Sentinel™ 6 von Novell

23. Mai 2007

Die Informationen dieser Readme-Datei beziehen sich auf Sentinel 6.0 von Novell®, das eine gesamtheitliche Ansicht der Sicherheits- und Compliance-Aktivitäten in Echtzeit anzeigt und Kunden bei der Überwachung, Berichterstattung sowie beim automatischen Reagieren auf Netzwerkereignisse im gesamten Unternehmen unterstützt.

Die aktuellste Readme-Datei für Sentinel 6ist in den folgenden Sprachen verfügbar: Englisch, Deutsch, Französisch, Italienisch, Spanisch, BrasilianischPortugiesisch, Japanisch, Traditionelles Chinesisch und Vereinfachtes Chinesisch. Zum Anzeigen oder Herunterladen dieser Readme-Dateien besuchen Sie die Novell-Dokumentations-Site unter http://www.novell.com/documentation/sentinel6.

Neue Funktionen in Sentinel 6

Sentinel 6 bietet viele neue Funktionen und Verbesserungen, die die Software leistungsfähiger, flexibler und benutzerfreundlicher machen. Dieser Abschnitt beschreibt die neuen Funktionen in Sentinel 6.

Neue Korrelationsfunktionen und Sprachkonstrukte

Die Korrelation von Sentinel 6 wurde mit neuen Konstrukten verbessert, die verschachtelte, sequenzielle und Ursache-Wirkung-Regeltypen sowie leistungsfähige Assistenten zur Unterstützung bei der Erstellung neuer Regeln ermöglichen. Andere Verbesserungen der Korrelation sind beispielsweise ein neues Modell zur Implementierung von Regeln, zusätzliche Optionen für die Reaktion auf wiederholte Angriffe, neue Korrelationsaktionen und verminderter administrativer Overhead für die Verwaltung von Regeln.

Korrelation mittels dynamischer Listen

Eine wichtige neue Funktion von Sentinel 6 ist die Korrelation mit dynamischen Listen. Diese dienen zur Korrelation mit ausgewählten Verlaufsereignisdaten und wichtigen Referenzdaten aus externen Quellen. Dynamische Listen können manuell über die Verwaltungsoberfläche oder automatisch durch das Hinzufügen oder Entfernen von Elementen mittels Aktionen beim Auslösen von Korrelationsregeln erstellt werden. Neue Korrelations-Sprachkonstrukte ermöglichen dann die Auslösung von Regeln basierend darauf, ob ein bestimmtes Attribut in einer Liste vorhanden ist oder nicht.

Neue globale Filteroptionen

Filter können nun so erstellt werden, dass Ereignisse nur an den Datenspeicher, an alle Sentinel-Komponenten oder nur an die Sentinel-Benutzeroberfläche und die Korrelations-Engine gesendet werden. Dadurch erhalten Benutzer die Option, große Mengen von Daten zu analysieren und nur die korrelierten Ereignisse zu speichern und somit zu vermeiden, große Mengen unwichtiger Daten zu speichern.

iTRAC-Vorfall-Verwaltungssystem der nächsten Generation

Das iTRAC-Vorfall-Verwaltungssystem in Sentinel 6 wurde deutlich verbessert und bietet erweitertes Potential sowie mehr Leistung und Flexibilität. Es ermöglicht nun umfassende Anpassung der Workflow-Vorgänge als Reaktion auf Vorfälle, damit diese den vorhandenen Vorfall-Behebungsplänen einer Organisation entsprechen. In Sentinel 6 unterstützt iTRAC Variablen, Anhänge, Anmerkungen, zeitbasierte und konditionelle Eskalation, verbesserte Verwendung von Arbeitslisten sowie zusätzliche Verwaltungsoptionen.

