Novell

Software for the Open Enterprise™

Versionshinweise zum Produkt

Sentinel™ 5.1.3 mit iTRAC™

HINWEIS: Wechseln Sie zum Herunterladen von Versionshinweisen in Deutsch, Französisch, Italienisch, Spanisch oder brasilianischem Portugiesisch zu http://www.novell.com/documentation/sentinel5.

Beschreibung

Dies ist eine Vollversion von Sentinel 5.1.3release mit iTRAC.

Diese Version unterstützt folgende Installationstypen:

- Vollständige Neuinstallation von Sentinel 5.1.3 unter Windows, Solaris und Linux (Novell SUSE Linux Enterprise Server 9 und Redhat).
- Datenmigrationsaufrüstung von Sentinel 4.2.x auf Sentinel 5.1.3 unter Windows und Solaris.
- Installation weiterer Komponenten von Sentinel 5.1.3 in eine bestehende Sentinel 5.1.3-Installation unter Windows, Solaris und Linux.

HINWEIS: Wenn Sie eine Sentinel 5-Installation verwenden, die älter ist als Version 5.1.3 und die Installation mithilfe eines Patch auf Version 5.1.3 aufrüsten möchten, müssen Sie dazu ein Sentinel 5.1.3-Patch-Installationsprogramm verwenden. Das Sentinel 5.1.3-Installationsprogramm, das zu diesen Versionshinweisen gehört ist kein Patch-Installationsprogramm. Um ein Sentinel 5.1.3-Patch-Installationsprogramm anzufordern, wenden Sie sich bitte an den technischen Support.

Betriebssysteme und Patches

Die unterstützten Betriebssysteme und Datenbanken für die lokalisierten Versionen von Sentinel 5.1.3. sind nachfolgend aufgeführt. Informationen zur englischen Version befinden sich im Installationshandbuch.

- **Server-Betriebssysteme:**
  - SLES 9 SP3 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)
  - Solaris 9 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)
  - MS Windows 2003 Server SP1 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)
  - MS Windows 2000 Server SP4 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)

- **Client-Betriebssysteme:**
  - MS Windows 2000 Professional SP4 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)
  - MS Windows XP Professional SP2 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)
  - Solaris 9 (Deutsch, Französisch, Italienisch, Spanisch, brasilianisches Portugiesisch)

- **Datenbank:**
  - Oracle 9.2.0.7 (nur Englisch)
  - MS SQL 2000 SP3a (nur Englisch)

Installation

Anweisungen zur Installation dieser Version finden Sie im Sentinel-Installationshandbuch für Sentinel 5.1.3.

Um eine Neuinstallation von Sentinel durchzuführen, befolgen Sie die Anweisungen in dem entsprechenden Kapitel für Ihre Plattform:

- Kapitel 3, Installation von Sentinel 5 für Oracle unter Solaris
- Kapitel 4, Installation von Sentinel 5 für Oracle unter Linux
- Kapitel 5, Installation von Sentinel 5 für MS SQL

Das Folgende ist als Teil der Vorinstallation von Oracle unter Linux zu betrachten. Diese Änderung bezieht sich auf Oracle Doc ID: HINWEIS:293988.1.

- Fügen Sie unter SUSE Linux Enterprise Server 9 SP2 die folgende Kernel-Parametereinstellung zur Datei „/etc/sysctl.conf“ hinzu:
  ```
  # Oracle requires MLOCK privilege for hugetlb memory.
  vm.disable_cap_mlock=1
  ```
- Führen Sie den folgenden Befehl aus, damit die Änderungen in der Datei „/etc/sysctl.conf“ geladen werden:
  ```
  sysctl -p
  ```

Um eine Datenmigrationsaufrüstung von einer bestehenden Sentinel 4.2.x-Installation auf Sentinel 5.1.3 vorzunehmen, befolgen Sie die Anweisungen in dem entsprechenden Kapitel für Ihre Plattform:

- Kapitel 6, Datenmigration und Patch für Oracle unter Solaris
- Kapitel 7, Datenmigration und Patch für MS SQL

Um weitere Komponenten von Sentinel 5.1.3 in eine bestehende Sentinel 5.1.3-Installation zu installieren, befolgen Sie die Anweisungen in folgendem Kapitel:

