RSA NETWITNESS® SUITE

Konfig. der Windows Legacy Collection

für Version 11.0

RSA

Copyright © 2017 EMC Corporation. Alle Rechte vorbehalten.

Marken

RSA, das RSA Logo und EMC sind Marken oder eingetragene Marken der EMC Corporation in den USA und/oder in anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber. Eine Liste der EMC Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden. Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verbreitung

Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von EMC ist eine entsprechende Softwarelizenz erforderlich. EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. DIE EMC CORPORATION MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.

Inhalt

NetWitness – Legacy Windows Collection – Aktualisierungs- und Installationsanweisungen

Mit der RSA NetWitness® Suite Legacy Windows Collection werden Ereignisdaten aus mehreren Windows-Ereignisquellendomains gesammelt.

Sie unterstützt die Sammlung von:

- Ereignisquellen aus Windows 2003 und früher
- NetApp ONTAP-Host-Ereignisdateien

Dieses Dokument enthält folgende Abschnitte:

Konfigurationsanforderungen

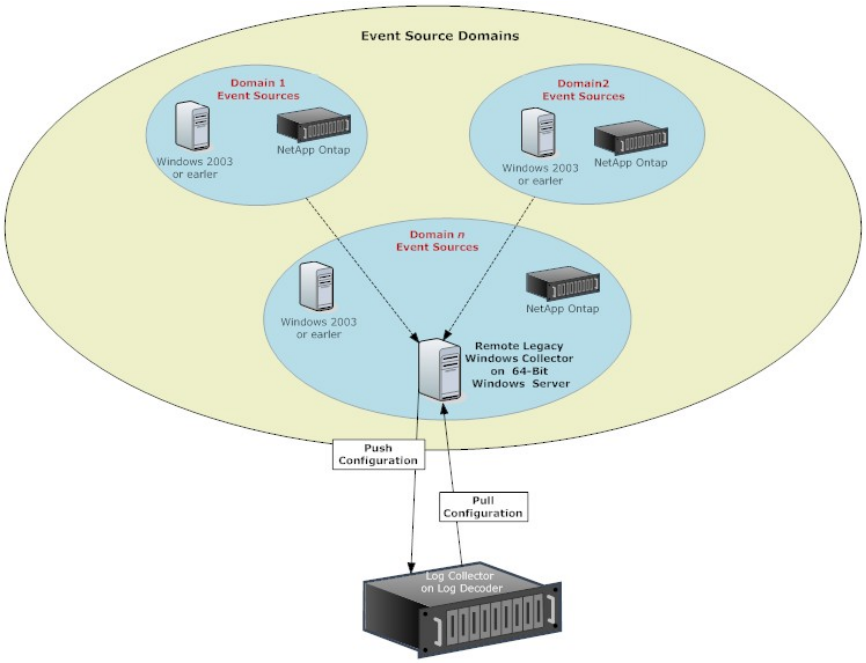
In diesem Thema werden die Konfigurationsanforderungen für den RSA NetWitness® Suite Legacy Windows Collector behandelt.

Achtung: Wenn Sie die Version 11.0 installieren oder auf diese aktualisieren möchten, müssen Sie zuerst das Windows-Update gemäß KB2999226 installieren, um den Security Analytics Legacy Windows Collector mit NetWitness verwenden zu können. Wenn das Update nicht installiert ist, erhalten Sie eine Fehlermeldung und der Legacy Windows Collector wird nicht installiert.

Für die Konfiguration des RSA NetWitness ® Suite Legacy Windows Collector benötigen Sie Folgendes:

- Einen beliebigen physischen oder virtuellen Windows 2008 R2 SP1 64-Bit-Server, der die Windows 2003-Ereignisquellendomains erreichen kann
- Mindestens 20 % freien Speicherplatz So benötigen Sie zum Beispiel mindestens 20 GB freien Speicherplatz, wenn Ihr Systemlaufwerk 100 GB umfasst.

Hinweis: Das Installieren des Legacy Windows Collector auf einem Domaincontroller kann die Performance des Systems beeinträchtigen.