Neues Framework zur Verwaltung von Ereignisquellen

Sentinel 6 bietet ein komplett neues Framework zur Verwaltung von Ereignisquellen zur Implementierung, Verwaltung und Fehlerbehebung von Ereignis-Sammelstellen von der Sentinel-Konsole aus. Mit diesem Framework können alle Komponenten zum Sammeln von Ereignissen von einer intuitiven, grafischen Oberfläche aus durchgeführt werden, die die ehemaligen Funktionen des Sentinel-Sammelstellen-Editors ersetzt und mehrere neue Funktionen zur Verfügung stellt, die frühere Versionen von Sentinel nicht enthielten. Sammelstellen und Connectors werden nun in einem zentralen Repository im Sentinel-System gespeichert und werden über eine einfache, assistentenbasierte Oberfläche konfiguriert und implementiert. Andere ESM-Funktionen sind beispielsweise ein Sammelstellen-Debugger, die Möglichkeit, Filter als einzelne Datenquelle mit einem einzigen Mausklick zu öffnen, und integrierte Rechtsklick-Aktionen für Analyse- und Verwaltungsaufgaben wie das Anzeigen von Rohdaten oder das Erstellen einer aktiven Sentinel-Ansicht.

Erweiterte Plattform-Unterstützung

Die Plattform-Unterstützung wurde verbessert und beinhaltet nun ausgewählte 64-Bit-Betriebssysteme, SUSE Linux Enterprise Server 10 und Oracle 10 inklusive Oracle Real Application Clusters (RAC). Im Sentinel-Installationshandbuch finden Sie eine vollständige Liste aller unterstützten Plattformen. Die Komponenten Java Virtual Machine und Sonic Message Bus von Sentinel wurden ebenfalls auf die neuesten verfügbaren Versionen aktualisiert, um Leistung und Verlässlichkeit zu verbessern.

Option für SSL-Proxy-Verbindung für Produktkomponenten

Sentinel 6 ermöglicht nun die Kommunikation zwischen Sammelstellen-Managern und dem Sentinel Control Center über den Sentinel-Nachrichtenbus mittels einer SSL-Proxy, so dass Sentinel-Komponenten in ein Remote-Netzwerk platziert werden können, ohne dass die Einstellungen von Router oder Firewall verändert werden müssen.

Offline-Abfrage

Sentinel 6 bietet nun ein Werkzeug zum Abrufen von Daten aus dem Ereignisspeicher bei Verfügbarkeit der Systemressourcen, ohne dass die Leistung des laufenden Sentinel-System oder der Datenbank negativ beeinflusst wird.

Aktiver Browser

Mit dem aktiven Browser von Sentinel 6 können Benutzer Ereignisse schnell und genau durchsuchen, um bestimmte Ereignisse zu identifizieren und Trends festzustellen, ohne SQL-Einträge oder Berichte erstellen zu müssen.

Unterstützung von Datenbank und Benutzeroberfläche für Double-Byte-Zeichen

Die Datenbank und Benutzeroberfläche von Sentinel unterstützen nun die manuelle Eingabe und das Speichern von Double-Byte-Zeichen.

Ereignis-Hashing

Sentinel 6 unterstützt das Speichern und Hashing des ursprünglichen Ereignisses, um Datenintegrität zu gewährleisten.

Verbesserte interne Protokollierung

Für Aktionen im Sentinel-System werden zusätzliche Ereignisse und Details angegeben.

Werkzeuge für Migration und Aktualisierung

Es werden Installationswerkzeuge und Datenbank-Skripts zur Verfügung gestellt, um die Aktualisierung von Sentinel 5 auf Sentinel 6 sowie die Migration von Sentinel 4 auf Sentinel 5 zu erleichtern.

Bekannte Probleme und Einschränkungen

HINWEIS: Diese Version der ReadMe-Datei enthält die bekannten Probleme und Einschränkungen von Sentinel 6 nicht. Diese Informationen finden Sie in der Online-Version der ReadMe-Datei.

Die Hilfedateien für das Sentinel Control Center sind nicht Teil dieser Version. Zur Installation der aktuellen Hilfedateien befolgen Sie diesen Vorgang:

1. Navigation http://www.novell.com/documentation/sentinel6
2. Laden Sie die aktuellen Hilfedateien herunter, die sich in einer .JAR-Datei namens eSentinelHelp.jar befinden.
3. Navigieren Sie zum folgenden Verzeichnis auf dem Rechner mit Sentinel Control Center: $ESEC_HOME/lib oder %ESEC_HOME%\lib
4. Erstellen Sie eine Sicherungskopie der alten Version von „eSentinelHelp.jar“.
5. Kopieren Sie die neue Datei eSentinelHelp.jar in das Verzeichnis.
6. Schließen Sie das Sentinel Control Center und öffnen Sie es erneut.

