fällen muss das Minimum kleiner als das oder gleich dem Maximum sein (beispielsweise ist „-234--235“ NICHT gültig).

## Bearbeiten von Zuordnungsdefinitionen

So bearbeiten Sie eine Zuordnungsdefinition

1. Klicken Sie auf die Registerkarte *Zuordnung*.
2. Erweitern Sie den gewünschten Ordner.
3. Markieren Sie eine Zuordnungsdefinition und klicken Sie auf *Bearbeiten*.

**HINWEIS**: Die Bearbeitungsfunktion ist deaktiviert für Zuordnungsdefinitionen, die sich im Systemordner befinden.




Mithilfe der Bearbeitungsfunktion können Sie Folgendes ausführen:

- Festlegen der Trennzeichen
- Festlegen der Startzeile der Zuordnung
- Umbenennen der Spalten
- Aktivieren bzw. Deaktivieren einer Spalte
- Festlegen der Spaltenschlüssel
- Filtern von Spalten

4. Wenn Sie die Änderungen vorgenommen haben, klicken Sie auf *OK*.

## Löschen von Zuordnungsdefinitionen

So löschen Sie eine Zuordnungsdefinition

1. Klicken Sie auf die Registerkarte *Zuordnung*.
2. Erweitern Sie den gewünschten Ordner.
3. Markieren Sie die zu löschende Zuordnungsdefinition.
4. Klicken Sie auf *Löschen.*.

**HINWEIS**: Zuordnungsdefinitionen unter dem Ordner „Sentinel“ können nicht gelöscht werden.

## Aktualisieren von Zuordnungsdaten

Beim Aktualisieren können Sie die Quelldatei mit Zuordnungsdaten einer Zuordnung auf dem DAS-Server durch eine andere Datei ersetzen. Die neue Quelldatei mit Zuordnungsdaten muss dasselbe Trennzeichen, dieselbe Anzahl von Spalten und dieselbe Gesamtstruktur wie die vorhandene Quelldatei mit Zuordnungsdaten aufweisen, damit die Zuordnung nach der Aktualisierung ordnungsgemäß funktioniert. Die neue Quelldatei mit Zuordnungsdaten darf nur in Bezug auf die Werte in den Spalten von der vorhandenen Datei abweichen. Wenn die neue Quelldatei mit Zuordnungsdaten eine andere Struktur als die vorhandene Datei aufweist, aktualisieren Sie die Zuordnungsdefinition mithilfe der Funktion Bearbeiten der SDM-GUI.

So aktualisieren Sie Zuordnungsdaten

1. Erstellen Sie eine Datei mit den Quelldaten für die neue Zuordnung auf dem Computer, auf dem SDM ausgeführt wird, wenn dies noch nicht erfolgt ist. Diese Datei kann automatisch generiert (z. B. aus einem Datendump-Skript) oder manuell völlig neu erstellt werden. Es kann sich aber auch um eine bearbeitete Version der vorhandenen Quelldatei mit Zuordnungsdaten handeln. Gegebenenfalls können Sie die vorhandene Quelldatei mit Zuordnungsdaten vom folgenden Speicherort abrufen:

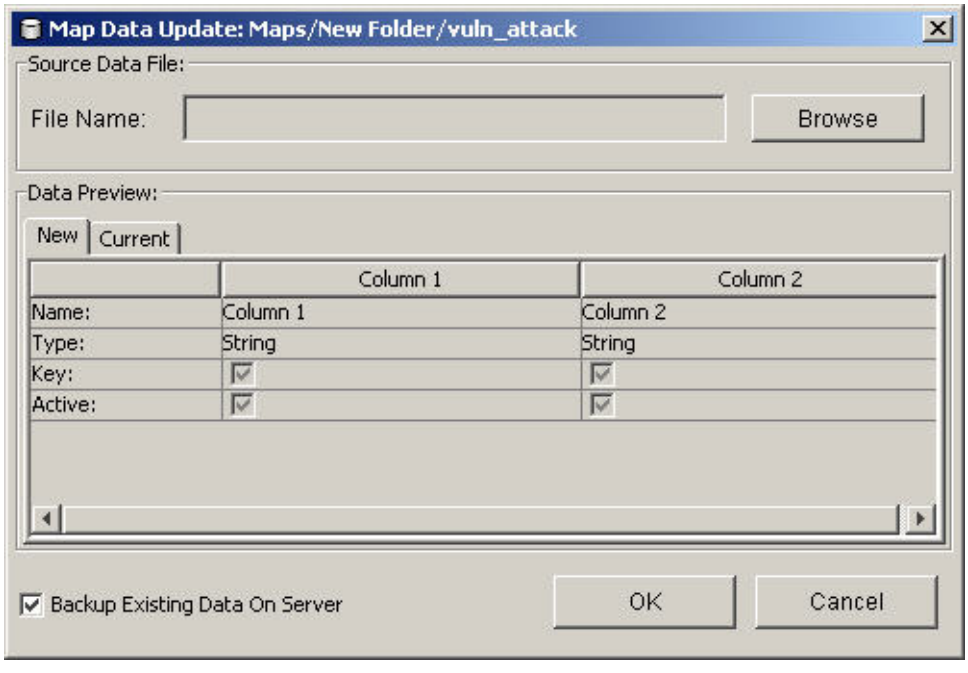
   Für Windows:

   ```
   %ESEC_HOME%\sentinel\bin\map_data
   ```

   Für UNIX:

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

2. Klicken Sie auf die Registerkarte *Zuordnung*.
3. Erweitern Sie den gewünschten Ordner. Markieren Sie die zu aktualisierende Zuordnung. Klicken Sie auf *Update* (Aktualisieren).



4. Wählen Sie die neue Quelldatei mit Zuordnungsdaten aus, indem Sie auf die Schaltfläche *Durchsuchen* klicken und die Datei mit den Daten für die neue Zuordnung auswählen. Nach dem Auswählen der Datei werden die Daten aus der Quelldatei mit Zuordnungsdaten auf der Registerkarte *Neu* angezeigt. Die zu ersetzenden Zuordnungsdaten werden auf der Registerkarte „Aktuell“ angezeigt.
5. Deaktivieren Sie die Standardeinstellung für *Auf Server vorhandene Daten sichern* oder behalten Sie diese bei. Wenn diese Option aktiviert ist, wird eine Sicherungskopie der vorhandenen Quelldatei mit Zuordnungsdaten im Ordner „%ESEC_HOME%\sentinel\bin\map_data“ (Windows) bzw. „$ESEC_HOME/sentinel/bin/map_data“ (UNIX) erstellt. Das Präfix des Namens der Sicherungskopie für die Quelldatei mit Zuordnungsdaten ist der Name der vorhandenen Quelldatei mit Zuordnungsdaten. Der restliche Teil des Dateinamens enthält einige nach dem Zufallsprinzip ausgewählte Zahlen, gefolgt von der Dateinamenerweiterung „.bak“. Beispiel: „vuln_attacks10197.bak“.
6. Klicken Sie auf *Ok*.
7. Die Daten aus der neuen Quelldatei mit Zuordnungsdaten werden auf den Server heraufgeladen und ersetzen den Inhalt der vorhandenen Quelldatei mit Zuordnungsdaten. Wenn die Quelldaten vollständig heraufgeladen wurden, werden die Zuordnungsdaten neu generiert und an die Zuordnungsclients verteilt (z. B. Collector Manager).

## Registerkarte „Ereignisse“

**HINWEIS**: Damit Sie die Registerkarte „Ereignisse“ verwenden können, muss die Datei „configuration.xml“ auf einen Kommunikationsserver verweisen, mit dem DAS_Binary und DAS_Query ebenfalls verbunden sind. Dies ist in der Standardeinstellung der Fall, sofern der Kommunikationsserver und DAS-Prozesse ausgeführt werden.

### Ereigniszuordnung

Die Ereigniszuordnung ist ein Mechanismus, mit dem Sie einem Ereignis Daten hinzufügen können, wobei mithilfe von bereits im Ereignis vorhandenen Daten auf Daten aus einer externen Quelle verwiesen wird und diese abgerufen werden. Die externe Datenquelle ist eine Zuordnung, die mithilfe der Registerkarte „Zuordnung“ definiert wird. Die bereits im Ereignis vorhandenen Daten, die als Verweis auf die Zuordnung fungieren sollen, und die Daten, die aus der Zuordnung in das Ereignis abgerufen werden sollen, werden auf der Registerkarte „Ereignisse“ festgelegt.

Da beliebige Daten in einer Zuordnung enthalten sein können, können mithilfe der Ereigniszuordnung Daten in den Ereignisstrom eingebunden werden, die aus beliebigen Quellen der jeweiligen Organisation stammen. Die Ereigniszuordnung bietet u. a. die folgenden Möglichkeiten:

- Überwachung der Regelkonformität
- Richtlinienkonformität
- Prioritätenfestlegung für Antworten
- Analyse von Sicherheitsdaten in Bezug auf Geschäftsvorgänge
- Verbesserung der Verantwortlichkeit

Wenn eine Ereigniszuordnung definiert ist, wird diese im gesamten System auf alle Ereignisse aller Collectors angewendet. Darüber hinaus verteilt Sentinel automatisch Zuordnungsdaten auf alle Prozesse, die Ereigniszuordnungen ausführen, und hält die Zuordnungsdaten in diesen Prozessen immer auf dem aktuellen Stand. Damit bietet die Ereigniszuordnung eine umfassende Unterstützung für Unternehmensbereitstellungen.

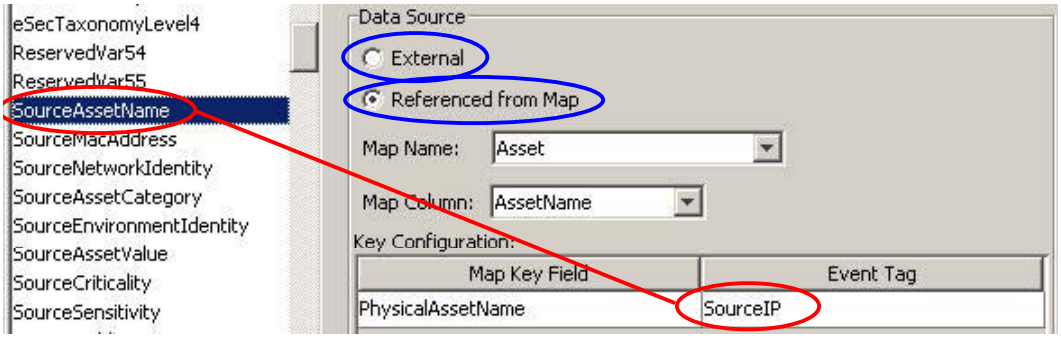
Die Ereigniszuordnung besteht aus vier Hauptbereichen:

- Controller – Hier werden alle Zuordnungsinformationen gespeichert.
- Distributor – Dieser verteilt die geänderten Zuordnungen automatisch neu an die Prozesse, die für die Zuordnung registriert sind.
- Monitor – Dies ist eine Überwachungsfunktion, die Änderungen in den Zuordnungsquelldaten erkennt.
- Generator – Hiermit werden Zuordnungen aus Quelldaten generiert.

Eine Anwendung der Ereigniszuordnung sind die Bestandsdatenfunktionen von Sentinel. Bestandsinformationen werden beispielsweise im Bestandsschema der Sentinel-Datenbank erfasst und gespeichert und mit einem physischen Bestandseintrag dargestellt. Immaterielle Bestände wie Services und Anwendungen werden durch einen Eintrag dargestellt, der mit einem physischen Bestand verknüpft ist. Der primäre automatisierte Aktualisierungsmechanismus für Bestandsdaten stützt sich auf einen Bestands-Collector, der Daten von einem Scanner wie Nmap liest. Der Bestands-Collector automatisiert das Abrufen von Bestandsinformationen durch das Lesen von Bestandsdaten vom Scanner und das Füllen der Bestandsschematabellen mit diesen Daten. Für die Ereigniszuordnung werden Bestandsinformationen von der Ziel-IP und der Quell-IP zugeordnet.

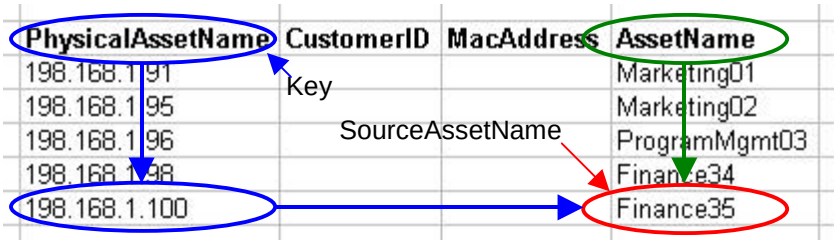
Es gibt zwei Typen von Datenquellen:

- „Extern“ – Ein Collector füllt diesen Wert in die Ereigniskennung.
- „Verweis von Zuordnung“ – Daten werden aus einer Zuordnung abgerufen, und die Kennung wird gefüllt.

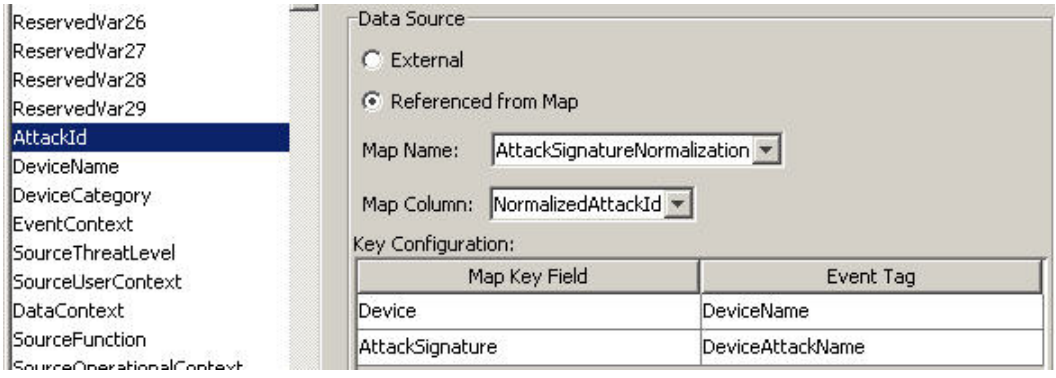


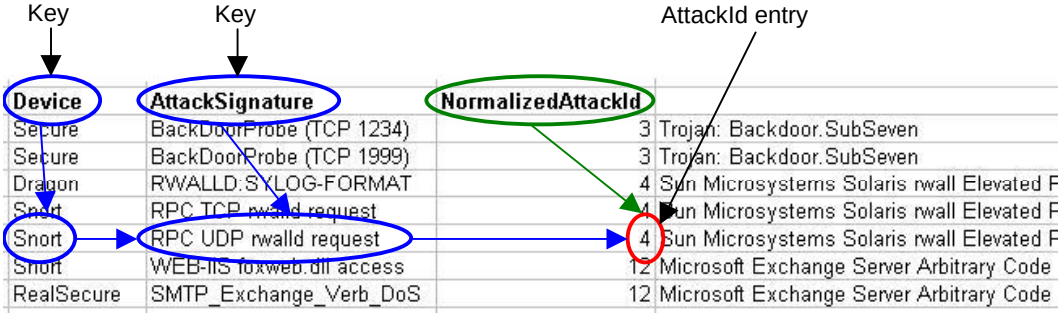

In der oben stehenden Abbildung wird die SourceAssetName-Kennung aus der Zuordnung „Asset“ gefüllt (deren Quelldatei mit Zuordnungsdaten „asset.csv“ ist). Der spezifische Wert für „SourceAssetName“ wird aus der Spalte „AssetName“ der Zuordnung „Asset“ übernommen. Die Spalte „PhysicalAssetName“ ist als Schlüssel festgelegt. Wenn die SourceIP-Kennung des Ereignisses einen der Quell-IP-Werte in der Spalte „PhysicalAssetName“ der Zuordnung findet, bildet die Zeile mit dem entsprechenden Schlüssel eine Schnittmenge mit der Spalte „AssetName“. Im unten stehenden Beispiel ist IP „198.168.1.100“ eine Entsprechung zu „AssetName Finance35“.

**HINWEIS**: Wenn eine Spalte als Schlüssel festgelegt ist, wird sie nicht im Dropdown-Feld „Spalte“ aufgelistet.




Sie können mehrere Spalten als Schlüssel festlegen, wenn die Zuordnung keine Bereichszuordnung sein soll (Bereichszuordnungen können nur eine Schlüsselspalte enthalten und der Spaltentyp muss auf „NumberRange“ festgelegt sein). Beispielsweise weist die AttackId-Kennung den Namen „DeviceName“ auf (Name des Sicherheitsgeräts), wenn der Spaltentyp auf „String“ festgelegt ist, die DeviceAttackName-Spalten sind als Schlüssel festgelegt und die Spalte „NormalizedAttackID“ in der Zuordnung „AttackNormalization“ wird als Wert verwendet. In einer Zeile, in der die DeviceName-Ereigniskennung den Daten in der Zuordnungsspalte „Device“ entspricht und der „DeviceAttackName“ den Daten in der Zuordnungsspalte „AttackSignature“ entspricht, ist der Wert für „AttackId“ der Wert in der Spalte „NormalizedAttackID“. Die soeben beschriebene Ereigniszuordnung ist wie folgt konfiguriert:

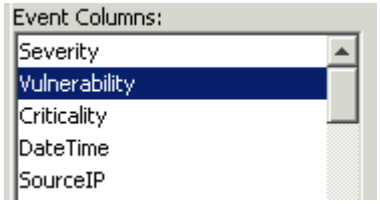


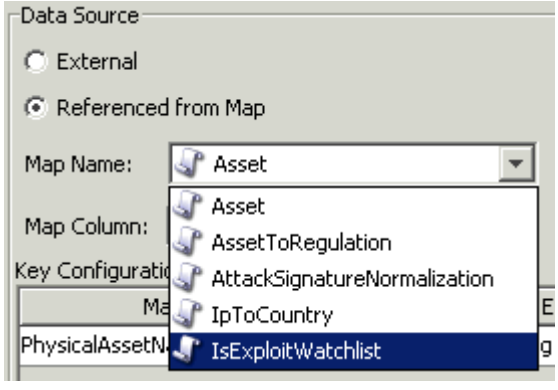

Konfigurieren von Ereigniskennungen (Spalten) für Zuordnungen

1. Klicken Sie auf die Registerkarte *Ereignisse*.
2. Markieren Sie einen Ereigniskennungseintrag in der Liste „Ereignisspalten“.

**HINWEIS**: Der ursprüngliche Name der Ereigniskennung wird über dem Feld „Label“ angezeigt. Darüber hinaus wird die Beschreibung der Ereignisspalte angegeben.



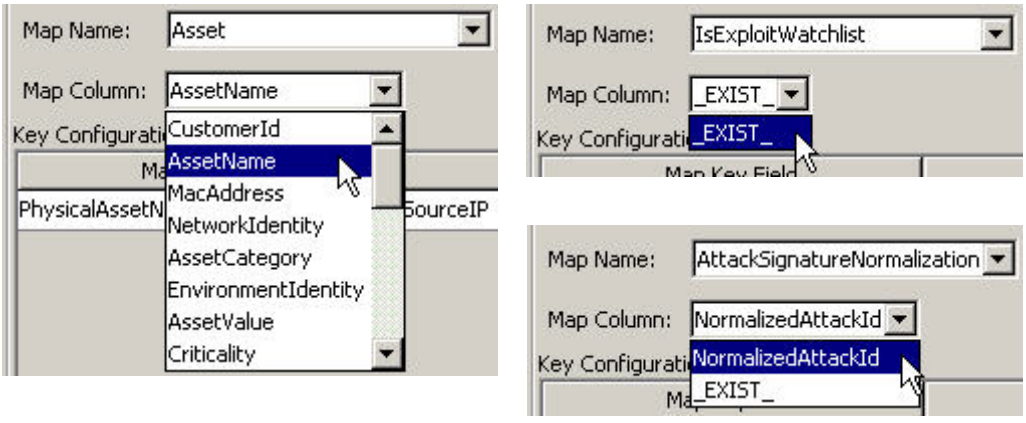

3. Klicken Sie auf *Verweis von Zuordnung*, um die Ereigniskennung so zu konfigurieren, dass sie mit Daten aus einer Zuordnung gefüllt wird. Klicken Sie auf *Extern*, um den Wert beizubehalten, der vom Collector in die Ereigniskennung geladen wurde (falls zutreffend).
4. Klicken Sie auf den Pfeil nach unten neben dem Feld *Zuordnungsname*.




Wählen Sie eine der Standardzuordnungen oder eine selbst erstellte Zuordnung aus:

- „Asset“ – Diese enthält die Daten aus der Quelldatei mit Zuordnungsdaten „asset.csv“. Die Datei „asset.csv“ wird automatisch aus Bestandsdaten aus der Sentinel-Datenbank generiert, wenn ein Bestands-Collector ausgeführt wird. Diese Datei kann ggf. auch manuell gefüllt werden.
- „AssetToRegulation“ – Diese enthält die Daten aus der Quelldatei mit Zuordnungsdaten „AssetToRegulation.csv“. Diese Datei muss manuell gefüllt werden.
- „AttackSignatureNormalization“ – Diese enthält die Daten aus der Quelldatei mit Zuordnungsdaten „attackNormalization.csv“ (IDS-Signaturen). Die Datei „attackNormalization.csv“ wird automatisch aus Advisor-Daten aus der Sentinel-Datenbank generiert, wenn ein Advisor-Feed ausgeführt wird.
- „IpToCountry“ – Diese enthält die Daten aus der Quelldatei mit Zuordnungsdaten „IpToCountry.csv“. Diese Datei muss manuell gefüllt werden.
- „IsExploitWatchlist“ – Diese enthält die Daten aus der Quelldatei mit Zuordnungsdaten „exploitDetection.csv“ (Anfälligkeiten und Bedrohungen). Die Datei „exploitDetection.csv“ wird automatisch aus Advisor- und Vulnerability-Daten aus der Sentinel-Datenbank generiert, wenn ein Advisor-Feed durchgeführt oder ein Anfälligkeits-Collector ausgeführt wird.