Aktualisieren des RSA NetWitness® Suite Legacy Windows Collector von 10.6.x auf 11.0

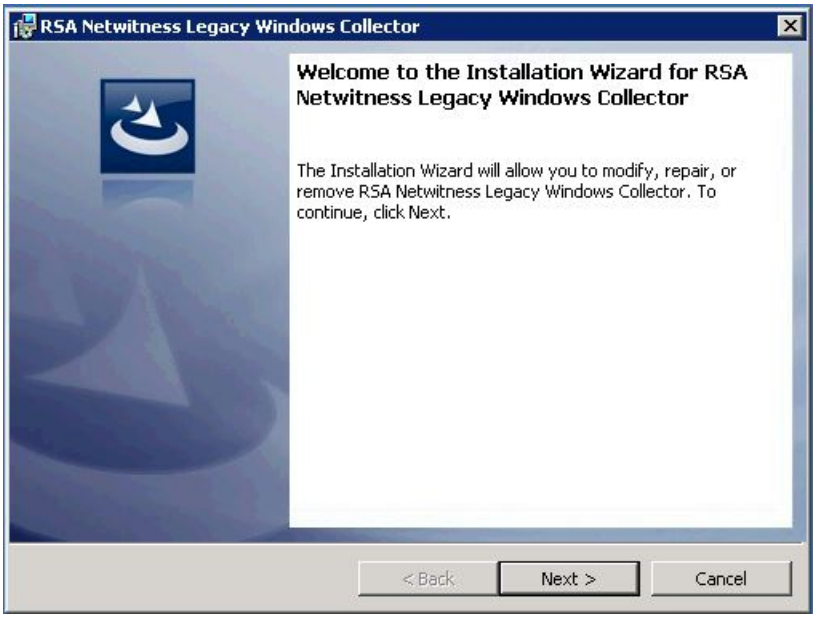
In diesem Thema erfahren Sie, wie Sie RSA NetWitness Suite 10.6.x Legacy Windows Collector auf Version 11 aktualisieren.

So aktualisieren Sie RSA NetWitness ® Suite 10.6x Legacy Windows Collector auf einem Windows 2008 R2 SP1 64-Bit-Server auf Version 11:

1. Navigieren Sie auf RSA Link zu https://community.rsa.com/docs/DOC-44986. Klicken Sie auf **SA-11.0.0.0-LegacyWindowsCollector.zip**, um die Datei herunterzuladen, und entpacken Sie sie.
2. Melden Sie sich an einem Windows 2008-Computer an.
3. Kopieren Sie die Datei **WindowsCollector-Versionsnummer.exe** auf den Windows 2008-Server.
4. Klicken Sie mit der rechten Maustaste auf die Datei **WindowsCollector-Versionsnummer.exe** und wählen Sie **Als Administrator ausführen** aus.

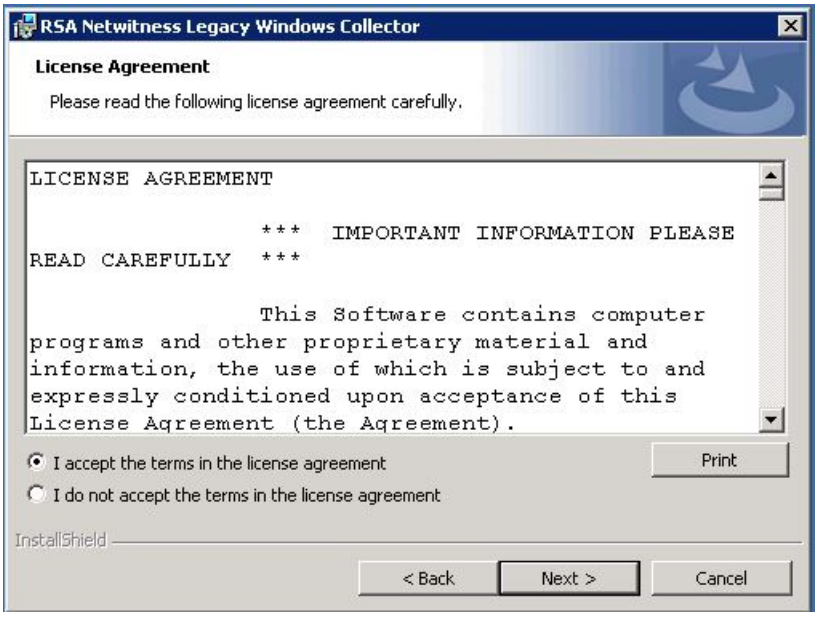
   Die Seite Vorbereitung der Installation… des Assistenten zur Installation der Aktualisierung wird angezeigt.

