Kurzanleitung für NetIQ Sentinel 7.0.1

März 2012

Novell

Einführung

Die folgenden Informationen helfen Ihnen, Sentinel in kurzer Zeit zu installieren und auszuführen.

Erfüllen der Systemanforderungen

Überprüfen Sie, ob die Mindestsystemanforderungen für die Installation von Sentinel erfüllt sind.

Hardwareanforderungen für 500 EPS:

- **Arbeitsspeicher:** 6.7 GB
- **Festplatte:** 4 x 500 GB, 7200-RPM-Festplatten auf RAID 1, mit 256 MB Cache oder gleichwertigem Storage Area Network (SAN)
- **Prozessoren:** 1 Intel Xeon X5470 3,33 GHz (4 Core)-CPU

Betriebssysteme:

- SUSE Linux Enterprise Server (SLES) 11 SP 1
- Red Hat Enterprise Linux (RHEL) 6

Virtuelle Maschinen:

- VMWare ESX 4.0
- Xen 4.0
- Hyper-V Server 2008 R2DVD, nur ISO-Datei

ISO-DVD:

- Hyper-V Server 2008 R2
- Hardware ohne installiertes Betriebssystem

Informationen zu den Hardwareanforderungen für weniger bzw. mehr als 500 EPS finden Sie unter “Erfüllen der Systemanforderungen” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

Installieren von Sentinel

Sie können Sentinel entweder als eigenständige Installation oder als Appliance installieren.

Installation auf Hardware

Bei der Standardinstallation von Sentinel werden alle Sentinel-Komponenten auf einem Computer installiert. Weitere Informationen zur benutzerdefinierten Installation und zur Installation von Sentinel mit einem anderen als dem `root`-Benutzer finden Sie unter “Installation von Sentinel” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

So installieren Sie Sentinel

1. Laden Sie die Sentinel-Installationsdatei von der Novell Downloads-Webseite (http://download.novell.com/index.jsp) herunter:
   - **1a** Wählen Sie im Feld *Product or Technology (Produkt bzw. Technologie)* den Eintrag *SIEM-Sentinel* aus.
   - **1b** Klicken Sie auf *Suchen*.
   - **1c** Klicken Sie in der Spalte mit dem Titel *Download* auf die Schaltfläche zum Herunterladen von *Sentinel 7.0 Evaluation (Sentinel 7.0-Evaluierung)*.

1d Klicken Sie auf *proceed to download (weiter zum Herunterladen)* und geben Sie dann Ihren Kundennamen und Ihr Passwort an.

1e Klicken Sie neben der Installationsversion für Ihre Plattform auf *download (herunterladen)*.

2 Extrahieren Sie die Installationsdatei mit folgendem Befehl:

```
tar xfz <install_filename>
```

Ersetzen Sie *<install_filename>* durch den tatsächlichen Namen der Installationsdatei.

3 Führen Sie das Skript `install-sentinel` mit folgendem Befehl aus:

```
./install-sentinel
```

4 Geben Sie die Nummer der gewünschten Sprache für die Installation an und drücken Sie die Eingabetaste.

Der Standardwert ist „3“ für Englisch.

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

5 Drücken Sie die Leertaste, um die Lizenzvereinbarung durchzulesen.

6 Geben Sie `yes` (ja) bzw. `y` ein, um die Lizenz zu akzeptieren und mit der Installation fortzufahren.

Diese Installation kann einige Minuten dauern.

7 Wenn Sie dazu aufgefordert werden, geben Sie „1“ ein, um mit der Standardinstallation von Sentinel 7.0 fortzufahren.

8 Geben Sie zweimal das Passwort für das standardmäßige Admin-Konto ein, das während der Konfiguration erstellt wird.

Detaillierte Informationen finden Sie unter “Installation von Sentinel” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

Installation der Appliance

Die Appliance ist für virtuelle VMWare ESX-, Xen- und Hyper-V-Plattformen verfügbar. Die Appliance kann auch auf Hardware installiert werden. Die folgenden Anweisungen gelten für VMWare ESX Server. Anweisungen für die anderen Plattformen finden Sie unter “Installation der Appliance” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

1 Laden Sie die Installationsdatei für die VMware-Appliance herunter.

Die korrekte Datei für die VMware-Appliance enthält `vmx` im Dateinamen.

