



Endpoint Insights Agent- Installationshandbuch

für Version 11,1



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Kontaktinformationen

Der RSA-Link unter <https://community.rsa.com> enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell 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 Dell ausgelegt werden.

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

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.

Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Juli 2018

Inhalt

Einführung	4
Unterstützte Betriebssysteme	4
Windows	4
Linux	5
Mac	5
Flussdiagramm der Installation	5
Voraussetzungen	7
Erzeugen eines Endpunkt-Agent-Packager	8
Erzeugen eines Agent-Packager zur Erfassung von Endpunktdaten	8
Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung	11
Erzeugen von Endpoint Agent-Installationsprogrammen	16
Bereitstellen und Überprüfen von Endpunkt-Agents	17
Bereitstellen von Agents (Windows)	17
Überprüfen von Windows-Agents	17
Bereitstellen von Agents (Linux)	17
Überprüfen von Linux-Agents	17
Bereitstellen von Agents (Mac)	18
Überprüfen von Mac-Agents	18
Konfigurieren der Kommunikation zwischen Endpoint-Server und Endpunkt-Agents unter Windows Vista, 2008 Server, Mac OS X 10.9 und 10.10	19
Deinstallieren von Agents	20
Deinstallieren des Windows-Agenten	20
Deinstallieren des Linux-Agenten	20
Deinstallieren des Mac-Agenten	20

Einführung

Hinweis: Die Informationen in diesem Leitfaden gelten für Version 11.1 und höher.

Hosts können Laptops, Workstations, Server, Tablets, Router oder jegliche Systeme – physisch oder virtuell – sein, auf denen ein unterstütztes Betriebssystem installiert ist. Ein Agent von Endpoint Insights kann auf einem Host mit Windows-, Mac- oder Linux-Betriebssystem bereitgestellt werden. Die Installation umfasst Folgendes:

1. Erzeugen eines Agent-Packagers zur ausschließlichen Erfassung von Endpunktdaten oder zur Erfassung von Endpunkt- und Protokolldaten (nur Windows)
2. Erzeugen des Agent-Installationsprogramms

Führen Sie das zu Ihrem Betriebssystem passende Agent-Installationsprogramm aus, um Agents auf den Hosts bereitzustellen. Die Agents erfassen Endpunktdaten und Windows-Protokolle (falls aktiviert) von diesen Hosts. Sie überwachen Aktivitäten und übertragen Daten und Scanergebnisse über HTTPS an den Endpoint Hybrid oder Endpoint Log Hybrid.

Unterstützte Betriebssysteme

Windows

Die Agent-Software wird auf folgenden Windows-Betriebssystemen ausgeführt:

- Windows Vista (32- und 64-Bit)
- Windows 7 (32- und 64-Bit)
- Windows 8 (32- und 64-Bit)
- Windows 8.1 (32- und 64-Bit)
- Windows 10 (32- und 64-Bit)
- Windows 2008 Server (32- und 64-Bit)
- Windows 2008 R2 (32- und 64-Bit)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 Server

Linux

Die Agent-Software wird auf der i386- oder x84_64-Architektur sowie auf folgenden Linux-Betriebssystemen ausgeführt:

- CentOS 6.x und 7.x
- Red Hat Linux 6.x und 7.x

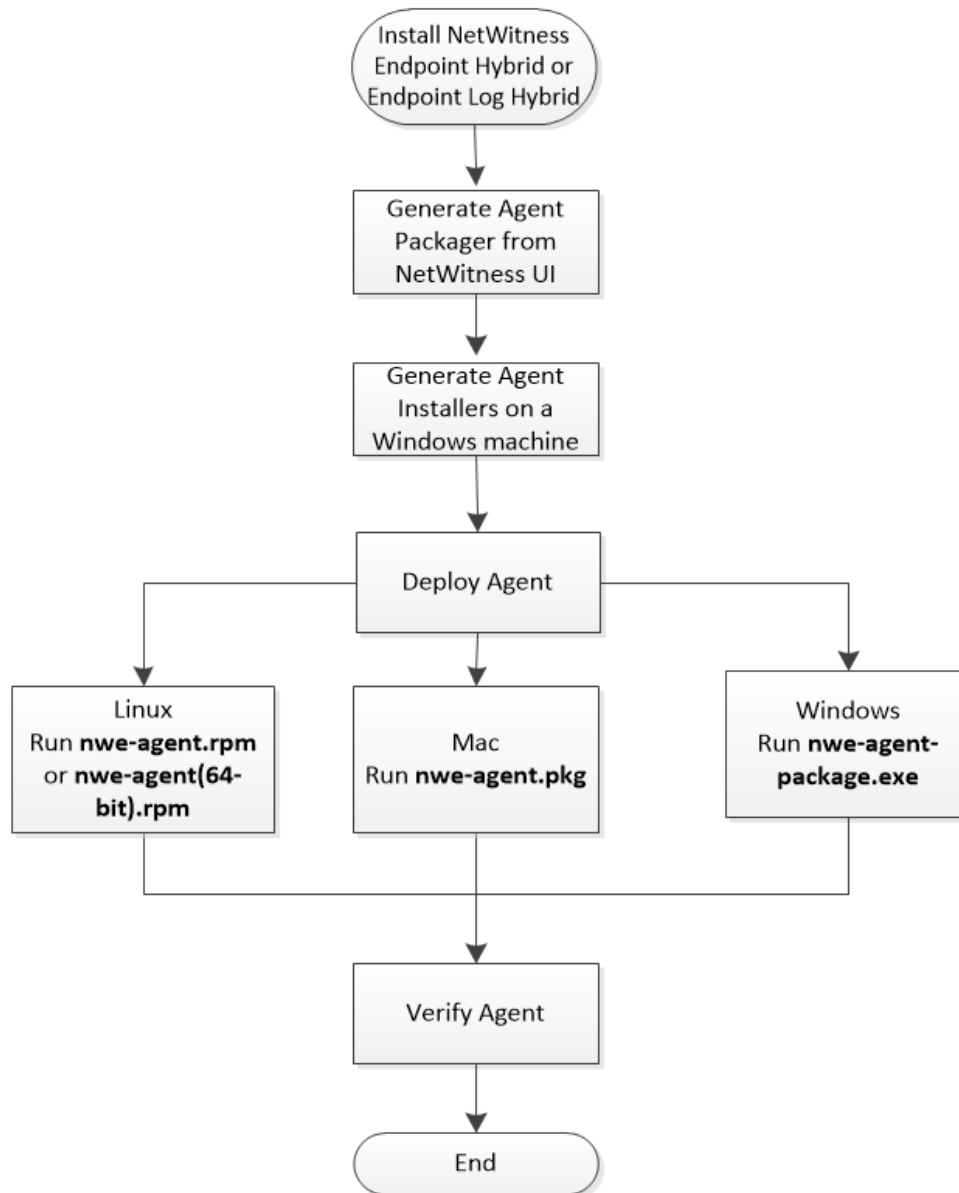
Mac

Die Agent-Software wird auf folgenden Mac-Betriebssystemen ausgeführt:

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.11 (El Capitan)
- Mac OS X 10.12 (Sierra)

Flussdiagramm der Installation

Das folgende Flussdiagramm zeigt den Installationsprozess für Endpunkt-Agents:




Voraussetzungen

- Installieren Sie die RSA NetWitness Suite. Weitere Informationen finden Sie im *Handbuch zur Installation physischer Hosts* oder im *Handbuch zur Installation virtueller Hosts*.
- Konfigurieren Sie NetWitness Endpoint Hybrid oder Endpoint Log Hybrid. Weitere Informationen finden Sie im *Endpoint Insights-Konfigurationsleitfaden*.