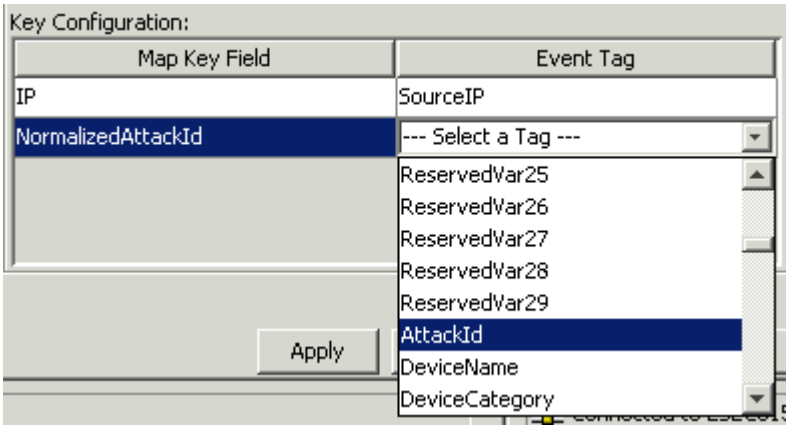
5. Klicken Sie auf den Pfeil nach unten neben dem Feld *Zuordnungsspalte* und wählen Sie einen Zuordnungsspaltennamen aus. Je nach dem ausgewählten Zuordnungsnamen im vorherigen Schritt variieren die verfügbaren Werte.




- „_EXIST_“ – Dies ist eine spezielle Zuordnungsspalte, die in jeder Zuordnung vorhanden ist. Wenn diese Zuordnungsspalte ausgewählt wird, wird eine „1“ in die Ereigniskennung eingefügt, wenn sich der Schlüssel in den Zuordnungsdaten befindet. Wenn der Schlüssel nicht in den Zuordnungsdaten enthalten ist, wird eine „0“ in die Ereigniskennung eingefügt.
- Alle anderen Auswahloptionen – Namen der aktiven Spalten in der Zuordnungsdefinition, die nicht als Schlüssel festgelegt sind (z. B. Spalte „CustomerId“ in „Asset“ oder Spalte „NormalizedAttackId“ in „AttackNormalization“).

6. Wählen Sie in „Schlüsselkonfiguration“ für jede Zeile in der Tabelle die Ereigniskennung in der Spalte „Ereigniskennung“ aus, mit dem die angegebene Zuordnungsschlüsselspalte in der entsprechenden Spalte „Schlüsselfeld zuordnen“ verglichen werden soll. Die vorhandenen Zeilen in der Tabelle „Schlüsselkonfiguration“ hängen vom ausgewählten Zuordnungsnamen ab.

**HINWEIS**: Ein Schlüssel ist ein eindeutiger Bezeichner für die Datenzeile in den Zuordnungsdaten.




7. Klicken Sie auf *Apply* (Anwenden).

**HINWEIS:** Wenn Sie auf *Anwenden* klicken, werden die an der zurzeit ausgewählten Ereignisspalte vorgenommenen Änderungen in einem temporären Puffer gespeichert. Wenn Sie nicht auf *Anwenden* klicken und eine andere Ereignisspalte auswählen, gehen die Änderungen an der zuvor ausgewählten Ereignisspalte verloren. Die Änderungen werden erst dann auf dem Server gespeichert, wenn Sie auf *Speichern* klicken.

8. Wenn Sie die *Ereigniszuordnung* einer anderen *Ereignis*spalte bearbeiten möchten, wiederholen Sie die obigen Schritte. Achten Sie darauf, dass Sie nach dem Bearbeiten der *Ereigniszuordnung* der einzelnen *Ereignis*spalten immer auf *Anwenden* klicken.
9. Klicken Sie auf *Speichern*.

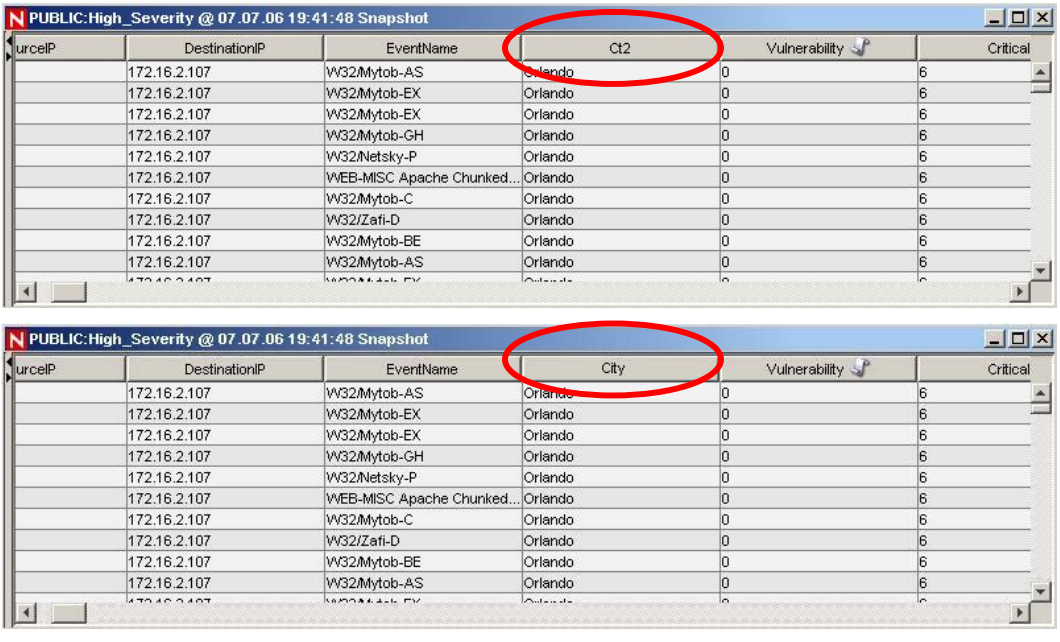
**HINWEIS**: Wenn Sie auf *Speichern* klicken, werden die Änderungen auf dem Server gespeichert. Mithilfe der Funktion *Speichern* werden alle (durch Auswahl von *Anwenden*) im temporären Puffer gespeicherten Änderungen auf dem Server gespeichert.

## Umbenennen von Kennungen

Auf der Registerkarte „Ereignisse“ können Sie auch Labeln von vorhandenen Ereigniskennungen Namen zuweisen. Sie können beispielsweise das Label für Ereigniskennung „Ct2“ in „City“ umbenennen. Dadurch wird die Ereigniskennung, die zuvor in Sentinel Control Center als „Ct2“ angezeigt wurde, mit dem Label „City“ angezeigt. Positionen, an denen Ereigniskennungen in Sentinel Control Center aufgeführt werden, sind Filter, Korrelationsregeln und Active Views.

Durch das Umbenennen von Kennungen wird jedoch nicht der Name der Variablen in Collector-Skripts geändert. Selbst wenn die Ereigniskennung mit dem Label „Ct2“ in „City“ umbenannt wurde, heißt die Variable, mit der in einem Collector-Skript auf dieses META-Tag verwiesen werden muss, „s_CT2“.

Im Folgenden finden Sie eine Abbildung dieser Funktion vor dem Vorgang und nach dem Vorgang in einer Active View.

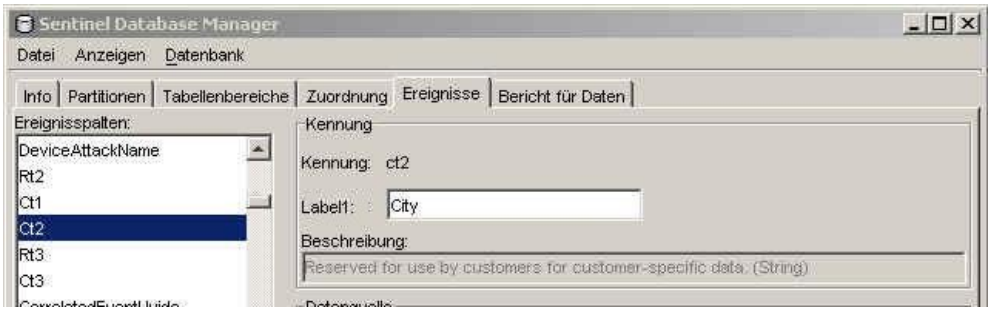



Umbenennen einer Ereignisspalte

1. Klicken Sie auf die Registerkarte *Ereignisse*.

**HINWEIS**: Der ursprüngliche Ereignisspaltenname wird über dem Feld „Label“ angezeigt. Darüber hinaus wird die Beschreibung der Ereignisspalte angegeben.

2. Markieren Sie einen Ereignisspalteneintrag.
3. Geben Sie im Feld „Label“ einen neuen Wert für die Ereignisspalte ein.




4. Klicken Sie auf *Apply* (Anwenden).

   **HINWEIS**: Wenn Sie auf *Anwenden* klicken, werden die an der zurzeit ausgewählten Ereigniskennung vorgenommenen Änderungen in einem temporären Puffer gespeichert. Wenn Sie nicht auf *Anwenden* klicken und eine andere Ereigniskennung auswählen, gehen die Änderungen an der zuvor ausgewählten Ereigniskennung verloren. Die Änderungen werden erst dann auf dem Server gespeichert, wenn Sie auf *Speichern* klicken.

5. Klicken Sie auf *Speichern*.

   **HINWEIS**: Wenn Sie auf *Speichern* klicken, werden die Änderungen auf dem Server gespeichert. Mithilfe der Funktion *Speichern* werden alle (durch Auswahl von *Anwenden*) im temporären Puffer gespeicherten Änderungen auf dem Server gespeichert.

6. Damit die Änderungen im Sentinel Control Center sichtbar werden, müssen ausgeführte Sentinel Control Centers geschlossen und erneut geöffnet werden.

## Registerkarte „Bericht für Daten“

**HINWEIS**: Damit Sie die Registerkarte „Bericht für Daten“ verwenden können, muss die Datei „configuration.xml“ auf einen Kommunikationsserver verweisen, mit dem DAS_Binary und DAS_Query ebenfalls verbunden sind. Dies ist in der Standardeinstellung der Fall, sofern der Kommunikationsserver und DAS-Prozesse ausgeführt werden.

Die Registerkarte *Bericht für Daten* stellt eine Schnittstelle zur Verwaltung von Zusammenfassungen für Sentinel dar. Mithilfe dieser Registerkarte können Sie **Zusammenfassungen** aktivieren und deaktivieren. Durch das Aktivieren einer Zusammenfassung kann die Aggregation mit dem Berechnen der Zählungen für die betreffende Zusammenfassung beginnen.

Eine Zusammenfassung ist eine definierte Menge von Attributen, aus denen sich der Schlüssel zusammensetzt, für den die Anzahl der eindeutigen Vorkommen (Anzahl der Ereignisse) pro Stunde (Ereigniszeitraum) berechnet werden soll. Im Fall von *EventSevDestPortSummary* wird bei einer Einstellung von „Aktiv“ die Anzahl der Ereignisse für jede eindeutige Kombination von Zielport und Schweregrad für einen Zeitraum von einer Stunde gespeichert. Diese gespeicherten Berechnungen der Ereignisdaten ermöglichen das schnellere Erstellen und Abfragen von Zusammenfassungsberichten. Diese Berichte werden von Crystal Reports verwendet. Weitere Informationen erhalten Sie in den Kapiteln zum Installieren von Crystal Reports im Sentinel-Installationshandbuch. Bestimmte Zusammenfassungen müssen *aktiv* sein, damit Zusammenfassungsberichte genau sind.

Die Aggregation ist der Prozess, bei dem die laufende Anzahl für alle aktiven Zusammenfassungen als Ereignisfluss im gesamten System berechnet wird. Diese laufenden Zählungen werden in der Datenbank in den entsprechenden Zusammenfassungstabellen gespeichert.

Vorteile von Zusammenfassungen:

- Stark reduzierte Menge von Ereignisdaten
- Angepasste Dimensionen, die Drill-down-, Rollup- und Drill-across-Vorgänge für Ereignisdaten ermöglichen
- Wesentlich schnellere Ausführung von Zusammenfassungsberichten mit vorab berechneten Zusammenfassungen

Vorteile der Aggregation:

- Nur aktive Zusammenfassungen werden verarbeitet.
- Es gibt keine Auswirkungen auf das Einfügen von Ereignissen in die Echtzeit-Datenbank.

Auf der Registerkarte „Bericht für Daten“ können Sie folgende Vorgänge ausführen:

- Aktivieren bzw. Deaktivieren vordefinierter Zusammenfassungen
- Anzeigen von Attributen für die einzelnen Zusammenfassungen
- Bestimmen der Gültigkeit einer Zusammenfassung für einen Zeitrahmen
- Abfragen der *Ereignisdateien*, die ausgeführt werden müssen, damit die Zusammenfassung vollständig ist

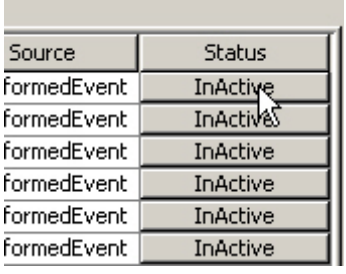
Bei den folgenden Zusammenfassungen handelt es sich um Zusammenfassungen, die bereits im System definiert sind. Dabei werden der Name der Zusammenfassung, der Name der Datenbanktabelle und die zugehörigen Attribute mit einer kurzen Beschreibung zur Zusammenfassung aufgelistet.

| **Name der Zusammenfassung** | **Tabelle/Beschreibung** |
|---|---|
| EventSrcSummary | EVT_SRC_SMRY_1<br>In dieser Zusammenfassung werden die Ereignisanzahl nach Quell-IP, Quellbestandsinformationen, Quellport, Quellbenutzer, Taxonomie, Ereignisname, Ressource, Collector, Protokoll, Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |
| EventDestSummary | EVT_DEST_SMRY_1<br>In dieser Zusammenfassung wird die Ereignisanzahl nach Ziel-IP, Zielbestandsinformationen, Zielport, Zielbenutzer, Taxonomie, Ereignisname, Ressource, Collector, Protokoll, Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |
| EventSevDestTxnmySummary | EVT_DEST_TXNMY_SMRY_1<br>In dieser Zusammenfassung wird die Ereignisanzahl nach Ziel-IP, Zielbestandsinformationen, Taxonomie, Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |

| Name der Zusammenfassung | Tabelle/Beschreibung |
|---|---|
| EventSevDestEvtSummary | EVT_DEST_EVT_NAME_SMRY_1<br>In dieser Zusammenfassung wird die Ereignisanzahl nach Ziel-IP, Zielereignisbestand, Taxonomie, Ereignisname, Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |
| EventSevDestPortSummary | EVT_PORT_SMRY_1<br>In dieser Zusammenfassung wird die Ereignisanzahl nach Zielport, Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |
| EventSevSummary | EVT_SEV_SMRY_1<br>In dieser Zusammenfassung wird die Ereignisanzahl nach Schweregrad und Ereigniszeit pro Stunde zusammengefasst. |

### Deaktivieren/Aktivieren von Zusammenfassungen

1. Klicken Sie auf die Registerkarte *Bericht für Daten.*
2. Klicken Sie zum Deaktivieren einer Zusammenfassung in der Spalte „Status“ auf die Schaltfläche *Aktiv*. Die Beschriftung der Schaltfläche wird in *Inaktiv* geändert.
3. Klicken Sie zum Aktivieren einer Zusammenfassung in der Spalte „Status“ auf die Schaltfläche *Inaktiv*. Die Beschriftung der Schaltfläche wird in *Aktiv* geändert.




So aktivieren Sie die *Aggregation für Top 10-Berichte* für Crystal Reports:

- Aktivieren Sie die folgenden drei Zusammenfassungen:
  - EventDestSummary
  - EventSevSummary
  - EventSrcSummary
- Aktivieren Sie „EventFileRedirectService“ in der Datei „das_binary.xml“ in folgendem Verzeichnis:

Für UNIX:

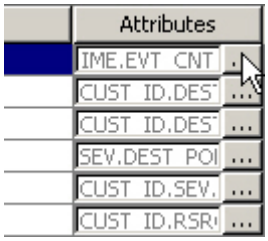
```
$ESEC_HOME/sentinel/config/das_binary.xml
```

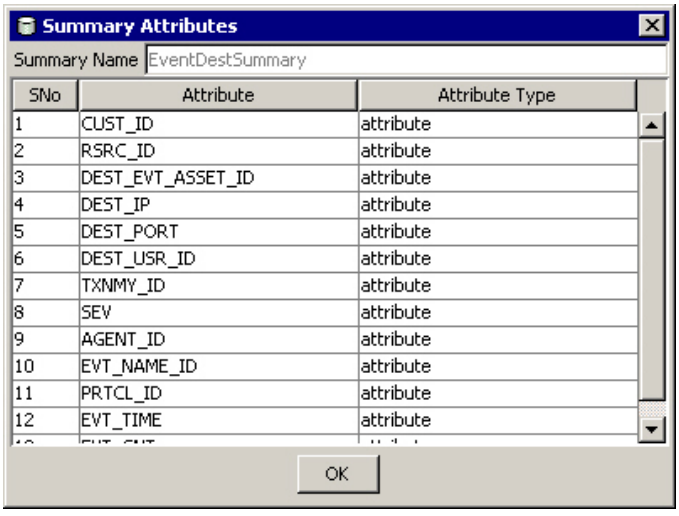
Für Windows:

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

### Anzeigen von Informationen für eine Zusammenfassung

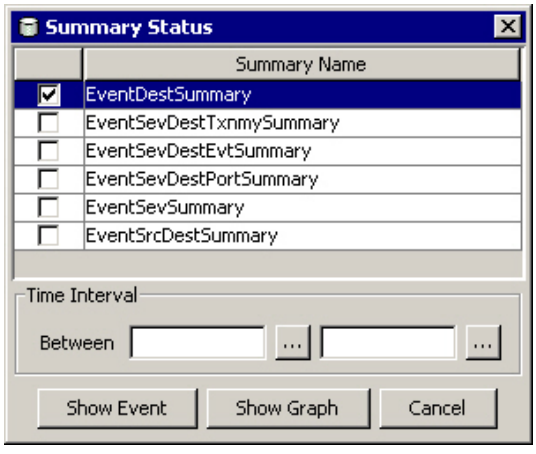
1. Klicken Sie auf die Registerkarte *Bericht für Daten.*
2. Klicken Sie auf die Schaltfläche mit den drei Punkten „…“ in der Spalte „Attribute“, um die Attribute anzuzeigen, aus denen sich eine Zusammenfassung zusammensetzt.



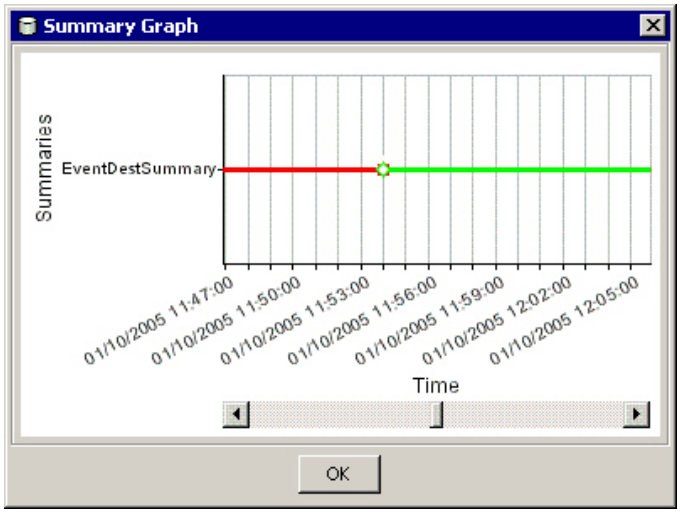




## Überprüfen der Gültigkeit einer Zusammenfassung

1. Klicken Sie auf die Registerkarte *Bericht für Daten.*
2. Wählen Sie *Status* aus.
3. Wählen Sie die abzufragende(n) Zusammenfassung(en) aus.



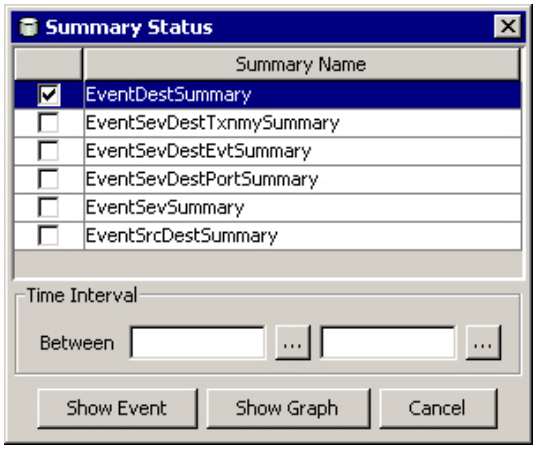

4. Wählen Sie ein Zeitintervall aus.
5. Klicken Sie auf *Diagramm anzeigen.*
6. Die grünen Balken verweisen darauf, dass die Zusammenfassung für den betreffenden Zeitrahmen vollständig ist. Die roten Bereiche geben an, dass in der Zusammenfassung für den betreffenden Zeitraum Daten fehlen.




**HINWEIS**: Weitere Informationen zum Vervollständigen von Zusammenfassungen finden Sie im Abschnitt *Ausführen von Ereignisdateien für eine Zusammenfassung*.