2 Richten Sie eine ESX-Datenablage ein, auf der das Appliance-Image installiert werden kann.

3 Melden Sie sich als Administrator an dem Server an, auf dem Sie die Appliance installieren möchten.

4 Extrahieren Sie mit folgendem Befehl das komprimierte Appliance-Image vom Computer, auf dem VM Converter installiert ist:

```
tar zxvf <install_file>
```

Ersetzen Sie *<install_file>* durch den tatsächlichen Dateinamen.

5 Um das VMware-Image auf den ESX-Server zu importieren, verwenden Sie den VMware Converter und folgen Sie den Anweisungen auf dem Bildschirm des Installationsassistenten.

6 Melden Sie sich am ESX-Server an.

7 Wählen Sie das importierte VMware-Image der Appliance und klicken Sie auf das Symbol *Einschalten*.

8 Wählen Sie die gewünschte Sprache aus und klicken Sie auf *Weiter*.

9 Wählen Sie das Tastatur-Layout aus und klicken Sie auf *Weiter*.

10 Lesen und akzeptieren Sie die Software-Lizenzvereinbarung für Novell SUSE Linux Enterprise Server.

11 Lesen und akzeptieren Sie die NetIQ Sentinel-Endbenutzer-Lizenzvereinbarung.

12 Geben Sie im Bildschirm für den Hostnamen und den Domänennamen die entsprechenden Namen ein.

13 Stellen Sie sicher, dass die Option *Hostname zur Loopback-ID zuweisen* ausgewählt ist.

14 Wählen Sie *Weiter*. Die Konfigurationen für den Hostnamen werden gespeichert.

15 Führen Sie einen der folgenden Vorgänge aus:

- Um die aktuellen Netzwerkeinstellungen zu verwenden, wählen Sie im Bildschirm *Netzwerkkonfiguration II* die Option *Folgende Konfiguration verwenden* aus.
- Um die Netzwerkeinstellungen zu ändern, wählen Sie *Ändern* aus und nehmen Sie die gewünschten Änderungen vor.

16 Klicken Sie auf *Weiter*, um die Netzwerkeinstellungen zu speichern.

17 Legen Sie Uhrzeit und Datum fest, klicken Sie auf *Weiter* und anschließend auf *Fertig stellen*.

Zum Ändern der NTP-Konfiguration nach der Installation rufen Sie YaST von der Befehlszeile der Appliance aus auf. Mit WebYast können Sie zwar die Uhrzeit und das Datum ändern, nicht jedoch die NTP-Konfiguration.

Wenn die Zeit unmittelbar nach der Installation nicht synchronisiert erscheint, führen Sie den folgenden Befehl aus, um NTP neu zu starten:

```
rcntp restart
```

18 Legen Sie das `root`-Passwort für Novell SUSE Linux Enterprise Server fest und klicken Sie auf *Weiter*.

19 Legen Sie das `root`-Passwort fest und klicken Sie auf *Weiter*.

20 Legen Sie das admin-Passwort für Sentinel und das dbauser-Passwort fest und klicken Sie auf *Weiter*.

21 Klicken Sie auf *Weiter*. Die Netzwerkeinstellungen werden gespeichert.

   Notieren Sie sich nach dem Abschluss der Installation die IP-Adresse der Appliance, die in der Konsole angezeigt wird.

Informationen zur Konfiguration nach der Installation finden Sie unter “Konfiguration der Appliance nach der Installation” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

Zugriff auf die Sentinel-Weboberfläche

Nach der Installation von Sentinel besteht der nächste Schritt im Zugriff auf die Sentinel-Weboberfläche, wo Sie Verwaltungsaufgaben ausführen und Sentinel zum Erfassen von Daten konfigurieren können.