Erzeugen eines Endpunkt-Agent-Packager

Erzeugen eines Agent-Packager zur Erfassung von Endpunktdaten

So erzeugen Sie einen Agent-Packager zur ausschließlichen Erfassung von Endpunktdaten von Hosts:

1. Melden Sie sich bei NetWitness Suite.
Geben Sie `https://<NW-Server-IP-Address>/login` in Ihrem Browser ein, um zum NetWitness Suite-Anmeldebildschirm zu gelangen.
2. Klicken Sie auf **ADMIN > Services**.
3. Wählen Sie den Service **Endpoint-Server** aus und klicken Sie auf  **> Ansicht > Konfiguration > Registerkarte „Packager“**. Die Registerkarte „Packager“ wird angezeigt.

RSA RESPOND INVESTIGATE MONITOR CONFIGURE **ADMIN**

Hosts Services **Event Sources** Health & Wellness System Security

Change Service | 1760NodeX - Endpoint Server | Config

General Data Retention Scheduler Scan Schedule **Packager**

Packager

SERVER* 10.40.15.171 HTTPS PORT* 443

SERVER VALIDATION
☐ None ☒ Certificate Thumbprint

CERTIFICATE PASSWORD*

AUTO UNINSTALL

☐ Force Overwrite

SERVICE NAME* NWEAgent DISPLAY NAME* RSA NWE Agent

DESCRIPTION
RSA Netwitness Endpoint

☒ Enable Windows Log Collection

CONFIGURATION NAME* Load Existing Configuration...

PRIMARY LOG DECODER/LOG COLLECTOR*
Make a selection

SECONDARY LOG DECODER/LOG COLLECTOR
Make a selection

CHANNEL FILTERS

CHANNEL NAME *	FILTER *	EVENT ID *
Make a selection	Include	ALL

PROTOCOL
TCP

☒ Send Test Log

Reset Generate Agent Generate Log Configuration Only

4. Geben Sie die Werte in die folgenden Felder ein:

Feld	Beschreibung
Endpoint-Server	Den Hostnamen oder die IP-Adresse des Endpoint-Servers. Beispiel: 10.10.10.3.
HTTPS-Port	Portnummer Beispiel: 443.
Servervalidierung	<p>Legt fest, wie der Agent das Zertifikat des Endpoint-Servers überprüft:</p> <ul style="list-style-type: none"> Keine: Der Agent überprüft das Serverzertifikat nicht. Fingerabdruck des Zertifikats: Dies ist die Standardauswahl. Der Agent identifiziert den Server durch Überprüfung des Fingerabdrucks der Stammzertifizierungsstelle des Serverzertifikats.
Zertifikatpasswort	Das Passwort, das zum Herunterladen des Packager verwendet wird. Das gleiche Passwort wird beim Erzeugen des Agent-Installationsprogramms verwendet. Beispielsweise „netwitness“.
Automatische Deinstallation	Datum und Uhrzeit der automatischen Deinstallation des Agent. Hier müssen Sie keine Angaben machen, sofern es nicht erforderlich ist.
Überschreiben erzwingen	<p>Überschreibt den installierten Windows-Agent unabhängig von der Version. Wenn diese Option nicht ausgewählt ist, kann dasselbe Installationsprogramm auf einem System mehrere Male ausgeführt werden. Der Agent wird jedoch nur einmal installiert.</p> <div> <p>Hinweis: Wenn Sie diese Option aktivieren, müssen Sie den gleichen Servicenamen wie für den zuvor installierten Agent angeben, während Sie einen neuen Agent erstellen.</p> </div>
Servicename	Der Name des Agent. Dieses Feld gilt nur für Windows. Beispiel: NWEAgent.
Anzeigename	Der Anzeigename des Agent. Dieses Feld gilt nur für Windows. Beispiel: NWE.
Beschreibung	Eine Beschreibung des Ereignisses. Dieses Feld gilt nur für Windows. Beispiel: RSA NetWitness Endpoint.
Agent erzeugen	Erzeugt einen Agent-Packager.

5. Klicken Sie auf **Agent erzeugen**.

Hierdurch wird ein Agent-Packager (**AgentPackager.zip**) auf den Host heruntergeladen, auf

dem Sie auf die NetWitness Suite-Benutzeroberfläche zugreifen.