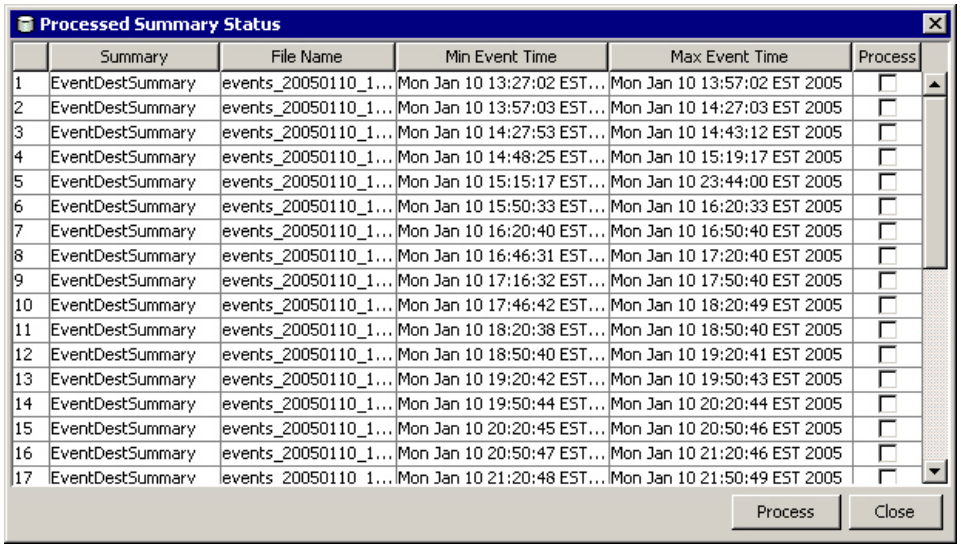
## Abfragen der Ereignisdateien für eine Zusammenfassung

1. Klicken Sie auf die Registerkarte *Bericht für Daten.*
2. Wählen Sie *Status* aus.
3. Wählen Sie die abzufragende(n) Zusammenfassung(en) aus.



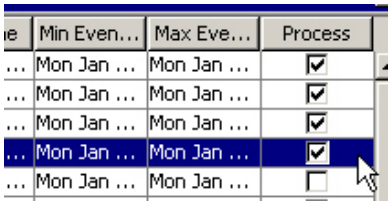

4. Wählen Sie ein Zeitintervall aus.
5. Click *Show Event.*
6. Die erforderlichen Ereignisdateien zum Vervollständigen der Zusammenfassung werden in einem Listenformat angezeigt.

**HINWEIS**: Weitere Informationen zum Vervollständigen von Zusammenfassungen finden Sie im Abschnitt *Ausführen von Ereignisdateien für eine Zusammenfassung*.




Ausführen von Ereignisdateien für eine Zusammenfassung

1. Klicken Sie auf die Registerkarte *Bericht für Daten.*
2. Wählen Sie *Status* aus.
3. Wählen Sie die abzufragende(n) Zusammenfassung(en) aus.
4. Wählen Sie ein Zeitintervall aus.
5. Click *Show Event.*
6. Die erforderlichen *Ereignisdateien* zum Vervollständigen der Zusammenfassung werden in einem Listenformat angezeigt.
7. Überprüfen Sie die Ereignisdateien, die ausgeführt werden sollen, um die Zusammenfassung zu vervollständigen.




8. Klicken Sie auf *Vorgang*.

# SDM-Befehlszeile

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

## Speichern von Verbindungseigenschaften für Sentinel Data Manager

Dieser Vorgang muss vor der Verwendung anderer Sentinel Data Manager-Befehlszeilenoptionen als „saveConnection“ ausgeführt werden.

Wenn Sie die SDM-GUI ausgeführt haben, können Sie die Datei „sdm.connect“ verwenden, die aus der GUI erstellt wurde. Diese befindet sich unter Windows im Verzeichnis „%ESEC_HOME%\sdm“ und unter UNIX im Verzeichnis „$ESEC_HOME/sdm“.

Die Funktion zum Speichern von Verbindungsinformationen speichert neben dem (mit dem in „configuration.xml“ angegebenen Keystore) verschlüsselten Passwort die folgenden Verbindungsdaten in der angegebenen Datei.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | saveConnection |
| -server | <Oracle oder MSSQL> |
| -host | <IP-Adresse des Datenbank-Host oder Hostname für Verbindung> |
| -port | <Datenbank-Portnummer für Verbindung [Standard bei Oracle: 1521/Standard bei SQL Server: 1433]> |
| -database | <Datenbankname/SID für Verbindung> |
| -user | <Datenbank-Benutzername> |
| -password | <Datenbankpasswort> |
| -winAuth | Für Windows-Authentifizierung verwendet. Bei Verwendung dieser Option, dürfen Sie -user und –password nicht verwenden. |
| -connectFile | <Dateiname zum Speichern der Verbindungsdetails [frei wählbarer Dateiname]> |

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

### Ausführen von „saveConnection“

1. Führen Sie den Befehl wie folgt aus:

```
sdm -action saveConnection -server <Oracle/MSSQL> -
   host <Host-IP/Hostname> -port <Portnummer> -
   database <Datenbankname/SID> [-driverProps
   <Eigenschaftendatei>] {-user <Datenbankbenutzer> -
   password <Datenbankpasswort>} -connectFile
   <Dateiname_zum_Speichern_der_Verbindung>
```

   Im folgenden Beispiel werden Verbindungen für einen Host mit der IP-Adresse 172.16.0.36 an Port 1521 (Standard für Oracle, für SQL Server ist der Standardport 1433) gespeichert.

   - Beispiel für Oracle:

```
./sdm -action saveConnection -server oracle -host
   172.16.0.36 -port 1521 -database esec -user esecdba
   -password XXXXXX -connectFile sdm.connect
```

   - Beispiel für SQL Server:

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

Im folgenden Beispiel werden Verbindungen für einen Host mit der IP-Adresse 172.16.0.36 und Port 1433 mit dem Datenbanknamen „esec_51“ für die Windows-Authentifizierung gespeichert.

- Beispiel für SQL Server (Windows-Authentifizierung):

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

Dadurch werden die Verbindungsdetails in der Datei „sdm.connect“ gespeichert. Die restlichen Befehle verwenden diesen Dateinamen als Eingabe, um die Verbindung mit der designierten Datenbank herzustellen und ihre Aktionen auszuführen.

## Verwaltung von Partitionen

### Partitionskonfiguration

Dieser Abschnitt bezieht sich ausschließlich auf Oracle. Mit dieser Aktion („partitionConfig“) werden Ihre Datenbankpartitionen konfiguriert. Mit dieser Konfiguration wird festgelegt, auf welche Weise die Partitionen zu sämtlichen partitionierten Sentinel-Tabellen hinzugefügt werden. Für diese Aktion werden folgende Flags verwendet:

| | |
|---|---|
| -action | partitionConfig |
| -freq | <entweder „3D“ oder „2D“ oder „1D“ oder „1W“><br><br>Es werden lediglich die folgenden Optionen unterstützt:<br>„3D“ – drei Partitionen pro Tag<br>„2D“ – zwei Partitionen pro Tag<br>„1D“ – eine Partition pro Tag<br>„1W“ – eine Partition pro Woche |
| -days | <Anzahl der hinzuzufügenden Tage bei jedem Auswählen von „addPartitions“> |
| -connectFile | <Pfad des Dateinamens, der von „saveConnection“ gespeichert wird> |

Ausführen von „partitionConfig“

1. Führen Sie diesen Befehl wie folgt aus:

```
./sdm -action partitionConfig –freq <either 3D or 2D
   or 1D or 1W> -days <Number Of days to be added
   whenever “addPartitions” is chosen> -connectFile
   <path to the filename saved by “saveConnection”
   (default: $ESEC_HOME/sdm/sdm.connect)>
```

Im folgenden Beispiel werden vom System 30 Partitionen (drei Partitionen pro Tag; 1 DAY = 3 * 10) hinzugefügt.

```
./sdm -action partitionConfig -freq 3D -days 10 -
   connectFile sdm.connect
```

Im folgenden Beispiel werden vom System 10 Partitionen (eine Partition pro Tag; 1 DAY = 1 * 10) hinzugefügt.

```
./sdm -action partitionConfig -freq 1D -days 10 -
   connectFile sdm.connect
```

Im folgenden Beispiel wird vom System eine Partition (eine Partition in sieben Tagen; 7 days = 1 * 10/7) hinzugefügt.

```
./sdm -action partitionConfig -size 1W -days 10 -
   connectFile sdm.connect
```

### Hinzufügen von Partitionen

Mit dieser Aktion („addPartitions“) wird die erforderliche Anzahl von Partitionen entsprechend der Partitionskonfiguration in den folgenden Tabellen hinzugefügt:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Wenn in der Konfiguration Partitionen für 10 Tage festgelegt sind, wird bei jedem Ausführen von *addPartitions* überprüft, ob Partitionen für die nächsten 10 Tage verfügbar sind. Wenn eine ausreichende Anzahl von Partitionen für die nächsten 10 Tage vorhanden ist, wird keine Aktion ausgeführt. Wenn dies nicht der Fall ist, wird die erforderliche Anzahl von Partitionen für 10 Tage hinzugefügt.

Für diese Aktion werden folgende Flags verwendet:

| | |
|---|---|
| -action | addPartitions |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

Ausführen von „addPartitions“

1. Führen Sie diesen Befehl wie folgt aus:

   ```
   sdm -action addPartitions -connectFile <path to the
      filename saved by “saveConnection”>
   ```

   Beispiel für Oracle:

   ```
   ./sdm -action addPartitions -connectFile sdm.connect
   ```

Beispiel für SQL Server:

```
sdm -action addPartitions -connectFile sdm.connect
```

### Verwerfen von Partitionen

Durch diese Aktion („dropPartition“) werden alle Partitionen aus den folgenden Tabellen verworfen, die älter sind, als im Flag „keepDays“ festgelegt ist:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Bei dieser Aktion werden keine Partitionen verworfen, die nicht archiviert wurden. Wenn nicht archivierte Partitionen gelöscht werden sollen, verwenden Sie das Flag *forceDelete*. Bei Verwendung von „forceDelete“ gilt Folgendes:

| | |
|---|---|
| „falsch“ oder nicht angegeben | Es werden nur die Partitionen verworfen, die älter sind als in „keepDays“ festgelegt, sowie die archivierten Partitionen. |
| „wahr“ | Es werden alle Partitionen verworfen, die älter sind als „keepDays“, auch wenn sie nicht archiviert wurden. |

Für diese Aktion werden folgende Flags verwendet:

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

**HINWEIS:** Wenn Sie eine nicht archivierte Partition verwerfen, kann diese nicht importiert werden.

Ausführen von „dropPartition“

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action dropPartitions [-forceDelete <false>] -
   keepDays <Anzahl> -connectFile <Pfad zu dem durch
   „saveConnection“ gespeicherten Dateinamen>
```

   In den folgenden Beispielen werden alle Partitionen verworfen, die älter als 30 Tage sind, wobei sichergestellt wird, dass alle Partitionen archiviert sind. Alle Partitionen, die übersprungen (nicht entfernt) werden, weil sie nicht archiviert sind, werden nach Abschluss des Vorgangs aufgelistet.

   Beispiel für Oracle:

```
./sdm -action dropPartitions -keepDays 30 -connectFile
   sdm.connect


./sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

   Beispiel für SQL Server:

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


sdm -action dropPartitions -forceDelete false -
   keepDays 30 -connectFile sdm.connect
```

## Anzeigen von Partitionszusammenfassungen

Mit dieser Aktion („ViewPartitions“) wird die Partitionszusammenfassung für die folgenden unterstützten Tabellen angezeigt:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | startGui |
| -tableName | <Name einer der oben aufgeführten Tabellen> |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

So zeigen Sie Partitionszusammenfassungen an

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action viewPartitions -tableName <Tabellenname> –
   connectFile <Pfad zu dem durch „saveConnection“
   gespeicherten Dateinamen>
```

   Im folgenden Beispiel werden die Liste der Partitionen der Tabelle „EVENTS“ und der Status der einzelnen Partitionen angezeigt.

   - Beispiel für Oracle:

```
./sdm -action viewPartitions -tableName EVENTS -
   connectFile sdm.connect
```

   - Beispiel für SQL Server:

```
sdm -action viewPartitions –tableName EVENTS –
   connectFile sdm.connect
```

# Verwaltung der Archivierung

## Konfiguration der Archivierung

Mit dieser Aktion („archiveConfig“) wird die Archivierung konfiguriert. Diese Konfiguration steuert, wie die Daten aus den Sentinel-Tabellen archiviert werden.

Für diese Aktion werden folgende Flags verwendet:

| | |
|---|---|
| -action | archiveConfig |
| -dirPath | <gültiger Verzeichnispfad, in den die archivierten Dateien geschrieben werden sollen> |
| -keepDays | <Beibehaltungsdauer in Tagen> |
| -fileSize | (nur für Oracle) <Maximale Größe der einzelnen archivierten Dateien. Geben Sie die Größe in KB, MB oder GB an.> |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

Für Oracle muss der dirPath-Verzeichnispfad als UTL_FILE_DIR-Parameter in der Datei „init.ora“ entsprechend den Oracle-Anforderungen angegeben werden. Folgendes muss angegeben werden:

- UTL_FILE_DIR = *
- UTL_FILE_DIR = bestimmtes Verzeichnis in der Datei „init.ora“, in das die Dateien geschrieben werden sollen

Ausführen von „archiveConfig“

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action archiveConfig  -dirPath <Pfad zu dem
   Verzeichnis, in das die archivierten Dateien
   geschrieben werden sollen> -keepDays <Beibehaltung
   in Tagen> -fileSize <maximale Größe der einzelnen
   archivierten Dateien, angegeben in KB, MB oder GB>
   -connectFile <Pfad zu dem durch „saveConnection“
   gespeicherten Dateinamen>
```

   - Beispiel für Oracle:

   Im folgenden Beispiel werden alle Daten, die älter als 13 Tage sind, in Abschnitten (größer als 1 GB) in das Verzeichnis „/tmp“ geschrieben.

```
./sdm -action archiveConfig  -dirPath /tmp -keepDays
   13 -fileSize 1GB -connectFile sdm.connect
```

   Im folgenden Beispiel werden alle Daten, die älter als 13 Tage sind, in Abschnitten (größer als 40 MB) in das Verzeichnis „/tmp“ geschrieben.

```
./sdm -action archiveConfig -dirPath /tmp -keepDays 13
   -fileSize 40MB -connectFile sdm.connect
```

## Archivieren von Daten

Führen Sie diese Aktion („archiveData“) aus, nachdem Sie die Archivierung konfiguriert haben („archiveConfig“). Mit dieser Aktion werden die Daten aus der angegebenen Tabelle entsprechend der Archivierungskonfiguration archiviert. Daten werden aus den folgenden Tabellen archiviert:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS

**HINWEIS**: Aggregationstabellen werden nicht archiviert.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | archiveData |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

Ausführen von „archiveData“

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action archiveData -connectFile <Pfad zu dem
   durch „saveConnection“ gespeicherten Dateinamen>
```

   - Beispiel für Oracle:

   Im folgenden Beispiel werden Ereignisse, deren benutzerdefinierte und reservierte Werte sowie korrelierte Ereignisse aus den Tabellen EVENTS, EVT_RESERVED_VALUES, EVT_CUSTOM_VALUES und ASSOCIATIONS entsprechend dem in der Archivierungskonfiguration („archiveConfig“) festgelegten Wert archiviert.. Wenn der im Beispiel aus dem Abschnitt Verwaltung der Archivierung festgelegte Wert verwendet wird, werden Daten archiviert, die älter als 13 Tage sind.

```
./sdm -action archiveData -connectFile sdm.connect
```

   - Beispiel für SQL Server:

   Im folgenden Beispiel werden Ereignisse und korrelierte Ereignisse entsprechend dem Wert archiviert, der in der Archivierungskonfiguration („archiveConfig“) festgelegt ist. Wenn der im Beispiel aus dem Abschnitt Verwaltung der Archivierung festgelegte Wert verwendet wird, werden Daten archiviert, die älter als 13 Tage sind.

```
sdm -action archiveData -connectFile sdm.connect
```

## Löschen von Daten

Mit dieser Aktion („deleteData“) werden die Daten aus der angegebenen Tabelle gelöscht, die älter sind, als in „keepDays“ festgelegt ist. Daten werden aus den folgenden Tabellen gelöscht:

- Oracle:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

- SQL Server:
  - EVENTS
  - CORRELATED_EVENTS
  - EVT_DEST_EVT_NAME_SMRY_1
  - EVT_DEST_SMRY_1
  - EVT_DEST_TXNMY_SMRY_1
  - EVT_PORT_SMRY_1
  - EVT_SEV_SMRY_1
  - EVT_SRC_SMRY_1

Bei dieser Aktion werden keine Partitionen verworfen, die nicht archiviert wurden. Wenn Sie nicht archivierte Partitionen löschen möchten, muss die optionale Flagge *forceDelete* angegeben sein und den Wert „true“ (wahr) aufweisen. Bei Verwendung von „forceDelete“ gilt Folgendes:

| | |
|---|---|
| „falsch“ oder nicht angegeben | Es werden nur die Partitionen verworfen, die älter sind als in „keepDays“ festgelegt, sowie die archivierten Partitionen. |
| „wahr“ | Es werden alle Partitionen verworfen, die älter sind als „keepDays“, auch wenn sie nicht archiviert wurden. |

Für diesen Befehl werden folgende Flags verwendet:

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

Ausführen von „deleteData“

1. Führen Sie diesen Befehl wie folgt aus:

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

   - Beispiel für Oracle:

   Im folgenden Beispiel werden die Partitionen aus allen Tabellen verworfen, die älter als 13 Tage sind. Dabei wird sichergestellt, dass alle verworfenen Partitionen archiviert wurden. Nach Abschluss des Vorgangs wird eine Liste der Partitionen generiert, die nicht gelöscht wurden, weil sie nicht archiviert wurden.

```
./sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

   - Beispiel für SQL Server:

   Im folgenden Beispiel werden die Partitionen aus allen Tabellen verworfen, die älter als 13 Tage sind. Dabei wird sichergestellt, dass alle verworfenen Partitionen archiviert wurden. Nach Abschluss des Vorgangs werden alle Partitionen aufgelistet, die nicht gelöscht wurden, weil sie nicht zuvor archiviert wurden.

```
sdm -action deleteData -keepDays 13 -connectFile
   sdm.connect
```

## Importverwaltung

### Auflisten der zu importierenden Dateien

Mit dieser Aktion („filesToImport“) werden die Dateien aufgelistet, die zum Importieren der Daten aus dem angegebenen Zeitraum aus den folgenden unterstützten Tabellen erforderlich sind:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS

- HIST_CORRELATED_EVENTS

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | filesToImport |
| -startDate | <MM/TT/JJJJ hh24:min:ss> |
| -endDate | <MM/TT/JJJJ hh24:min:ss> |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

**HINWEIS:** „hh24“ sind die im 24-Stunden-Format dargestellten Stunden. 1:15:00 p.m. steht beispielsweise für 13:15:00, und 3:00:00 a.m. stellt 03:00:00 dar.

### Ausführen von „filesToImport“

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action filesToImport -startDate <MM/TT/JJJJ
   hh24:min:ss> -endDate <MM/TT/JJJJ hh24:min:ss> -
   connectFile <Pfad zu dem durch „saveConnection“
   gespeicherten Dateinamen>
```

   Im folgenden Beispiel werden alle Dateien mit Daten aus dem Zeitraum zwischen „09/25/2003 00:00:00“ (25. September, Mitternacht) und „09/26/2003 00:00:00“ (26. September, Mitternacht) aufgelistet, die zuvor archiviert wurden und wieder importiert werden können.

   - Beispiel für Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

   - Beispiel für SQL Server:

```
./sdm -action filesToImport -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

   Im folgenden Beispiel werden alle Dateien mit Daten aus dem Zeitraum zwischen „09/25/2003 16:00:00“ (25. September, 16:00 Uhr) und „09/26/2003 18:00:00“ (26. September, 18:00 Uhr) aufgelistet, die zuvor archiviert wurden und wieder archiviert werden können.

   - Beispiel für Oracle:

```
./sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

   - Beispiel für SQL Server:

```
./sdm -action filesToImport -startDate 09/25/2003
   16:00:00 -endDate 09/26/2003 18:00:00 -connectFile
   sdm.connect
```

### Importieren von Daten

Mit dieser Aktion („importData“) werden Daten aus dem angegebenen Zeitraum in die folgenden unterstützten Tabellen importiert:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Wenn die Daten bereits importiert wurden oder für den angegebenen Zeitraum keine archivierten Daten gefunden wurden, wird eine entsprechende Meldung zurückgegeben.

Die Anwendung importiert die einzelnen Dateien in eine Tabelle und erstellt die Verlaufsansicht für alle historischen Tabellen. In der Berichtsansicht sind die ursprüngliche Tabelle und die Verlaufsansicht zusammengefasst. Alle Berichte stützen sich auf die Berichtsansicht, und daher werden alle importierten Daten angezeigt.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | importData |
| -startDate | <MM/TT/JJJJ hh24:min:ss> |
| -endDate | <MM/TT/JJJJ hh24:min:ss> |
| -dirPath | <Verzeichnis, aus dem die Dateien importiert werden sollen> |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

**HINWEIS:** „hh24“ sind die im 24-Stunden-Format dargestellten Stunden. 1:15:00 p.m. steht beispielsweise für 13:15:00, und 3:00:00 a.m. stellt 03:00:00 dar.