Geben Sie in einem Webbrowser folgende URL ein, um auf die Weboberfläche zuzugreifen:

`https://<IP_Adresse_Sentinel_Server>:8443`

„8443“ ist der Standardwert für den Port.

Erfassen von Daten

Die Datenerfassung erfolgt durch die Connectors und Collectors. In Sentinel sind standardmäßig einige Connectors und Collectors installiert und konfiguriert.

Standardmäßig sind auf dem Sentinel-Server TCP-, UDP- und SSL-Server installiert. Wenn Sie die Appliance verwenden, werden die Syslog-Server automatisch konfiguriert, sobald sie Ereignisse aus der lokalen Syslog-Datei empfangen.

Sie können Syslog-Geräte, z. B. Linux-Server, so konfigurieren, dass diese Geräte Informationen an die Syslog-Server senden. Außerdem können Sie zusätzlich Connectors konfigurieren, mit denen Sentinel Daten erfasst.

- „Konfiguration eines Linux-Servers zum Senden von Syslog-Informationen an Sentinel“, auf Seite 3
- „Konfiguration der Datenerfassung für Windows“, auf Seite 3
- „Konfiguration zusätzlicher Connectors und Collectors“, auf Seite 6

Konfiguration eines Linux-Servers zum Senden von Syslog-Informationen an Sentinel

Der Sentinel-Server enthält einen vorkonfigurierten Syslog-Ereignisquellenserver, der folgende Ports auf eingehende Verbindungen überwacht:

- **TCP:** 1468
- **UDP:** 1514
- **SSL:** 1443

Befolgen Sie die nachstehenden Anweisungen, um einen Linux-Server zum Senden von Ereignissen an den TCP-Syslog-Ereignisquellenserver zu konfigurieren.

So konfigurieren Sie die Syslog-Datei unter Linux:

1 Öffnen Sie die Datei `/etc/syslog-ng/syslog-ng.conf`.

2 Fügen Sie am Ende der Datei `syslog-ng.conf` folgende Befehlszeilen hinzu.

```
# Forward all messages to Sentinel:
#
destination d_slm { tcp("127.0.0.1"
port(1468)); };
log { source(src); destination(d_slm); };
```

3 Ändern Sie den TCP-Wert in die IP-Adresse des Linux-Servers.

4 Speichern und schließen Sie die Datei.

5 Starten Sie den Syslog-Dienst neu:

```
/etc/init.d/syslog restart
```

Details dazu, wie Sie Geräte zum Senden von Informationen an den Syslog-Connector konfigurieren können, finden Sie in der Syslog-Connector-Dokumentation auf der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Konfiguration der Datenerfassung für Windows

Um Daten aus einem Windows-System zu erfassen müssen Sie einen Windows-Ereignis (WMI)-Connector konfigurieren. Der Windows-Ereignis-Connector wird auf dem Collector-Manager installiert und empfängt Ereignisse vom Windows-Ereigniserfassungsdienst, der auf dem Windows-Server installiert ist.

- „Windows-Ereignis-Connector konfigurieren“, auf Seite 3
- „Windows-Ereigniserfassungsdienst auf dem Windows-Server installieren“, auf Seite 4
- „Windows-Ereigniserfassungsdienst konfigurieren“, auf Seite 5

Windows-Ereignis-Connector konfigurieren

1 Melden Sie sich an der Sentinel-Weboberfläche an.

`https://<IP_Adresse_Sentinel_Server>:8443`

„8443“ ist der Standardport.

2 Klicken Sie in der Symbolleiste auf *Anwendungen* und dann auf *Control Center starten*.

3 Melden Sie sich am Sentinel Control Center mit dem Benutzernamen und Passwort des Administrators an und klicken Sie auf *Anmelden*.

4 Klicken Sie in der Symbolleiste auf *Ereignisquellenverwaltung* > *Live-Ansicht*.

5 Fügen Sie im Collector-Manager einen Windows-spezifischen Collector hinzu.

Ein Windows-spezifischer Collector muss konfiguriert sein, bevor Sie einen Windows-Ereignis-Connector hinzufügen können.

