Installation und Konfiguration des Vscan-Servers

ONTAP 9

NetApp
September 12, 2024

Inhalt

Installation und Konfiguration des Vscan-Servers . . . 1
Installation und Konfiguration des Vscan-Servers . . . 1
Installieren Sie den ONTAP Antivirus Connector . . . 1
Konfigurieren Sie den ONTAP-Virenschutzanschluss . . . 4

Installation und Konfiguration des Vscan-Servers

Installation und Konfiguration des Vscan-Servers

Richten Sie einen oder mehrere Vscan-Server ein, um sicherzustellen, dass Dateien auf Ihrem System auf Viren gescannt werden. Befolgen Sie die Anweisungen Ihres Anbieters, um die Antivirensoftware auf dem Server zu installieren und zu konfigurieren.

Befolgen Sie die Anweisungen in der von NetApp bereitgestellten README-Datei, um den ONTAP Antivirus Connector zu installieren und zu konfigurieren. Befolgen Sie alternativ die Anweisungen auf der "Installieren Sie die Seite ONTAP Antivirus Connector".

> Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie separate Vscan-Server für die primären/lokalen und sekundären/Partner-ONTAP-Cluster einrichten und konfigurieren.

Anforderungen an die Virenschutz-Software

- Informationen zu den Anforderungen an Antivirensoftware finden Sie in der Dokumentation des Anbieters.
- Informationen über die von Vscan unterstützten Hersteller, Software und Versionen finden Sie auf der "Partnerlösungen von Vscan" Seite.

Anforderungen für den Antivirus Connector von ONTAP

- Sie können den ONTAP Antivirus Connector von der Seite **Software-Download** auf der NetApp Support-Website herunterladen. "NetApp Downloads: Software"
- Informationen zu den Windows-Versionen, die vom ONTAP Antivirus Connector unterstützt werden, sowie zu den Interoperabilitätsanforderungen finden Sie unter "Partnerlösungen von Vscan".

> Sie können verschiedene Versionen von Windows-Servern für verschiedene Vscan-Server in einem Cluster installieren.

- .NET 3.0 oder höher muss auf dem Windows-Server installiert sein.
- SMB 2.0 muss auf dem Windows Server aktiviert sein.

Installieren Sie den ONTAP Antivirus Connector

Installieren Sie den ONTAP-Virenschutzanschluss auf dem Vscan-Server, um die Kommunikation zwischen dem System, auf dem ONTAP ausgeführt wird, und dem Vscan-Server zu ermöglichen. Bei der Installation des ONTAP Antivirus Connectors kann die Virenschutzsoftware mit einer oder mehreren Storage Virtual Machines (SVMs) kommunizieren.

Über diese Aufgabe

- Auf der "Partnerlösungen von Vscan" Seite finden Sie Informationen zu den unterstützten Protokollen, Softwareversionen von Antivirenanbietern, ONTAP-Versionen, Interoperabilitätsanforderungen und Windows-Servern.
- .NET 4.5.1 oder höher muss installiert sein.

- Der ONTAP Antivirus Connector kann auf einer virtuellen Maschine ausgeführt werden. Um die beste Performance zu erzielen, empfiehlt NetApp jedoch die Verwendung einer dedizierten Virtual Machine für Virenschutzprüfungen.
- SMB 2.0 muss auf dem Windows-Server aktiviert sein, auf dem Sie den ONTAP-Antivirus-Connector installieren und ausführen.

Bevor Sie beginnen

- Laden Sie die Installationsdatei für den ONTAP Antivirus Connector von der Support-Website herunter und speichern Sie sie in einem Verzeichnis auf Ihrer Festplatte.
- Stellen Sie sicher, dass Sie die Anforderungen für die Installation des ONTAP-Virenschutzanschlusses erfüllen.
- Überprüfen Sie, ob Sie über Administratorrechte für die Installation des Antivirus Connectors verfügen.