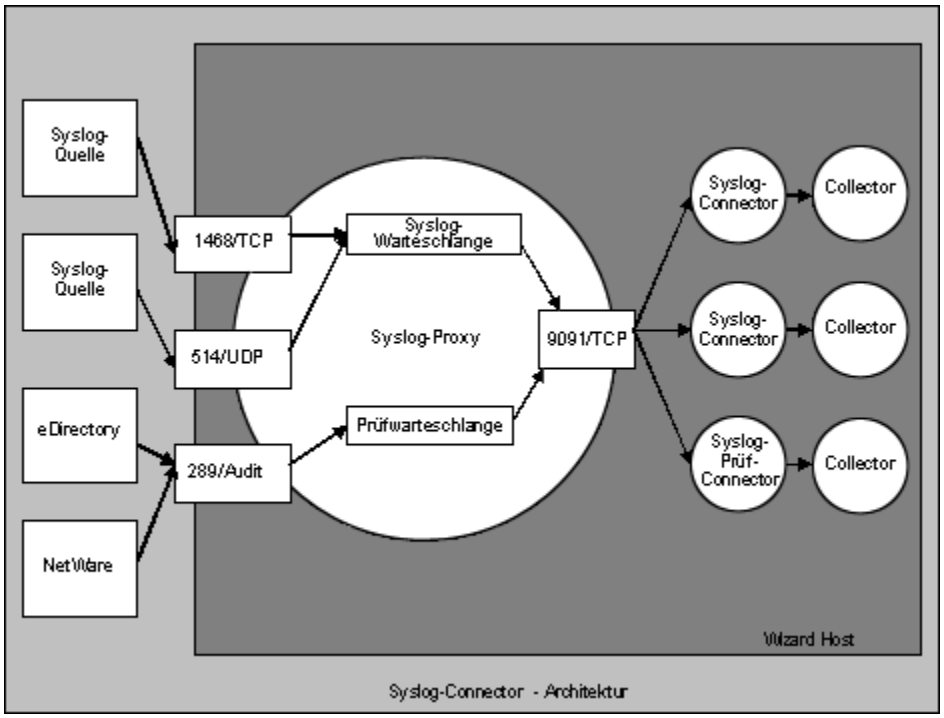
- Kapitel 14, Hinzufügen von Komponenten zu einer bestehenden Installation

Um weitere Komponenten von Sentinel 5.1.3 in eine bestehende Installation einer früheren Version von Sentinel 5 zu installieren, müssen Sie zunächst die Sentinel-Installation mithilfe des entsprechenden Patch-Installationsprogramms auf 5.1.3 aufrüsten und dann die Anweisungen im oben angegebenen Kapitel befolgen.

Neue Funktionen

- Neu in dieser Version ist die Unterstützung für mehrere Sprachen, darunter brasilianisches Portugiesisch, Französisch, Italienisch, Deutsch, Spanisch und Englisch in der Sentinel-Steuerungskonsole und in Sentinel Data Manager.
- Der Syslog-Connector wurde erweitert und kann nun mit NAudit-instrumentierten Anwendungen umgehen. Die Erweiterung ist mit einem Agenten gekoppelt, der NAudit-Daten im Allgemeinen und insbesondere für folgende Anwendungen verarbeitet: eDirectory, Netware, Identity Manager, Secure Login und Access Manager. Andere Erweiterungen sind:

o Filtern des Rumpfteils von Syslog-Meldungen mithilfe regulärer Ausdrücke.
o Automatische Neuverbindung zwischen Collector-Connector und Syslog-Server.
o Datenfluss-Steuerung für TCP-Verbindungen – verhindert Datenverlust durch vollen Meldungspuffer. Dies gilt sowohl für Syslog TCP- als auch für NAudit-Verbindungen.

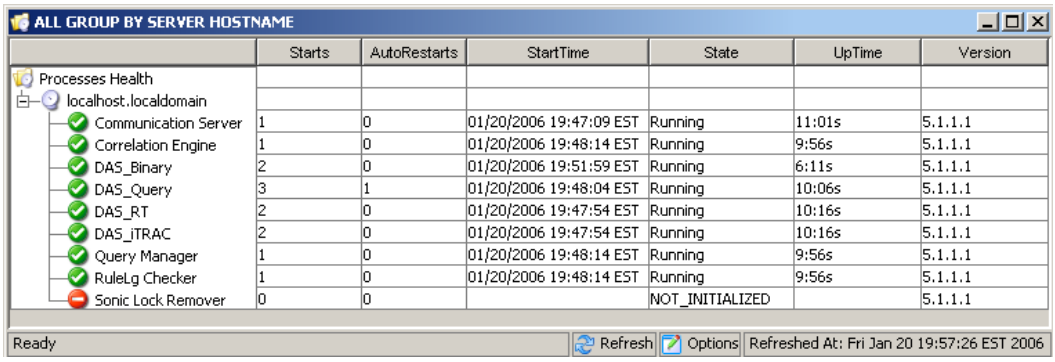


- Der Syslog-Connector wird nun mit Skripts installiert, die unter Windows und UNIX ausgeführt werden, sowie mit verbesserten Konfigurationsdateien. Außerdem wurde die Installation des Syslog-Proxyservers als Service vereinfacht. Führen Sie folgende Befehle aus, um den Syslog-Proxyserver als Service mit der Standardkonfiguration auszuführen:

