Installieren Sie das SnapCenter Plug-in für Unix-Dateisysteme

SnapCenter software

NetApp
November 06, 2025

Inhalt

Installieren Sie das SnapCenter Plug-in für Unix-Dateisysteme

Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux

Bevor Sie einen Host hinzufügen und das Plug-In-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder Nicht-Root-Benutzer oder die SSH-Schlüssel-basierte Authentifizierung verwenden.

  Das SnapCenter Plug-in für Unix-Dateisysteme kann von einem Nicht-Root-Benutzer installiert werden. Sie sollten jedoch die Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um den Plug-In-Prozess zu installieren und zu starten. Nach der Installation des Plug-Ins werden die Prozesse effektiv als Nicht-Root-Benutzer ausgeführt.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus „Linux“ für den Installationsbenutzer.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

  Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben.

  Informationen zum Herunterladen von JAVA finden Sie unter: "Java-Downloads für alle Betriebssysteme"

- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

Linux-Hostanforderungen

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren.

Artikel	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	2 GB

Artikel	Anforderungen
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben. Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux über die GUI

Sie können auf der Seite „Host hinzufügen“ Hosts hinzufügen und dann das SnapCenter Plug-In-Paket für Linux installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Hosttyp	Wählen Sie **Linux** als Hosttyp.

Für dieses Feld…	Machen Sie Folgendes…
Hostname	Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.
Anmeldeinformationen	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen. Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die Option **Unix-Dateisysteme** aus.
6. (Optional) Klicken Sie auf **Weitere Optionen**.

Für dieses Feld…	Machen Sie Folgendes…
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist */opt/ NetApp/snapcenter*. Optional können Sie den Pfad anpassen. Wenn Sie den benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass der Standardinhalt der Sudoers mit dem benutzerdefinierten Pfad aktualisiert wird.
Überspringen optionaler Vorinstallationsprüfungen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

7. Klicken Sie auf **Senden**.

   Wenn Sie das Kontrollkästchen „Vorabprüfungen überspringen“ nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob er die Anforderungen für die Installation des Plug-Ins erfüllt.

   Das Vorabprüfungsskript validiert den Firewall-Status des Plug-In-Ports nicht, wenn dieser in den Ablehnungsregeln der Firewall angegeben ist.

   Sollten die Mindestanforderungen nicht erfüllt sein, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt. Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei web.config unter *C:\Programme\ NetApp\ SnapCenter WebApp* aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, sollten Sie das Problem beheben.

   Wenn Sie in einem HA-Setup die Datei web.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

8. Überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

   SnapCenter unterstützt den ECDSA-Algorithmus nicht.

Die Überprüfung des Fingerabdrucks ist obligatorisch, auch wenn derselbe Host zuvor zu SnapCenter hinzugefügt und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Protokolldateien befinden sich unter */custom_location/snapcenter/logs*.

Ergebnis

Alle auf dem Host gemounteten Dateisysteme werden automatisch erkannt und auf der Ressourcenseite angezeigt. Wenn nichts angezeigt wird, klicken Sie auf **Ressourcen aktualisieren**.

Überwachen des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü „Typ“ die Option „Plug-in-Installation“ aus.
   d. Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.
   e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

Konfigurieren des SnapCenter Plug-in Loader -Dienstes

Der SnapCenter Plug-in Loader -Dienst lädt das Plug-in-Paket für Linux, um mit dem SnapCenter -Server zu interagieren. Der SnapCenter Plug-in Loader -Dienst wird

installiert, wenn Sie das SnapCenter Plug-ins-Paket für Linux installieren.

Über diese Aufgabe

Nach der Installation des SnapCenter Plug-ins-Pakets für Linux wird der SnapCenter Plug-in Loader -Dienst automatisch gestartet. Wenn der SnapCenter Plug-in Loader -Dienst nicht automatisch gestartet wird, sollten Sie:

- Stellen Sie sicher, dass das Verzeichnis, in dem das Plug-In ausgeführt wird, nicht gelöscht wird
- Erhöhen Sie den der Java Virtual Machine zugewiesenen Speicherplatz

Die Datei spl.properties, die sich unter */custom_location/ NetApp/snapcenter/spl/etc/* befindet, enthält die folgenden Parameter. Diesen Parametern sind Standardwerte zugewiesen.

Parametername	Beschreibung
LOG_LEVEL	Zeigt die unterstützten Protokollebenen an. Die möglichen Werte sind TRACE, DEBUG, INFO, WARN, ERROR und FATAL.
SPL_PROTOCOL	Zeigt das vom SnapCenter Plug-in Loader unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOKOLL	Zeigt das vom SnapCenter Server unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den Java-Pfad und aktualisiert den JAVA_HOME-Parameter. Daher ist der Standardwert auf FALSE gesetzt. Sie können es auf TRUE setzen, wenn Sie das Standardverhalten deaktivieren und den Java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Passwort der Keystore-Datei an. Sie können diesen Wert nur ändern, wenn Sie das Kennwort ändern oder eine neue Keystore-Datei erstellen.