Probleme bei der Installation

SEN-5895 – Die Sentinel-Installation schlägt fehlt, wenn das Installationsprogramm von einem Verzeichnis aus durchgeführt wird, in dessen Pfad ein Sonderzeichen enthalten ist. Sie können dies umgehen, indem Sie das Installationsverzeichnis in ein Verzeichnis kopieren, in dessen Pfad keine Leerzeichen enthalten sind.

SEN-3394, SEN-5524 – Das Sentinel Control Center und die Deinstallations-Shortcuts funktionieren nicht, wenn Sentinel in ein Verzeichnis kopiert wird, das Nicht-ASCII-Zeichen enthält. Sie umgehen dies für Sentinel Control Center, indem Sie die Anwendung von %ESEC_HOME%\sentinel\console\console.exe oder $ESEC_HOME/sentinel/console/console.exe aus starten. Sie umgehen dies für die Deinstallation, indem Sie den manuellen Vorgang für die Deinstallation im Installationshandbuch befolgen.

SEN-5610 – Bei der Deinstallation der Sentinel-Datenbank auf SLES 10 werden nicht alle Datenbank-Filter entfernt, die während der Installation erstellt wurden (*.DBF, *.CTL, *.LOG). Sie umgehen dies, indem Sie diese Dateien manuell mittels der Anweisungen im Installationshandbuch entfernen..

SEN-6041 – Sentinel kann die Datenbank von Oracle 10 aufgrund von Fehlern in den Skripts dbstart und dbshut von Oracle nicht starten. Die Anweisungen für die Bearbeitung der beiden Skripts für Oracle 10unter Solaris 10 und Red Hat 3 finden Sie im Installationshandbuch. Für SUSE Linux Enterprise Server 10 sind keine Änderungen erforderlich.

SEN-6542 – Nur für Oracle gilt Folgendes: Bei der Installation von DAS und der Sentinel-Datenbank muss die Sprache des Installationsprogramms von der installierten Oracle-Software unterstützt werden. Angenommen, das Sentinel-Installationsprogramm wird zum Installieren von DAS und der Sentinel-Datenbank auf Französisch ausgeführt und die Oracle-Datenbank unterstützt nur Englisch. In diesem Fall werden in der Datei „das_query_*.log“ NLS-Fehler protokolliert.

SEN-6881 – Wenn der Benutzer an der Eingabeaufforderung für den Kommunikationsport bis zur Seite für die Funktionsauswahl auf „Zurück“ klickt und zu installierende Komponenten deaktiviert, fordert das Installationsprogramm möglicherweise weiterhin zur Eingabe von COM-Anschlüssen auf, die nicht erforderlich sind.{166}~{167}~Dieses Problem umgehen Sie, indem Sie die richtigen Anschlüsse angeben, selbst wenn sie von den aktuell für die Installation ausgewählten Komponenten nicht verwendet werden.\~ Wenn später zusätzliche Komponenten installiert werden, werden dann diese Anschlüsse verwendet.

SEN-6882 – Falls bei der Installation des Collector Manager der falsche Hostname oder Port eingegeben wird und der Collector Manager so eingestellt ist, dass die Verbindung mit dem Sentinel-Server über den Proxy erfolgt, kommt es zu Fehlern, wenn Sie die Installation bis zur Eingabeaufforderung "Geben Sie den

Sentinel-Benutzernamen sowie das -Passwort ein, das über Berechtigungen zum Registrieren des vertrauenswürdigen Clients verfügt" fortsetzen. Wenn Sie zurückgehen und den Hostnamen oder den Port im Installationsprogramm bearbeiten, werden die neuen Informationen nicht für die Datei „configuration.xml“ aktualisiert, und die Registrierung des verbürgten Client kann nicht erfolgen. Sie umgehen dies, indem Sie, wenn das Installationsprogramm mit der Eingabeaufforderung zum Registrieren des verbürgten Client auf dem Bildschirm angezeigt wird, den Hostnamen oder die Anschlüsse in der Datei „ESEC_HOME/config/configuration.xml“ manuell bearbeiten. Wenn der Benutzername und das Passwort für den verbürgten Client erneut eingegeben wurden, übernimmt das Installationsprogramm die Änderung für die Datei „configuration.xml“ und setzt den Vorgang entsprechend fort.