▫ Unter Windows:
1. Melden Sie sich als Administrator an.
2. Wechseln Sie in das Verzeichnis /d %ESEC_HOME%\wizard\syslog
3. .\syslog-server.bat install

▫ Unter UNIX:
4. Melden Sie sich als „root“ an.
5. Wechseln Sie in das Verzeichnis $ESEC_HOME/wizard/syslog
6. ./syslog-server.sh install

- Die neuen Agentenskript-Befehle „encodemime“ und „decodemime“ ermöglichen Base-64-Ver- und -Entschlüsselung.
- CV30–CV34 werden von 255 Zeichen auf eine Obergrenze von 4000 Zeichen erweitert.
- Diese Version unterstützt erstmals die direkte Installation der Sentinel-Datenbank auf einem MS SQL 2005-Datenbankserver.
- Sentinel Control Center weist nun auf der Registerkarte „Admin“ den neuen Bildschirm „Serveransichten“ auf. Dieser Bildschirm bietet folgende Funktionen:
  - Er zeigt den Status aller Sentinel Server-Prozesse im System an (Berechtigung „Administration->Serveransichten->Server anzeigen+++“ erforderlich). Dies ähnelt der bestehenden Collector-Ansicht, nur dass Sentinel Server-Prozesse angezeigt werden.
  - Sie können damit Prozesse starten, stoppen und neu starten (dazu ist die Anzeige erforderlich sowie die Berechtigung „Administration->Serveansichten->Server steuern“).



- Die Passwort-Eingabeaufforderungen für die folgenden Wizard-Prozess-Connectors wurden verbessert, um zu versuchen, das Psswort bei der Eingabe in der Befehlszeile zu maskieren:
  - dbconnector
  - rdep_client
- Die Komponente, die die zur Exploit-Erkennung dienende Datei attackNomarlization.csv generiert, wurde so bearbeitet, dass sie weniger Arbeitsspeicher beansprucht. Dies ermöglicht eine bessere Leistung auf Demonstrationshardware.
- Weitere Konfigurationsoptionen für Prozesse in der Datei configuration.xml:
  - name [Standard: „Uknown“] – Der Name des Prozesses. Dies ist der von Ihnen gewählte Name für den Prozess, der in Protokolldateien und in der Serveransicht in Sentinel Control Center als Prozessname angezeigt wird.
  - auto_restart_threshold [Standard: „5,10“] – Das Format für diesen Wert lautet „<Anzahl Neustarts>,<Anzahl Minuten>“. Wenn die Anzahl der automatischen Neustarts des Prozesses (z. B. auf weil ein Prozess von selbst endet oder über einen Betriebssystembefehl zwangsweise beendet wird) den angegebenen Neustartwert für den angegebenen Zeitraum überschreitet, wird er nicht mehr automatisch neu gestartet. Damit soll verhindert werden, dass ein Prozess ständig neu gestartet wird, wenn vermutlich ein Konfigurationsfehler vorliegt. Wenn dieser Fall eintritt wird das interne Ereignis „ProcessAutoRestartError“ gesendet.
  - depends [Standard: <keine Abhängigkeiten>] – Das Format des Werts ist eine kommagetrennte Liste mit Prozessnamen, wie durch das neue Prozessattribut „name“ angegeben. Bei den in der Liste angegebenen Prozessen handelt es sich um Prozesse, die ausgeführt werden müssen, bevor dieser Prozess erfolgreich ausgeführt warden kann.

- type [Standard: „normal“] – Die gültigen Werte sind entweder „normal“ oder „container“. Der Wert „container“ gibt an, dass es sich bei dem Prozess um einen eSecurity Container-Prozess handelt (d. h. um einen Prozess, der über eine Container-xml-Datei gestartet wird) und dass der Prozess problemlos heruntergefahren werden kann, indem dem Container eine entsprechende Nachricht gesendet wird. Der Wert „normal“ gibt alle anderen Prozesse an.
- Die Funktionen der folgenden Prozesse wurden in Java neu geschrieben, um eine bessere Funktionsweise zu erreichen oder die Komplexität zu verringern:
  - watchdog
  - data_synchronizer (nun Teil von DAS).
- Die Funktion Sentinel-Basisservices, die früher für eine separate Installation zur Verfügung stand wurde in die DAS-Installationsfunktion integriert. Die Prozesse, die früher aktiviert wurden, wenn die Sentinel-Basisservices für die Installation ausgewählt wurden, werden nun aktiviert, wenn DAS zur Installation ausgewählt wird. Diese Änderung wurde vorgenommen, um die Komplexität des Installationsprogramms zu verringern. Die frühere Möglichkeit zur separaten Installation dieser Funktion brachte keine bekannten Vorteile mit sich.
- Die Lizenzüberprüfung wurde erweitert: Nun wird auch der vom Benutzer angegebene Lizenzschlüssel anhand aller verfügbaren Netzwerkschnittstellenkarten (NICs) überprüft. Wenn eine der NICs die richtige MAC-Adresse aufweist, ist die Lizenzüberprüfung erfolgreich.