5a Klicken Sie mit der rechten Maustaste auf den Collector-Manager und klicken Sie dann auf *Collector hinzufügen*.

5b Wählen Sie *Microsoft* in der Spalte *Hersteller* aus und wählen Sie dann in der Spalte *Version* die entsprechende Windows- bzw. Active Directory-Version.

5c Klicken Sie auf *Weiter*.

5d Wählen Sie die anzuzeigenden Skripte aus und klicken Sie auf *Weiter*.

5e Ändern Sie beliebige Konfigurationsparameter und klicken Sie dann auf *Weiter*.

5f Legen Sie zusätzliche Konfigurationsparameter für den Collector fest und klicken Sie dann auf *Fertig stellen*.

6 Fügen Sie den Windows-Ereignis-Connector zum in Schritt 5 erstellten Collector hinzu:

6a Klicken Sie mit der rechten Maustaste auf den Collector und klicken Sie dann auf *Connector hinzufügen*.

6b Wählen Sie den Windows-Ereignis-Connector aus und klicken Sie auf *Weiter*.

6c Konfigurieren Sie die Netzwerkeinstellungen für den Windows-Ereignis-Connector-Server und klicken Sie dann auf *Weiter*.

6d Konfigurieren Sie die SSL-Einstellungen und klicken Sie dann auf *Weiter*.

6e Wählen Sie aus, wie der Windows-Ereignis-Connector verwaltet werden soll:

- **Manuell:** Wählen Sie diese Option aus, um die Ereignisquelle manuell zu verwalten.
- **Automatisch:** Wählen Sie diese Option aus, um automatisch mit Active Directory zu synchronisieren.

6f Klicken Sie auf *Weiter*.

6g Geben Sie den Benutzerberechtigungsnachweis für die Verbindung zum Windows-Ereigniserfassungsdienst und zur Ereignisquelle an.

6h Geben Sie die Konfigurationsparameter an und klicken Sie dann auf *Fertig stellen*.

7 Fügen Sie eine Ereignisquelle zum Windows-System hinzu, in dem die Daten erfasst werden sollen.

7a Klicken Sie mit der rechten Maustaste auf den Windows-Ereignis-Connector und klicken Sie dann auf *Ereignisquelle hinzufügen*.

7b Geben Sie die IP-Adresse oder den Hostname des Windows-Systems an

oder

Wählen Sie ein Windows-System aus Active Directory aus. Klicken Sie dann auf *Weiter*.

7c Wählen Sie einen Verbindungsmodus für die Ereignisquelle aus und klicken Sie dann auf *Weiter*.

7d Geben Sie die Konfigurationsparameter für die Ereignisquelle an und klicken Sie dann auf *Fertig stellen*.

Windows-Ereigniserfassungsdienst auf dem Windows-Server installieren

1 Vergewissern Sie sich, dass Sie auf dem Windows-Server ein Benutzerkonto erstellt haben, das über die entsprechenden Rechte verfügt, um den Windows-Ereigniserfassungsdienst auszuführen und Ereignisse von den Windows-Ereignisprotokollen auf Windows-Fernsystemen zu erfassen. Folgende Rechte sind erforderlich:

- Zugriffsberechtigung auf die Windows-Ereignisprotokolle
- WMI-Berechtigungen
- DOCM-Berechtigungen
- Der Distributed COM-Benutzergruppe müssen ACL-Rechte zum Lesen, Schreiben und Löschen für alle Ereignisprotokolltypen zugewiesen werden.
- Leseberechtigung für das Sicherheitsereignisprotokoll
- Der Benutzer muss über Administratorrechte zum Installieren des Windows-Agenten verfügen.
- Der Benutzer muss über das Recht *Als Dienst anmelden* verfügen.

Weitere Informationen finden Sie in der Windows-Ereignis-Connector-Dokumentation auf der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). Informationen zu den Berechtigungen finden Sie in den Kapiteln 4 und 5.

2 Kopieren Sie die Datei `WindowsEvent-CollectionService.msi` aus der `.zip`-Datei des Windows-Ereignis-Connectors auf den Windows-Server, auf dem der Windows-Ereigniserfassungsdienst installiert werden soll.