Ausführen von „importData“

1. Platzieren Sie alle Dateien, die importiert werden sollen, in einem bestimmten Verzeichnis (d. h. „dirPath“ – <Verzeichnis, aus dem die Dateien importiert werden sollen>).
2. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action importData -dirPath <Verzeichnis, aus dem
   die Dateien importiert werden sollen> -startDate
   <MM/TT/JJJJ hh24:min:ss> -endDate <MM/TT/JJJJ
   hh24:min:ss> -connectFile <Pfad zu dem durch
   „saveConnection“ gespeicherten Dateinamen>
```

   Im folgenden Beispiel werden die archivierten Dateien mit den Daten aus dem Zeitraum zwischen „09/25/2003 00:00:00“ (25. September, Mitternacht) und „09/26/2003 00:00:00“ (26. September, Mitternacht) aus dem Verzeichnis „tmp“ in die oben aufgeführten Tabellen importiert.

   - Beispiel für Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003 00:00:00
   -connectFile sdm.connect
```

- Beispiel für SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 00:00:00 -endDate 09/26/2003 00:00:00
   -connectFile sdm.connect
```

Im folgenden Beispiel werden die archivierten Dateien mit den Daten aus dem Zeitraum zwischen „09/25/2003 08:30:00“ (25. September, 08:30 Uhr) und „09/26/2003 20:00:00“ (26. September, 20:00 Uhr) aus dem Verzeichnis „tmp“ in die oben aufgeführten Tabellen importiert.

- Beispiel für Oracle:

```
./sdm -action importData -dirPath /tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003 20:00:00
   -connectFile sdm.connect
```

- Beispiel für SQL Server:

```
sdm -action importData -dirPath c:\tmp -startDate
   09/25/2003 08:00:00 -endDate 09/26/2003 20:00:00
   -connectFile sdm.connect
```

### Löschen von importierten Daten

Mit dieser Aktion („dropImported“) werden die importierten Daten aus dem angegebenen Zeitraum aus den unterstützten Tabellen gelöscht:

- Oracle:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS
- SQL Server:
  - HIST_EVENTS
  - HIST_CORRELATED_EVENTS

Wenn für den angegebenen Zeitraum keine importierten Daten vorhanden sind, wird eine entsprechende Meldung zurückgegeben.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | dropImported |
| -startDate | <MM/TT/JJJJ hh24:min:ss> |
| -endDate | <mm/tt/jj hh24:mi:ss> |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

**HINWEIS:** „hh24“ sind die im 24-Stunden-Format dargestellten Stunden. 1:15:00 p.m. steht beispielsweise für 13:15:00, und 3:00:00 a.m. stellt 03:00:00 dar.

Ausführen von „dropImported“

1. Führen Sie diesen Befehl wie folgt aus:

```
sdm -action dropImported -startDate <MM/TT/JJJJ
   hh24:min:ss> -endDate <MM/TT/JJJJ hh24:min:ss> -
   connectFile <Pfad zu dem durch „saveConnection“
   gespeicherten Dateinamen>
```

Im folgenden Beispiel werden die importierten Daten aus dem angegebenen Zeitraum aus den oben aufgeführten Tabellen gelöscht.

- Beispiel für Oracle:

```
./sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

- Beispiel für SQL Server:

```
sdm -action dropImported -startDate 09/25/2003
   00:00:00 -endDate 09/26/2003 00:00:00 -connectFile
   sdm.connect
```

## Verwaltung von Tabellenbereichen

Für die Verwaltung von Tabellenbereichen verfügen Sie über eine Befehlszeilenoption und eine GUI-Option. Über die Befehlszeile können Sie Folgendes ausführen:

- Anzeigen der Sentinel-Datenbank-Speicherplatzauslastung

Über die GUI können Sie Folgendes ausführen:

- Anzeigen von Partitionen
- Anzeigen von archivierten Partitionen
- Anzeigen von Importpartitionen
- Anzeigen der Speicherplatzauslastung

### Anzeigen der Sentinel-Datenbank-Speicherplatzauslastung (Befehlszeile)

Mit dieser Aktion („dbstats“) wird die Sentinel-Datenbankauslastung für alle Sentinel-Tabellenbereiche in Oracle und alle Sentinel-Dateigruppen in MS SQL angezeigt.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | dbstats |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

Anzeigen der Sentinel-Datenbank-Speicherplatzauslastung (Befehlszeile)

1. Führen Sie den folgenden Befehl aus:

```
sdm -action dbStats -connectFile <Pfad zu dem durch
   „saveConnection“ gespeicherten Dateinamen>
```

- Beispiel für Oracle:

Im folgenden Beispiel werden die Tabellenbereiche der Sentinel-Datenbank mit ihrem Gesamtspeicherplatz, dem belegten Speicherplatz sowie dem verfügbaren freien Speicherplatz angezeigt.

```
./sdm -action dbStats -connectFile sdm.connect
```

- Beispiel für SQL Server:

Im folgenden Beispiel werden die Dateigruppen der Sentinel-Datenbank mit ihrem Gesamtspeicherplatz, dem belegten Speicherplatz sowie dem verfügbaren freien Speicherplatz angezeigt.

```
sdm -action dbStats -connectFile sdm.connect
```

## Aktualisieren von Zuordnungen (Befehlszeile)

Mithilfe dieser Aktion („updateMapData“) können Sie eine Quelldatei mit Zuordnungsdaten durch eine andere ersetzen. Die neue Quelldatei mit Zuordnungsdaten muss dieselben Trennzeichen, Schlüsselspalten und aktivierten Spalten wie die frühere Zuordnung aufweisen. Wenn dies nicht der Fall ist, verwenden Sie die Funktion Bearbeiten der SDM-GUI.

Für diesen Befehl werden folgende Flags verwendet:

| | |
|---|---|
| -action | updateMapData |
| -map | <Zuordnungsname> |
| -file | <Dateiname> |
| -backup | <„wahr“/„falsch“> (Standardwert: „wahr“) |
| -connectFile | <Pfad zu dem durch „saveConnection“ gespeicherten Dateinamen> |

Mithilfe des Flags „–backup“ können Sie die ursprüngliche Zuordnungsdatei im Ordner „map_data“ sichern. Die gesicherte Zuordnungsdatei wird als BAK-Datei mit einigen nach dem Zufallsprinzip ausgewählten Zahlen am Ende des Dateinamens gespeichert. Beispiel: „threat10197.bak“

Aktualisieren (Ersetzen) einer Zuordnung

1. Führen Sie den folgenden Befehl aus:

```
sdm -action updateMapData -map <Zuordnungsname> -file
   <Dateiname> [-backup <true/false> (DEFAULT: true)]
   -connectFile <Pfad zu dem durch „saveConnection“
   gespeicherten Dateinamen>
```

   Im folgenden Beispiel werden die Zuordnungen in der Zuordnung „threat“ durch die Zuordnungen aus der Zuordnungsdatei „vuln_attacks.txt“ ersetzt.

```
sdm -action updateMapData -map threat -file
   vuln_attacks.txt -connectFile sdm.connect
```

Da das Flag „–backup“ nicht angegeben wurde, wird im Rahmen des Standardvorgangs eine Sicherungskopie der ursprünglichen Zuordnung erstellt, bevor die Aktualisierung mit der Zuordnungsdatei „vuln_attack.txt“ erfolgt.

## Verwenden des von Novell bereitgestellten Skripts für die automatische Verwaltung (nur Windows)

Novell hat eine Stapeldatei entwickelt, die so geplant werden kann, dass viele der Verwaltungsvorgänge von SDM automatisch ausgeführt werden können.

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

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

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

**HINWEIS**: Wenn beim Ausführen der geplanten Aufgabe ein Fehler auftritt, wird eine Benachrichtigung ausgegeben. Diese wird in „SDM_*.log“ protokolliert.

## Einrichten der Datei „Manage_data.bat“ für das Archivieren von Daten und das Hinzufügen von Partitionen

### Vorkonfiguration

Vor dem Konfigurieren der automatischen Ausführung des Archivierens von Daten und des Hinzufügens von Partitionen müssen Sie folgende Aufgaben ausführen:

- Speichern von Verbindungseigenschaften
- Festlegen von Archivierungsparametern

**HINWEIS**: Wenn Sie eine Verbindungsdatei an einem anderen Speicherort oder mit einem anderen Dateinamen als der Standardeinstellung („%ESEC_HOME%\sdm\sdm.connect“) gespeichert haben, müssen Sie die Datei „manage_data.bat“ so bearbeiten, dass der Pfad zur Verbindungsdatei aktualisiert wird.

### Festlegen von Archivierungsparametern

Dieser Vorgang kann über die Befehlszeile ausgeführt werden.

Mithilfe dieser Aktion („archiveConfig“) wird die Archivierung konfiguriert. Diese Konfiguration steuert, wie die Daten aus den Sentinel-Tabellen archiviert werden.

Für diese Aktion werden folgende Flags verwendet:

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

Erstellen von Archivierungsparametern über die Befehlszeile

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

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

2. Führen Sie diesen Befehl wie folgt aus:

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

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

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

Erstellen von Archivierungsparametern über die GUI

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

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

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

## Löschen von Daten (Verwerfen von Partitionen)

Mit dieser Aktion („deleteData“) werden die Daten aus der angegebenen Tabelle gelöscht, die älter sind, als in „keepDays“ festgelegt ist. Daten werden aus den folgenden Tabellen gelöscht:

- EVENTS
- CORRELATED_EVENTS
- EVT_DEST_EVT_NAME_SMRY_1
- EVT_DEST_SMRY_1
- EVT_DEST_TXNMY_SMRY_1
- EVT_PORT_SMRY_1
- EVT_SEV_SMRY_1
- EVT_SRC_SMRY_1

Bei dieser Aktion werden keine Partitionen verworfen, die nicht archiviert wurden. Wenn Sie nicht archivierte Partitionen löschen möchten, muss die optionale Flagge *forceDelete* angegeben sein und den Wert „true“ (wahr) aufweisen. Bei Verwendung von „forceDelete“ gilt Folgendes:

| | |
|---|---|
| „falsch“ oder nicht angegeben | Es werden nur die Partitionen verworfen, die älter sind als in „keepDays“ festgelegt, sowie die archivierten Partitionen. |
| „wahr“ | Es werden alle Partitionen verworfen, die älter sind als „keepDays“, auch wenn sie nicht archiviert wurden. |

Für diesen Befehl werden folgende Flags verwendet:

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

Ausführen von „deleteData“

1. Führen Sie diesen Befehl wie folgt aus:

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

   Im folgenden Beispiel werden die Partitionen aus Tabellen verworfen, die älter als 30 Tage sind. Dabei wird sichergestellt, dass alle verworfenen Partitionen archiviert wurden. Nach Abschluss des Vorgangs werden alle Partitionen aufgelistet, die nicht gelöscht wurden, weil sie nicht zuvor archiviert wurden.

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

## Planen der Ausführung von „Manage_data.bat“ für das Archivieren von Daten und das Hinzufügen von Partitionen

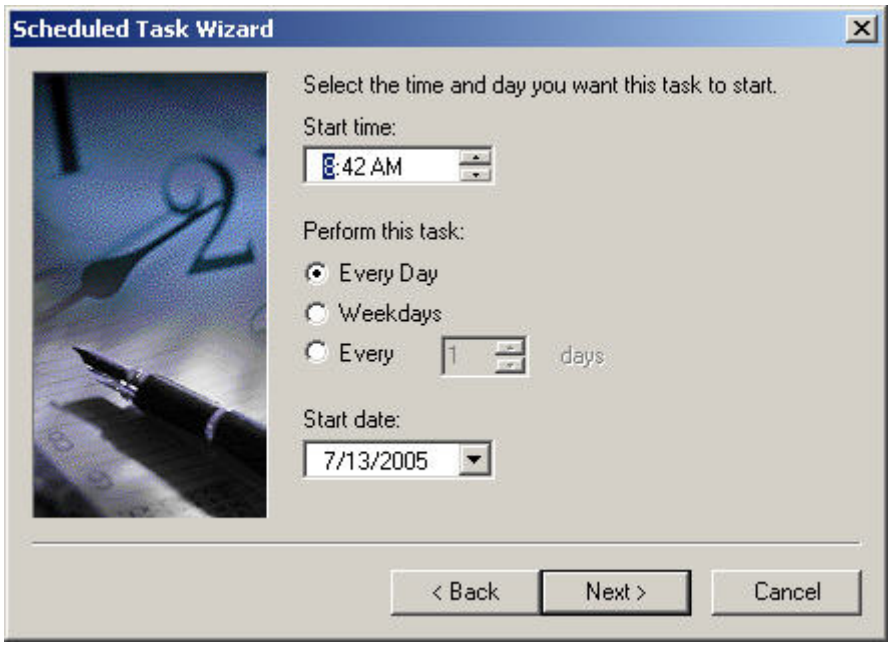
**HINWEIS**: Für die Datei „manage_data.bat“ ist der keepDays-Wert auf 30, die Archivausgabe auf „c:\SDM_archive“ und die Verbindungsdatei auf „%ESEC_HOME%\sdm\sdm.connect“ festgelegt. Wenn Ihre Werte abweichen, müssen Sie die Datei „manage_data.bat“ bearbeiten.

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

So können Sie automatisch Daten archivieren und Partitionen hinzufügen

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

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




8. Geben Sie einen Benutzer ein, für den der Task ausgeführt werden soll. Bei dem Benutzer kann es sich nicht um ein lokales Systemkonto handeln. Er muss als bestimmter Benutzer ausgeführt werden. Klicken Sie auf *Weiter*.
9. Klicken Sie auf *Fertig stellen*, um den Vorgang als geplanten Task fertig zu stellen.

# 11 Dienstprogramme

## Starten und Beenden des Sentinel Server und des Collector Manager – UNIX

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

### Starten des UNIX Sentinel Server

Beim Starten des Sentinel Server unter UNIX wird auch der Kommunikationsserver gestartet.

Starten des UNIX Sentinel Server

1. Wechseln Sie als Benutzer „esecadm“ in das Verzeichnis „$ESEC_HOME/sentinel/scripts“.
2. Führen Sie den folgenden Befehl aus:

```
./sentinel.sh start
```

### Beenden des UNIX Sentinel Server

Beim Beenden des Sentinel Server unter UNIX wird auch der Kommunikationsserver beendet.

Beenden des UNIX Sentinel Server

1. Wechseln Sie als Benutzer „esecadm“ in das Verzeichnis „$ESEC_HOME/sentinel/scripts“.
2. Führen Sie den folgenden Befehl aus:

```
./sentinel.sh stop
```

### Starten des UNIX Collector Manager

Starten des UNIX Collector Manager

1. Wechseln Sie als Benutzer „esecadm“ in das Verzeichnis „$WORKBENCH_HOME“.
2. Führen Sie den folgenden Befehl aus:

```
./agent-manager.sh start
```

## Beenden des UNIX Collector Manager

Beenden des UNIX Collector Manager

1. Wechseln Sie als Benutzer „esecadm“ in das Verzeichnis „$WORKBENCH_HOME“.
2. Führen Sie den folgenden Befehl aus:

```
./agent-manager.sh stop
```

# Starten und Beenden des Sentinel Server und des Collector Manager – Windows

Je nach Konfiguration der Installation können bis zu drei Sentinel-Services auf dem Computer ausgeführt werden. Hierbei handelt es sich um:

- Sentinel – Dieser Service startet alle anderen Sentinel Server-Prozesse.
- Sentinel Communication – Dieser Service ist unser verschlüsselter Kommunikationsserver.
- Collector Manager – Dieser Service stellt unseren Wizard dar.

Unter den Windows-Diensten können Sie jeden dieser Services manuell starten, neu starten und beenden.

## Starten des Windows Collector Manager

Starten des Windows Collector Manager

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Klicken Sie mit der rechten Maustaste auf *Collector Manager* und klicken Sie anschließend auf *Starten*.

## Beenden des Windows Collector Manager

Beenden des Windows Collector Manager

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Klicken Sie mit der rechten Maustaste auf *Collector Manager* und klicken Sie anschließend auf *Beenden*.

## Starten des Sentinel Server für Windows

Starten des Windows Sentinel Server

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Markieren Sie im Fenster „Dienste“ den Dienst *Sentinel*.

5. Klicken Sie mit der rechten Maustaste und wählen Sie *Starten* aus oder klicken Sie auf der Symbolleiste auf die Schaltfläche zum Starten.

## Beenden des Sentinel Server für Windows

Beenden des Windows Sentinel Server

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Markieren Sie im Fenster „Dienste“ den Dienst *Sentinel*.
5. Klicken Sie mit der rechten Maustaste und wählen Sie *Beenden* aus oder klicken Sie auf der Symbolleiste auf die Schaltfläche zum Beenden.

## Starten des Sentinel Communication Server für Windows

Starten des Windows Sentinel Communication Server

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Markieren Sie im Fenster „Dienste“ den Dienst *Sentinel Communication*.
5. Klicken Sie mit der rechten Maustaste und wählen Sie *Starten* aus oder klicken Sie auf der Symbolleiste auf die Schaltfläche zum Starten.

## Beenden des Sentinel Communication Server für Windows

Beenden des Windows Sentinel Communication Server

1. Klicken Sie auf *Start* > *Einstellungen* > *Systemsteuerung*.
2. Doppelklicken Sie auf *Verwaltung*.
3. Doppelklicken Sie auf *Dienste*.
4. Markieren Sie im Fenster „Dienste“ den Dienst *Sentinel Communication*.
5. Klicken Sie mit der rechten Maustaste und wählen Sie *Beenden* aus oder klicken Sie auf der Symbolleiste auf die Schaltfläche zum Beenden.

# Sentinel-Skriptdateien

Je nach der Konfiguration der Installation kann das Verzeichnis $ESEC_HOME/sentinel/scripts bzw. %ESEC_HOME%\sentinel\scripts einige oder alle der folgenden Skriptdateien enthalten:

| Skriptdatei: | Beschreibung: |
|---|---|
| ▪ remove_sonic_lock.bat | Dieses Skript entfernt die Kommunikationsserver-Sperrdatei(en). |
| ▪ start_broker.bat<br>▪ start_broker.sh | Diese Skripts starten den Kommunikationsserver in der Befehlszeile im Konsolenmodus. |
| ▪ stop_broker.bat<br>▪ stop_broker.sh | Diese Skripts beenden den Kommunikationsserver in der Befehlszeile im Konsolenmodus. |

| | |
|---|---|
| ▪ stop_container.bat<br>▪ stop_container.sh | Dieses Skript startet die folgenden Container neu:<br>▪ DAS_Aggregation<br>▪ DAS_RT<br>▪ DAS_iTRAC<br>▪ DAS_Binary<br>▪ DAS_Query |
| ▪ sentinel.sh | Dieses Skript beendet bzw. startet den Sentinel Server. Weitere Informationen finden Sie unter Starten des UNIX Sentinel Server bzw. Beenden des UNIX Sentinel Server. |

## Entfernen der Kommunikationsserver-Sperrdateien

Bei einem nicht ordnungsgemäßen Herunterfahren kann der Kommunikationsserver gesperrt werden. Nach dem Entfernen der Sperrdateien müssen Sie den Kommunikationsserver neu starten. Diese Dateien befinden sich an folgenden Speicherorten:

Für Windows:

```
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\esecDomain\data\_MFSys
   tem\lock
%ESEC_HOME%\3rdparty\SonicMQ\MQ6.1\SonicMQStore\db.lck
```

Für UNIX:

```
$ESEC_HOME/3rdparty/SonicMQ/MQ6.1/esecDomain/data/_MFSyst
   em/lock
$ESEC_HOME /3rdparty/SonicMQ/MQ6.1/SonicMQStore/db.lck
```

### Entfernen der Kommunikationsserver-Sperrdatei (Windows)

1. Navigieren Sie in Windows Explorer bzw. mit dem Befehl „cd“ in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Führen Sie die folgende Datei aus, bzw. doppelklicken Sie (in Windows Explorer) auf die folgende Datei:

   ```
   remove_sonic_lock.bat
   ```

### Entfernen der Kommunikationsserver-Sperrdatei (UNIX)

Das Entfernen der Sperrdatei ist unter UNIX normalerweise nicht erforderlich, da diese i. d. R. beim Start von Sentinel Server automatisch entfernt wird. Wenn diese Dateien manuell entfernt werden müssen, sind dazu die typischen Befehle des UNIX-Dateisystems auszuführen (beispielsweise „rm“).

## Starten des Kommunikationsservers im Konsolenmodus

Diese Skripts starten den Kommunikationsserver in der Befehlszeile im Konsolenmodus. Diese Skripts sind hilfreich beim Debuggen des Kommunikationsservers, wobei Sie nicht die übrigen Teile von Sentinel Server ausführen müssen. Es wird davon abgeraten, diese Skripts während des normalen Betriebs zu verwenden (befolgen Sie stattdessen die Anweisungen unter Starten des UNIX Sentinel Server bzw. Starten des Sentinel Server für Windows).

### Starten des Kommunikationsservers (Windows)

**HINWEIS**: Wenn Sie dieses Skript in Windows starten, wird es im Fenster „Dienste“ nicht als gestartet aufgeführt. Es wird nur ausgeführt, wenn die Befehlseingabeaufforderung geöffnet bleibt.

1. Navigieren Sie in Windows Explorer bzw. mit dem Befehl „cd“ in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Führen Sie die folgende Datei aus, bzw. doppelklicken Sie (in Windows Explorer) auf die folgende Datei:

   ```
   start_broker.bat
   ```

### Startem des Kommunikationsservers (UNIX)

1. Melden Sie sich als Benutzer „esecadm“ an.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Geben Sie Folgendes ein:

   ```
   ./start_broker.sh
   ```

## Beenden des Kommunikationsservers im Konsolenmodus

Diese Skripts beenden den Kommunikationsserver in der Befehlszeile im Konsolenmodus. Diese Skripts sind hilfreich beim Debuggen des Kommunikationsservers, wobei Sie nicht die übrigen Teile von Sentinel Server beenden müssen. Es wird davon abgeraten, diese Skripts während des normalen Betriebs zu verwenden (befolgen Sie stattdessen die Anweisungen unter Beenden des UNIX Sentinel Server bzw. Beenden des Sentinel Server für Windows).