Fehlerkorrekturen

Sentinel

7424

Problem: Bei der exploitDetection.csv-Generierung fehlen einige Daten.

Korrektur: Generator für Exploit-Erkennung wurde so verändert, dass die fehlenden Daten zur Datei exploitDetection.csv hinzugefügt werden.

7460

Problem: Wenn der Kommunikationsserver unter UNIX alleine installiert war, ließ er sich nicht automatisch starten. Dies lag daran, dass das Installationsprogramm die Komponente „watchdog“ nicht installierte, die für das starten des Kommunikationsservers unter UNIX zuständig ist.

Korrektur: DerKommunikationsserver wurde im Installationsprogramm unter „Sentinel Services“ verschoben, wodurch sichergestellt wird, dass auch „watchdog“ installiert wird.

7463

Problem: Der Generator für die Exploit-Erkennung startet eine zweite erneute Generierung, selbst wenn gerade eine verarbeitet wird, was zusätzliche CPU-Auslastung bei DAS Query verursacht.

Korrektur: Der Generator für die Exploit-Erkennung verarbeitet jeweils nur eine einzige erneute Generierung.

SEN-2819

Problem: SDM % zeigt beim Hinzufügen von Partitionen nicht den Verlauf an, sondern bleibt immer bei 0 %.

Korrektur: Der Prozentwert erhöht sich ständig gemäß dem Ausführungsstand der SDM-Aktivität.

SEN-3684

Problem: Der Argumenttyp unter „Befehlsaktivität bei Vorfall“ funktioniert nicht.

Korrektur: Jetzt funktionieren alle Parameter („Keine“, „Vorfallsausgabe“ und „Benutzerdefiniert“) als Argumenttyp..

SEN-3713

Problem: Die Exploit-Erkennung erkennt nur einen einzigen Angriff für jede Anfälligkeit.

Korrektur: Die Exploit-Erkennung erkennt nun alle Angriffe, die mit einer Anfälligkeit im Advisor-Feed verknüpft sind als Exploit der betreffenden Anfälligkeit, sofern die Anfälligkeit auf dem angegriffenen Computer gemeldet wurde.

SEN-3732

Problem: Der Zustand „Rejected“ (Zurückgewiesen) kann nicht mehr in der Vorfallsverwaltung der Sentinel-GUI ausgewählt werden.

Korrektur: Der Status „Rejected“ (Zurückgewiesen) wird in den Vorfallsverwaltung der Sentinel-GUI aufgenommen.

SEN-3760

Problem: Problem bei der Weiterleitung von Parametern mit Leerzeichen bei der Ausführung von Skripts über Kontextmenü oder Korrelationsregeln.

Korrektur: Die Ausführung der Befehle von Kontextmenü und Korrelationsregeln wurde so korrigiert, dass Leerzeichen in Parametern ordnungsgemäß verarbeitet werden können.

SEN-3763

Problem: Die Exploit-Erkennung funktioniert manchmal nicht, da für jeden Device Attack Name mehrere normalisierte Angriffs-IDs vorhanden sind.

Korrektur: Die Exploit-Erkennung erkennt nun alle Angriffe, die mit einer Anfälligkeit im Advisor-Feed verknüpft sind, als Exploit der betreffenden Anfälligkeit, sofern die Anfälligkeit auf dem angegriffenen Computer gemeldet wurde.

SEN-3764

Problem: Begrenzung der Häufigkeit, mit der die Daten für die Exploit-Erkennung neu generiert werden

Korrektur: Die erneute Generierung ist nun standardmäßig auf einmal alle 30 Minuten begrenzt. Dieser Wert kann durch Bearbeitung der Datei das_query.xml konfiguriert werden.

SEN-3766

Problem: Wenn der Aufruf von DAS RT zum Abrufen der Benutzereinstellungen scheitert, werden alle permanenten Filter entfernt

Korrektur: Die Fehlerbehandlung wurde so verbessert, dass nicht alle permanenten Filter entfernt werden, wenn ein Fehler beim Abrufen der Benutzereinstellungen auftritt.

SEN-3775 (Erweiterung)

Problem: Verarbeiten von Ereignistransformationen mit zyklischen Abhängigkeiten für den Zuordnungsservice.

Korrektur: Der Zuordnungsservice versucht, die Verarbeitung von Ereignistransformationen fortzusetzen, auch wenn eine zyklische Abhängigkeit vorliegt. Die zyklische Abhängigkeit muss weiterhin vom Benutzer korrigiert werden, doch durch diese Erweiterung kann das System so gut wie möglich weiterarbeiten, selbst wenn ein Problem mit einer zyklischen Abhängigkeit besteht.