Schritte

1. Starten Sie den Antivirus Connector-Installationsassistenten, indem Sie die entsprechende Setup-Datei ausführen.
2. Wählen Sie *Next*. Das Dialogfeld Zielordner wird geöffnet.
3. Wählen Sie *Next*, um den Antivirus Connector in dem Ordner zu installieren, der aufgelistet ist, oder wählen Sie *Change*, um ihn in einem anderen Ordner zu installieren.
4. Das Dialogfeld ONTAP AV-Connector Windows-Dienstanmeldeinformationen wird geöffnet.
5. Geben Sie Ihre Windows-Dienstanmeldeinformationen ein, oder wählen Sie **Hinzufügen**, um einen Benutzer auszuwählen. Bei einem ONTAP-System muss dieser Benutzer ein gültiger Domänenbenutzer sein und in der Scannerpoolkonfiguration für die SVM vorhanden sein.
6. Wählen Sie **Weiter**. Das Dialogfeld bereit zur Installation des Programms wird geöffnet.
7. Wählen Sie **Installieren**, um mit der Installation zu beginnen, oder wählen Sie **Zurück**, wenn Sie Änderungen an den Einstellungen vornehmen möchten. Ein Statusfeld wird geöffnet und zeigt den Fortschritt der Installation an, gefolgt vom Dialogfeld InstallShield Wizard abgeschlossen.
8. Aktivieren Sie das Kontrollkästchen ONTAP LIFs konfigurieren, wenn Sie mit der Konfiguration von ONTAP Management oder Daten-LIFs fortfahren möchten. Sie müssen mindestens eine ONTAP Management- oder Daten-LIF konfigurieren, bevor dieser Vscan-Server verwendet werden kann.
9. Aktivieren Sie das Kontrollkästchen Windows Installer-Protokoll anzeigen*, wenn Sie die Installationsprotokolle anzeigen möchten.
10. Wählen Sie **Fertig stellen**, um die Installation zu beenden und den InstallShield-Assistenten zu schließen. Das Symbol **Configure ONTAP LIFs** wird auf dem Desktop gespeichert, um die ONTAP LIFs zu konfigurieren.
11. Fügen Sie dem Antivirus Connector eine SVM hinzu. Sie können dem VirenschutzConnector eine SVM hinzufügen, indem Sie entweder eine ONTAP-Management-LIF hinzufügen, die zum Abrufen der Liste der Daten-LIFs abgefragt wird, oder die Daten-LIF oder LIFs direkt konfigurieren. Wenn die ONTAP Management LIF konfiguriert ist, müssen Sie außerdem die Abfrageinformationen und die Anmeldeinformationen des ONTAP Administratorkontos angeben.
    - Vergewissern Sie sich, dass die Management-LIF oder die IP-Adresse der SVM für aktiviert ist `management-https`. Dies ist nicht erforderlich, wenn Sie nur die Daten-LIFs konfigurieren.
    - Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das hat `/api/network/ip/interfaces` REST-API: Weitere Informationen zum Erstellen eines Benutzers finden Sie im "Rolle für Sicherheits-Login erstellen" Und "Sicherheits-Login erstellen" ONTAP-man-Pages.

> Sie können den Domänenbenutzer auch als Konto verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen. Weitere Informationen finden Sie im "Sicherheit Login Domain-Tunnel erstellen" ONTAP-man-Page verwenden oder `/api/security/acccounts` Und `/api/security/roles` REST-APIs zum Konfigurieren des Administratorkontos und der Rolle.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus.
2. Wählen Sie im Dialogfeld ONTAP LIFs konfigurieren den bevorzugten Konfigurationstyp aus und führen Sie dann die folgenden Aktionen durch:

Um diesen Typ von LIF zu erstellen…	Führen Sie diese Schritte aus…
Daten-LIF	a. „Rolle“ auf „Daten“ setzen b. Stellen Sie das „Datenprotokoll“ auf „cifs“ ein. c. Firewall-Richtlinie auf „Daten“ setzen d. Setzen Sie „Service Policy“ auf „default-Data-files“
Management-LIF	a. „Rolle* auf „Daten“ setzen b. Stellen Sie „Datenprotokoll“ auf „keine“ ein. c. Firewall-Richtlinie auf „Management“ setzen d. Service-Richtlinie auf Standardmanagement setzen

   Lesen Sie mehr über "Erstellen einer LIF".