### Beenden des Kommunikationsservers (Windows)

1. Navigieren Sie in Windows Explorer bzw. mit dem Befehl „cd“ in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Führen Sie die folgende Datei aus, bzw. doppelklicken Sie (in Windows Explorer) auf die folgende Datei:

   ```
   stop_broker.bat
   ```

Beenden des Kommunikationsservers (UNIX)

1. Melden Sie sich als Benutzer „esecadm“ an.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Geben Sie Folgendes ein:

   ```
   ./stop_broker.sh
   ```

## Neustarten von Sentinel-Containern

Diese Skripts starten die unten aufgelisteten Container neu: Das Skript sendet eine Meldung an den angegebenen Dienst, in der dieser zum Herunterfahren angewiesen wird. Der Dienst wird anschließend durch den Sentinel Watchdog neu gestartet.

Die bevorzugte Methode zum Beenden, Starten und Neustarten dieser Container-Services besteht darin, die Server-Ansichten auf der Registerkarte „Admin“ im Sentinel Control Center zu verwenden.

| Name | Beschreibung |
|---|---|
| ▪ DAS_Aggregation | (das_aggregation.xml) wird zum Ausführen und Konfigurieren des Aggregationsdienstes verwendet. |
| ▪ DAS_RT | (das_rt.xml) wird zum Ausführen und Konfigurieren des Dienstes für Ansichten in Echtzeit verwendet. |
| ▪ DAS_iTRAC | (das_itrac.xml) wird zum Konfigurieren des iTRAC-Dienstes verwendet. |
| ▪ DAS_Binary | (das_binary.xml) wird für Einfügevorgänge von Ereignissen und korrelierten Ereignissen verwendet. |
| ▪ DAS_Query | (das_query.xml) wird für alle anderen Datenbankoperationen verwendet. |

Neustarten eines Sentinel-Containers (Windows)

1. Wechseln Sie in das folgende Verzeichnis:

   ```
   %ESEC_HOME%\sentinel\scripts
   ```

2. Geben Sie Folgendes ein:

   ```
   stop_container.bat <Hostcomputer> <Containername>
   ```

   Beispiel:

   ```
   stop_container.bat localhost DAS_RT
   ```

Neustarten eines Sentinel-Containers (UNIX)

1. Melden Sie sich als Benutzer „esecadm“ an.
2. Wechseln Sie in das folgende Verzeichnis:

   ```
   $ESEC_HOME/sentinel/scripts
   ```

3. Geben Sie Folgendes ein:

```
./stop_container <Hostcomputer> <Containername>
```

Beispiel:

```
./stop_container localhost DAS_RT
```

# Versionsinformationen

## Sentinel Server-Versionsinformationen

Sentinel Server verfügt über eine Befehlszeilenoptionen, mit der die Versionsinformationen für die folgenden Prozesse angezeigt werden können:

- watchdog
- rulelg_checker
- correlation_engine
- data_synchronizer
- query_manager
- DAS

Abrufen von Sentinel-Versionsinformationen (UNIX)

1. Wechseln Sie in das folgende Verzeichnis:

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

2. Geben Sie Folgendes ein:

```
./<Prozess> -version
```

Beispiel:

```
./correlation_engine –version
```

Abrufen von Sentinel-Versionsinformationen (Windows)

1. Wechseln Sie in das folgende Verzeichnis:

```
%ESEC_HOME%\sentinel\bin
```

2. Geben Sie Folgendes ein:

```
<Prozess> -version
```

Beispiel:

```
correlation_engine –version
```

## Sentinel-Versionsinformationen für DLL- und EXE-Dateien

Abrufen von Sentinel-Versionsinformationen für DLL- und EXE-Dateien

1. Wechseln Sie in das Verzeichnis „%ESEC_HOME%“.
2. Klicken Sie in einem der verschiedenen Unterverzeichnisse mit der rechten Maustaste auf eine DLL-Datei oder eine EXE-Datei, und wählen Sie „Eigenschaften“ aus.
3. Klicken Sie auf die Registerkarte „Version“.

4. Wählen Sie im Bereich „Elementname“ „Produktversion“ aus. Die Versionsnummer der Datei wird im Bereich „Wert“ angezeigt.

### Sentinel-Versionsinformationen für JAR-Dateien

Abrufen von Sentinel-Versionsinformationen für JAR-Dateien

1. Melden Sie sich beim Sentinel Server als „user“ an:

   Für UNIX:

   ```
   esecadm
   ```

   Melden Sie sich unter Windows als Benutzer mit entsprechenden Rechten für Sentinel Server an.
2. Wechseln Sie in das folgende Verzeichnis:

   Für UNIX:

   ```
   $ESEC_HOME/utilities
   ```

   Für Windows:

   ```
   %ESEC_HOME%\utilities
   ```
3. Geben Sie an der Befehlszeile Folgendes ein:

   Für UNIX:

   ```
   ./versionreader.sh <Pfad/JAR-Dateiname>
   ```

   Für Windows:

   ```
   versionreader <Pfad/JAR-Dateiname>
   ```

## Konfigurieren von Email-Einstellungen unter Sentinel

Sentinel-Konfigurationseinstellungen für Email-Nachrichten werden während des Installationsvorgangs in der Datei „execution.properties“ gespeichert. Diese Datei kann nach der Installation bearbeitet werden. Die Datei befindet sich auf dem Computer, auf dem DAS installiert ist und erkannt wird:

Für Windows:

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

Für UNIX:

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

Es sind zwei Skripts („mailconfig.sh“ und „mailconfigtest.sh“ für UNIX und „mailconfig.bat“ und „mailconfigtest.bat“ für Windows) vorhanden, die die Email-Einstellungen in der Datei „execution.properties“ ändern und testen. Das Skript „mailconfig.*“ ändert die Email-Einstellungen, während das Skript „mailconfigtest.*“ die Email-Einstellungen testet. Die fett formatierten Bereiche stellen die Email-Einstellungen dar, die geändert werden können.

Die folgenden Eigenschaften sind in „execution.properties“ enthalten:

**mail.authentication.user=<domain\\user>**

correlated events retry wait=5000

| | |
|---|---|
| **mail.smtp.host=<SMTP_HOST>** | Der SMTP-Host, über den Email-Nachrichten gesendet werden. |
| mail.events.max=1000 | Die maximale Anzahl der Ereignisse, die in einer Email gesendet werden, die automatisch von der Correlation Engine generiert wird. Das Ziel besteht darin, die Größe der Emails für korrelierte Ereignisse zu beschränken, die über eine große Menge von Auslöseereignissen verfügen. |

correlated events retry count=10

| | |
|---|---|
| **mail.address.from=<SMTP_FROM_ADDR>** | Die Email-Adresse, die im Feld „Von“ der von DAS gesendeten Email angezeigt wird. |
| **mail.authentication.password=<password>** | Das Passwort für „mail.authentication.user“. |

Die Skripts „mailconfig.sh“ und „mailconfig.bat“ verwenden die folgenden Argumente:

| | |
|---|---|
| -host | SMTP-Hostname oder IP-Adresse |
| -from | Feld „Von“ der Email |
| -user | Der Mail-Authentifizierungsbenutzer |
| -password | Das Passwort für den Mail-Authentifizierungsbenutzer |

**HINWEIS**: Geben Sie Ihr Passwort nicht nach dem Argument „–password“ ein. Nach dem Eingeben des Befehls werden Sie zum Eingeben eines neuen Passworts aufgefordert. Die Konsolenausgabe weist eine Maske von Sternchen (*) auf.

Die Dateien „mailconfigtest.sh“ und „mailconfig.bat“ verwenden die folgenden Argumente:

| | |
|---|---|
| -to | Ziel-Email-Adresse |

So legen Sie die Email-Eigenschaften in der Datei „execution.properties“ fest

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

   Für UNIX:

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

   Für Windows:

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

2. Führen Sie „mailconfig“ wie folgt aus:

   Für UNIX:

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

   Für Windows:

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

   UNIX-Beispiel:

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

   Windows-Beispiel:

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

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

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

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

So testen Sie die Email-Einstellungen in der Datei „execution.properties“

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

   Für UNIX:

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

   Für Windows:

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

2. Führen Sie „mailconfigtest“ wie folgt aus:

   Für UNIX:

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

   Für Windows:

   ```
   mailconfigtest.bat -to <Ziel-Email-Adresse>
   ```

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

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

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

```
Subject: Testing Sentinel mail property
```

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

# Aktualisieren des Lizenzschlüssels

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

### Aktualisieren Ihres Lizenzschlüssels (UNIX)

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

   ```
   ./softwarekey
   ```

4. Geben Sie die Ziffer 1 ein, um Ihren Primärschlüssel festzulegen. Drücken Sie die EINGABETASTE.

### Aktualisieren Ihres Lizenzschlüssels (Windows)

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

   ```
   softwarekey.exe
   ```

4. Geben Sie die Ziffer 1 ein, um Ihren Primärschlüssel festzulegen. Drücken Sie die EINGABETASTE.

# 12 Schnellstart

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

Dieses Kapitel behandelt die Schnellstartverfahren für:

- Sicherheitsanalysten
- Berichtsanalyst
- Administratoren

Folgende Themen werden erläutert:

- Active Views™
- Exploit-Erkennung
- Bestandsdaten
- Ereignisabfrage
- Analyseberichte über Crystal Reports
- Allgemeine Korrelation

## Sicherheitsanalysten

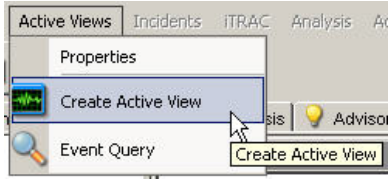
**HINWEIS**: Es wird vorausgesetzt, dass Ihr Sicherheitsadministrator oder Sie selbst die erforderlichen Filter erstellt und die erforderlichen Collectors für Ihr System konfiguriert haben.

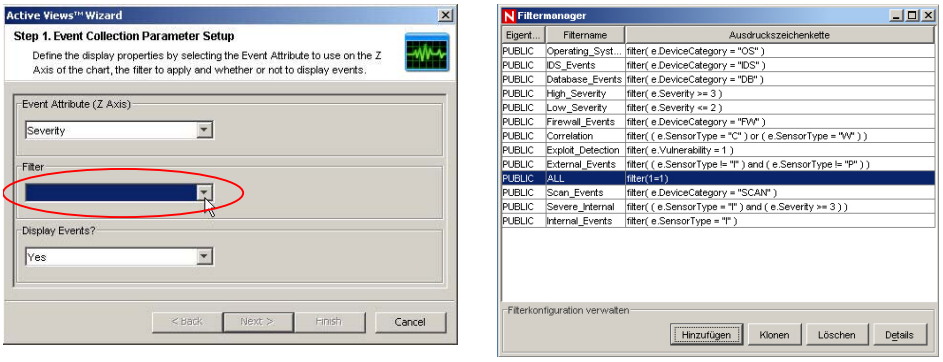
### Registerkarte „Active Views“

Auf der Registerkarte „Active Views“ können Sie Ereignisse überwachen, wenn sie eintreten, und Abfragen an diese Ereignisse senden. Die Ereignisse können in einem Tabellenformat oder in einer grafischen 3D-Darstellung überwacht werden.

So bringen Sie ein Echtzeitereignis ins Laufen

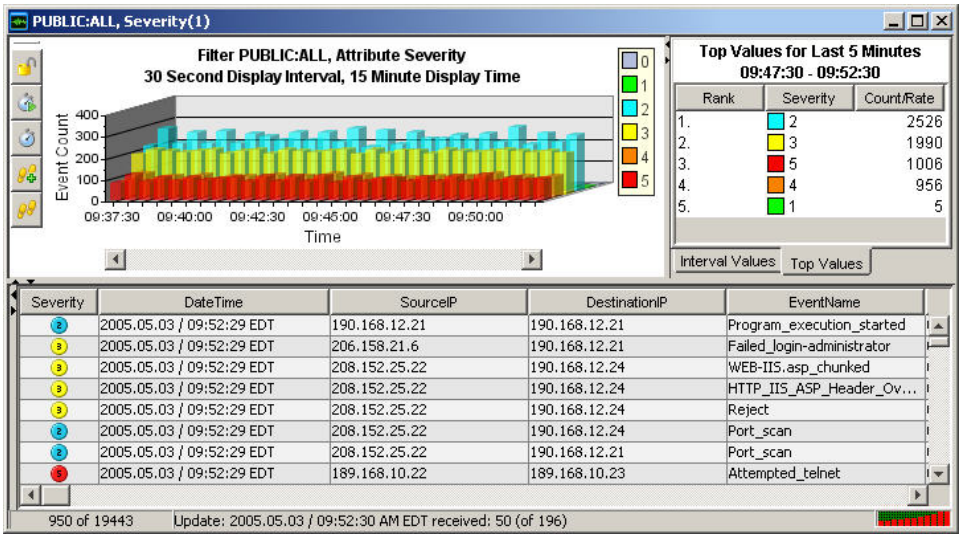
1. Klicken Sie auf *Active Views* > *Aktive Ansicht erstellen*, klicken Sie auf den Filter-Abwärtspfeil, wählen Sie einen Filter aus und klicken Sie auf *Auswählen*.






2. Klicken Sie auf *Fertig stellen*. Wenn Sie über ein aktives Netzwerk verfügen, wird ein ähnliches Fenster angezeigt wie unten dargestellt:

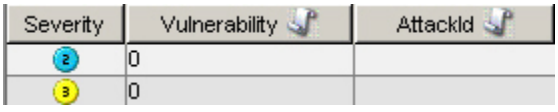
**HINWEIS**: Zum Anzeigen eines 3D-Diagramms ohne Echtzeitereignisse klicken Sie auf den Abwärtspfeil für „Ereignisse anzeigen?“ und wählen Sie *Nein*.




## Exploit-Erkennung

Zum Anzeigen von Ereignissen, die auf eine mögliche Ausnutzung hinweisen, müssen Sie über Folgendes verfügen:

- Advisor-Feed
- Intrusion Detection
- Anfälligkeits-Absuchvorgänge




Wenn bei einem Ereignis das Feld für die Anfälligkeit (*vul*) 1 entspricht, wird der Bestand bzw. das Zielgerät ausgenutzt. Wenn das Feld für die Anfälligkeit 0 entspricht, wird der Bestand bzw. das Zielgerät nicht ausgenutzt. Wenn das Feld für die Anfälligkeit leer ist, ist die Exploit-Erkennungsfunktion von Sentinel nicht aktiv.

Zum Anzeigen von Ereignissen, die eine mögliche Ausnutzung aufzeigen, erstellen Sie eine aktive Ansicht mit einem Filter, bei dem die Anfälligkeit 1 entspricht. Wenn Sie über Nmap verfügen und den Nmap Collector ausführen, können Sie Bestandsinformationen zum ausgenutzten Bestand oder zu einem anderen Bestand anzeigen.

Weitere Informationen zur Funktionsweise der Exploit-Erkennung und zu den unterstützten Intrusion Detection-Systemen und Anfälligkeits-Absuchprogrammen finden Sie in *Kapitel 1 – Einführung* oder in *Kapitel 10 – Sentinel Data Manager*.

## Bestandsdaten

Zum Anzeigen von Bestandsinformationen für ein Ereignis klicken Sie mit der rechten Maustaste auf ein oder mehrere Ereignisse und klicken Sie dann auf *Analyse > Inventardaten*. Ein ähnliches Fenster wie unten zu sehen ist, wird eingeblendet.

**Asset Report**

| desk.acmeinc.net | | | | |
|---|---|---|---|---|
| **Hardware** | **MAC Address** | A0:12:56:78:90:00 | | |
| | **Name** | Build Machine | **Value** | 500 |
| | **Type** | Server | **Criticality** | High |
| | **Vendor** | Dell | **Sensitivity** | Low |
| | **Product** | Precision | **Environment** | Production |
| | **Version** | 360 | **Location** | Internal |

| **Network** | **IP** | **Hostname** |
|---|---|---|
| | 199.16.2.23 | desk.acmeinc.net |

| **Software** | **Name** | **Type** | **Vendor** | **Product** | **Version** |
|---|---|---|---|---|---|
| | ClearCase | APPLICATION | IBM | ClearCase | 5.0 |
| | C++ | APPLICATION | Microsoft | Visual C++ | 6.0 |

| **Contacts** | **Order** | **Name** | **Role** | **Email** | **Phone Number** |
|---|---|---|---|---|---|
| | 1 | Erickson, Stein | USER | serickson@acmedomain.net | (703) 555-8865 |
| | 2 | IT | Administrator | LAN_FOLKS@acemedomain.net | (703) 555-9876 |

| **Location** | | |
|---|---|---|
| | **Room** | server room |
| | **Rack** | #17 |
| | **Address** | HQ<br>Agent 86 Security Circle<br>Suite 86<br>Washington DC 12345 USA |

## Ereignisabfrage

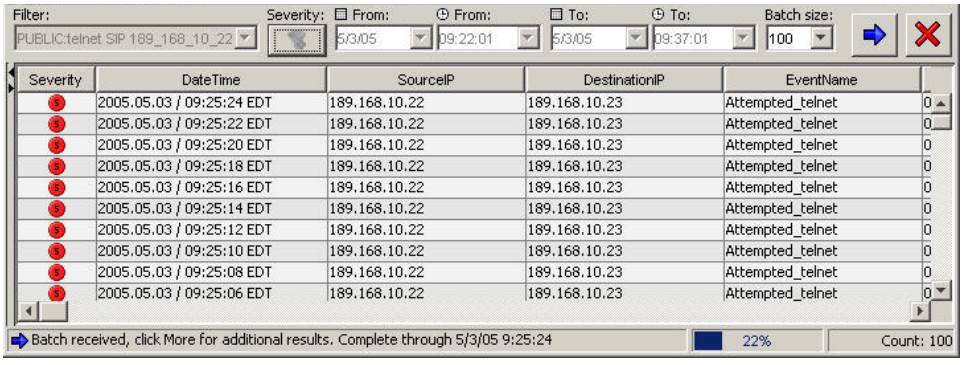
Beispielszenario: Während der Überwachung sehen Sie zahlreiche Telnet-Versuche der Quellen-IP 189.168.10.22. Bei diesen Telnet-Versuchen könnte es sich um einen Angriff handeln. Telnet ermöglicht es einem Angreifer, eine Remote-Verbindung zu einem Computer so herzustellen, als ob es sich um eine lokale Verbindung handeln würde. Dies kann zu nicht autorisierten Konfigurationsänderungen sowie zur Installation von Programmen, Viren usw. führen.

Mithilfe der Ereignisabfrage können Sie feststellen, wie oft ein möglicher Angreifer einen Telnet-Versuch unternommen hat, und Sie können einen Filter zur Abfrage dieses speziellen Angreifers erstellen. Sie verfügen beispielsweise über die folgenden Informationen:

- Quellen-IP: 189.168.10.22
- Ziel-IP: 189.168.10.23
- Schweregrad: 5
- Ereignisname: Attempted_telnet
- Sensortyp: H (Host Intrusion Detection)

So führen Sie eine Ereignisabfrage durch

1. Klicken Sie auf *Ereignisabfrage* (Lupensymbol) und dann auf den Abwärtspfeil des Felds „Filter“.
2. Klicken Sie auf *Hinzufügen* und geben Sie als Filternamen „telnet SIP 189_168_10_22“ ein. Geben Sie in das Feld unter „Filter“ Folgendes ein:
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet
   - Abgleichen, wenn; wählen Sie (und)
   - Schweregrad = 5
   - SensorType = H
   - DestinationIP = 189.168.10.23
3. Klicken Sie auf *Speichern*. Markieren Sie Ihren Filter und klicken Sie auf *Auswählen*.
4. Geben Sie den relevanten Zeitraum ein und klicken Sie auf *Suchen* (Lupensymbol). Die Ergebnisse Ihrer Abfrage werden angezeigt.




Wenn Sie sehen möchten, wie oft dieser Benutzer im Allgemeinen einen Telnet-Versuch unternimmt, entfernen Sie „DestinationIP“, „SensorType“ und „Schweregrad“ aus Ihrem Filter oder erstellen Sie einen neuen Filter. Die Ergebnisse zeigen alle Ziel-IPs an, zu denen dieser Benutzer einen Telnet-Versuch unternommen hat.

Wenn es sich bei manchen Ereignissen um korrelierte Ereignisse handelt (SensorType = C oder W), können Sie mit der rechten Maustaste darauf klicken und *Auslöseereignisse anzeigen* wählen, um herauszufinden, welche Ereignisse das korrelierte Ereignis ausgelöst haben.

Ein anderes Ereignis von Interesse könnten exzessive FTP-Ereignisse sein. Es kann sich auch um eine Remote-Verbindung handeln, die das Übertragen, Kopieren und Löschen von Dateien ermöglicht.

Nachfolgend sehen Sie eine kurze Liste mit Angriffen, die von Interesse sein können. Die Liste der Angriffstypen ist recht lang. Weitere Informationen zu Netzwerk-/Hostangriffen finden Sie in zahlreichen Ressourcen (z. B. in Büchern und im Internet), in denen die verschiedenen Angriffstypen detailliert beschrieben werden.

- SYN-Flood
- ICMP- und UDP-Flood
- Packet-Sniffing
- Denial-of-Service
- Schlumpf und Fraggle
- Wörterbuch-Angriff

# Berichtsanalyst

**HINWEIS**: Es wird vorausgesetzt, dass Ihr Sicherheitsadministrator Ihren Crystal Enterprise-Webserver konfiguriert und eine Liste der verfügbaren Berichte veröffentlicht hat.

## Registerkarte „Analyse“

Die Registerkarte „Analyse“ ermöglicht Ihnen das Erstellen von Verlaufsberichten. Verlaufs- und Anfälligkeitsberichte werden auf einem Crystal-Webserver veröffentlicht. Sie werden direkt mit der Sentinel-Datenbank ausgeführt. Diese Berichte können hilfreich sein, um Aktivitäten über einen längeren Zeitraum, beispielsweise eine Woche oder einen Monat, hinweg zu verfolgen und zu untersuchen. Sie können diese Berichte auch zur Berichterstattung bei Ihren Vorgesetzten verwenden. Wenn Ihr Berichts-Webserver installiert ist, können Sie in der Navigationsleiste sehen, welche Berichte verfügbar sind.