SEN-5843 –Beim Installieren eines Collector Manager mit einer Proxy-Verbindung zum Sentinel-System muss der DAS-Proxy neu gestartet werden, damit das neue verbürgte Zertifikat geladen werden und der Collector Manager eine Verbindung herstellen kann. Sie umgehen dies, indem Sie den gesamten Sentinel-Service auf dem Computer, auf dem DAS installiert ist, neu starten oder den DAS-Proxy-Prozess beenden, der dann automatisch neu gestartet wird.

SEN-5843 - Wenn bei der Installation des Collector Manager dessen Verbindung zum Sentinel-Server so eingestellt ist, dass sie über den Proxy erfolgt, konfiguriert das Installationsprogramm alle für die automatische Herstellung der Proxy-Verbindung erforderlichen Einstellungen. \~Der Collector Manager kann jedoch erst dann eine Verbindung mit dem Proxy herstellen, wenn der DAS-Proxy-Prozess neu gestartet wurde, sodass das neue verbürgte Zertifikat geladen werden kann. Sie umgehen dies, indem Sie entweder den gesamten Sentinel-Service, unter dem der DAS-Proxy ausgeführt wird, neu starten oder den DAS-Proxy-Prozess beenden (der automatisch vom Watchdog des Sentinel-Services neu gestartet wird).

SEN-6884 – Wenn ein Collector Manager mit einer Proxy-Verbindung installiert wird und für das Installationsprogramm der GUI-Modus aktiviert ist, werden dem Benutzer drei Optionen für die Verbürgungsregistrierung mit dem DAS-Proxy angeboten. Der Benutzer muss „Immer akzeptieren“ (nicht „Akzeptieren“) auswählen, damit der Collector Manager ordnungsgemäß ausgeführt wird.

SEN-6885 – Nur für Windows gilt Folgendes: Falls die Windows-Authentifizierung für den Sentinel-Anwendungsbenutzer (esecapp) verwendet wird und die Datenbank und andere Nicht-DAS-Prozesse installiert sind, wird der Sentinel-Service als Windows-Authentifizierungsbenutzer installiert, jedoch ohne das erforderliche Passwort. Deshalb wird der Service nicht gestartet. Sie umgehen dies, indem Sie für den Service die Ausführung unter dem Konto „Lokales System“ mithilfe des Windows-Dienst-Managers festlegen. Der Service muss nicht als Sentinel-Anwendungsbenutzer (esecapp) ausgeführt werden, falls DAS nicht ausgeführt wird.

SEN-6886 – Nur für Windows gilt Folgendes: Falls die DAS-Komponente zu einem Computer hinzugefügt wird, auf dem bereits andere Sentinel-Serverkomponenten installiert sind, und falls der Sentinel-Anwendungsbenutzer (esecapp) die Windows-Authentifizierung verwendet, ist nach Abschluss der DAS-Installation für den Sentinel-Service weiterhin fälschlicherweise die Ausführung unter dem Konto „Lokales System“ festgelegt. Sie umgehen dies, indem Sie für den Sentinel-Service manuell die Ausführung als Sentinel-Anwendungsbenutzer mithilfe des Windows-Dienst-Managers festlegen.

Weitere Probleme

DAT-160 – Nur für SQL Server 2005 gilt, dass das Importieren von Übersichtstabellenpartitionen mit dem Eintrag „Ungültiger Objektname“ in der Datei „sdm.log“ nicht erfolgt.

DAT-216 – Nur für SQL Server 2005 gilt, dass das Einfügen von Übersichtstabellen nicht erfolgt, wenn P_MAX die aktuelle Online-Partition ist. Sie umgehen dies, indem Sie sicherstellen, dass immer zukünftige Partitionen verfügbar sind, sodass niemals in P_MAX geschrieben wird.