Erzeugen eines Agent-Packager mit der Windows-Protokollsammlung

Sie können die Windows-Protokollsammlung im Agent aktivieren, während Sie den Agent-Packager erzeugen. Durch das Aktivieren dieser Option wird eine Protokollkonfigurationsdatei erzeugt und der Agent kann Windows-Protokolle erfassen und weiterleiten. So aktivieren Sie die Windows-Protokollsammlung:

1. Führen Sie die Schritte 1 bis 4 unter [Erzeugen eines Agent-Packager zur Erfassung von Endpunktdaten](#) aus.
2. Wählen Sie **Windows-Protokollsammlung aktivieren** aus.

☒ Enable Windows Log Collection

CONFIGURATION NAME*

Load Existing Configuration...

PRIMARY LOG DECODER/LOG COLLECTOR*

Make a selection

SECONDARY LOG DECODER/LOG COLLECTOR

Make a selection

CHANNEL FILTERS

+

CHANNEL NAME *	FILTER *	EVENT ID *
Make a selection	Include	ALL



PROTOCOL

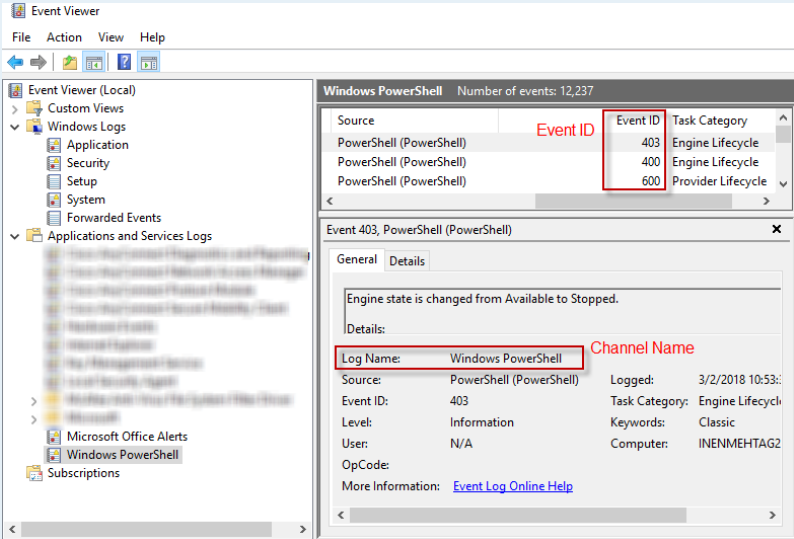
TCP

☒ Send Test Log

3. Geben Sie die Werte in die folgenden Felder ein oder wählen Sie sie aus:

Feld	Beschreibung
Konfigurationsname	Der Name der Konfiguration. Konfigurationsnamen können Sonderzeichen, alphanumerische Werte, Bindestriche, Leerzeichen und Unterstriche enthalten.
Vorhandene Konfiguration wird geladen	<p>Lädt eine vorhandene Konfiguration vom Benutzersystem. Bei einem erfolgreichen Upload werden die Informationen in die Felder der Windows-Protokollsammlung eingetragen.</p> <p>Hinweis: Bei Fehlern oder Warnungen werden während dem Upload Warnmeldungen angezeigt.</p>
Primärer Log Decoder/Log Collector	Der primäre Log Decoder oder Log Collector für die Weiterleitung von Protokollen. Dies zeigt die Liste der Log Decoder oder Remote Log Collectors in der aktuellen Bereitstellung an. Dieses Feld stellt eine Kombination aus Anzeigenname des Service, Hostname und Servicetyp dar.
(Optional) Sekundärer Log Decoder/Log Collector	<p>Der sekundäre Log Decoder oder Log Collector für die Weiterleitung von Protokollen. Der sekundäre Log Decoder oder Log Collector empfängt die Windows-Ereignisse, wenn der Agent den primären Log Decoder oder Log Collector nicht erreichen kann.</p> <p>Hinweis: Für das UDP-Protokoll kann der sekundäre Log Decoder oder Log Collector nicht verwendet werden. Die Protokolle werden nicht an den sekundären Log Decoder oder Log Collector weitergeleitet, wenn der primäre nicht verfügbar ist, was einen Ereignisverlust zur Folge hat.</p>
Protokoll	Wählen Sie im Drop-down-Menü das Protokoll aus. Die verfügbaren Optionen sind UDP, TCP und TLS. Standardmäßig ist für das Protokoll „TCP“ ausgewählt.