**HINWEIS**: Nachfolgend finden Sie ein Beispiel für Crystal 9. In Crystal 11 sind die Verfahren identisch, es werden jedoch andere Berichtsnamen verwendet.

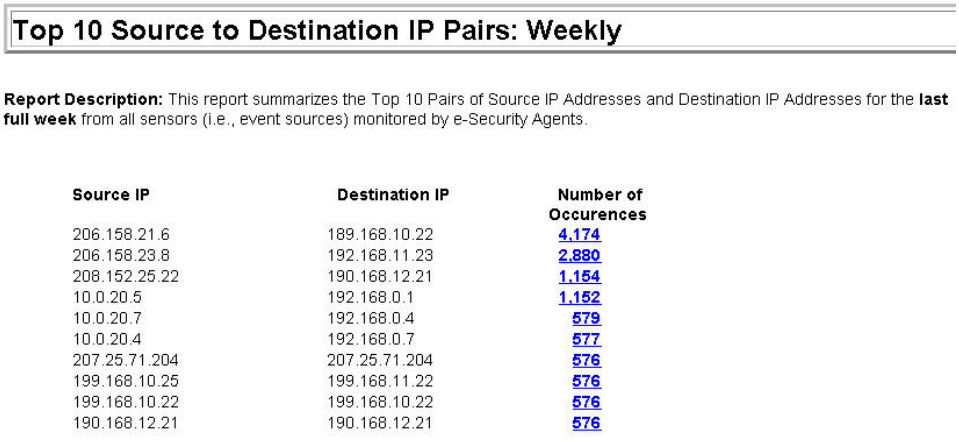
Angenommen, Sie sind in Ihrem Unternehmen für die Erstellung von Berichten für das höhere Management verantwortlich. In diesem Fall verwenden Sie wahrscheinlich SourceDestinationReports. Dieser Bericht liefert die Top 10-Quellen-IP/Ziel-IP-Paare unter den Hostnamen, Ports, IPs und Benutzern. Zur Ausführung dieses Berichts gehen Sie wie folgt vor:

### Ausführen eines Crystal Report

1. Erweitern Sie die Top 10, markieren Sie die Zusammenfassung der Top 10-Quellen-IP/Ziel-IP-Paare und klicken Sie auf *Berichte erstellen* (Lupensymbol).
2. Geben Sie als Benutzername esecrpt (zur SQL-Authentifizierung und Oracle) bzw. Ihren Benutzernamen für die Windows-Authentifizierung sowie Ihr Passwort ein.
3. Wählen Sie unter „Berichtstyp“ die *Option Wochenbericht* (wählen Sie „Spezifischer Datenbereich“, wenn ein bestimmter Datumsbereich verwendet werden soll).

**HINWEIS**: Andere Berichte können weitere Parameter wie den Ressourcennamen und den Schweregradbereich aufweisen.

4. Klicken Sie auf *Bericht anzeigen*.

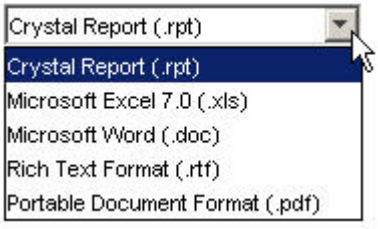


**Top 10 Source to Destination IP Pairs: Weekly**

**Report Description:** This report summarizes the Top 10 Pairs of Source IP Addresses and Destination IP Addresses for the **last full week** from all sensors (i.e., event sources) monitored by e-Security Agents.

| Source IP | Destination IP | Number of Occurences |
|---|---|---|
| 206.158.21.6 | 189.168.10.22 | 4,174 |
| 206.158.23.8 | 192.168.11.23 | 2,880 |
| 208.152.25.22 | 190.168.12.21 | 1,154 |
| 10.0.20.5 | 192.168.0.1 | 1,152 |
| 10.0.20.7 | 192.168.0.4 | 579 |
| 10.0.20.4 | 192.168.0.7 | 577 |
| 207.25.71.204 | 207.25.71.204 | 576 |
| 199.168.10.25 | 199.168.11.22 | 576 |
| 199.168.10.22 | 199.168.10.22 | 576 |
| 190.168.12.21 | 190.168.12.21 | 576 |

5. Sie können diese Datei als Word-, PDF-, RTF- oder Excel-Datei oder als Crystal Report exportieren, indem Sie auf *Exportieren* (Umschlag) klicken.




## Ereignisabfrage

Ähnlich wie ein Sicherheitsanalyst können Sie auf der Registerkarte „Analyse“ eine Ereignisabfrage durchführen, wenn Ihre Berichte ein oder mehrere Ereignisse von Interesse enthalten. Zum Ausführen einer Abfrage markieren Sie *Verlaufsereignisse > Alte Ereignisabfragen* und klicken Sie dann auf *Berichte erstellen* (Lupensymbol). Weitere Informationen finden Sie unter Sicherheitsanalysten - Beispielszenario für Ereignisabfrage.

# Administratoren

## Grundlegende Korrelation

Unter Korrelation versteht man den Vorgang des Analysierens von Sicherheitsereignissen zum Ermitteln von potenziellen Beziehungen zwischen zwei oder mehr Ereignissen. Durch die Korrelation werden schnelle Verknüpfungen von Prioritätsangriffen auf allgemeine Elemente der Ereignisdaten ermöglicht.

In Verbindung mit dem Telnet-Szenario unter Sicherheitsanalysten - Beispielszenario für Ereignisabfrage kann eine grundlegende Korrelationsregel erstellt werden, die ein korreliertes Ereignis auslöst, wenn in einem Zeitraum von 10 Sekunden 4 Telnet-Versuche unternommen werden.

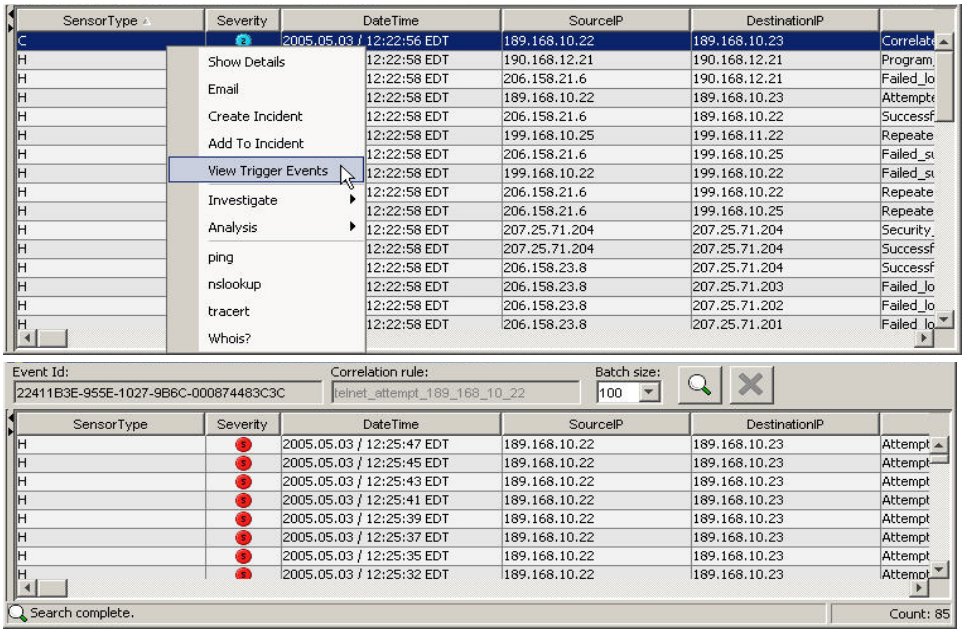
### So erstellen Sie eine Korrelationsregel

1. Wechseln Sie zur Registerkarte „Admin“ und markieren Sie die Option „Korrelationsregeln“ in der Navigationsleiste.
2. Erstellen Sie einen neuen Ordner und legen Sie die Regel darin ab. Hierfür können Sie eine Kontextmenüoption verwenden.
3. Markieren Sie „Grundlegende Korrelation“, geben Sie einen Namen ein und klicken Sie auf *Weiter*. Klicken Sie im nächsten Fenster auf den Abwärtspfeil und wählen Sie *Filter-Manager*. Klicken Sie auf den Abwärtspfeil für „Ausgewählter Filter“ und klicken Sie im Bereich „Filterauswahl“ auf *Hinzufügen*.
4. Geben Sie Folgendes ein:
   - Name: telnet_attempt_189_168_10_22
   - Filtername: telnet attempt 189_168_10_22
   - SourceIP = 189.168.10.22
   - EventName = Attempted_telnet

- Wählen Sie *Und*.
- Schweregrad = 5
- SensorType = H
- DestinationIP = 189.168.10.23

5. Klicken Sie auf *Speichern*. Markieren Sie Ihren Filter und klicken Sie auf *Auswählen*.
6. Klicken Sie auf *Weiter*, geben Sie für „Wenn Bedingung erfüllt ist“ den Wert 4 und in den Bereich „Schwellenwert und Gruppierungskriterien“ den Wert 10 Sekunden ein. Klicken Sie auf *Weiter*.
7. Ändern Sie im Bereich „In Korrelation stehende Ereignisse und Aktionen“ den Schweregrad in 2 (klicken Sie auf den Abwärtspfeil). Klicken Sie auf *Fertig stellen*.
8. Zur Bereitstellung dieser Regel markieren Sie den Correlation Engine-Manager im Navigationsbereich, markieren Sie eine Correlation Engine und klicken Sie mit der rechten Maustaste auf *Bereitstellungsregeln.* Suchen Sie im Bereich „Bereitstellungsregeln“ nach Ihrer Regel und aktivieren Sie diese. Klicken Sie auf *OK* (Hinzufügen). Stellen Sie sicher, dass die Correlation Engine und Ihre Korrelationsregel mit einem grünen Häkchen gekennzeichnet (aktiviert) sind. Sie können hierfür mit der rechten Maustaste klicken.
9. Es gibt verschiedene Methoden, um zu prüfen, ob korrelierte Ereignisse vorhanden sind. Einige Methoden sind:
   - Erstellen Sie ein Ereignisfenster mit aktiven Ansichten unter Verwendung des von Ihnen erstellten Korrelationsfilters.
   - Erstellen Sie ein Ereignisfenster mit aktiven Ansichten unter Verwendung des bereitgestellten Korrelationsfilters.
   - Erstellen Sie ein Ereignisfenster mit aktiven Ansichten unter Verwendung des bereitgestellten Filters „Alle“, erstellen Sie einen Snapshot und nehmen Sie eine Sortierung nach SensorType vor. Zeigen Sie anschließend alle Ereignisse mit dem SensorType C an.
   - Führen Sie unter Verwendung des von Ihnen erstellten Filters oder des Korrelationsfilters eine Schnellabfrage durch.

Klicken Sie mit der rechten Maustaste auf das korrelierte Ereignis und wählen Sie *Auslöseereignisse anzeigen*, um zu sehen, wie viele Telnet-Ereignisse (es können mehr als 4 sein) diese Korrelationsregel ausgelöst haben.



## Doppelte Benutzerobjekte

Wenn ein unerwartetes zweites aktives Benutzerobjekt vorhanden ist (dies ist nicht zulässig), wird das folgende Ereignis generiert. Dies ist ein interner Fehler.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | TooManyActiveUsers |
| Ressource | UserAuthentication |
| Teilressource | Authenticate |
| Meldung | Error in user table: Multiple users with the name <*name*> found (Fehler in Benutzertabelle: Es wurden mehrere Benutzer mit dem Namen <*Name*> gefunden) |

## Gesperrtes Konto

Beim Versuch einer Anmeldung mit einem gesperrten Benutzerkonto wird das folgende Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | LockedUser |
| Ressource | UserAuthentication |
| Teilressource | Authentication |
| Meldung | Attempt to login using locked account <acct> (Versuch der Anmeldung mit dem gesperrten Konto <Kto>) |

# Benutzersitzungen

## Abgemeldeter Benutzer

Beim Abmelden eines Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedOut |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | Closing session for <*user*> OS name <*osName*> from <*IP*> was on since <*date*>; currently <*num*> active users (Sitzung für <*Benutzer*>, Betriebssystemname <*OSName*>, von <*IP*> seit <*Datum*> wird geschlossen; zurzeit sind <*n*> aktive Benutzer vorhanden) |

## Angemeldeter Benutzer

Beim Anmelden eines Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedIn |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | User <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Benutzer <*Benutzer*> mit Betriebssystemname <*OSName*> an <*IP*> hat sich angemeldet; zurzeit sind <*n*> aktive Benutzer vorhanden) |

## Erkannter Benutzer

Wenn der Server neu gestartet wird, gehen die Sitzungsinformationen verloren. In einem solchen Fall wird die Sitzung wiederhergestellt, wenn Nachrichten von den aktiven Benutzern empfangen werden. Beim Erkennen eines verbundenen Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedIn |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | Discovered active user <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Aktiver Benutzer <*Benutzer*> mit Betriebssystemname <*OSName*> angemeldet an <*IP*> wurde erkannt; zurzeit sind <*n*> aktive Benutzer vorhanden) |

# Ereignis

## Fehler beim Verschieben von abgeschlossener Datei

Wenn eine Ereignisdatei abgeschlossen wurde, wird sie in das Ausgabeverzeichnis verschoben. Wenn dieser Verschiebevorgang nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | MoveArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error moving completed archive file *<fname>* to *<dir>* (Fehler beim Verschieben von abgeschlossener Archivdatei *<Dateiname>* nach *<Verz>*) |

## Fehler beim Einfügen von Ereignissen

Wenn beim Einfügen von Ereignissen in die Datenbank Fehler auftreten, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | InsertEventsFailed |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Error inserting events into the Database—the events may be permanently lost. Please check the Database and backend server logs *<Exception>* (Fehler beim Einfügen von Ereignissen in die Datenbank – die Ereignisse können endgültig verloren gehen. Überprüfen Sie die Datenbank- und die Back-End-Server-Protokolle *<Ausnahme>*) |

## Fehler beim Öffnen von Archivdatei

Wenn das Öffnen einer Archivdatei zum Speichern der Ereignisse für die Aggregation nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | OpenArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error opening archive file *<name>* in *<dir>* (Fehler beim Öffnen von Archivdatei *<Name>* in *<Verz>*) |

## Fehler beim Schreiben in Archivdatei

Wenn das Öffnen einer Archivdatei zum Speichern der Ereignisse für die Aggregation nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | WriteArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error writing newly received events to aggregation archive file *<fname>* (Fehler beim Schreiben neu empfangener Ereignisse in Archivdatei für die Aggregation *<Dateiname>*) |

## Schreiben auf die Überlaufpartition (P_MAX)

Etwa alle 5 Minuten wird ein Ereignis gesendet, um den Benutzer über das Schreiben von Ereignissen auf die Überlaufpartition (P_MAX) zu benachrichtigen. Wenn dies der Fall ist, muss der Administrator mithilfe von SDM weitere Partitionen hinzufügen, damit die Leistung nicht beeinträchtigt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | InsertIntoOverflowPartition |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Error: currently inserting into the overflow partitions (P_MAX), add more partitions (Fehler: Zurzeit wird auf die Überlaufpartitionen (P_MAX) geschrieben, fügen Sie weitere Partitionen hinzu) |

## Einfügen von Ereignissen ist gesperrt

Wenn DAS auf die Überlaufpartition schreibt und der Benutzer versucht, Partitionen hinzuzufügen, sendet SDM eine Anforderung an DAS, dass das Einfügen von Ereignissen in die Datenbank vorübergehend unterbrochen werden soll. Wenn dies der Fall ist, sendet DAS bei jedem Versuch, Ereignisse in die Datenbank einzufügen, interne Ereignisse.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | EventInsertionIsBlocked |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Event insertion is blocked, waiting *<num>* sec (Einfügen von Ereignissen ist gesperrt, warten Sie *<n>* Sekunden) |

## Einfügen von Ereignissen wird fortgesetzt

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventInsertionResumed |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Event insertion has resumed after being blocked (Einfügen von Ereignissen wird nach vorübergehender Unterbrechung fortgesetzt) |

## Speicherplatz der Datenbank hat angegebenen Zeitschwellenwert erreicht

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | DbSpaceReachedTimeThrshld |
| Ressource | Database |
| Teilressource | Database |
| Meldung | Tablespace <*string*> has <*num*> MB left and growing <*num*> bytes per second and will run out space within the time threshold specified <*num*> seconds (Tabellenbereich <*Zeichenkette*> verfügt noch über <*n*> MB und wächst um <*n*> Byte pro Sekunde an, der Speicherplatz wird innerhalb des angegebenen Zeitschwellenwerts erschöpft sein, <*n*> Sekunden) |

## Speicherplatz der Datenbank hat angegebenen prozentualen Schwellenwert erreicht

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | DbSpaceReachedPercentThrshld |
| Ressource | Database |
| Teilressource | Database |

| Tag | Wert |
|---|---|
| Meldung | Tablespace <*string*> has current size of <*num*> MB with a max size of <*num*> MB and has reached the percentage threshold of <*num*> % (Tabellenbereich <*Zeichenkette*> hat eine aktuelle Größe von <*n*> MB bei einer maximalen Größe von <*n*> MB und der prozentuale Schwellenwert von <*n*> % wurde erreicht) |

### Sehr wenig Datenbankspeicher

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | DbSpaceVeryLow |
| Ressource | Database |
| Teilressource | Database |
| Meldung | Tablespace <*string*> has current size of <*num*> MB and has reached the physical threshold of <*num*> MB (Tabellenbereich <*Zeichenkette*> hat zurzeit eine Größe von <*n*> MB und den physischen Schwellenwert von <*n*> MB erreicht) |

## Aggregation

### Fehler beim Einfügen von Zusammenfassungsdaten in die Datenbank

Bei einem Fehler während des Schreibens von Aggregationsdaten in die Datenbank wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | SummaryUpdateFailure |
| Ressource | Aggregation |
| Teilressource | Summary |
| Meldung | Error saving summary batch to the database for summary <*summaryName*> (Fehler beim Speichern des Zusammenfassungsstapels in der Datenbank für Zusammenfassung <*Zusammenfassung*>) |

# Zuordnungsservice

## Fehler beim Initialisieren von Zuordnung mit ID

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Dieser Fehler wird generiert, wenn der Collector Manager versucht, eine nicht vorhandene Zuordnung abzurufen. Dies sollte nicht vorkommen, kann jedoch der Fall sein, wenn Zuordnungen erstellt und gelöscht werden.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorNoSuchMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Error initializing map with id <*ID*>: no such map (Fehler beim Initialisieren von Zuordnung mit ID <*ID*>: keine solche Zuordnung vorhanden) |

## Aktualisieren von Zuordnung aus Cache

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass der zugehörige Cache auf dem aktuellen Stand ist und dass die Zuordnung aus dem Cache aktualisiert wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | LoadingMapFromCache |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Loading from cache v<*version*> of map <*mapName*> (ID <*id*>) (Laden aus Cache <*Version*> von Zuordnung <*Zuordnung*> (ID <*ID*>)) |

## Aktualisieren von Zuordnung von Server

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass die Zuordnung entweder nicht im Cache enthalten war oder dass die Version im Cache nicht aktuell ist, sodass der Collector Manager die Zuordnung vom Server abruft.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RefreshingMapFromServer |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Refreshing from server map <*name*> with id <*ID*> (Aktualisieren der Zuordnung <*Name*> mit ID <*ID*> vom Server) |

## Zeitüberschreitung beim Aktualisieren von Zuordnung

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass der Collector Manager versucht hat, die Zuordnung vom Server abzurufen, und die Anforderung wurde vom Server nicht akzeptiert, sodass eine Zeitüberschreitung aufgetreten ist. Dieser Fehler wird als flüchtig angesehen und der Collector Manager versucht erneut, den Vorgang auszuführen.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | TimeoutRefreshingMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Request timed out while refreshing map <*name*>: <*exception*> (Zeitüberschreitung der Anforderung beim Aktualisieren von Zuordnung <*Name*>: <*Ausnahme*>) |

## Fehler beim Aktualisieren von Zuordnung

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass beim Aktualisieren einer Zuordnung ein unerwarteter, nicht flüchtiger Fehler aufgetreten ist. Der Collector Manager wartet 15 Minuten und versucht anschließend erneut, den Vorgang auszuführen. Wenn dieser Fehler während der Initialisierung auftritt, wird diese fortgesetzt und die betreffende Zuordnung wird so lange ignoriert, bis sie erfolgreich geladen werden kann.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorRefreshingMapData |

| Tag | Wert |
|---|---|
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Error refreshimg map <*mapName*>: <*exc*> (Fehler beim Aktualisieren von Zuordnung <*Zuordnung*>: <*Ausnahme*>) |

## Laden von großer Zuordnung

Dieses interne Ereignis ist ein Informationsereignis, das vom Zuordnungsservice gesendet wird. Damit wird darüber informiert, dass eine große Zuordnung in den Collector Manager geladen wurde. Eine Zuordnung gilt als groß, wenn die Anzahl der Zeilen 100.000 überschreitet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | LoadedLargeMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Finished loading map <*name*> with id <*ID*> and <*num*> entries and total size <#>Kb in <##>sec (Zuordnung <*Name*> mit ID <*ID*> und <*n*> Einträgen und einer Gesamtgröße von <*n*> Kb in <*n*> Sekunden wurde geladen) |

## Langes Laden von Zuordnung

Dieses interne Ereignis ist ein Informationsereignis, das vom Zuordnungsservice gesendet wird. Damit wird darüber informiert, dass das Laden einer Zuordnung außergewöhnlich lange (länger als 1 Minute) gedauert hat.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | LongTimeToLoadMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | It took <##>sec to load map <name> with id <*ID*> and <*num*> entries and total size <##>Kb (Das Laden von Zuordnung <*Name*> mit ID <*ID*> und <*n*> Einträgen und einer Gesamtgröße von <*n*> Kb dauerte <*n*> Sekunden) |

## TimedoutWaitingForCallback

Wenn der Collector Manager eine Zuordnung aktualisieren muss, sendet er eine Anforderung an das Back-End. Diese Anforderung enthält einen Rückruf. Das Back-End generiert die Zuordnung und sendet diese anschließend mithilfe des Rückrufs an den Collector Manager. Wenn der Eingang der Antwort zu lange dauert (länger als 10 Minuten), sendet der Collector Manager eine zweite Anforderung und die erste Anforderung wird als verloren gegangen angesehen. Wenn dies der Fall ist, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | TimedoutWaitingForCallback |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Map <*name*> timed out waiting for callback with new map data--retrying (Zeitüberschreitung für Zuordnung <*Name*> beim Warten auf Rückruf mit neuen Zuordnungsdaten; neuer Versuch) |

## ErrorApplyingIncrementalUpdate

Dieses Ereignis wird gesendet, wenn beim Übernehmen einer Aktualisierung auf eine vorhandene Clientzuordnung durch den Zuordnungsservice ein Fehler auftritt.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorApplyingIncrementalUpdate |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | The error <*error*> occurred while applying updates to map <*mapName*> (ID <*mapId*>) v.<*version*>. Rescheduling a refresh to complete map update. (Fehler <*Fehler*> beim Übernehmen von Aktualisierungen für Zuordnung <*Zuordnung*> (ID <*ID*>), Version <*Version*>. Eine Aktualisierung für die Zuordnung wird neu geplant.) |

### OutOfSyncDetected

Dieses Ereignis wird gesendet, wenn der Zuordnungsservice feststellt, dass eine Zuordnung veraltet ist. Der Zuordnungsservice plant automatisch eine Aktualisierung.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | OutOfSyncDetected |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Map <*mapName*> detected the map data is out-of-sync, probably due to a missed update notification--scheduling a refresh (Zuordnung <*Zuordnung*> mit nicht synchronisierten Zuordnungsdaten festgestellt, evtl. aufgrund fehlender Aktualisierungsbenachrichtigung – eine Aktualisierung wird geplant) |

## Ereignisrouter

### Ereignisrouter wird ausgeführt

Der Ereignisrouter ist die Hauptkomponente des Collector Manager (die Komponente, die die Zuordnungen durchführt, globale Filter anwendet und die Ereignisse veröffentlicht). Dieses interne Ereignis wird gesendet, wenn der Ereignisrouter während der Initialisierung bereit ist. Bei einem Neustart des Collector Manager wird ein weiteres Ereignis gesendet, um seine Bereitschaft anzuzeigen.