DAT-284 – Nur für Oracle gilt Folgendes: Partitionsverwaltungsaufträge (z. B. das Hinzufügen von Partitionen oder das Offlineschalten von Partitionen) können nicht erfolgen, wenn mehrere Aufträge gleichzeitig ausgeführt werden oder wenn ein Partitionsverwaltungsauftrag und die Aktualisierung der Partitionsliste in der Benutzeroberfläche des Sentinel Data Manager gleichzeitig ausgeführt werden. Sie umgehen dies, indem Sie Partitionsverwaltungsaufträge so planen, dass Überschneidungen sowie

die Verwendung des SDM während der Ausführung von Partitionsverwaltungsaufträgen vermieden werden.

DAT-294 – Nur für SQL Server 2005 gilt Folgendes: Wenn Partitionen archiviert werden und der Benutzer dann versucht, diese Partitionen zu archivieren und abzulegen, erfolgt der Auftrag nicht und es wird ein Fehler wegen einer Primärschlüsselverletzung generiert.

SEN-3515 – Die Benutzer können iTRAC-Prozesse beenden, selbst wenn ihnen die entsprechende Berechtigung nicht erteilt wurde.

SEN-3897 – Der Server View Manager zeigt Prozesse, die nicht auf einem bestimmten Computer installiert sind, mit dem Status NOT_INITIALIZED an. Beispielsweise zeigt Sentinel unter Windows den Prozess „UNIX Communication Server“ als NOT_INITIALIZED an und Sentinel unter UNIX zeigt den Prozess „Windows Communication Server“ als NOT_INITIALIZED an. Prozesse, die mit dem Status NOT_INITIALIZED angezeigt werden, sollten ignoriert werden.

SEN-4066 – Benutzer , die nur die Berechtigungen zum Anzeigen des Status für die Verwaltung von Ereignisquellen haben, können Knoten starten und beenden, falls mehrere Knoten gleichzeitig ausgewählt sind.

SEN-4617 Nur für UNIX gilt, dass nur der Sentinel-Administrator (esecadm) das Sentinel Control Center ausführen kann. Wenn andere Benutzer in der Lage sein sollen, das Sentinel Control Center auszuführen, finden Sie Informationen hierzu in der Knowledgebase mit den TIDs (Technical Information Documents; Dokumente für Technische Informationen) auf der Novell Technical Service-Website .

SEN-5284 – Wenn ein Ereignisquellen-, Connector- oder Collector-Knoten auf „Ausführen“ festgelegt ist, indem die Konfiguration des Knotens bearbeitet und auf „OK“ geklickt wird, werden die übergeordneten Knoten nicht entsprechend auf „Ausführen“ aktualisiert. Wenn deshalb zwar eine Ereignisquelle, aber nicht deren Collector auf „Ausführen“ festgelegt ist, werden die Ereignisse nicht vom System verarbeitet. Sie umgehen dies, indem Sie mit der rechten Maustaste auf den Knoten klicken und dann auf „Starten“ klicken. Dieser Bug betrifft auch das System, wenn die Einstellung „Ausführen“ eines Knotens deaktiviert ist. In diesem Fall werden die untergeordneten Knoten nicht aktualisiert, sodass sie ebenfalls nicht ausgeführt werden. Sie umgehen dies, indem Sie mit der rechten Maustaste auf den Knoten klicken und „Stoppen“ auswählen.

SEN-5524 – Wenn unter Windows die Sentinel-Komponenten in ein Verzeichnis kopiert werden, das Nicht-ASCII-Zeichen enthält, funktionieren das Sentinel Control Center und die Sentinel-Deinstallations -Shortcuts nicht. Für das Sentinel Control Center umgehen Sie dies, indem Sie die Datei „%ESEC_HOME%\bin\control_center.bat“ ausführen. Für die Sentinel-Deinstallation umgehen Sie dies, indem Sie die Schritte für die manuelle Deinstallation, die im Sentinel-Installationshandbuch beschrieben sind, ausführen.

SEN-5931 – Weist ein Collector im Debugger-Modus den Stopp-Status auf, sind die Schaltflächen „Einzelschritt“, „Pause“ und „Stoppen“ zwar weiterhin aktiviert, haben jedoch keinerlei Auswirkung. Sie umgehen dies, indem Sie den Debugger schließen und erneut öffnen.