3 Doppelklicken Sie auf die Datei `WindowsEvent-CollectionService.msi`, um den Einrichtungsassistenten für den Windows-Ereigniserfassungsdienst zu starten.

4 Klicken Sie auf dem Begrüßungsbildschirm auf *Weiter*.

5 (Bedingt) Lesen Sie den Warnhinweis zum beschränkten Support und klicken Sie dann auf *Weiter*.

6 Akzeptieren Sie den Endbenutzer-Lizenzvertrag und klicken Sie auf *Weiter*.

7 Befolgen Sie die nachstehenden Anweisungen, um die Konfiguration des Windows-Ereigniserfassungsdienst benutzerdefiniert anzupassen:

Weitere Funktionen: Wählen Sie die zu installierenden Funktionen aus. Nicht alle Funktionen werden standardmäßig installiert. Folgende Funktionen sind verfügbar:

- **Datenerfassungsdienst:** Installiert den Windows-Ereigniserfassungsdienst, der mit Sentinel kommuniziert.
- **Dokumentation:** Installiert die Dokumentation, die im Lieferumfang des Connectors enthalten ist.

Standort: (Optional) Ändern Sie den standardmäßigen Installationsstandort, indem Sie auf *Durchsuchen* klicken und einen neuen Standort auswählen. Der Standardinstallationsstandort ist `Programme\Novell\SentinelWECS`.

Speicherplatzauslastung: (Optional) Klicken Sie auf *Speicherplatzauslastung*, um zu ermitteln, ob ausreichend Speicherplatz für die Installation des Windows-Ereigniserfassungsdiensts verfügbar ist.

8 Klicken Sie auf *Weiter*.

9 Legen Sie das Dienstkonto fest, das der Windows-Ereigniserfassungsdienst zur Verbindung mit externen Windows-Ereignisquellen verwendet.

Lokales Systemkonto: Wählen Sie diese Option aus, um den Windows-Ereigniserfassungsdienst als Benutzer mit lokalem Systemkonto auszuführen. Wenn Sie diese Option auswählen, müssen Sie beim Bereitstellen des Windows-Ereigniserfassungsdiensts auf dem Collector-Manager den Benutzerberechtigungsnachweis angeben.

Dieser Kontoname: Wählen Sie diese Option aus, um den Windows-Ereigniserfassungsdienst als bestimmten Benutzer bzw. Domänenbenutzer auszuführen. Geben Sie den Berechtigungsnachweis des Benutzers an, der über die Rechte zum Ausführen des Windows-Ereigniserfassungsdiensts verfügt.

Das System mit dem Windows-Ereigniserfassungsdienst muss auf jedem zu überwachenden Ereignisquellensystem über Zugriff zum Lesen des Windows-Ereignisprotokolls verfügen. Den erstellten Benutzern müssen daher auf jedem Ereignisquellensystem entsprechende Berechtigungen zugewiesen werden.

Starten Sie nach der Installation den Dienst:

Wählen Sie diese Option aus, wenn der Windows-Ereigniserfassungsdienst sofort nach der Installation gestartet werden soll.

10 Klicken Sie auf *Weiter*.

11 Klicken Sie auf *Installieren*, um den Windows-Ereigniserfassungsdienst zu installieren.

12 Klicken Sie zum Beenden des Konfigurationsassistenten auf *Beenden*.

Nach der Installation muss der Windows-Ereigniserfassungsdienst konfiguriert werden.

Windows-Ereigniserfassungsdienst konfigurieren

1 Öffnen Sie die Datei `eventManagement.config` in einem Texteditor.

Standardmäßig befindet sich die Datei unter `Programme\Novell\SentinelWECS`.

2 Kopieren Sie im Abschnitt <`client`> die Zeile mit der Angabe `endPoint address` und fügen Sie die Zeile unterhalb der bestehenden Zeile ein. Ersetzen Sie die bestehende IP-Adresse mit der IP-Adresse des Servers (Collector-Manager), mit dem der Windows-Ereigniserfassungsdienst eine Verbindung erstellt. Fügen Sie die Portnummer hinzu, über die der Dienst mit dem Connector kommuniziert.