SEN-3779

Problem: DAS JDBCLoadStrategy fügt die Ereignisfelder RV37, RV38 und RV47-RV48 nicht in die Datenbank ein.

Korrektur: JDBCLoadStrategy wurde so korrigiert, dass die fehlenden Ereignisfelder eingefügt werden.

SEN-3781

Problem: Advisor kann keine Verbindung zum Server über einen Proxy herstellen.

Korrektur: Der Advisor-Client wurde so korrigiert, dass nun eine Verbindung mit dem Server mittels eines Proxy über https möglich ist.

SEN-3785

Problem: Anzeige eines SummaryUpdateFailure-Ereignisses in SCC

Korrektur: Der Fehler, der dieses Ereignis versursachte, wurde behoben.

SEN-3788

Problem: Die Regelsprache für die Korrelationsregeln „in“ und „not in“ funktioniert nicht ordnungsgemäß.

Korrektur: Die betreffenden Aspekte der Regelsprache wurden geändert.

SEN-3792

Problem: Wenn die Auslösung einer Korrelationsregel dazu führt, dass ein Befehl ausgeführt wird, und der Parameter für den Befehl „%all%“ lautet, ist das 26. Argument, das an den Befehl weitergeleitet wird, der in der Korrelationsregel festgelegt Ereignisname (mit dem 13. Argument identisch) und nicht der Ereignisname aus dem Ereignis, das tatsächlich die Regel ausgelöst hat.

Korrektur: Das 13. Argument ist nun der Ereignisname aus der Korrelationsregel und das 26. Argument ist der Ereignisname des ersten Ereignisses (das für das Auslösen des korrelierten Ereignisse verantwortlich war).

SEN-3793

Problem: Im Abschnitt „Ausgewählte Ereignisse“ des Fensters „Anfälligkeitsergebnisse“ werden keine Ereignisse angezeigt.

Korrektur: Die ausgewählten Ereignisse werden nun unter „Anfälligkeitsergebnisse“ sowie im Diagramm Ereignis/Anfälligkeit angezeigt.

SEN-3812

Problem: Dateien werden nicht aus dem Ordner $ESEC_HOME/sentinel/bin/eventfiles/done gelöscht, selbst wenn sie für das Löschen nach der Verarbeitung konfiguriert wurden.

Korrektur: Die Dateien werden nun nach der Verarbeitung gelöscht.

SEN-3814 (Erweiterung)

Problem: Textausgabe bei Befehlsaktivitäten bei Vorfall sollte in XML erfolgen.

Korrektur: Diese Funktion wurde hinzugefügt.

SEN-3835

Problem: Falls einer der in den Benutzereinstellungen gespeicherten Filter ungültig ist, werden alle aktiven Ansichten mit Filtern für Benutzer als nicht permanente aktive Ansicht behandelt.

Korrektur: Die Fehlerbehandlung wurde verbessert, um dieses Problem zu beheben.

SEN-3851

Problem: Die Schnellabfrage enthält keine Optionen zum Speichern der Daten.

Korrektur: Zum Schnellabfragefeld wurden zwei Schaltflächen hinzugefügt. Mit der einen können die Daten in einer HTML-Datei gespeichert werden, mit der anderen in einer CSV-Datei.

SEN-3877

Problem: Ereignisse werden nicht in die Datenbank geschrieben, wenn der Speicherplatz des Transaktionsprotokolls völlig aufgebraucht ist.

Korrektur: Das Problem wurde behoben, indem Komponenten hinzugefügt wurden, die weiterhin versuchen, Ereignisse in die Datenbank einzutragen, wenn ein Datenbankfehler auftritt. Diese Komponenten werden von diesem Installationsprogramm automatisch aktiviert.

SEN-3880

Problem: Dem Workflow-Server stehen keine Verbindungen mehr zur Verfügung und er reagiert nicht mehr, nachdem viele Prozesse über Vorfälle erstellt werden, die durch die Korrelation ausgelöst werden.

Korrektur: Das Problem wurde behoben, indem sichergestellt wird, dass Workflow-Verbindungen nach der Verwendung wieder geschlossen werden.

SEN-3914

Problem: Die Funktion zum erneuten Einfügen von Ereignissen behandelt in Korrelation stehende Ereignisse nicht ordnungsgemäß.

Korrektur: Die Funktion zum erneuten Einfügen von Ereignissen wurde so korrigiert, dass in Korrelation stehende Ereignisse nicht ordnungsgemäß behandelt werden.

SEN-3916

Problem: Die Taxonomie ist bei der Korrelationsdokumentation und bei Seed-Daten für Korrelationsregeln veraltet.