SEN-6182 – Wenn ein ausgeführtes Collector-Skript den Stopp-Status aufweist, werden die untergeordneten Knoten des Collectors nicht gestoppt. Deshalb wird zwar der C ollector gestoppt, aber dessen Connectors und Ereignisquellen werden in der Live-Ansicht der Verwaltung von Ereignisquellen weiterhin ausgeführt. Es werden keine Prozesse verarbeitet. Sie umgehen dies, indem Sie mit der rechten Maustaste auf den Collector klicken und ihn manuell stoppen.

SEN-6198 – Bei Collectors ohne eine Ereignisquelle (z. B. ODBC-Collectors) kann „Verbürgte Ereignisquelle Uhrzeit“ nicht in der grafischen Benutzeroberfläche der Verwaltung von Ereignisquellen festgelegt werden. Sie umgehen dies, indem Sie die Datei „package.xml“ für den Collector bearbeiten und das Element <DefaultTrustEventSourceTime>1</DefaultTrustEventSourceTime> unter dem Element „CollectorPackage“ hinzufügen.

SEN-6397 – Wenn Sie im Correlation Action Manager in einer Aktion zum Senden von Email „Formatierungsname“ auf „xml“ festlegen, wird der Nachrichtentext der Email im Namenswertpaarformat gesendet.

SEN-6398 – Wenn die Aktion zum Senden von Email für eine Korrelationsregel ausgelöst wird, ist die Email-Anlage leer.

SEN-6429 – Wenn Sie im Funktionsmanager auf der Registerkarte „Admin“ zwei Funktionsnamen erstellen, die sich nur bezüglich der Groß-/Kleinschreibung unterscheiden (z. B. „Admin“ und „admin“), haben Hinzufüge- und Löschvorgänge für die eine Funtkion auch Auswirkungen auf die andere Funktion. Sie umgehen dies, indem Sie sicherstellen, dass sich alle Funktionsnamen nicht nur bezüglich der Groß-/Kleinschreibung unterscheiden.

SEN-6473 – Wenn Sie in der Live-Ansicht der Verwaltung von Ereignisquellen eine Filterbedingungzu einem Knoten in Rohdaten hinzufügen und dann zum Speichern der neuen Filterbedingung auf die Schaltfläche „OK“ klicken, wird der Status des Knotens auf den Status vor dem Öffnen der Rohdaten zurückgesetzt.

SEN-6532 – Die Benutzer können Skripts nur mit der Berechtigung „Zwischenspeicher anzeigen“ in das Plugin-Repository importieren.

SEN-6573 – Wenn alle Attribute in der Attributliste als „Gruppieren nach“-Felder in einer Gesamt-, Aggregat- oder Sequenzregel ausgewählt sind, wird die Meldung „invalid RuleLg“ angezeigt.

SEN-6591 – Wenn Sie Änderungs- oder Löschvorgänge für eine untergeordnete Regel ausführen, während eine Gesamtregel erstellt wird, und wenn Sie auf die Schaltfläche „Abbrechen“ klicken, werden die Änderungs- oder Löschvorgänge nicht rückgängig gemacht.

SEN-6608 – Zuordnungen, die zum Ordner „Maps“ auf der obersten Ebene in der grafischen Benutzeroberfläche des Zuordnungsservice hinzugefügt werden, werden erst nach der Aktualisierung angezeigt. Sie umgehen dies, indem Sie neue Zuordnungen in einem Unterordner erstellen.

SEN-6629 – Wenn die Parameter eines Collector-Skript-Plugins geändert werden und diese Änderungen in Sentinel importiert werden, werden die Parameter für bereitgestellte Collectors, die dieses Plugin verwenden, nicht sofort aktualisiert. Deshalb funktioniert der Collector nicht ordnungsgemäß, wenn der Collector neu gestartet wird (weshalb der Collector das aktualisierte Collector-Skript verwendet). Sie umgehen dies, indem Sie den Collector zum Bearbeiten öffnen und dann zum Speichern auf „OK“ klicken.

SEN-6701 – Das Verschieben oder Klonen eines Knotens, der sich auf einen Ereignisquellenserver bezieht, direkt oder über einen über- bzw. untergeordneten Knoten, erfolgt nicht. Sie umgehen dies, indem Sie den Knoten exportieren und danach importieren.

