Novell Sentinel 6.1 Rapid Deployment SP2 – Readme

April 2011

Novell®

Sentinel Rapid Deployment (RD) ist eine neue Paketoption für die marktführende Sicherheitsinformations- und Ereignisverwaltungslösung Novell Sentinel. Sentinel Rapid Deployment umfasst die vollständige Sentinel-Funktionalität und eignet sich hervorragend für kleinere Unternehmen und regionale Installationen.

Sentinel 6.1 Rapid Deployment SP2 steht zur Neuinstallation oder als Upgrade zur Verfügung. Das Upgrade-Installationsprogramm aktualisiert eine vorhandene Version von Sentinel Rapid Deployment 6.1 SP1 mit den neuesten Softwareverbesserungen und -fehlerbehebungen.

1 Neue Funktionen

1.1 Neuerungen in Sentinel Rapid Deployment 6.1 SP2

1.1.1 Unterstützung für SLES 11 SP1

Sentinel Rapid Deployment wird nun auf der SUSE Linux Enterprise Server (SLES) 11 SP1 64-Bit-Plattform unterstützt.

1.1.2 Eingeschränkte Unterstützung für Legacy Collectors

Novell stellt die Unterstützung für Legacy Collectors in der Sentinel-Produktlinie schrittweise ein. In früheren Versionen von Sentinel Rapid Deployment wird beim Importieren eines Legacy Collectors eine Warnmeldung ausgegeben. Ab Version SP2 werden in Erstinstallationen von

Sentinel Rapid Deployment und Collector-Manager keine Legacy Collectors mehr ausgeführt. Aufgerüstete Sentinel Rapid Deployment-Systeme bzw. Collector-Manager führen weiterhin Legacy Collectors aus.

Hinweis: Legacy Collectors wurden unter Verwendung des Legacy Collector Builders geschrieben, der nicht mehr im Lieferumfang von Sentinel-Produkten enthalten ist. Sie werden durch JavaScript-Collectors ersetzt, die mithilfe des Sentinel-Plugin-SDKs geschrieben werden. Die JavaScript-Collectors sind auf der Sentinel 6.1-Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinel61.html) verfügbar.

1.1.3 Verbesserung der Sicherheit

Sentinel Rapid Deployment 6.1 SP2 enthält mehrere Aktualisierungen zur Verbesserung der Sicherheit des Produkts:

- Java Runtime Environment (JRE) wurde auf Version 1.6.0_24 aufgerüstet.
- Apache Tomcat wurde auf Version 6.0.29 aufgerüstet.
- Die PostgreSQL-Datenbank wurde auf Version 8.3.12 aufgerüstet.

1.2 Neuerungen in Sentinel Rapid Deployment SP1

Informationen über die Neuerungen in Sentinel Rapid Deployment 6.1 SP1 finden Sie im „Sentinel Rapid Deployment SP1-Readme“ (http://www.novell.com/documentation/sentinel61rd/readme/data/s61rd_readme.html#bqtqd85).

2 Systemanforderungen

Ausführliche Informationen über die Hardware-Anforderungen sowie die unterstützten Betriebssysteme und Browser finden Sie unter „Systemanforderungen“ im *Sentinel Rapid Deployment-Installationshandbuch*.

3 Installieren von Novell Sentinel Rapid Deployment

Die Installation wurde vereinfacht, sodass es nicht mehr erforderlich ist, den Namen der TAR-Datei einzugeben. Laden Sie das Installationsprogramm herunter und extrahieren Sie es in das gewünschte Verzeichnis. Führen Sie anschließend als Benutzer `root` oder Nicht-root-Benutzer das Skript aus, um die Installation durchzuführen. Mithilfe von Befehlszeilenargumenten können Sie zudem festlegen, ob nur der Benutzer erstellt, Rapid Deployment-Server installiert und ein Dienst zum automatischen Starten von Sentinel Rapid Deployment beim Systemstart eingerichtet wird oder Rapid Deployment-Server ohne Erstellen des Benutzers bzw. des Dienstes installiert wird.