Korrektur: Die Korrelationsregeln, die als Teil der Seed-Daten installiert werden, wurden aktualisiert, um bei der nächsten Taxonomie Sinn zu ergeben. Darüber hinaus wurde Kapitel 7 des Referenzhandbuchs aktualisiert, um mit der neuen Taxonomie und den neuen Korrelationsregeln übereinzustimmen.

SEN-3800

Problem: Ein geplanter Bericht verursacht Probleme in der Berichtsordnerhierarchie, die in Sentinel angezeigt wird.

Korrektur: GetReports.asp/GetReports.jsp wurde so geändert, dass die Ordnerhierarchie aus dem Repository anders empfangen wird.

SEN-3832

Problem: Die Schnellabfrage wird bei Ausdrücken zum Abgleichen von Teilnetzen nicht ausgeführt.

Korrektur: Die Abfrage, die für Ausdrücke zum Abgleichen von Teilnetzen ausgegeben wird, wurde so aktualisiert, dass sie der Änderung in der Speicherung der IP-Adressen in den Datenbanken entspricht.

SEN-3924

Problem: Correlation Engine reagiert nicht mehr (Fenster-Zeichenfolgenoperation mit !=)

Korrektur: Wenn eine Literal-Zeichenkette mit der Auswertung „!=“ in der Fensteroperation verglichen wurde, wurde eine Segmentierungsverletzung verursacht. Dieses Problem wurde behoben. Beispielsweise Fenster(e.evt!= „bob“,10).

SEN-3933

Problem: Tortendiagramme geben bei der Anzeige von Details in Schnellabfragen nicht die richtige Anzahl an Ereignissen zurück; Teile von Tortendiagrammen geben bei der Anzeige von Details keine Werte zurück.

Korrektur: Das Beheben des Problems stand im Zusammenhang mit einer leeren Kennung. Da rulelg keinen isnull-Vorgang unterstützt, werden die leeren Kennungen von der Abfrage entfernt. Dadurch wurden jedoch die Indizes deaktiviert, wodurch die Ergebnisse verfälscht werden. Wenn Sie allerdings nur die leere Kennung auswählen und die Details anzeigen, werden alle Ereignisse für diesen Zeitraum angezeigt, nicht nur die Ereignisse mit der leeren Kennung. Dies wird durch eine Einschränkung von rulelg verursacht.

SEN-3999 (Erweiterung)

Problem: Erhöhen der Feldlänge für cv30 bis cv34 von 255 auf 4000.

Korrektur: Diese Felder können mehr Zeichenkettendaten enthalten.

SEN-4056

Problem: Problem bei den Workflow-/Benutzerberechtigungen.

Korrektur: Wenn ein Benutzer bei nicht verfügbarem Workflow-Service erstellt wird, wird der Benutzer teilweise in einer von zwei Datenbanken erstellt, die die Benutzerinformationen enthalten. Dadurch ist die Benutzererstellung beschädigt und kann nicht mehr wiederhergestellt werden. Dieses Problem wurde behoben, indem die Benutzererstellung zu einer Transaktion konfiguriert wurde.

SEN-4087

Problem: Beim Klicken auf die Schaltfläche „Entfernen“ in der Registerkarte „Advisor“ eines Vorfalls wird KEINE entsprechende Bestätigungsmeldung angezeigt.

Korrektur: Die Bestätigungsmeldung wurde so bearbeitet, dass beim Löschen eines Angriffs in der Registerkarte „Advisor“ die richtigen Informationen angezeigt werden.

SEN-4094

Problem: Menükonfigurationen werden im internen Browser nicht gestartet, wenn die Option „Externen Browser verwenden“ nicht ausgewählt ist.

Korrektur: Das Problem beim Starten des Browsers wurde behoben.

SEN-4302

Problem: UpgradePortCfgFile-Dateien müssen zum VOLLSTÄNDIGEN Installationsprogramm hinzugefügt werden.

Korrektur: Die Dateien wurden zum Installationsprogramm hinzugefügt.

Wizard

7414 (HD 101689)

Problem: Collector Builder reagiert beim Anmeldebildschirm wegen fehlerhafter Initialisierung von Variablen nicht mehr.

Korrektur: Das Problem wurde durch ordnungsgemäße Initialisierung der Variablen behoben.

WIZ-1649

Problem: Collector Manager schneidet SNMP-Trap-Daten ab, wenn ein Trap-Wert über 57 Zeichen enthält. Dadurch geht die gesamte Trap verloren.

Korrektur: Das Abschneiden der Trap wurde behoben, sodass nun große Trap-Werte mit mehr als 57 Zeichen akzeptiert werden.

WIZ-1651

Problem: Die SNMP-Unterstützung von Collector Manager verarbeitet nur „öffentliche“ Gemeinschafts-Traps.

Korrektur: Collector Manager verarbeitet nun auch nicht öffentliche Gemeinschafts-Traps.