   Nachdem Sie eine LIF erstellt haben, geben Sie die Daten- oder Management-LIF- oder IP-Adresse der hinzuzufügenden SVM ein. Sie können auch die Cluster-Management-LIF eingeben. Wenn Sie die Cluster-Management-LIF angeben, können alle SVMs innerhalb des Clusters, die SMB verwenden, den Vscan-Server verwenden.

   > Wenn Kerberos-Authentifizierung für Vscan-Server erforderlich ist, muss jede SVM-Daten-LIF über einen eindeutigen DNS-Namen verfügen. Sie müssen diesen Namen als Server-Principal-Name (SPN) im Windows Active Directory registrieren. Wenn für jede Daten-LIF kein eindeutiger DNS-Name verfügbar oder als SPN registriert ist, verwendet der Vscan-Server den NT LAN Manager-Mechanismus zur Authentifizierung. Wenn Sie die DNS-Namen und SPNs nach der Verbindung mit dem Vscan-Server hinzufügen oder ändern, müssen Sie den Antivirus Connector-Dienst auf dem Vscan-Server neu starten, um die Änderungen anzuwenden.

3. Geben Sie zum Konfigurieren einer Management-LIF die Abfragedauer in Sekunden ein. Die Abfragedauer ist die Häufigkeit, mit der der Antivirus Connector auf Änderungen an den SVMs oder der LIF-Konfiguration des Clusters prüft. Das standardmäßige Abfrageintervall beträgt 60 Sekunden.
4. Geben Sie den Namen und das Passwort des ONTAP Administratorkontos ein, um eine Management-LIF zu konfigurieren.

5. Klicken Sie auf **Test**, um die Verbindung zu überprüfen und die Authentifizierung zu überprüfen. Die Authentifizierung wird nur für eine Management-LIF-Konfiguration verifiziert.
6. Klicken Sie auf **Update**, um die LIF zur Liste der LIFs hinzuzufügen, zu denen Sie die Abfrage durchführen oder eine Verbindung herstellen möchten.
7. Klicken Sie auf **Speichern**, um die Verbindung zur Registrierung zu speichern.
8. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Siehe "Konfigurieren Sie die Seite ONTAP Antivirus Connector" Für Konfigurationsoptionen.

Konfigurieren Sie den ONTAP-Virenschutzanschluss

Konfigurieren Sie den ONTAP Antivirus Connector so, dass eine oder mehrere Storage Virtual Machines (SVMs) angegeben werden, zu denen Sie eine Verbindung herstellen möchten, indem Sie entweder die ONTAP Management-LIF eingeben, Abfrageinformationen und die Anmeldedaten des ONTAP Administratorkontos oder nur die Daten-LIF eingeben. Sie können auch die Details einer SVM-Verbindung ändern oder eine SVM-Verbindung entfernen. Standardmäßig verwendet der ONTAP Antivirus Connector REST-APIs, um die Liste der Daten-LIFs abzurufen, wenn die ONTAP Management-LIF konfiguriert ist.

Ändern Sie die Details einer SVM-Verbindung

Sie können die Details einer SVM-Verbindung (Storage Virtual Machine) aktualisieren, die dem VirenschutzConnector hinzugefügt wurde, indem Sie die ONTAP-Verwaltungs-LIF und die Abfrageinformationen ändern. Sie können die Daten-LIFs nicht aktualisieren, nachdem sie hinzugefügt wurden. Zum Aktualisieren der Daten-LIFs müssen Sie sie zunächst entfernen und sie dann erneut mit der neuen LIF oder IP-Adresse hinzufügen.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das hat `/api/network/ip/interfaces` REST-API: Weitere Informationen zum Erstellen eines Benutzers finden Sie im "Rolle für Sicherheits-Login erstellen" Und das "Sicherheits-Login erstellen" Befehle. Sie können den Domänenbenutzer auch als Konto verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen. Weitere Informationen finden Sie im "Sicherheit Login Domain-Tunnel erstellen" ONTAP-Hauptseite.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie die SVM-IP-Adresse aus, und klicken Sie dann auf **Update**.
3. Aktualisieren Sie die Informationen nach Bedarf.
4. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
5. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in einen Registry-Import oder eine Registry-Exportdatei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Entfernen Sie eine SVM-Verbindung aus dem Antivirus Connector