Anweisungen zur Installation von Novell Sentinel Rapid Deployment 6.1 SP2 finden Sie unter „Installation“ im *Sentinel Rapid Deployment-Installationshandbuch*.

4 Upgrade auf Sentinel Rapid Deployment SP2

Stellen Sie vor der Ausführung zunächst sicher, dass auf dem Computer, auf dem Sie das Service Pack installieren möchten, Sentinel 6.1 Rapid Deployment SP1 installiert ist:

Anweisungen zum Upgrade auf Sentinel 6.1 Rapid Deployment SP2 finden Sie unter „Aufrüstung von Sentinel Rapid Deployment“ im *Sentinel Rapid Deployment-Installationshandbuch*.

5 Zugriff auf die Hilfedateien zu Sentinel Rapid Deployment

Klicken Sie zum Öffnen des Online-Benutzerhandbuchs zu Sentinel Rapid Deployment im Sentinel Control Center auf *Hilfe* > *Hilfe*. Wenn Sie in einer sicheren Umgebung ohne direkten Zugang zum Internet arbeiten, können Sie in einem Arbeitsschritt die Online-Hilfedateien auf den Sentinel Rapid Deployment-Server herunterladen und extrahieren. Nachdem die Hilfedateien in den ausgewählten Speicherort extrahiert wurden, können Sie die Online-Dokumentation auf dem Server bzw. dem Fernsystem öffnen. Sie können die Hilfedateien mithilfe eines beliebigen Webbrowsers anzeigen.

Hinweis: Die Hilfedateien stehen nur in Englisch zur Verfügung.

So laden Sie die Online-Hilfe herunter:

1. Wechseln Sie zur Dokumentations-Site von Sentinel Rapid Deployment (http://www.novell.com/documentation/sentinel61rd/).
2. Klicken Sie im Abschnitt „Downloadable User Guide Help“ (Online-Benutzerhandbuch zum Herunterladen) auf *zip* und laden Sie die Datei `s61rd_user_help.zip` auf Ihren Computer herunter.
3. Verwenden Sie zum Kopieren und Extrahieren der heruntergeladenen Datei folgende Befehle:

   ```
   cp s61rd_user_help.zip <Installationsverzeichnis>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
   ```

   ```
   cd <Installationsverzeichnis>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help
   ```

   ```
   unzip s61rd_user_help.zip
   ```

   Wichtig: Sie müssen die Datei `s61rd_user_help.zip` zuerst im angegebenen Verzeichnis extrahieren, damit Sie die Hilfedateien öffnen können.

   ---

4. Wählen Sie zum Anzeigen der Hilfedateien eine der folgenden Vorgehensweisen:
   - Klicken Sie im Sentinel Control Center auf *Hilfe* > *Hilfe*.
   - Öffnen Sie die Datei `<Installationsverzeichnis>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help/s61rd_user_help/index.html`.

   Die Datei `Index.html` listet die Themen der Hilfedateien in einem Navigationsfenster auf. Zum Öffnen der Hilfeseite zu einem Thema, klicken Sie auf das gewünschte Thema.

Hinweis: Wenn Sie die Hilfedateien in das ausgewählte Verzeichnis auf dem Sentinel Rapid Deployment-Server herunterladen und speichern, wird im Hilfemenü im Sentinel Control Center der Inhalt der heruntergeladenen Online-Hilfe angezeigt, wenn Sie im Sentinel Control Center auf das Menü *Help* (Hilfe) klicken.

Wenn Sie über das Menü *Hilfe* das *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch) öffnen möchten, das online zur Verfügung steht, löschen Sie den Ordner `s61rd_user_help` unter `<Installationsverzeichnis>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/help` vom Sentinel Rapid Deployment-Server.