WIZ-1656

Problem: Collector Manager verarbeitet nur SNMP v1- und v3-Traps. Insbesondere werden SNMP v2- und v2c-Traps nicht verarbeitet.

Korrektur: In Collector Manager wurde die Unterstützung für SNMP v2- und v2c-Traps hinzugefügt.

WIZ-1661

Problem: Beim Einstellen der Variablen s_VULN und s_CRIT unter Verwendung des EVENT-Befehls werden leere Anfälligkeits- und Gefährlichkeits-Tag-Felder erstellt.

Korrektur: Diese Felder werden unter Verwendung des EVENT-Befehls nun ordnungsgemäß erstellt.

WIZ-1664

Problem: Falls das Begrenzungszeichen beim Einlesen von der Quelle (z. B. einer Datei) am Anfang eines neuen Datenblocks steht, wird dieses Begrenzungszeichen vom Rx-Status übersprungen.

Korrektur: Dieses Problem wurde behoben.

WIZ-1665

Problem: Wenn die Größe des Begrenzungszeichens unter einem Zeichen liegt und das Begrenzungszeichen über die Blockgrenze hinausgeht, überspringt der Rx-Status das Begrenzungszeichen.

Korrektur: Dieses Problem wurde behoben.

WIZ-1675

Problem: Collector Manager befindet sich zeitweise in einem Status, in dem nahezu die volle Leistung der CPU verwendet, jedoch keine Ereignisse verarbeitet werden, obwohl die Collector Engine ausgeführt wird.

Korrektur: Der Fehler, der zu diesem Problem führte, wurde behoben.

WIZ-1676

Problem: Bei Verwendung des ALERT-Befehls tritt ein Arbeitsspeicherleck auf.

Korrektur: Das Arbeitsspeicherleck wurde behoben.

WIZ-1682

Problem: Die Datenbankverbindungsfunktion wird in einer Endlosschleife immer wieder ausgeführt, wenn die Abfrage einen Tabellennamen enthält, der in der Datenbank nicht vorhanden ist.

Korrektur: Das Problem wurde durch ordnungsgemäße Initialisierung der Ergebnissetvariablen behoben.

WIZ-1699

Problem: Entfernen des Skriptbefehls „exportvar“ und von GUI-Elementen für Collector Builder.

Korrektur: Dieser Befehl wurde entfernt.

WIZ-1713

Problem: Der NVP-Parser konvertiert 32-Bit-Ganzzahlen ohne Vorzeichen nicht in 32-Bit-Ganzzahlen mit Vorzeichen. Die Befehle Parsing/STONUM ermöglichen keine Konvertierung, die über dem Maximum der positiven Ganzzahl mit Vorzeichen iegt.

Korrektur: Diese Skriptbefehle wurden so bearbeitet, dass große 32-Bit-Ganzzahlen ohne Vorzeichen konvertiert werden können. Bei allen Skriptganzzahlen handelt es sich um 32-Bit-Werte mit Vorzeichen. Eine große 32-Bit-Ganzzahl ohne Vorzeichen führt zu einer Skriptvariablen, die den 32-Bit-Wert (mit dem wichtigsten Bit-Satz) als negativen Wert darstellt.

Datenbank

DAT-145

Problem: Beim Verwerfen von Partitionen wurde die Indexpartition von SDM nicht von P_TEMP in P_MIN umbenannt.

Korrektur: Beim Verwerfen von Partitionen wird die Indexpartition von SDM nun von P_TEMP in P_MIN umbenannt.

DAT-147

Problem: SERVICE_PACK_ID fehlt in ADV_ATTACK_PLUGIN_RPT_V.

Korrektur: Die Spalte SERVICE_PACK_ID ist nun in der Ansicht ADV_ATTACK_PLUGIN_RPT_V enthalten.

DAT-151

Problem: Im Datenbankinstallationsprogramm tritt ein Fehler auf, wenn beim Benutzer TNS_ADMIN eingestellt ist und die Datei tnsnames.ora in einem anderen Verzeichnis als $ORACLE_HOME/network/admin gespeichert ist.

Korrektur: Das Datenbankinstallationsprogramm wurde so korrigiert, dass dieser Vorgang ordnungsgemäß ausgeführt wird.

DAT-157

Problem: Fehler beim Archivieren von EVT_DEST_SMRY_1 in SDM.

Korrektur: Es wurden Fehler in zwei Fällen behoben, durch die in SDM ein Fehler beim Archivieren von EVT_DEST_SMRY_1 auftritt. Beim ersten Fall handelt es sich um eine eindeutige Beschränkung durch die zu kurze Spalte ARCH_SEQ. Der Fehler beim zweiten Fall hängt mit der MSSQL-Anmeldung bei SDM unter Verwendung der Windows-Authentifizierung zusammen. Dadurch sind alle Ereignis- und Ereigniszusammenfassungstabellen betroffen.