Wenn Sie keine SVM-Verbindung mehr benötigen, können Sie sie entfernen.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie eine oder mehrere SVM-IP-Adressen aus, und klicken Sie dann auf **Entfernen**.
3. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
4. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Fehlerbehebung

Bevor Sie beginnen

Wenn Sie in diesem Verfahren Registrierungswerte erstellen, verwenden Sie den rechten Fensterbereich.

Sie können Antivirus Connector-Protokolle für Diagnosezwecke aktivieren oder deaktivieren. Diese Protokolle sind standardmäßig deaktiviert. Um die Leistung zu verbessern, sollten Sie die Antivirus Connector-Protokolle deaktiviert halten und nur für kritische Ereignisse aktivieren.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann `regedit.exe` In der Liste Programme.
2. Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Erstellen Sie Registrierungswerte, indem Sie den Typ, den Namen und die Werte angeben, die in der folgenden Tabelle aufgeführt sind:

Typ	Name	Werte
Zeichenfolge	Tracepath	c:\avshim.log

   Dieser Registrierungswert kann jeder andere gültige Pfad sein.

4. Erstellen Sie einen weiteren Registrierungswert, indem Sie den Typ, den Namen, die Werte und die Protokollinformationen in der folgenden Tabelle angeben:

Typ	Name	Kritische Protokollierung	Zwischenprotokollierung	Ausführliche Protokollierung
DWORD	Tracelevel	1	2 oder 3	4

   Dadurch werden die Protokolle des Antivirus Connector aktiviert, die unter dem im TracePath in Schritt 3 angegebenen Pfadwert gespeichert werden.

5. Deaktivieren Sie Antivirus Connector-Protokolle, indem Sie die in Schritt 3 und 4 erstellten Registrierungswerte löschen.
6. Erstellen Sie einen weiteren Registrierungswert vom Typ "MULTI_SZ" mit dem Namen "LogRotation" (ohne Anführungszeichen). In „LogRotation“ Geben Sie „logFileSize:1“ als Eintrag für die Rotationsgröße an (wobei 1 für 1MB steht) und geben Sie in der nächsten Zeile „logFileCount:5“ als an an an Eingabe für Rotationsgrenze (5 ist die Grenze).

> Diese Werte sind optional. Wenn sie nicht angegeben werden, werden für die Rotationsgröße bzw. die Rotationsgrenze Standardwerte von 20MB und 10 Dateien verwendet. Die angegebenen Ganzzahlwerte enthalten keine Dezimalwerte oder Bruchwerte. Wenn Sie Werte angeben, die höher als die Standardwerte sind, werden stattdessen die Standardwerte verwendet.

7. Um die benutzerdefinierte Protokollrotation zu deaktivieren, löschen Sie die Registrierungswerte, die Sie in Schritt 6 erstellt haben.

Anpassbares Banner

Ein benutzerdefiniertes Banner ermöglicht es Ihnen, eine rechtsverbindliche Aussage und einen Haftungsausschluss für den Systemzugriff im Fenster *Configure ONTAP LIF API* zu platzieren.

Schritt

1. Ändern Sie das Standard-Banner, indem Sie den Inhalt im aktualisieren `banner.txt` Datei im Installationsverzeichnis speichern und dann die Änderungen speichern. Sie müssen das Fenster ONTAP LIF-API konfigurieren erneut öffnen, um die Änderungen im Banner anzuzeigen.