Beispiel:

```
<client>
    <!-- Additional collectors/plugins can be
added with different host/
port configurations -->
     <!-- <endPoint address="tcp://
127.0.0.1:1024"
behaviorConfiguration="localhost" />-->
     <endPoint address="tcp://
<IP_address_Sentinel_server:<port_number>"
behaviorConfiguration="localhost" />-->
  </client>
```

3 Sie können beliebig viele Connectors konfigurieren, indem Sie Schritt 2 wiederholen. Es kann ein Agent für mehrere Connectors oder ein Agent pro Connector konfiguriert werden.

4 Speichern und schließen Sie die Datei `eventManagement.config`.

5 Öffnen Sie das Fenster „Dienste“, um den Windows-Ereigniserfassungsdienst zu starten.

   5a Klicken Sie auf *Start* > *Ausführen*, um das Dialogfeld „Ausführen“ zu öffnen.

   5b Geben Sie `services.msc` ein und klicken Sie auf *OK*.

6 Wählen Sie den Eintrag *Windows-Ereigniserfassungsdienst* aus, drücken Sie die rechte Maustaste und wählen Sie *Starten* aus, um Windows-Ereigniserfassungsdienst zu starten.

7 Schließen Sie das Fenster „Dienste“.

Weitere Informationen über Microsoft Active Directory, den Windows-Collector und den Windows-Ereignis (WMI)-Connector finden Sie auf der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Konfiguration zusätzlicher Connectors und Collectors

Die verfügbaren Connectors und Collectors werden während der Installation von Sentinel auf dem Sentinel-Server installiert. Oft sind jedoch neue und aktualisierte Connectors und Collectors verfügbar.

Überprüfen Sie auf der Sentinel-Plugins-Webseite (http://support.novell.com/products/sentinel/secure/sentinelplugins.html), ob aktualisierte Versionen der Connectors bzw. Collectors verfügbar sind.

Informationen zur Konfiguration eines nicht bereits standardmäßig konfigurierten Connectors oder Collectors finden Sie unter “Hinzufügen zusätzlicher Sentinel-Komponenten” im *NetIQ Sentinel 7.0.1-Installations- und Konfigurationshandbuch*.

Weitere Schritte

Sentinel ist nun installiert. Um Sie bei der Konfiguration von Sentinel zu unterstützen, stehen Ihnen zwei Handbücher zur Verfügung: *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* und *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Das Administrationshandbuch enthält Informationen zu Konfigurationsaufgaben, die nur von einem Benutzer mit Administratorrechten ausgeführt werden können. Beispiel:

- “Konfigurieren von Benutzern und Rollen”
- “Konfigurieren der Datenspeicherung”
- “Konfigurieren der Datenerfassung”
- “Ereignissuche und -berichterstellung in einer verteilten Umgebung”

Weitere Informationen zu diesen und anderen Administrationsaufgaben finden Sie im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)*.

Das Benutzerhandbuch enthält Anleitungen zu Aufgaben, die von Benutzern in Sentinel ausgeführt werden können. Beispiel:

- “Suchen von Ereignissen”
- “Analysieren von Datentrends”
- “Berichterstellung”
- “Konfigurieren von Vorfällen”

Weitere Informationen zu diesen und anderen Benutzeraufgaben finden Sie im *NetIQ Sentinel 7.0.1 User Guide (NetIQ Sentinel 7.0.1-Benutzerhandbuch)*.

Die Konfigurationsmöglichkeiten in Sentinel umfassen unter anderem die Ereignisanalyse, das Hinzufügen von Daten anhand von Korrelationsregeln, das Erstellen von Grundwerten und die Konfiguration von Workflows. Die Informationen im *NetIQ Sentinel 7.0.1 Administration Guide (NetIQ Sentinel 7.0.1-Administrationshandbuch)* unterstützen Sie bei der Konfiguration dieser Sentinel-Funktionen.