Feld	Beschreibung
Kanalfilter	<p>Kanäle, aus denen die Protokolle erfasst werden. Sie können einen Kanalfilter hinzufügen oder entfernen. Zur Erfassung der Protokolle sollte mindestens ein Kanalfilter vorhanden sein.</p> <ul style="list-style-type: none"> Kanalname: Wählen Sie im Drop-down-Menü den Kanal aus. Zur Auswahl stehen die Optionen „System“, „Sicherheit“, „Anwendung“, „Setup“ und „Weitergeleitete Ereignisse“. Sie können auch einen benutzerdefinierten Kanal erstellen, indem Sie einen benutzerdefinierten Kanalnamenpfad eingeben. Dieser wird zur Liste der Kanalnamen hinzugefügt. Um benutzerdefinierte Kanäle zu finden, navigieren Sie zur Windows-Ereignisanzeige auf Ihrem Rechner. Filter: Klicken Sie auf , um einen Kanalfilter hinzuzufügen. Klicken Sie auf das Drop-down-Menü, um die Ereignis-IDs eines bestimmten Kanals ein- oder auszuschließen, wenn Sie den Agent-Packager oder die Protokollkonfigurationsdatei erzeugen. Standardmäßig ist die Ereignis-ID für die Option „Einschließen“ auf ALLE festgelegt. Die Ereignis-ID für die Option „Ausschließen“ ist leer. Klicken Sie auf , um einen Kanalfilter zu löschen. Ereignis-ID: Geben Sie die Ereignis-IDs für diesen Kanal ein. Diese IDs sind kanalspezifisch und es handelt sich dabei um die IDs, die erfasst werden müssen. Die Ereignis-IDs können eine Zahl sein oder einen Bereich umfassen. Mit 15–32 geben Sie beispielsweise einen Bereich an. Ein umgekehrter Bereich (z. B. 32–15) ist jedoch nicht zulässig. Ereignis-IDs können auch als Kombinationen angegeben werden, beispielsweise als eine Liste durch Kommas getrennter Ereignis-IDs (z. B. 248, 903, 16384 usw.). <div data-bbox="630 1629 1419 1728" style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Hinweis: Wenn Sie ALLE eingeben, schließt dies alle Ereignis-IDs für diesen Kanal ein.</p> </div> <p>Sie können die Windows-Ereignisanzeige verwenden, um Ereignis-IDs und Kanalnamen zu identifizieren, die in der Benutzeroberfläche konfiguriert werden sollen. Das folgende</p>

Feld	Beschreibung
	<p>Beispiel zeigt die Navigation, um die Ereignis-ID und den Kanalnamen für Windows Powershell zu erhalten. Um die Informationen anzuzeigen, geben Sie im Dialogfeld „Ausführen“ Event Viewer ein. Navigieren Sie anschließend zu Anwendungs- und Serviceprotokolle > Windows Powershell. Die Ereignis-IDs und der Kanalname in den Anwendungs- und Serviceprotokollen für Windows Powershell werden angezeigt.</p> 
Testprotokoll senden	<p>Sendet eine Testprotokollmeldung. Diese Option ist standardmäßig aktiviert. Eine Testprotokollnachricht wird bei der Bereitstellung eines neuen Agent oder bei Konfigurationsänderungen vom Agent an den Log Decoder gesendet. Sie enthält alle Felder, die für den Agent konfiguriert sind. Diese Ereignisse können dazu beitragen, dass Sie die Konnektivität der Agents zum Ziel besser verstehen.</p>
Agent erzeugen	<p>Erzeugt einen Agent-Packager. Die Protokollkonfigurationsdatei wird in der Datei „AgentPackager.zip“ erstellt.</p>
Nur Protokollkonfiguration erzeugen	<p>Erzeugt die Protokollkonfigurationsdatei gemäß den oben angegebenen Parametern oder im Falle eines Uploads mit der Option „Vorhandene Konfiguration wird geladen“.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Hinweis: Der Inhalt der erzeugten Protokollkonfigurationsdatei sollte nicht manipuliert werden. Wenn Sie Änderungen vornehmen, kann der Agent die Informationen aus der Datei nicht lesen.</p> </div>