SEN-6703 – Nachdem Sie mit dem Dialogfeld für die Connector-Bearbeitung den Ereignisquellenserver, dem ein Connector zugeordnet ist, geändert haben, werden in der grafischen Benutzeroberfläche zur Verwaltung von Ereignisquellen untergeordnete Ereignisquellen dieses Connectors angezeigt, die sowohl mit dem vorherigen als auch dem neuen Ereignisquellenserver verbunden sind. Der Status einiger Knoten wird von „Ein“ auf „Aus“ geändert. Sie umgehen dies, indem Sie auf die Schaltfläche „Aktualisieren“ klicken und die Ereignisquelle neu starten.

SEN-6732 – Die Schaltfläche „Hilfe“ funktioniert im Assistenten „Mit Ereignisquelle verbinden“ nicht. Sie umgehen dies, indem Sie in einem der anderen Dialogfelder (z. B. Assistent zum Hinzufügen eines Collector oder Dialogfeld „Collector bearbeiten“) auf die Schaltfläche „Hilfe“ klicken.

SEN-6747 – Beim Importieren von Collectors aus 511_SP2_06_GA wird der Bildschirm „Collector-Details“ nicht angezeigt und ein ClassCastException-Fehler wird in der Datei „control_center0.0.log“ protokolliert. Sie umgehen dies, indem Sie die Datei „package.xml“ aus dem Collector-Paket entfernen und den Importvorgang wiederholen.

SEN-6779 – Die Syntaxprüfung für Korrelationsregeln hindert Benutzer nicht am Erstellen einer Sequenzregel ohne untergeordnete Regeln.

SEN-6783 – Das Erstellen eines Windows-Authentifizierungsbenutzers im Sentinel Control Center erfolgt nicht, wenn der Benutzer bereits in der SQL Server 2005-Liste mit den Benutzeranmeldungen vorhanden ist.

SEN-6784 – Bereitgestellte Korrelationsregeln können standardmäßig nicht bearbeitet werden. „Correlation RuleLG“ kann nicht ausgewählt oder kopiert werden. Die Fehlermeldung „Bereitgestellte Regel kann nicht bearbeitet werden“ wird angezeigt.

SEN-6800 – Korrelationsregeln, die einen Inlist-Operator enthalten, der auf eine dynamische Liste verweist, sind nach dem Import in Sentinel nicht funktionsfähig. Sie umgehen dies, indem Sie Korrelationsregeln mit „inlist“ neu erstellen, anstatt sie zu importieren.

SEN-6818 – Das Kontrollkästchen „Fehler“ in „Attributfilter“ zeigt Knoten mit einem Fehlerstatus nicht ordnungsgemäß an..

SEN-6821 – Mit dem Befehl „UpdateMapdata“ in der Befehlszeilenschnittstelle des Sentinel Data Manager werden die Zuordnungen nicht aktualisiert. Sie umgehen dies, indem Sie Zuordnungen über” Sentinel Control Center->Admin->Zuordnungskonfiguration” aktualisieren.

SEN-6698 – Der Operator „e.all“ wird von der Korrelationsregelsprache nicht unterstützt. Regeln, die aus früheren Sentinel-Versionen importiert wurden und „e.all“ verwenden, funktionieren nicht.

SEN-6895 – Nur für Windows gilt Folgendes: Wenn eine andere als eine Unicode-Datenbank bei der Installation ausgewählt wird, werden in der grafischen Benutzeroberfläche keine lateinischen Zeichen erzwungen.

SEN-6896 – Für die meisten Schaltflächen gibt es keine mnemonischen Zeichen (Hotkeys).

WIZ-1839 – Mit dem Befehl ALERT in der Collector-Skriptsprache werden die Felder ConnectorID (RV23), EventSourceID (RV24) und TrustDeviceTime nicht automatisch gesendet. Sie umgehen dies, indem Sie diese Felder an die Warnungsmeldung in Collectors anfügen, die den Befehl ALERT verwenden, oder Collectors aktualisieren, sodass der Befehl EVENT verwendet wird. Codebeispiele finden Sie im Sentinel-Referenzhandbuch.

Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder Eignung für einen bestimmten Zweck aus.