Parametername	Beschreibung
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter Plug-in Loader -Dienst ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Sie sollten den Wert nach der Installation der Plug-Ins nicht mehr ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter -Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Keystore-Datei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter -Server ausgeführt wird.
LOGS_MAX_COUNT	Zeigt die Anzahl der Protokolldateien des SnapCenter Plug-in Loader an, die im Ordner */custom_location/snapcenter/spl/logs* gespeichert sind. Der Standardwert ist auf 5000 eingestellt. Wenn die Anzahl größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Überprüfung der Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader -Dienstes. Wenn Sie die Datei „spl.properties“ manuell löschen, wird die Anzahl der beizubehaltenden Dateien auf 9999 festgelegt.
JAVA_HOME	Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird. Dieser Pfad wird während der Installation und beim Starten von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Protokolldatei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei komprimiert und die Protokolle in die neue Datei dieses Auftrags geschrieben.

Parametername	Beschreibung
Protokolle der letzten Tage aufbewahren	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
Zertifikatsvalidierung aktivieren	Zeigt „true“ an, wenn die CA-Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder durch Bearbeiten der spl.properties oder mithilfe der SnapCenter -GUI oder des Cmdlets aktivieren oder deaktivieren.

Wenn einem dieser Parameter nicht der Standardwert zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei „spl.properties“ überprüfen und bearbeiten, um alle Probleme im Zusammenhang mit den den Parametern zugewiesenen Werten zu beheben. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter Plug-in Loader -Dienst neu starten.

Schritte

1. Führen Sie je nach Bedarf eine der folgenden Aktionen aus:
   - Starten Sie den SnapCenter Plug-in Loader -Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Stoppen Sie den SnapCenter Plug-in Loader -Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Sie können die Option -force mit dem Stoppbefehl verwenden, um den SnapCenter Plug-in Loader -Dienst zwangsweise zu stoppen. Allerdings sollten Sie dabei vorsichtig sein, da dadurch auch die bestehenden Vorgänge beendet werden.
   - Starten Sie den SnapCenter Plug-in Loader -Dienst neu:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Ermitteln Sie den Status des SnapCenter Plug-in Loader Dienstes:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo`

```
/custom_location/NetApp/snapcenter/spl/bin/spl status
```

- Suchen Sie die Änderung im SnapCenter Plug-in Loader -Dienst:
  - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
  - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host

Sie sollten das Kennwort des SPL-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den SPL-Truststore konfigurieren und das von der CA signierte Schlüsselpaar für den SPL-Truststore mit dem SnapCenter Plug-in Loader -Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

SPL verwendet die Datei „keystore.jks“, die sich unter „/var/opt/snapcenter/spl/etc“ befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den SPL-Schlüsselspeicher und den Alias des verwendeten CA-signierten Schlüsselpaars

Schritte

1. Sie können das Standardkennwort für den SPL-Schlüsselspeicher aus der SPL-Eigenschaftendatei abrufen.

   Dies ist der Wert, der dem Schlüssel „SPL_KEYSTORE_PASS“ entspricht.

2. Ändern Sie das Keystore-Passwort:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
   ```

   ```
   keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
   ```

   Aktualisieren Sie dasselbe für den Schlüssel SPL_KEYSTORE_PASS in der Datei spl.properties.

3. Starten Sie den Dienst nach der Änderung des Kennworts neu.

Das Kennwort für den SPL-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den SPL-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner, der den SPL-Schlüsselspeicher enthält: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder
Zwischenzertifikate für den SPL-Truststore konfiguriert haben.
```

Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Vertrauensspeicher

Sie sollten das von der CA signierte Schlüsselpaar für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel
hinzu.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.
```

```
 keytool -list -v -keystore keystore.jks
. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem
neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt
wurde.
. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-
Zertifikat in das Schlüsselspeicherkennwort.
```

Das Standardkennwort für den SPL-Schlüsselspeicher ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der Datei spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Wenn der Aliasname im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen („*“, „,“) enthält, ändern Sie den Aliasnamen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in der
Datei spl.properties.
```

Aktualisieren Sie diesen Wert anhand des Schlüssels SPL_CERTIFICATE_ALIAS.

4. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL sucht in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SPL ist */var/opt/snapcenter/spl/etc/crl*.

Schritte

1. Sie können das Standardverzeichnis in der Datei spl.properties anhand des Schlüssels SPL_CRL_PATH ändern und aktualisieren.
2. Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen.

   Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss angezeigt und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- *  * zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-In-Host zugewiesen ist.
- *  * zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.
- *  * zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- *  * zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.