Nachdem das Programm zur Installation der Aktualisierung die Installationsdateien des RSA NetWitness ® Suite Legacy Windows Collector extrahiert hat, wird die Seite **Willkommen** angezeigt.



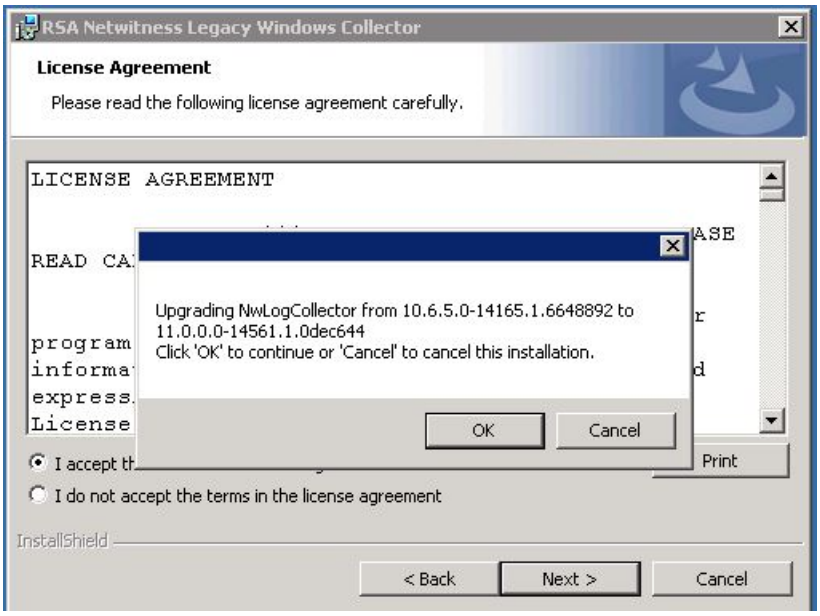
5. Klicken Sie auf **Weiter**.

   Die Seite Lizenzvereinbarung wird angezeigt.



6. Lesen Sie die Lizenzvereinbarung und wählen Sie das Optionsfeld **Ich stimme den Bedingungen des Lizenzvertrags zu**. Klicken Sie anschließend auf **Weiter**.

   Bevor die Aktualisierung gestartet wird, werden Sie im Assistenten gefragt, ob Sie die Installation der Aktualisierung fortsetzen oder abbrechen möchten.