DAT-161 (Erweiterung)

Problem: Trennen von Archivieren und Löschen von Zusammenfassungtabellen von Ereignistabellen.

Korrektur: Zusammenfassungtabellenpartitionen werden nun nicht mehr verworfen, wenn Ereignistabellenpartitionen verworfen werden.

Bekannte Probleme

Installationsprogramm

- Beim Versuch, ein Bildschirmabbild des Installationsprogramms durch Verwendung der Taste Alt mit der Drucktaste zu erstellen, wird die Grafik im Installationsprogramm verzerrt angezeigt. Dies wird durch einen Fehler im InstallShield verursacht. Sie können dieses Problem umgehen, indem Sie nur die Drucktaste verwenden.

Sentinel

- WorkFlow fährt nach dem Vorgang zum Starten von Eradication nicht fort, wenn versucht wird, den Befehl arp –a auszuführen. Dieses Problem kann folgendermaßen umgangen werden:
  1. Melden Sie sich an dem Computer, der die DAS-Komponente ausführt, als Benutzer „esecadm“ an.
  2. Öffnen Sie die Datei „.bash_profile“ im Basisverzeichnis des Benutzers „esecadm“ und bearbeiten Sie sie so, dass die Umgebungsvariable PATH das Verzeichnis „/usr/sbin“ enthält.
  3. Bearbeiten Sie die Schablonenaktivität so, dass eine andere Aktivität ausgeführt wird.
- Beim Einstellen eines Filters in den Ansichtsoptionen für Vorfälle, Collectors, Collector Managers oder iTRAC arbeiten die Attributfelder mit den Daten möglicherweise nicht ordnungsgemäß, wenn sie Teil des Filters sind.
- Unter „Sentinel Control Center“ > Registerkarte „Admin“´zeigt die Option „Aktive Benutzersitzungen“ vorübergehend eine Sitzung für einen Benutzer an, der sich bei Collector Builder angemeldet hat.
- Falls die Funktion „Analyst“ leer ist (bei Installation des Produkts ist diese Funktion leer) und ein Workflow mit automatischer Reaktion instanziiert wird, weist der Server _WORKFLOW_SERVER zu. Falls ein Benutzer jedoch später zur Funktion „Analyst“ hinzugefügt wird, werden die Zuweisungen nicht neu berechnet und der neue Benutzer erhält keine Arbeitselemente, die diesem Vorgang zugewiesen sind. Im Folgenden finden Sie eine Umgehung dieses Problems:
  - Stellen Sie vor dem Starten von Workflow-Vorgängen sicher, dass alle zugewiesenen Gruppen mindestens einen Benutzer aufweisen. Dadurch wird das zuvor beschriebene Problem umgangen.
  - Falls ein iTRAC-Vorgang instanziiert wurde, bei dem die zugewiesenen Gruppen nicht mindestens einen Benutzer aufweisen, führen Sie die folgenden Schritte aus, um das Problem zu beheben:
    - Fügen Sie einen Benutzer zur betroffenen Gruppe hinzu.
    - Bearbeiten Sie die entsprechende Schablone und speichern Sie sie. Dazu sind keine Änderungen in der Schablone erforderlich. Sie können einfach auf die manuelle Aktivität doppelklicken, um das Anpassungsdialogfeld anzuzeigen, die gleiche Ressource nochmals auswählen, auf „OK“ klicken und die Schablone speichern.

      Dadurch sollte eine Neuberechnung der Arbeitselementzuweisungen erzwungen werden. Benutzern in der Analystengruppe werden nun Arbeitselemente für diese Aktivität angezeigt.
- Keine Bearbeitung während des Erstellens einer benutzerdefinierten Schablone in der gleichen Schablonenanpassung nach dem Speichern möglich. Dieses Problem kann umgangen werden, indem nach dem Speichern der neu erstellten Schablone Änderungen an der Schablone vorgenommen werden, das Schablonenfenster geschlossen und dann erneut geöffnet wird.

Wizard

- Bei Verwendung der Funktion „Netzwerk auffüllen“ in Collector Builder werden UUIDs in den kopierten Port-Konfigurationen nicht zurückgesetzt. Dadurch erhalten die Ereignisse der kopierten Port-Konfigurationen die gleiche Quell-ID.
  - [WIZ-1684] Bei der Fehlersuche in Collector unter Verwendung von Collector Builder wird Collector Builder unter Umständen unerwarteterweise beendet. Dieser Fehler tritt weniger häufig auf, wenn auf die Schalftlächen zur Fehlersuche für die Ausführung eines einzelnen Befehls und für die Wiederaufnahme der Befehlsausführung in Collector Builder langsam geklickt wird (weniger als einmal alle zwei Sekunden).

Technischer Support von Novell

Website: http://www.novell.com

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