Hinweis: Sie können die Windows-Protokollsammlung später aktivieren, indem Sie die Protokollkonfigurationsdatei herunterladen und bereitstellen. Weitere Informationen finden Sie im Abschnitt „Hinzufügen/Aktualisieren der Windows-Protokollsammlungsdatei mit dem Endpunkt-Agent“ im *Protokollsammlung-Konfigurationsleitfaden*.

Erzeugen von Endpoint Agent-Installationsprogrammen

So erzeugen Sie Endpoint Agent-Installationsprogramme zur Bereitstellung auf Hosts:

Hinweis: Verwenden Sie einen Windows-Rechner, um die folgende Agent-Packager-Datei auszuführen.

1. Entpacken Sie die Datei **AgentPackager.zip**. Dazu gehört Folgendes:
 - Ordner **Agents**: enthält ausführbare Dateien für Linux, Mac und Windows.
 - Datei **config**: enthält die Konfigurationsdatei und die Zertifikate für die Kommunikation zwischen dem Endpoint-Server und dem Agent.
 - Datei **AgentPackager.exe**.
2. Führen Sie die Datei **AgentPackager.exe** aus.
3. Geben Sie das gleiche Kennwort an, das Sie beim Erzeugen der Agent-Packager-Datei verwendet haben, und drücken Sie die Eingabetaste.
Dadurch werden die folgenden Installationsprogramme im Stammordner erstellt:
 - nwe-agent-package.exe (für Windows)
 - nwe-agent.pkg (für Mac)
 - nwe-agent.rpm (für Linux 32-Bit)
 - nwe-agent(64-bit).rpm (für Linux 64-Bit)

Bereitstellen und Überprüfen von Endpunkt-Agents

Dieser Abschnitt enthält Anweisungen zum Bereitstellen und Überprüfen von Agents.

Bereitstellen von Agents (Windows)

Um den Agent bereitzustellen, führen Sie die Datei **nwe-agent-package.exe** auf den Hosts aus, die Sie überwachen möchten.

Überprüfen von Windows-Agents

Nach der Bereitstellung von Windows-Agents können Sie mit einer der folgenden Methoden überprüfen, ob ein Windows-Agent ausgeführt wird:

- Mit der NetWitness Endpoint-Benutzeroberfläche

Die Ansicht „Hosts“ enthält die Liste aller Hosts mit einem Agent. Sie können nach dem Hostnamen suchen, auf dem der Agent installiert ist.

Hinweis: Klicken Sie auf **Untersuchen > Hosts** oder drücken Sie F5, um die Liste für die neuesten Daten zu aktualisieren.

- Mit dem Task-Manager

Öffnen Sie den Task-Manager und suchen Sie nach dem Servicenamen, den Sie beim Erzeugen des Agent-Packager konfiguriert haben.

- Mit der Datei „Services.msc“

Öffnen Sie die Datei „Services.msc“ im Dialogfeld „Ausführen“ und suchen Sie nach NWEAgent.

Bereitstellen von Agents (Linux)

Um den Agent bereitzustellen, führen Sie die Datei **nwe-agent.rpm** (für 32 Bit) oder die Datei **nwe-agent(64-bit).rpm** (für 64 Bit) auf den Hosts aus, die Sie überwachen möchten.

Verwenden Sie die RPM-Datei für 32 Bit für i386 und die RPM-Datei für 64 Bit für Rechner mit x84_64.

Überprüfen von Linux-Agents

Nach der Bereitstellung von Linux-Agents können Sie mit einer der folgenden Methoden überprüfen, ob ein Linux-Agent ausgeführt wird:

- Mit der NetWitness Endpoint-Benutzeroberfläche

Die Ansicht „Hosts“ enthält die Liste aller Hosts mit einem Agent.