6 Behobene Probleme und Verbesserungen

6.1 Behobene Probleme

Die folgende Tabelle enthält die Fehlernummern der in Sentinel Rapid Deployment 6.1 SP2 behobenen Probleme und eine Beschreibung der Behebung des jeweiligen Fehlers:

Fehlernummer	Behebung
451892	Die Sentinel WebStart-Anwendung lädt jetzt bei Bedarf die benötigten Schriftarten automatisch herunter.
497131	Die neueste Version von eDirectory Collector unterstützt jetzt Doppelbyte-Zeichen des japanischen Zeichensatzes in der Berichterstellungsfunktion.
531114	Wenn Sie ZIP-Dateien, die keine Berichtsdateien sind, über die Berichts-Weboberfläche hochladen, wird die Fehlermeldung `Fehler beim Abrufen eines PluginPackage aus package.xml` angezeigt.
556730	In der Correlation Engine werden keine künftigen Ereignisse mehr gespeichert, die über 30 Sekunden in die Zukunft reichen, wodurch die Fehlermeldung über ungenügenden Arbeitsspeicher nicht mehr ausgegeben wird.
566973	Im Fenster des Correlation Engine-Managers wird jetzt die Liste der Correlation Engines angezeigt, selbst wenn sie in der zuvor gespeicherten Senitnel Control Center-Sitzung geöffnet wird.
569849	Sentinel Rapid Deployment wird jetzt mit der neuesten Version von Apache Tomcat, Version 6.0.29, ausgeliefert, um Sicherheitsschwachstellen zu beseitigen.
573181	Die Speicherzuteilung für Sentinel-Prozesse wird jetzt in Prozent zugeteilt. Außerdem ist es jetzt möglich, die in der Datei `memory.conf` festgelegten Speicherzuteilungen zu überschreiben.
600604	Die Systemleistung wurde dahingehend verbessert, dass beim Ausführen umfangreicher Berichte ausreichend Arbeitsspeicher zur Verfügung steht.
607145	Zum Überwachen der administrativen Sentinel-Vorgänge sowie der Konfigurationsänderungen bezüglich Datenzuordnung, Filter, Korrelationsregeln, Aktionen und Ereignisquellenverwaltung werden zusätzliche Audit-Ereignisse erstellt.
621509	Wenn der Benutzer zum Erstellen eines Vorfalls Ereignisse auswählt, werden diese jetzt im Fenster *Neuer Vorfall* aufgeführt. Die Ereignisse werden auch als Teil des Vorfalls gespeichert.
623834	Die Meldung `Festplattenspeicher am oberen Grenzwert` wird nur angezeigt, wenn die Speicherauslastung den oberen Grenzwert, der auf Grundlage des tatsächlichen Speicherplatzes des Dateisystems berechnet wird, erreicht.
625930	Im Ereignis „RulePerformanceSummary“ wird der Regelname nicht mehr als null-Zeichenfolge angezeigt.
626402	Das Problem, dass beim Neustart eines Connectors mit mehreren Ereignisquellen in ESM eine Zeitüberschreitungsausnahme eintritt, wurde behoben.