Dieses Ereignis wird erst dann gesendet, wenn der Ereignisrouter alle globalen Filter und alle Zuordnungsinformationen erfolgreich geladen hat.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EventRouterIsRunning |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router completed its initialization in <*mode*> mode (Initialisierung des Ereignisrouters im Modus <*Modus*> wurde abgeschlossen) |

## Ereignisrouter wird initialisiert

Dieses interne Ereignis wird gesendet, wenn die Initialisierung eines Ereignisrouters gestartet wird. Die Initialisierung des Ereignisrouters wird gestartet, wenn dieser eine Verbindung mit dem Back-End (DAS Query) hergestellt hat.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EventRouterInitializing |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is initializing in <*mode*> mode (Der Ereignisrouter wird im Modus <*Modus*> initialisiert) |

## Ereignisrouter wird angehalten

Dieses Ereignis wird gesendet, wenn der Ereignisrouter während des Herunterfahrens eine Anforderung zum Beenden empfängt.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventRouterStopping |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is stopping (Der Ereignisrouter wird angehalten) |

## Ereignisrouter wird beendet

Dieses Ereignis wird gesendet, wenn der Ereignisrouter während des Herunterfahrens eine Anforderung zum Beenden empfängt.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventRouterTerminating |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is terminating (Der Ereignisrouter wird beendet) |

# Correlation Engine

## Correlation Engine wird ausgeführt

Der Correlation Engine-Prozess kann vom Benutzer in den Bereitschaftszustand versetzt werden. Der Ausführungszustand bestimmt, ob Ereignisse vom aktiven Prozess verarbeitet werden oder nicht. Der Prozess startet im Bereitschaftszustand (im angehaltenen Zustand) und wartet darauf, dass seine Konfiguration von der Datenbank abgerufen werden kann. Dieses Ereignis wird gesendet, wenn die Correlation Engine vom angehaltenen in den ausgeführten Zustand wechselt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EngineRunning |
| Ressource | CorrelationEngine |
| Teilressource | CorrelationEngine |
| Meldung | Correlation Engine is processing events (Die Correlation Engine verarbeitet Ereignisse) |

## Correlation Engine wird angehalten

Dieses Ereignis wird gesendet, wenn die Correlation Engine vom ausgeführten in den angehaltenen Zustand wechselt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EngineStopped |
| Ressource | CorrelationEngine |
| Teilressource | CorrelationEngine |
| Meldung | Correlation Engine has stopped processing events (Die Correlation Engine hat das Verarbeiten von Ereignissen eingestellt) |

## Regelbereitstellung wurde gestartet

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung lädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentStarted |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | deployment <*name*> started (Bereitstellung <*Name*> wurde gestartet) |

## Regelbereitstellung wurde beendet

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung entlädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentStopped |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | deployment <*name*> stopped (Bereitstellung <*Name*> wurde beendet) |

### Regelbereitstellung wurde geändert

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung neu lädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentModified |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | Deployment <*name*> modified (Bereitstellung <*Name*> wurde geändert) |

## WatchDog

### Gesteuerter Prozess wurde gestartet

Watchdog wird als Service ausgeführt. Seine Hauptaufgabe besteht darin, die Ausführung der Sentinel-Prozesse zu gewährleisten. Beim Anhalten eines Prozesses wird dieser von Watchdog automatisch neu gestartet. Dieses Ereignis wird gesendet, wenn ein Prozess gestartet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | ProcessStart |
| Ressource | WatchDog |
| Teilressource | Process |
| Meldung | Process <*ProgramName*> spawned (<*pid*>) (Prozess <*Programmname*> wurde erzeugt (<*PID*>)) |

### Gesteuerter Prozess wurde beendet

Dieses Ereignis wird gesendet, wenn ein Prozess beendet wird. Der Schweregrad ist auf 5 festgelegt, wenn für den Prozess eine Neugenerierung festgelegt ist (d. h., wenn er nicht beendet werden darf). Der Schweregrad ist auf 1 festgelegt, wenn für den Prozess eine einmalige Ausführung festgelegt ist.

| Tag | Wert |
|---|---|
| Schweregrad | 1/5 |
| Ereignisname | ProcessStop |
| Ressource | WatchDog |
| Teilressource | Process |
| Meldung | Process <*ProgramName*> exited with code <*exit_code*> (Prozess <*Programmname*> wurde beendet mit Code <*Exit_Code*>) |

### Watchdog-Prozess wurde gestartet

Beim Starten des Watchdog-Prozesses wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | ProcessStart |
| Ressource | WatchDog |
| Teilressource | WatchDog |
| Meldung | WatchDog Service Starting (WatchDog-Service wird gestartet) |

### Watchdog-Prozess wurde beendet

Beim Beenden des Watchdog-Prozesses wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | ProcessStop |
| Ressource | WatchDog |
| Teilressource | WatchDog |
| Meldung | WatchDog Service Ended (WatchDog-Service wurde beendet) |

## Collector Engine und Collector Manager

### Start eines Ports

Collector Manager sendet dieses Ereignis, wenn ein Port gestartet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PortStart |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Processing started for port_<*port id*> (Verarbeitung wurde für Port <*Port-ID*> gestartet) |

### Beenden eines Ports

Collector Manager sendet dieses Ereignis, wenn ein Port beendet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PortStop |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Processing stopped for port_<*port id*> (Verarbeitung wurde für Port <*Port-ID*> beendet) |

## Permanenter Prozess wurde beendet

Die Collector Engine sendet dieses Ereignis, wenn der Connector des permanenten Prozesses feststellt, dass sein gesteuerter Prozess beendet wurde.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | PersistentProcessDied |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Persistent Process on port <*port id*> has died (Permanenter Prozess an Port <*Port-ID*> wurde beendet) |

## Permanenter Prozess wurde neu gestartet

Die Collector Engine sendet dieses Ereignis, wenn der Connector des permanenten Prozesses den beendeten gesteuerten Prozess neu starten kann.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PersistentProcessRestarted |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Persistent Process on port <*port id*> has restarted (Permanenter Prozess an Port <*Port-ID*> wurde neu gestartet) |

# Event Service

## Zyklische Abhängigkeit

Der Event Service sendet dieses Ereignis, wenn er einen Zyklus in der Ereignisdefinition feststellt (in Abhängigkeiten zwischen Tags, aufgrund referenzieller Zuordnungen). Überprüfen Sie die Ereigniskonfiguration in SDM und korrigieren Sie die Abhängigkeit.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | CyclicalDependency |
| Ressource | EventService |
| Teilressource | ObjectAttrInfos |
| Meldung | Cyclical dependency detected in event transformations. Check event configuration. (Zyklische Abhängigkeit in Ereignistransformationen festgestellt. Überprüfen Sie die Ereigniskonfiguration.) |

# Active Views

## Active View wurde erstellt

DAS_Binary sendet dieses Ereignis, wenn eine Active View erstellt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartCreated |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Creating new Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Neue Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wird erstellt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Verbindung mit Active View hergestellt

DAS_Binary sendet dieses Ereignis, wenn ein Benutzer eine Verbindung mit einer vorhandenen Active View herstellt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartJoiningExistingData |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Joining existing Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Verbindung mit vorhandener Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wird hergestellt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Inaktive Active View entfernt

DAS_Binary sendet dieses Ereignis, wenn eine nicht permanente Active View wegen Inaktivität entfernt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartInactiveAndRemoved |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Removed idle Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Inaktive Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wurde entfernt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Inaktive permanente Active View entfernt

DAS_Binary sendet dieses Ereignis, wenn eine permanente Active View wegen Inaktivität entfernt wird. Permanente Active Views sind in den Benutzereinstellungen gespeichert und in der Standardeinstellung tritt nach mehreren Tagen der Inaktivität eine Zeitüberschreitung auf.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtPermanentChartRemoved |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Removed idle permanent Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Inaktive permanente Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wurde entfernt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Active View ist nun permanent

DAS_Binary sendet dieses Ereignis, wenn festgestellt wird, dass eine Active View nun als permanent festgelegt ist. Eine solche Überprüfung wird regelmäßig ausgeführt, daher kann dieses Ereignis wenige Minuten nach dem Speichern einer Active View in den Einstellungen generiert werden.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartIsNowPermanent |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*> is now permanent. (Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> ist nun permanent.) |

## Active View ist nicht mehr permanent

DAS_Binary sendet dieses Ereignis, wenn festgestellt wird, dass eine zuvor permanente Active View nicht mehr als permanent festgelegt ist. Eine solche Überprüfung wird regelmäßig ausgeführt, daher kann dieses Ereignis wenige Minuten nach dem Entfernen einer Active View aus den Einstellungen generiert werden.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartNotPermanent |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*> is no longer permanent. (Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> ist nicht mehr permanent.) |

# Zusammenfassung

| Ereignisname | Schweregrad | Quelle | SubResource | Komponente |
|---|---|---|---|---|
| AuthenticationFailed | 4 | UserAuthentication | Authenticate | Authentication |
| NoSuchUser | 4 | UserAuthentication | Authenticate | Authentication |
| TooManyActiveUsers | 4 | UserAuthentication | Authenticate | Authentication |
| LockedUser | 4 | UserAuthentication | Authenticate | Authentication |
| UserLoggedOut | 1 | UserSessionManager | User | User Session |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| MoveArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| InsertEventsFailed | 5 | EventSubSystem | Events | Event |
| OpenArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| WriteArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| SummaryUpdateFailure | 4 | Aggregation | Summary | Aggregation |
| InsertIntoOverflowPartition | 5 | EventSubSystem | Events | Event |
| EventInsertionIsBlocked | 4 | EventSubSystem | Events | Event |
| EventInsertionResumed | 2 | EventSubSystem | Events | Event |
| EventRouterIsRunning | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterInitializing | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterStopping | 2 | AgentManager | EventRouter | EventRouter |
| EventRouterTerminating | 2 | AgentManager | EventRouter | EventRouter |
| ErrorNoSuchMap | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadingMapFromCache | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| RefreshingMapFromServer | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| TimeoutRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| ErrorRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadedLargeMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| LongTimeToLoadMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| TimedoutWaitingForCallback | 2 | MappingService | ReferentialDataObjectMap | Mapping |
| ErrorApplyingIncrementalUpdate | 4 | MappingService | ReferentialDataObjectMap | Mapping |

| Ereignisname | Schweregrad | Quelle | SubResource | Komponente |
|---|---|---|---|---|
| OutOfSyncDetected | 2 | MappingService | ReferentialDataObjectMap | Mapping |
| EngineRunning | 1 | CorrelationEngine | CorrelationEngine | |
| EngineStopped | 1 | CorrelationEngine | CorrelationEngine | |
| DeploymentStarted | 1 | CorrelationEngine | Deployment | |
| DeploymentStopped | 1 | CorrelationEngine | Deployment | |
| DeploymentModified | 1 | CorrelationEngine | Deployment | |
| ProcessStart | 1 | WatchDog | Process | |
| ProcessStop | 1/5 | WatchDog | Process | |
| ProcessStart | 1 | WatchDog | WatchDog | |
| ProcessStop | 5 | WatchDog | WatchDog | |
| PortStart | | AgentManager | AgentManager | |
| PortStop | | AgentManager | AgentManager | |
| PersistentProcessDied | 5 | AgentManager | AgentManager | |
| PersistentProcessRestarted | 1 | AgentManager | AgentManager | |
| SortDependencies | 5 | EventService | ObjectAttrInfo | EventService |
| DbSpaceReachedTimeThrshld | 0 | Database | Database | Event |
| DbSpaceReachedPercentThrshld | 0 | Database | Database | Event |
| DbSpaceVeryLow | 5 | Database | Database | Event |
| RtChartCreated | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartJoiningExistingData | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartInactiveAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartPermanentAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartIsNowPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartNotPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |

# A Systemereignisse für Sentinel 5

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

In den unten stehenden Beschreibungstabellen werden kursiv formatierte und in <…> eingeschlossene Begriffe in den tatsächlichen Meldungen durch die relevanten Werte ersetzt.

## Authentifizierungsereignisse

### Fehler bei der Authentifizierung

Wenn eine Benutzerauthentifizierung nicht erfolgt, wird das folgende Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | AuthenticationFailed |
| Ressource | UserAuthentication |
| Teilressource | Authenticate |
| Meldung | Authentication of user <*name*> with OS name <*domUser*> from <*IP*> failed (Authentifizierung von Benutzer <*Name*> mit Betriebssystemname <*DomBenutzer*> von <*IP*> ist nicht erfolgt) |

### Kein solches Benutzerereignis vorhanden

Wenn sich ein Benutzer bei der Anwendung anmeldet und die Authentifizierung erfolgreich ausgeführt wird, der Benutzer jedoch kein Sentinel-Benutzer ist, wird das folgende Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | NoSuchUser |
| Ressource | UserAuthentication |
| Teilressource | Authenticate |
| Meldung | No existing user with name <*name*> found (Es wurde kein vorhandener Benutzer mit dem Namen <*Name*> gefunden) |

## Doppelte Benutzerobjekte

Wenn ein unerwartetes zweites aktives Benutzerobjekt vorhanden ist (dies ist nicht zulässig), wird das folgende Ereignis generiert. Dies ist ein interner Fehler.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | TooManyActiveUsers |
| Ressource | UserAuthentication |
| Teilressource | Authenticate |
| Meldung | Error in user table: Multiple users with the name <*name*> found (Fehler in Benutzertabelle: Es wurden mehrere Benutzer mit dem Namen <*Name*> gefunden) |

## Gesperrtes Konto

Beim Versuch einer Anmeldung mit einem gesperrten Benutzerkonto wird das folgende Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | LockedUser |
| Ressource | UserAuthentication |
| Teilressource | Authentication |
| Meldung | Attempt to login using locked account <acct> (Versuch der Anmeldung mit dem gesperrten Konto <Kto>) |

# Benutzersitzungen

## Abgemeldeter Benutzer

Beim Abmelden eines Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedOut |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | Closing session for <*user*> OS name <*osName*> from <*IP*> was on since <*date*>; currently <*num*> active users (Sitzung für <*Benutzer*>, Betriebssystemname <*OSName*>, von <*IP*> seit <*Datum*> wird geschlossen; zurzeit sind <*n*> aktive Benutzer vorhanden) |

## Angemeldeter Benutzer

Beim Anmelden eines Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedIn |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | User <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Benutzer <*Benutzer*> mit Betriebssystemname <*OSName*> an <*IP*> hat sich angemeldet; zurzeit sind <*n*> aktive Benutzer vorhanden) |

## Erkannter Benutzer

Wenn der Server neu gestartet wird, gehen die Sitzungsinformationen verloren. In einem solchen Fall wird die Sitzung wiederhergestellt, wenn Nachrichten von den aktiven Benutzern empfangen werden. Beim Erkennen eines verbundenen Benutzers wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | UserLoggedIn |
| Ressource | UserSessionManager |
| Teilressource | User |
| Meldung | Discovered active user <*user*> with OS name <*osName*> at <*IP*> logged in; currently <*num*> active users (Aktiver Benutzer <*Benutzer*> mit Betriebssystemname <*OSName*> angemeldet an <*IP*> wurde erkannt; zurzeit sind <*n*> aktive Benutzer vorhanden) |

# Ereignis

## Fehler beim Verschieben von abgeschlossener Datei

Wenn eine Ereignisdatei abgeschlossen wurde, wird sie in das Ausgabeverzeichnis verschoben. Wenn dieser Verschiebevorgang nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | MoveArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error moving completed archive file *<fname>* to *<dir>* (Fehler beim Verschieben von abgeschlossener Archivdatei *<Dateiname>* nach *<Verz>*) |

## Fehler beim Einfügen von Ereignissen

Wenn beim Einfügen von Ereignissen in die Datenbank Fehler auftreten, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | InsertEventsFailed |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Error inserting events into the Database—the events may be permanently lost. Please check the Database and backend server logs *<Exception>* (Fehler beim Einfügen von Ereignissen in die Datenbank – die Ereignisse können endgültig verloren gehen. Überprüfen Sie die Datenbank- und die Back-End-Server-Protokolle *<Ausnahme>*) |

## Fehler beim Öffnen von Archivdatei

Wenn das Öffnen einer Archivdatei zum Speichern der Ereignisse für die Aggregation nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | OpenArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error opening archive file *<name>* in *<dir>* (Fehler beim Öffnen von Archivdatei *<Name>* in *<Verz>*) |

## Fehler beim Schreiben in Archivdatei

Wenn das Öffnen einer Archivdatei zum Speichern der Ereignisse für die Aggregation nicht erfolgt, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 3 |
| Ereignisname | WriteArchiveFileFailed |
| Ressource | *<DAS-Name>* |
| Teilressource | ArchiveFile |
| Meldung | Error writing newly received events to aggregation archive file *<fname>* (Fehler beim Schreiben neu empfangener Ereignisse in Archivdatei für die Aggregation *<Dateiname>*) |

## Schreiben auf die Überlaufpartition (P_MAX)

Etwa alle 5 Minuten wird ein Ereignis gesendet, um den Benutzer über das Schreiben von Ereignissen auf die Überlaufpartition (P_MAX) zu benachrichtigen. Wenn dies der Fall ist, muss der Administrator mithilfe von SDM weitere Partitionen hinzufügen, damit die Leistung nicht beeinträchtigt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | InsertIntoOverflowPartition |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Error: currently inserting into the overflow partitions (P_MAX), add more partitions (Fehler: Zurzeit wird auf die Überlaufpartitionen (P_MAX) geschrieben, fügen Sie weitere Partitionen hinzu) |

## Einfügen von Ereignissen ist gesperrt

Wenn DAS auf die Überlaufpartition schreibt und der Benutzer versucht, Partitionen hinzuzufügen, sendet SDM eine Anforderung an DAS, dass das Einfügen von Ereignissen in die Datenbank vorübergehend unterbrochen werden soll. Wenn dies der Fall ist, sendet DAS bei jedem Versuch, Ereignisse in die Datenbank einzufügen, interne Ereignisse.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | EventInsertionIsBlocked |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Event insertion is blocked, waiting *<num>* sec (Einfügen von Ereignissen ist gesperrt, warten Sie *<n>* Sekunden) |

## Einfügen von Ereignissen wird fortgesetzt

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventInsertionResumed |
| Ressource | EventSubSystem |
| Teilressource | Events |
| Meldung | Event insertion has resumed after being blocked (Einfügen von Ereignissen wird nach vorübergehender Unterbrechung fortgesetzt) |

## Speicherplatz der Datenbank hat angegebenen Zeitschwellenwert erreicht

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | DbSpaceReachedTimeThrshld |
| Ressource | Database |
| Teilressource | Database |
| Meldung | Tablespace <*string*> has <*num*> MB left and growing <*num*> bytes per second and will run out space within the time threshold specified <*num*> seconds (Tabellenbereich <*Zeichenkette*> verfügt noch über <*n*> MB und wächst um <*n*> Byte pro Sekunde an, der Speicherplatz wird innerhalb des angegebenen Zeitschwellenwerts erschöpft sein, <*n*> Sekunden) |