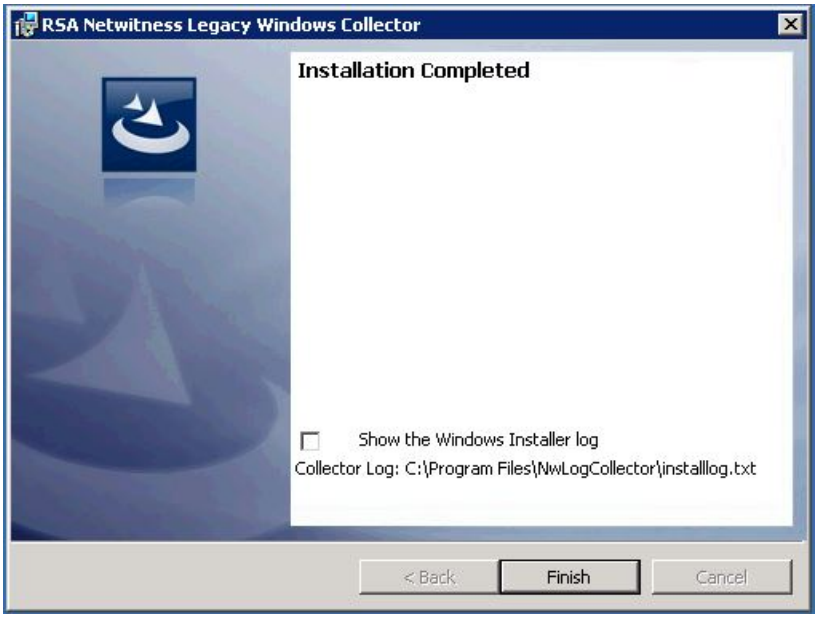
7. Klicken Sie auf **OK**, um mit der Installation der Aktualisierung fortzufahren.
8. Klicken Sie auf „Installieren“.

   Der Installationsbildschirm für den Legacy Windows Collector wird angezeigt.

Nachdem die Installation der Aktualisierung abgeschlossen ist, wird die Schaltfläche **Weiter** aktiv.

9. Klicken Sie auf **Next**.

   Die Seite Installation abgeschlossen wird angezeigt.



11. (Optional) Wenn Sie ein Protokoll der Installation der Aktualisierung anzeigen möchten, aktivieren Sie das Kontrollkästchen **Protokolldatei von Windows Installer anzeigen**.

12. Klicken Sie auf **Fertigstellen**.
13. Starten Sie den Rechner neu.

Damit ist das Update des Legacy Windows Collector auf RSA NetWitness Suite 11.0 abgeschlossen.

Neuinstallation des 11.0 Legacy Windows Collector

In diesem Thema erfahren Sie, wie Sie den 11.0 Legacy Windows Collector auf einem Windows 2008 R2 SP1 64-Bit-Server installieren.

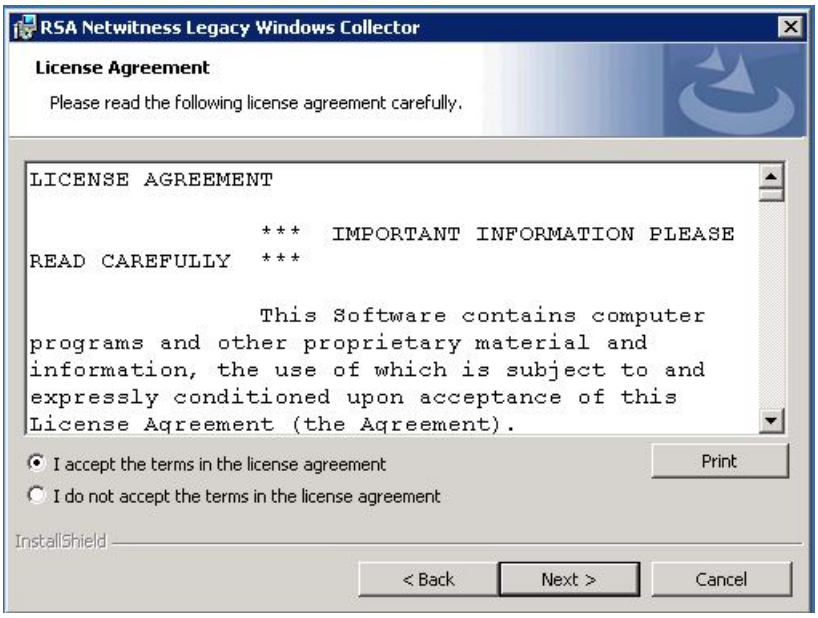
So installieren Sie den RSA NetWitness Suite Legacy Windows Collector auf einem Windows 2008 2 SP1 64-Bit-Server:

1. Navigieren Sie auf RSA Link zu https://community.rsa.com/docs/DOC-44986. Klicken Sie auf **SA-11.0.0.0-LegacyWindowsCollector.zip**, um die Datei herunterzuladen, und entpacken Sie sie.
2. Kopieren Sie die Datei **SALegacyWindowsCollector-Versionsnummer.exe** auf den Windows 2008-Server.
3. Klicken Sie mit der rechten Maustaste auf die Datei **SALegacyWindowsCollector-Versionsnummer.exe** und wählen Sie **Als Administrator ausführen** aus.