Novell, Inc. behält sich das Recht vor, dieses Dokument jederzeit teilweise oder vollständig zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen davon in Kenntnis zu setzen.

Novell, Inc. gibt ebenfalls keine Erklärungen oder Garantien in Bezug auf Novell-Software und schließt insbesondere jegliche ausdrückliche oder stillschweigende Garantie für handelsübliche Qualität oder Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software jederzeit ganz oder teilweise zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie stimmen zu, alle Gesetze zur Exportkontrolle einzuhalten, und alle für den Export, Reexport oder Import von Lieferungen erforderlichen Lizenzen oder Klassifikationen zu erwerben. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen genannte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden.

Weitere Informationen zum Export von Novell-Software finden Sie im Internet unter www.novell.com/info/exports/. Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt gewerbliche Schutzrechte für die Technologie, die in dem in diesem Dokument beschriebenen Produkt integriert ist. Insbesondere, jedoch nicht beschränkt auf, können diese gewerblichen Schutzrechte eines oder mehrere der unter http://www.novell.com/company/legal/patents/ aufgeführten US-Patente und eines oder mehrere Patente oder zum Patent angemeldete Anwendungen in den USA und in anderen Ländern beinhalten.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

USA.

www.novell.com

Novell-Marken

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

Materialien von Drittanbietern

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

Rechtliche Hinweise zu Drittanbietern

Dieses Produktkann die folgenden Open Source-Programme beinhalten, die im Rahmen der LGPL-Lizenz verfügbar sind. Den Wortlaut dieser Lizenz finden Sie im Verzeichnis „Licenses“.

- edtFTPj-1.2.3 ist lizenziert unter: Lesser GNU Public License. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Esper. Copyright © 2005–2006, Codehaus.
- jTDS-1.2.jar 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.
- Enhydra Shark, lizenziert unter der Lesser General Public License, verfügbar unter: http://shark.objectweb.org/license.html.
- Tagish 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.

Dieses Produkt kann Software beinhalten, die von der Apache Software Foundation (http://www.apache.org/) unter der Apache-Lizenz, Version 2.0 (die „Lizenz“), entwickelt und lizenziert wurde; den Wortlaut dieser Lizenz finden Sie im Verzeichnis „Licenses“ oder unter http://www.apache.org/licenses/LICENSE-2.0. Die Software wird unter dieser LizenzWIE BESEHEN weitergegeben, OHNE AUSDRÜCKLICHE ODER IMPLIZITE GEWÄHRLEISTUNGEN ODER KONDITIONEN. Die Lizenz für die jeweilige Sprache bestimmt die Rechte und Einschränkungen unter dieser Lizenz.

Die betreffenden Open Source-Programme sind im Folgenden aufgeführt.

- 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/
- Apache Lucene, Copyright © 1999–2005, Apache Software Foundation. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.apache.org/licenses/
- 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/.
- 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.

Dieses Produkt kann die folgenden Open Source-Programme beinhalten, die im Rahmen der Java-Lizenz verfügbar sind.

- 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“.
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html
- 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“.

Dieses Produkt kann auch die folgenden Open Source-Programme beinhalten.

- ANTLR. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.antlr.org
- Boost. Copyright © 1999, Boost.org.
- Concurrent, Dienstprogrammpaket. Copyright © Doug Lea. Wird ohne die Klassen CopyOnWriteArrayList und ConcurrentReaderHashMap verwendet
- Java Ace, von Douglas C. Schmidt und seinem Forschungsteam an der Washington 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
- JLDAP. Copyright 1998–2005 The OpenLDAP Foundation. Alle Rechte vorbehalten. Es gelten folgende Copyright-Informationen: © 1999–2003 Novell, Inc. Alle Rechte vorbehalten.
- OpenSSL, durch das OpenSSL-Projekt. Copyright © 1998–2004. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://www.openssl.org.
- Tao (mit ACE-Wrappern) von Douglas C. Schmidt und seinem Forschungsteam 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
- Tinyxml. Weitere Informationen, Haftungsausschlüsse und Beschränkungen finden Sie unter http://grinninglizard.com/tinyxmldocs/index.html.
- Java Service Wrapper. Es gelten folgende Copyright-Informationen: 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.