Fehlernummer	Behebung
629716	Das Problem, dass die Sentinel Control Center-Instanzen (SCC) infolge von Deadlocks einfrieren, wurde behoben.
641087	Sentinel Rapid Deployment wird jetzt mit dem neuesten PostgreSQL-Patch, Version 8.3.12, ausgeliefert, um Sicherheitsschwachstellen zu beseitigen.
644821	Benutzer mit Anzeigeberechtigung in ESM können die Knoten (Ereignisquellen, Collectors, Collector Manager) nicht löschen, indem sie die ENTF-Taste drücken.
648554	Die Konfigurationsdatei für Sentinel Data Manager (SDM) wird jetzt im Basisverzeichnis des Benutzers erstellt und nicht im Verzeichnis, von dem aus SDM gestartet wird.
651181	Bei der Ausführung von umfassenden Berichten wird die Abfragezeit mithilfe eines Jasper-Virtualisierers verkürzt.
651524	Die Datenfeed-Dateien für den Advisor können jetzt unter Verwendung eines Proxyservers heruntergeladen werden. Das Proxypasswort wird über den Download-Manager aktualisiert.
656595	Während der Verbindung zur Datenbank gehen keine Verbindungen verloren, da die Sperren für offene Transaktionen, die längere Zeit inaktiv sind, freigegeben werden.
656715	Zur Verringerung der Netzwerkbelastung werden die Daten, die über ActiveMQ übertragen werden, jetzt komprimiert.
662213	Das Senden von Emails an mehrere Empfänger ist jetzt beim Mailen von Ereignissen und Vorfällen möglich.
668443	Die Verbindung zur PostgreSQL-Datenbank ist jetzt neben dem Verbinden mithilfe von pgadmin über die Befehlszeile möglich.
672058	Ereignisquellen, die eine Warnmeldung ausgeben, wenn für eine bestimmte Zeitspanne keine Daten empfangen wurden, geben die Ereignisse (NoDataAlert) und Protokollmeldungen nicht mehr doppelt aus, wenn sie neu gestartet werden.
682235	Sentinel Rapid Deployment wird jetzt mit Java-Version 1.6.0_24 ausgeliefert, um Sicherheitsschwachstellen zu beseitigen.

6.2 Erweiterungen

In der folgenden Tabelle wird beschrieben, welche Funktionen in Sentinel Rapid Deployment 6.1 SP2 verbessert wurden:

Fehlernummer	Beschreibung
547390	Offline-Abfragen können jetzt mithilfe der Eigenschaft für maximale Ereignisse in der Datei `das_core.xml` eingeschränkt werden.
642690	Für Offline-Abfragen ist jetzt die Konfiguration von Unterintervallabfragezeiten in der Datei `das_core.xml` möglich.
642691	Der Aktualisierungsstatus für Offline-Abfragen wird jetzt in der Protokolldatei `das_core` gespeichert.
648108	Das Fenster „Advisor-Status“ enthält jetzt Informationen zu allen Feed-Dateien.

Fehlernummer	Beschreibung
673362	Die JasperPrint-Objektdatei (d. h. die Rohdatenergebnisdatei namens „results“) wird nicht mehr in den Berichtsergebnissen gespeichert. Die Datei wurde von Sentinel nicht verwendet. Daher wurde sie entfernt, wodurch die Systemleistung der Berichterstellung verbessert und Speicherplatz eingespart werden konnte.
680054	Als Failover-Mechanismus werden auf Sentinel Rapid Deployment-Servern jetzt gebundene IP-Adressen unterstützt.

7 Bekannte Probleme

Fehlernummer	Beschreibung
486932	**Problem:** Benutzer können Aktivitäten, die mit einem aktiven iTRAC-Prozess verknüpft sind, löschen. **Behelfslösung:** Keine.
517568	**Problem:** Solution Designer kann nicht separat installiert werden. Die Installation schlägt fehl. **Behelfslösung:** Installieren Sie Solution Designer gemeinsam mit Sentinel Control Center oder Sentinel Data Manager.
525334	**Problem:** Der Identitäts-Browser zeigt redundante Daten für die Active Directory-Domäne an. **Behelfslösung:** Keine.
598473	**Problem:** Wenn die ESM-Benutzeroberfläche von einem nicht-englischen System aus gestartet wird, ruft der 6r9 File Connector die Remote-Dateien nicht mithilfe des SCP-Protokolls wie erwartet ab. **Behelfslösung:** Keine. Dieses Problem wird in File Connector Version 6r10 behoben.
674008	**Problem:** Unter Linux werden im Installshield-Assistent das Novell-Symbol und die Copyright-Informationen nicht angezeigt. **Behelfslösung:** Keine.
674720	**Problem:** In der Lizenzvereinbarung werden Informationen zu Collector Builder angezeigt, obwohl Collector Builder in Sentinel 6.1 Rapid Deployment SP2 nicht unterstützt wird. **Behelfslösung:** Keine.

Fehlernummer	Beschreibung

679830	**Problem:** Unter Windows funktioniert die Zuordnungsfunktion im Collector-Manager gelegentlich nicht wie erwartet.
	