   Die Seite **Willkommen** des Installationsassistenten wird angezeigt.

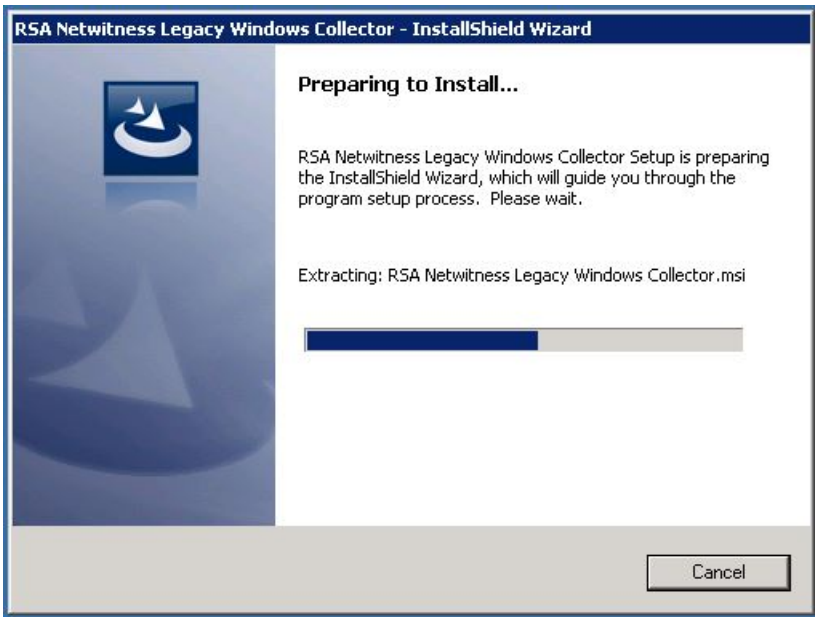
4. Klicken Sie auf **Weiter**.

   Die Seite Lizenzvereinbarung wird angezeigt.



5. Lesen Sie sich die Lizenzvereinbarung genau durch und aktivieren Sie das Optionsfeld **Ich stimme den Bedingungen der Lizenzvereinbarung**. Klicken Sie anschließend auf **Weiter**.

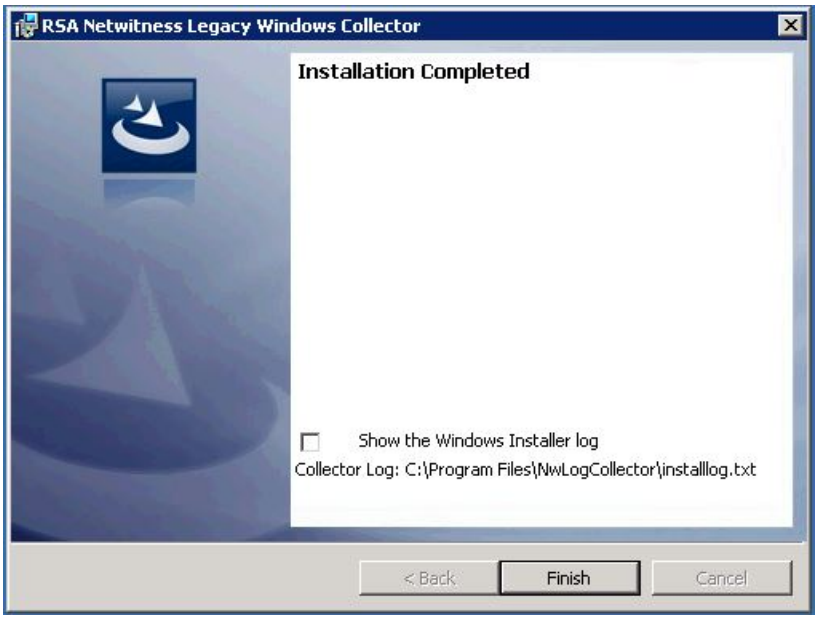
   Die Seite Das Programm kann jetzt installiert werden wird angezeigt.