## Speicherplatz der Datenbank hat angegebenen prozentualen Schwellenwert erreicht

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | DbSpaceReachedPercentThrshld |
| Ressource | Database |
| Teilressource | Database |

| Tag | Wert |
|---|---|
| Meldung | Tablespace <*string*> has current size of <*num*> MB with a max size of <*num*> MB and has reached the percentage threshold of <*num*> % (Tabellenbereich <*Zeichenkette*> hat eine aktuelle Größe von <*n*> MB bei einer maximalen Größe von <*n*> MB und der prozentuale Schwellenwert von <*n*> % wurde erreicht) |

### Sehr wenig Datenbankspeicher

Wenn nach einer vorübergehenden Unterbrechung mit dem Einfügen von Ereignissen fortgefahren wird, wird das folgende Ereignis gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | DbSpaceVeryLow |
| Ressource | Database |
| Teilressource | Database |
| Meldung | Tablespace <*string*> has current size of <*num*> MB and has reached the physical threshold of <*num*> MB (Tabellenbereich <*Zeichenkette*> hat zurzeit eine Größe von <*n*> MB und den physischen Schwellenwert von <*n*> MB erreicht) |

## Aggregation

### Fehler beim Einfügen von Zusammenfassungsdaten in die Datenbank

Bei einem Fehler während des Schreibens von Aggregationsdaten in die Datenbank wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | SummaryUpdateFailure |
| Ressource | Aggregation |
| Teilressource | Summary |
| Meldung | Error saving summary batch to the database for summary <*summaryName*> (Fehler beim Speichern des Zusammenfassungsstapels in der Datenbank für Zusammenfassung <*Zusammenfassung*>) |

# Zuordnungsservice

## Fehler beim Initialisieren von Zuordnung mit ID

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Dieser Fehler wird generiert, wenn der Collector Manager versucht, eine nicht vorhandene Zuordnung abzurufen. Dies sollte nicht vorkommen, kann jedoch der Fall sein, wenn Zuordnungen erstellt und gelöscht werden.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorNoSuchMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Error initializing map with id <*ID*>: no such map (Fehler beim Initialisieren von Zuordnung mit ID <*ID*>: keine solche Zuordnung vorhanden) |

## Aktualisieren von Zuordnung aus Cache

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass der zugehörige Cache auf dem aktuellen Stand ist und dass die Zuordnung aus dem Cache aktualisiert wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | LoadingMapFromCache |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Loading from cache v<*version*> of map <*mapName*> (ID <*id*>) (Laden aus Cache <*Version*> von Zuordnung <*Zuordnung*> (ID <*ID*>)) |

## Aktualisieren von Zuordnung von Server

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass die Zuordnung entweder nicht im Cache enthalten war oder dass die Version im Cache nicht aktuell ist, sodass der Collector Manager die Zuordnung vom Server abruft.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RefreshingMapFromServer |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Refreshing from server map <*name*> with id <*ID*> (Aktualisieren der Zuordnung <*Name*> mit ID <*ID*> vom Server) |

## Zeitüberschreitung beim Aktualisieren von Zuordnung

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass der Collector Manager versucht hat, die Zuordnung vom Server abzurufen, und die Anforderung wurde vom Server nicht akzeptiert, sodass eine Zeitüberschreitung aufgetreten ist. Dieser Fehler wird als flüchtig angesehen und der Collector Manager versucht erneut, den Vorgang auszuführen.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | TimeoutRefreshingMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Request timed out while refreshing map <*name*>: <*exception*> (Zeitüberschreitung der Anforderung beim Aktualisieren von Zuordnung <*Name*>: <*Ausnahme*>) |

## Fehler beim Aktualisieren von Zuordnung

Dieses interne Ereignis wird Client-seitig vom Zuordnungsservice generiert (dem Service, der Bestandteil des Collector Manager ist). Wenn der Collector Manager eine Anweisung zum Aktualisieren der Zuordnung erhält, weil diese selbst oder deren Definition geändert wurde, wird ein internes Ereignis gesendet. Das heißt, dass beim Aktualisieren einer Zuordnung ein unerwarteter, nicht flüchtiger Fehler aufgetreten ist. Der Collector Manager wartet 15 Minuten und versucht anschließend erneut, den Vorgang auszuführen. Wenn dieser Fehler während der Initialisierung auftritt, wird diese fortgesetzt und die betreffende Zuordnung wird so lange ignoriert, bis sie erfolgreich geladen werden kann.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorRefreshingMapData |

| Tag | Wert |
|---|---|
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Error refreshimg map <*mapName*>: <*exc*> (Fehler beim Aktualisieren von Zuordnung <*Zuordnung*>: <*Ausnahme*>) |

## Laden von großer Zuordnung

Dieses interne Ereignis ist ein Informationsereignis, das vom Zuordnungsservice gesendet wird. Damit wird darüber informiert, dass eine große Zuordnung in den Collector Manager geladen wurde. Eine Zuordnung gilt als groß, wenn die Anzahl der Zeilen 100.000 überschreitet.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | LoadedLargeMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Finished loading map <*name*> with id <*ID*> and <*num*> entries and total size <#>Kb in <##>sec (Zuordnung <*Name*> mit ID <*ID*> und <*n*> Einträgen und einer Gesamtgröße von <*n*> Kb in <*n*> Sekunden wurde geladen) |

## Langes Laden von Zuordnung

Dieses interne Ereignis ist ein Informationsereignis, das vom Zuordnungsservice gesendet wird. Damit wird darüber informiert, dass das Laden einer Zuordnung außergewöhnlich lange (länger als 1 Minute) gedauert hat.

| Tag | Wert |
|---|---|
| Schweregrad | 0 |
| Ereignisname | LongTimeToLoadMap |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | It took <##>sec to load map <name> with id <*ID*> and <*num*> entries and total size <##>Kb (Das Laden von Zuordnung <*Name*> mit ID <*ID*> und <*n*> Einträgen und einer Gesamtgröße von <*n*> Kb dauerte <*n*> Sekunden) |

## TimedoutWaitingForCallback

Wenn der Collector Manager eine Zuordnung aktualisieren muss, sendet er eine Anforderung an das Back-End. Diese Anforderung enthält einen Rückruf. Das Back-End generiert die Zuordnung und sendet diese anschließend mithilfe des Rückrufs an den Collector Manager. Wenn der Eingang der Antwort zu lange dauert (länger als 10 Minuten), sendet der Collector Manager eine zweite Anforderung und die erste Anforderung wird als verloren gegangen angesehen. Wenn dies der Fall ist, wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | TimedoutWaitingForCallback |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Map <*name*> timed out waiting for callback with new map data--retrying (Zeitüberschreitung für Zuordnung <*Name*> beim Warten auf Rückruf mit neuen Zuordnungsdaten; neuer Versuch) |

## ErrorApplyingIncrementalUpdate

Dieses Ereignis wird gesendet, wenn beim Übernehmen einer Aktualisierung auf eine vorhandene Clientzuordnung durch den Zuordnungsservice ein Fehler auftritt.

| Tag | Wert |
|---|---|
| Schweregrad | 4 |
| Ereignisname | ErrorApplyingIncrementalUpdate |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | The error <*error*> occurred while applying updates to map <*mapName*> (ID <*mapId*>) v.<*version*>. Rescheduling a refresh to complete map update. (Fehler <*Fehler*> beim Übernehmen von Aktualisierungen für Zuordnung <*Zuordnung*> (ID <*ID*>), Version <*Version*>. Eine Aktualisierung für die Zuordnung wird neu geplant.) |

### OutOfSyncDetected

Dieses Ereignis wird gesendet, wenn der Zuordnungsservice feststellt, dass eine Zuordnung veraltet ist. Der Zuordnungsservice plant automatisch eine Aktualisierung.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | OutOfSyncDetected |
| Ressource | MappingService |
| Teilressource | ReferentialDataObjectMap |
| Meldung | Map <*mapName*> detected the map data is out-of-sync, probably due to a missed update notification--scheduling a refresh (Zuordnung <*Zuordnung*> mit nicht synchronisierten Zuordnungsdaten festgestellt, evtl. aufgrund fehlender Aktualisierungsbenachrichtigung – eine Aktualisierung wird geplant) |

## Ereignisrouter

### Ereignisrouter wird ausgeführt

Der Ereignisrouter ist die Hauptkomponente des Collector Manager (die Komponente, die die Zuordnungen durchführt, globale Filter anwendet und die Ereignisse veröffentlicht). Dieses interne Ereignis wird gesendet, wenn der Ereignisrouter während der Initialisierung bereit ist. Bei einem Neustart des Collector Manager wird ein weiteres Ereignis gesendet, um seine Bereitschaft anzuzeigen.

Dieses Ereignis wird erst dann gesendet, wenn der Ereignisrouter alle globalen Filter und alle Zuordnungsinformationen erfolgreich geladen hat.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EventRouterIsRunning |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router completed its initialization in <*mode*> mode (Initialisierung des Ereignisrouters im Modus <*Modus*> wurde abgeschlossen) |

## Ereignisrouter wird initialisiert

Dieses interne Ereignis wird gesendet, wenn die Initialisierung eines Ereignisrouters gestartet wird. Die Initialisierung des Ereignisrouters wird gestartet, wenn dieser eine Verbindung mit dem Back-End (DAS Query) hergestellt hat.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EventRouterInitializing |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is initializing in <*mode*> mode (Der Ereignisrouter wird im Modus <*Modus*> initialisiert) |

## Ereignisrouter wird angehalten

Dieses Ereignis wird gesendet, wenn der Ereignisrouter während des Herunterfahrens eine Anforderung zum Beenden empfängt.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventRouterStopping |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is stopping (Der Ereignisrouter wird angehalten) |

## Ereignisrouter wird beendet

Dieses Ereignis wird gesendet, wenn der Ereignisrouter während des Herunterfahrens eine Anforderung zum Beenden empfängt.

| Tag | Wert |
|---|---|
| Schweregrad | 2 |
| Ereignisname | EventRouterTerminating |
| Ressource | AgentManager |
| Teilressource | EventRouter |
| Meldung | Event router is terminating (Der Ereignisrouter wird beendet) |

# Correlation Engine

## Correlation Engine wird ausgeführt

Der Correlation Engine-Prozess kann vom Benutzer in den Bereitschaftszustand versetzt werden. Der Ausführungszustand bestimmt, ob Ereignisse vom aktiven Prozess verarbeitet werden oder nicht. Der Prozess startet im Bereitschaftszustand (im angehaltenen Zustand) und wartet darauf, dass seine Konfiguration von der Datenbank abgerufen werden kann. Dieses Ereignis wird gesendet, wenn die Correlation Engine vom angehaltenen in den ausgeführten Zustand wechselt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EngineRunning |
| Ressource | CorrelationEngine |
| Teilressource | CorrelationEngine |
| Meldung | Correlation Engine is processing events (Die Correlation Engine verarbeitet Ereignisse) |

## Correlation Engine wird angehalten

Dieses Ereignis wird gesendet, wenn die Correlation Engine vom ausgeführten in den angehaltenen Zustand wechselt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | EngineStopped |
| Ressource | CorrelationEngine |
| Teilressource | CorrelationEngine |
| Meldung | Correlation Engine has stopped processing events (Die Correlation Engine hat das Verarbeiten von Ereignissen eingestellt) |

## Regelbereitstellung wurde gestartet

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung lädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentStarted |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | deployment <*name*> started (Bereitstellung <*Name*> wurde gestartet) |

## Regelbereitstellung wurde beendet

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung entlädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentStopped |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | deployment <*name*> stopped (Bereitstellung <*Name*> wurde beendet) |

### Regelbereitstellung wurde geändert

Dieses Ereignis wird gesendet, wenn eine Engine erfolgreich eine Regelbereitstellung neu lädt. Diese Meldung wird ungeachtet des Ausführungszustands der Engine gesendet.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | DeploymentModified |
| Ressource | CorrelationEngine |
| Teilressource | Deployment |
| Meldung | Deployment <*name*> modified (Bereitstellung <*Name*> wurde geändert) |

## WatchDog

### Gesteuerter Prozess wurde gestartet

Watchdog wird als Service ausgeführt. Seine Hauptaufgabe besteht darin, die Ausführung der Sentinel-Prozesse zu gewährleisten. Beim Anhalten eines Prozesses wird dieser von Watchdog automatisch neu gestartet. Dieses Ereignis wird gesendet, wenn ein Prozess gestartet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | ProcessStart |
| Ressource | WatchDog |
| Teilressource | Process |
| Meldung | Process <*ProgramName*> spawned (<*pid*>) (Prozess <*Programmname*> wurde erzeugt (<*PID*>)) |

### Gesteuerter Prozess wurde beendet

Dieses Ereignis wird gesendet, wenn ein Prozess beendet wird. Der Schweregrad ist auf 5 festgelegt, wenn für den Prozess eine Neugenerierung festgelegt ist (d. h., wenn er nicht beendet werden darf). Der Schweregrad ist auf 1 festgelegt, wenn für den Prozess eine einmalige Ausführung festgelegt ist.

| Tag | Wert |
|---|---|
| Schweregrad | 1/5 |
| Ereignisname | ProcessStop |
| Ressource | WatchDog |
| Teilressource | Process |
| Meldung | Process <*ProgramName*> exited with code <*exit_code*> (Prozess <*Programmname*> wurde beendet mit Code <*Exit_Code*>) |

### Watchdog-Prozess wurde gestartet

Beim Starten des Watchdog-Prozesses wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | ProcessStart |
| Ressource | WatchDog |
| Teilressource | WatchDog |
| Meldung | WatchDog Service Starting (WatchDog-Service wird gestartet) |

### Watchdog-Prozess wurde beendet

Beim Beenden des Watchdog-Prozesses wird das folgende interne Ereignis generiert.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | ProcessStop |
| Ressource | WatchDog |
| Teilressource | WatchDog |
| Meldung | WatchDog Service Ended (WatchDog-Service wurde beendet) |

## Collector Engine und Collector Manager

### Start eines Ports

Collector Manager sendet dieses Ereignis, wenn ein Port gestartet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PortStart |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Processing started for port_<*port id*> (Verarbeitung wurde für Port <*Port-ID*> gestartet) |

### Beenden eines Ports

Collector Manager sendet dieses Ereignis, wenn ein Port beendet wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PortStop |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Processing stopped for port_<*port id*> (Verarbeitung wurde für Port <*Port-ID*> beendet) |

## Permanenter Prozess wurde beendet

Die Collector Engine sendet dieses Ereignis, wenn der Connector des permanenten Prozesses feststellt, dass sein gesteuerter Prozess beendet wurde.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | PersistentProcessDied |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Persistent Process on port <*port id*> has died (Permanenter Prozess an Port <*Port-ID*> wurde beendet) |

## Permanenter Prozess wurde neu gestartet

Die Collector Engine sendet dieses Ereignis, wenn der Connector des permanenten Prozesses den beendeten gesteuerten Prozess neu starten kann.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | PersistentProcessRestarted |
| Ressource | AgentManager |
| Teilressource | AgentManager |
| Meldung | Persistent Process on port <*port id*> has restarted (Permanenter Prozess an Port <*Port-ID*> wurde neu gestartet) |

# Event Service

## Zyklische Abhängigkeit

Der Event Service sendet dieses Ereignis, wenn er einen Zyklus in der Ereignisdefinition feststellt (in Abhängigkeiten zwischen Tags, aufgrund referenzieller Zuordnungen). Überprüfen Sie die Ereigniskonfiguration in SDM und korrigieren Sie die Abhängigkeit.

| Tag | Wert |
|---|---|
| Schweregrad | 5 |
| Ereignisname | CyclicalDependency |
| Ressource | EventService |
| Teilressource | ObjectAttrInfos |
| Meldung | Cyclical dependency detected in event transformations. Check event configuration. (Zyklische Abhängigkeit in Ereignistransformationen festgestellt. Überprüfen Sie die Ereigniskonfiguration.) |

# Active Views

## Active View wurde erstellt

DAS_Binary sendet dieses Ereignis, wenn eine Active View erstellt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartCreated |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Creating new Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Neue Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wird erstellt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Verbindung mit Active View hergestellt

DAS_Binary sendet dieses Ereignis, wenn ein Benutzer eine Verbindung mit einer vorhandenen Active View herstellt.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartJoiningExistingData |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Joining existing Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Verbindung mit vorhandener Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wird hergestellt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Inaktive Active View entfernt

DAS_Binary sendet dieses Ereignis, wenn eine nicht permanente Active View wegen Inaktivität entfernt wird.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartInactiveAndRemoved |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Removed idle Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Inaktive Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wurde entfernt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Inaktive permanente Active View entfernt

DAS_Binary sendet dieses Ereignis, wenn eine permanente Active View wegen Inaktivität entfernt wird. Permanente Active Views sind in den Benutzereinstellungen gespeichert und in der Standardeinstellung tritt nach mehreren Tagen der Inaktivität eine Zeitüberschreitung auf.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtPermanentChartRemoved |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Removed idle permanent Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*>. Currently <*n*> Active View(s) Collecting. (Inaktive permanente Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> wurde entfernt. Zurzeit wird die Erfassung für <*n*> Active View(s) ausgeführt.) |

## Active View ist nun permanent

DAS_Binary sendet dieses Ereignis, wenn festgestellt wird, dass eine Active View nun als permanent festgelegt ist. Eine solche Überprüfung wird regelmäßig ausgeführt, daher kann dieses Ereignis wenige Minuten nach dem Speichern einer Active View in den Einstellungen generiert werden.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartIsNowPermanent |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*> is now permanent. (Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> ist nun permanent.) |

## Active View ist nicht mehr permanent

DAS_Binary sendet dieses Ereignis, wenn festgestellt wird, dass eine zuvor permanente Active View nicht mehr als permanent festgelegt ist. Eine solche Überprüfung wird regelmäßig ausgeführt, daher kann dieses Ereignis wenige Minuten nach dem Entfernen einer Active View aus den Einstellungen generiert werden.

| Tag | Wert |
|---|---|
| Schweregrad | 1 |
| Ereignisname | RtChartNotPermanent |
| Ressource | RealTimeSummaryService |
| Teilressource | ChartManager |
| Meldung | Active View with filter <*filter*> and attribute <*attribute*> for users with security filter <*security filter*> is no longer permanent. (Active View mit Filter <*Filter*> und Attribut <*Attribut*> für Benutzer mit Sicherheitsfilter <*Sicherheitsfilter*> ist nicht mehr permanent.) |

# Zusammenfassung

| Ereignisname | Schweregrad | Quelle | SubResource | Komponente |
|---|---|---|---|---|
| AuthenticationFailed | 4 | UserAuthentication | Authenticate | Authentication |
| NoSuchUser | 4 | UserAuthentication | Authenticate | Authentication |
| TooManyActiveUsers | 4 | UserAuthentication | Authenticate | Authentication |
| LockedUser | 4 | UserAuthentication | Authenticate | Authentication |
| UserLoggedOut | 1 | UserSessionManager | User | User Session |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| UserLoggedIn | 1 | UserSessionManager | User | User |
| MoveArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| InsertEventsFailed | 5 | EventSubSystem | Events | Event |
| OpenArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| WriteArchiveFileFailed | 3 | *DAS-Name* | ArchiveFile | Event |
| SummaryUpdateFailure | 4 | Aggregation | Summary | Aggregation |
| InsertIntoOverflowPartition | 5 | EventSubSystem | Events | Event |
| EventInsertionIsBlocked | 4 | EventSubSystem | Events | Event |
| EventInsertionResumed | 2 | EventSubSystem | Events | Event |
| EventRouterIsRunning | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterInitializing | 1 | AgentManager | EventRouter | EventRouter |
| EventRouterStopping | 2 | AgentManager | EventRouter | EventRouter |
| EventRouterTerminating | 2 | AgentManager | EventRouter | EventRouter |
| ErrorNoSuchMap | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadingMapFromCache | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| RefreshingMapFromServer | 1 | MappingService | ReferentialDataObjectMap | Mapping |
| TimeoutRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| ErrorRefreshingMapData | 4 | MappingService | ReferentialDataObjectMap | Mapping |
| LoadedLargeMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| LongTimeToLoadMap | 0 | MappingService | ReferentialDataObjectMap | Mapping |
| TimedoutWaitingForCallback | 2 | MappingService | ReferentialDataObjectMap | Mapping |
| ErrorApplyingIncrementalUpdate | 4 | MappingService | ReferentialDataObjectMap | Mapping |

| Ereignisname | Schweregrad | Quelle | SubResource | Komponente |
|---|---|---|---|---|
| OutOfSyncDetected | 2 | MappingService | ReferentialDataObjectMap | Mapping |
| EngineRunning | 1 | CorrelationEngine | CorrelationEngine | |
| EngineStopped | 1 | CorrelationEngine | CorrelationEngine | |
| DeploymentStarted | 1 | CorrelationEngine | Deployment | |
| DeploymentStopped | 1 | CorrelationEngine | Deployment | |
| DeploymentModified | 1 | CorrelationEngine | Deployment | |
| ProcessStart | 1 | WatchDog | Process | |
| ProcessStop | 1/5 | WatchDog | Process | |
| ProcessStart | 1 | WatchDog | WatchDog | |
| ProcessStop | 5 | WatchDog | WatchDog | |
| PortStart | | AgentManager | AgentManager | |
| PortStop | | AgentManager | AgentManager | |
| PersistentProcessDied | 5 | AgentManager | AgentManager | |
| PersistentProcessRestarted | 1 | AgentManager | AgentManager | |
| SortDependencies | 5 | EventService | ObjectAttrInfo | EventService |
| DbSpaceReachedTimeThrshld | 0 | Database | Database | Event |
| DbSpaceReachedPercentThrshld | 0 | Database | Database | Event |
| DbSpaceVeryLow | 5 | Database | Database | Event |
| RtChartCreated | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartJoiningExistingData | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartInactiveAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartPermanentAndRemoved | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartIsNowPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |
| RtChartNotPermanent | 1 | RealTimeSummaryService | ChartManager | Active Views |