	Behelfslösung: Gehen Sie wie folgt vor:
	
	1. Beenden Sie den Collector-Manager.
	
	`<Installationsverzeichnis>/bin/sentinel.bat stop`
	
	2. Öffnen Sie die Protokolldatei `collector_mgr0.0.log` des Collector-Managers. Die Datei befindet sich im Verzeichnis `<`*`Installationsverzeichnis`*`>/log`.
	
	3. Suchen Sie nach einem Fehler, der mit dem folgenden Fehler in etwa übereinstimmt:
	
	`Das temporäre Systemverzeichnis (java.io.tmpdir-Eigenschaft) C:\Windows\system32\config\systemprofile\AppData\Local\Temp\ scheint ungültig zu sein.`
	
	4. Erstellen Sie den Ordner `Temp` in folgendem Verzeichnis:
	
	Unter Windows 64 Bit:
	
	`C:\Windows\syswow64\config\systemprofile\AppData\Local\`
	
	Unter Windows 32 Bit:
	
	`C:\Windows\system32\config\systemprofile\AppData\Local\`
	
	5. Starten Sie den Collector-Manager neu:
	
	`<Installationsverzeichnis>/bin/sentinel.bat start`

680054	**Problem:** Der Sentinel Rapid Deployment-Server kann die IP-Adresse nicht automatisch ermitteln.
	
	Behelfslösung: Gehen Sie wie folgt vor:
	
	1. Erstellen Sie die Datei `start_tomcat.properties` im Verzeichnis `<`*`Installationsverzeichnis`*`>/sentinel_rd/config`.
	
	Stellen Sie sicher, dass der Benutzer, der den Sentinel Rapid Deployment-Server ausführt, Eigentümer der Datei ist und über Ausführungsberechtigungen verfügt.
	
	2. Geben Sie die IP-Adresse in die neu erstellte Datei ein, indem Sie die folgende Zeile einfügen:
	
	`SERVER_IP=<ip_address_value>`
	
	3. Speichern Sie die Datei.
	
	4. Melden Sie sich als Eigentümer der Sentinel-Installationsdateien an und führen Sie einen Neustart des Servers mithilfe des folgenden Befehls durch:
	
	`sentinel.sh restart`
	
	5. Prüfen Sie die IP-Adresse im folgenden Verzeichnis, um festzustellen, ob die überschriebene IP-Adresse verwendet wird:
	
	`jnlp-Dateien unter $ESEC_HOME/3rdparty/tomcat/webapps/ROOT/ novellsiemdownloads`

680154	**Problem:** Im Sentinel Data Manager sind auf der Registerkarte *Tablespace* (Tabellenbereich) die Werte für den belegten und freien Speicherplatz fehlerhaft. Der belegte und freie Speicherplatz werden auf Grundlage des Tabellenbereichs sendata1 und nicht anhand des tatsächlichen Speicherplatzes ermittelt. **Behelfslösung:** Keine.

Fehlernummer	Beschreibung
685187	**Problem:** Wenn Sie den Remote-Collector-Manager im Konsolenmodus installieren, schlägt der Import des Broker-Zertifikats vom Server fehl. **Behelfslösung:** Sie können den Collector-Manager im Konsolenmodus auf einem Remote-System installieren, indem Sie `ssh` im Grafikmodus verwenden, um eine Verbindung mit dem System herzustellen. Beispiel: `ssh -x <System-IP>`.

8 Dokumentation

Die aktualisierte Dokumentation und Versionshinweise stehen auf der Dokumentations-Site von Sentinel Rapid Deployment (http://www.novell.com/documentation/sentinel61rd/index.html)zur Verfügung.

9 Rechtliche Hinweise

Novell, Inc. übernimmt für Inhalt oder Verwendung dieser Dokumentation keine Haftung und schließt insbesondere jede ausdrückliche oder implizite Garantie für 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 jede ausdrückliche oder implizite 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 aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Exportieren von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

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

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