6. Klicken Sie auf **Installieren**.

   Der Installationsbildschirm für den Legacy Windows Collector wird angezeigt.

Die Seite Installation abgeschlossen wird angezeigt.



7. (Optional) Wenn Sie ein Protokoll der Installation anzeigen möchten, aktivieren Sie das Kontrollkästchen **Protokolldatei von Windows Installer anzeigen**.
8. Klicken Sie auf **Fertigstellen**.
9. Starten Sie den Rechner neu.

Damit ist die Installation von 11.0 Legacy Windows Collector abgeschlossen. Genaue Anweisungen zur Konfiguration der Windows Legacy Collection in RSA NetWitness Suite finden Sie im **Konfigurationsleitfaden für Windows-Legacy- und NetApp-Sammlung** auf RSA Link.

Troubleshooting für neue oder Upgrade-Installationen

Beziehen Sie sich auf die folgenden Protokolldateien, wenn Sie Probleme beheben müssen:

- `%systemDrive%\Netwitness\ng\logcollector\MessageBroker.log`
- `%systemDrive%\Program Files\NwLogCollector\installlog.txt`

Führen Sie `C:\Program Files\NwLogCollector\ziplogfiles.vbs` aus, um ***`hostname`***`_WLCversion_timestamp.zip` zu generieren, die alle Protokolldateien und anderen Informationen zum Troubleshooting enthält.

(Optional) Backup und Wiederherstellung des Legacy Windows Collector

In diesem Thema erfahren Sie, wie Sie den Legacy Windows Collector sichern und wiederherstellen.

Hinweis: Sie müssen dies nur ausführen, wenn Sie die Windows-VM ändern, auf der Sie den Windows Legacy Collector ausführen.

Für Version 10.6.4

Für die Version 10.6.4 von RSA NetWitness Suite Legacy Windows Collector werden manuelle Skripte für Backup- und Installationsvorgänge zur Verfügung gestellt:

- WLC-Backup.bat
- WLC-Restore.bat

Diese Dateien stehen auf RSA Link unter folgendem Link zum Download zur Verfügung: https://community.rsa.com/docs/DOC-71397.

Backup

So sichern Sie den Windows Legacy Collector:

1. Laden Sie die Backup- und Wiederherstellungsskripte von RSA Link in den Windows Legacy Collector herunter.
2. Öffnen Sie aus dem Windows Legacy Collector ein Eingabeaufforderungsfenster und navigieren Sie zu dem Ordner, in dem die Skripte gespeichert sind.
3. Führen Sie folgende Befehle für die Erstellung eines Backups aus:
   - Sichern der Konfigurationsdateien: `WLC-Backup.bat config`
   - Sichern der Laufzeitdateien: `WLC-Backup.bat runtime`

   Hinweis: Sichern Sie Laufzeitdateien nur, wenn Sie bereits mit Sammlungen begonnen haben.

   Die Backupordner werden in **C:\Program Files\NwLogCollector** erstellt.

   Die Dateinamen lauten wie folgt:

- Config-bkup_*Zeitstempel*.zip
- Runtime-bkup_*Zeitstempel*.zip

Wiederherstellung

So stellen Sie ein Backup des Legacy Windows Collector wieder her:

1. Öffnen Sie aus dem Windows Legacy Collector ein Eingabeaufforderungsfenster und navigieren Sie zu dem Ordner, in dem die Skripte gespeichert sind.
2. Führen Sie den folgenden Befehl aus, um ein Backup wiederherzustellen:
   - Gesicherte Konfigurationsdateien: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Gesicherte Laufzeitdateien: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
3. Sobald die Wiederherstellung abgeschlossen ist, legen Sie für den Lockbox-SSV das Passwort fest, das Sie während der 10.6.4-Konfiguration erstellt haben.
   a. Wählen Sie im Menü **Security Analytics** die Option **Services**, den Windows Legacy Collector und dann **Durchsuchen** aus.
   b. Erweitern Sie im linken Navigationsbereich **logcollection > properties > crypto**.
   c. Führen Sie den folgenden Befehl aus: `op=setssv pw=password_for_10.6.x_lockbox` und klicken Sie auf **Senden**.