Hinweis: Klicken Sie auf **Untersuchen > Hosts** oder drücken Sie F5, um die Liste für die neuesten Daten zu aktualisieren.

- Mit der Befehlszeile

Führen Sie den folgenden Befehl aus, um die PID anzuzeigen:

```
pgrep nwe-agent
```

- Um die Version von NetWitness Endpoint zu überprüfen, führen Sie den folgenden Befehl aus:

```
cat /opt/rsa/nwe-agent/config/nwe-agent.config | grep version
```

Bereitstellen von Agents (Mac)

Um den Agent bereitzustellen, führen Sie die Datei **nwe-agent.pkg** auf den Hosts aus, die Sie überwachen möchten.

Überprüfen von Mac-Agents

Nach der Bereitstellung von Mac-Agents können Sie mit einer der folgenden Methoden überprüfen, ob ein Mac-Agent ausgeführt wird:

- Mit der NetWitness Endpoint-Benutzeroberfläche

Die Ansicht „Hosts“ enthält die Liste aller Hosts mit einem Agent.

Hinweis: Klicken Sie auf **Untersuchen > Hosts** oder drücken Sie F5, um die Liste für die neuesten Daten zu aktualisieren.

- Mit Activity Monitor

Öffnen Sie Activity Monitor (/Applications/Utilities/Activity Monitor.app) und suchen Sie nach NWEAgent.

- Mit der Befehlszeile

Führen Sie den folgenden Befehl aus, um die PID anzuzeigen

```
pgrep NWEAgent
```

- Um die Version von NetWitness Endpoint zu überprüfen, führen Sie den folgenden Befehl aus:

```
grep a /var/log/system.log | grep NWEAgent | grep Version:
```

Konfigurieren der Kommunikation zwischen Endpoint-Server und Endpunkt-Agents unter Windows Vista, 2008 Server, Mac OS X 10.9 und 10.10

Standardmäßig ist auf dem Endpoint-Server der FIPS-Modus aktiviert, was bedeutet, dass unter Windows Vista, 2008 Server, Mac OS X 10.9 und 10.10 installierte Agents nicht mit dem Endpoint-Server kommunizieren können.

Führen Sie zur Lösung dieses Problems auf dem Endpoint Hybrid oder dem Endpoint Log Hybrid die folgenden Schritte aus, um den FIPS-Modus zu deaktivieren:

1. Navigieren Sie zu `/etc/pki/tls/owb.cnf` und bearbeiten Sie die Datei, um den FIPS-Modus zu deaktivieren.

```
# FIPS Mode
#   Configures the BSAFE Libraries to be in FIPS Mode.
#
#   Values: "on", "off".
#   Default: "off"
fips mode = off
```

2. Navigieren Sie zu `/etc/nginx/conf.d/nginx.conf` und bearbeiten Sie die Datei, um die folgenden Zeilen zu kommentieren:

```
# ssl_ciphers AES256+EECDH:AES256+EDH:!aNULL;
# ssl_prefer_server_ciphers on;
```

3. Starten Sie den Nginx-Server mit dem folgenden Befehl neu:

```
systemctl restart nginx
```

Deinstallieren von Agents

Dieser Abschnitt enthält die Befehle, um den Agenten zu deinstallieren.

Deinstallieren des Windows-Agenten

Führen Sie den folgenden Befehl aus:

```
msiexec /x{63AC4523-5F19-42F0-BC43-97C8B5373589}
```

Deinstallieren des Linux-Agenten

Führen Sie den folgenden Befehl aus:

```
rpm -ev nwe-agent
```

Deinstallieren des Mac-Agenten

Führen Sie folgende Befehle aus:

1. `sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
2. `sudo rm -Rf /usr/local/nwe`
3. `sudo rm -Rf '/Library/Application Support/NWE'`
4. `sudo rm -Rf /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
5. `sudo pkgutil --forget com.rsa.pkg.nwe`