Upgrade von 10.6.4 auf NetWitness 11

Während des Upgrades auf RSA NetWitness Suite 11 wird das Backupskript für den Windows Legacy Collector automatisch aufgerufen, das die 10.6.4-Konfigurations- und -Laufzeitbackups erstellt. Nachdem die Installation von 11.0 abgeschlossen ist, führen Sie das Wiederherstellungsskript aus, um die Konfigurations- und Laufzeitdateien für die aktualisierte Windows Legacy Collection wiederherzustellen.

Wiederherstellen des Backups der Windows Legacy Collection nach dem Upgrade

So stellen Sie die Konfiguration der Windows Legacy Collection auf einer gerade aktualisierten RSA NetWitness Suite 11-Plattform wieder her:

1. Öffnen Sie über den Windows Legacy Collector ein Eingabeaufforderungsfenster.
2. Navigieren Sie zu **C:\Program Files\NwLogCollector**, wo die Skripte gespeichert sind.

3. Führen Sie die folgenden Befehle aus, um das Backup wiederherzustellen:
   - Gesicherte Konfigurationsdateien: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Gesicherte Laufzeitdateien: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
4. Sobald die Wiederherstellung abgeschlossen ist, legen Sie für den Lockbox-SSV das Passwort fest, das Sie während der 10.6.4-Konfiguration erstellt haben.
   a. Wählen Sie im Menü **Security Analytics** die Option **Services**, dann den Windows Legacy Collector und dann **Durchsuchen** aus.
   b. Erweitern Sie im linken Navigationsbereich **logcollection > properties > crypto**.
   c. Führen Sie den folgenden Befehl aus: `op=setssv pw=password_for_10.6.x_lockbox` und klicken Sie auf **Senden**.

Zurücksetzen der Windows Legacy Collection von 11.0 zurück auf 10.6.4

So setzen Sie die Konfiguration der Windows Legacy Collection von 11.0 zurück auf 10.6.4:

1. Deinstallieren Sie die 11.0-Konfiguration. Merken Sie sich den Speicherort des Backupordners, der während des Deinstallationsvorgangs vom System erstellt wird.
2. Installieren der Version 10.6.4 des Windows Legacy Collector
3. Navigieren Sie zu **C:\Program Files\NwLogCollector**, wo die Skripte gespeichert sind.
4. Führen Sie das Wiederherstellungsskript aus dem Backupordner unter **C:\Program Files\NwLogCollector** aus, um die Konfiguration und die Laufzeiteinrichtung auf dem 10.6.4 Windows Legacy Collector wiederherzustellen.
   - Gesicherte Konfigurationsdateien: `WLC-Restore.bat "Config-bkup_timestamp.zip"`
   - Gesicherte Laufzeitdateien: `WLC-Restore.bat "Runtime-bkup_timestamp.zip"`
5. Sobald die Wiederherstellung abgeschlossen ist, legen Sie für den Lockbox-SSV das Passwort fest, das Sie während der 10.6.4-Konfiguration erstellt haben.
   a. Wählen Sie im Menü **Security Analytics** die Option **Services**, dann den Windows Legacy Collector und dann **Durchsuchen** aus.
   b. Erweitern Sie im linken Navigationsbereich **logcollection > properties > crypto**.
   c. Führen Sie den folgenden Befehl aus: `op=setssv pw=password_for_10.6.x_lockbox` und klicken Sie auf **Senden**.

Hinzufügen eines Windows Legacy Collector-Hosts und -Service in RSA NetWitness® Suite

Für diese Version des Windows Legacy Collector stellt RSA ein Skript bereit, durch das die manuellen Schritte beim Hinzufügen eines Windows Legacy Collector-Hosts und -Service in der NetWitness-Benutzeroberfläche entfallen.

So erstellen Sie einen Windows Legacy Collector-Host und -Service in NetWitness:

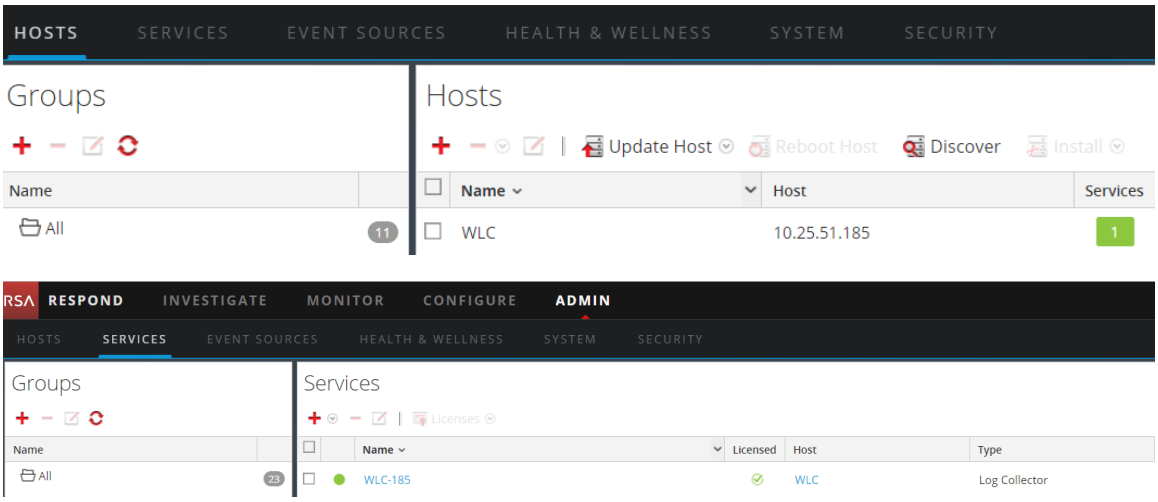
1. Verbinden Sie sich über SSH mit Ihrem NetWitness-Server.
2. Führen Sie den folgenden Befehl aus:

   ```
   wlc-cli-client --host-display-name hostDisplayName --service-display-name serviceDisplayName --host WLChostIPAddress --port 50101 --use-ssl false
   ```

   Die Parameter werden nachfolgend erklärt:

   - **--host-display-name**: der Name des Hosts, wie er auf der Seite mit den NetWitness-Hosts angezeigt wird
   - ***--service-display-name***: der Name des Hosts, wie er auf der Seite mit den NetWitness-Services angezeigt wird
   - **--host**: die IP-Adresse für den Windows Legacy Collector
   - **--port**: der Port, den NetWitness verwendet, um mit dem Windows Legacy Collector zu kommunizieren Der empfohlene Wert ist 50101.
3. Sie werden aufgefordert, folgende Informationen anzugeben:
   - **Windows Log Collector-REST-Benutzername** und **Windows Log Collector-REST-Passwort**: Sie müssen Administrator-Anmeldedaten für den Windows Legacy Collector angeben.
   - **Security Server-Benutzernamen** und **Security Server-Passwort**: Sie müssen Administrator-Anmeldedaten für die RSA NetWitness-Suite angeben.

Wenn Sie dieses Verfahren abgeschlossen haben, sollte der Windows Legacy Collector-Host und -Service wie in folgendem Screenshot zu sehen sein.


HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
11
Hosts
Update Host
Reboot Host
Discover
Install
Name
Host
Services
WLC
10.25.51.185
1

RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
23
Services
Licenses
Name
Licensed
Host
Type
WLC-185
WLC
Log Collector