Aktivieren Sie den Modus Erweiterte Verordnung (EO)

Sie können den EO-Modus (Extended Ordinance) für einen sicheren Betrieb aktivieren und deaktivieren.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der Liste Programme.
2. Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Erstellen Sie im rechten Fensterbereich einen neuen Registrierungswert vom Typ "DWORD" mit dem Namen "EO_Mode" (ohne Anführungszeichen) und dem Wert "1" (ohne Anführungszeichen), um den EO-Modus zu aktivieren oder den Wert "0" (ohne Anführungszeichen), um den EO-Modus zu deaktivieren.

> Standardmäßig, wenn die `EO_Mode` Registrierungseintrag fehlt, EO-Modus ist deaktiviert. Wenn Sie den EO-Modus aktivieren, müssen Sie sowohl den externen Syslog-Server als auch die gegenseitige Zertifikatauthentifizierung konfigurieren.

Konfigurieren Sie den externen Syslog-Server

Bevor Sie beginnen

Beachten Sie, dass Sie beim Erstellen von Registrierungswerten in diesem Verfahren den rechten Fensterbereich verwenden.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der Liste Programme.
2. Erstellen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector für die Syslog-Konfiguration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Erstellen Sie einen Registrierungswert, indem Sie den Typ, den Namen und den Wert wie in der folgenden Tabelle dargestellt angeben:

Typ	Name	Wert
DWORD	Syslog_aktiviert	1 oder 0

   Bitte beachten Sie, dass ein Wert „1“ das Syslog aktiviert und mit einem Wert „0“ deaktiviert.

4. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Host

   Geben Sie die IP-Adresse oder den Domänennamen des Syslog-Hosts für das Wertfeld an.

5. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Port

   Geben Sie im Feld Wert die Portnummer an, auf der der Syslog-Server ausgeführt wird.

6. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Protocol

   Geben Sie das Protokoll, das auf dem Syslog-Server verwendet wird, entweder „tcp“ oder „udp“ in das Wertfeld ein.

7. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_Level	2	5	6	7

8. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	Wert
DWORD	Syslog_tls	1 oder 0

Bitte beachten Sie, dass ein Wert von „1“ Syslog mit Transport Layer Security (TLS) aktiviert und ein Wert von „0“ das Syslog mit TLS deaktiviert.

Stellen Sie sicher, dass ein konfigurierter externer Syslog-Server reibungslos ausgeführt wird

- Wenn der Schlüssel fehlt oder einen Nullwert hat:
  - Das Protokoll ist standardmäßig auf „tcp“ eingestellt.
  - Der Port ist standardmäßig auf "514" für einfaches "tcp/udp" und standardmäßig auf "6514" für TLS.
  - Die Syslog-Ebene ist standardmäßig auf 5 (LOG_NOTICE) eingestellt.
- Sie können bestätigen, dass Syslog aktiviert ist, indem Sie überprüfen, ob das aktiviert ist `syslog_enabled` Wert ist „1“. Wenn der `syslog_enabled` Der Wert ist „1“, Sie sollten sich beim konfigurierten Remote-Server anmelden können, unabhängig davon, ob der EO-Modus aktiviert ist.
- Wenn der EO-Modus auf „1“ eingestellt ist und Sie den ändern `syslog_enabled` Wert von „1“ bis „0“, gilt:
  - Sie können den Service nicht starten, wenn syslog im EO-Modus nicht aktiviert ist.
  - Wenn das System in einem stabilen Zustand ausgeführt wird, erscheint eine Warnung, die besagt, dass Syslog im EO-Modus nicht deaktiviert werden kann und syslog zwangsweise auf „1“ gesetzt ist, was Sie in der Registrierung sehen können. In diesem Fall sollten Sie zuerst den EO-Modus deaktivieren und dann syslog deaktivieren.
- Wenn der Syslog-Server bei Aktivierung von EO-Modus und Syslog nicht erfolgreich ausgeführt werden kann, wird der Dienst nicht mehr ausgeführt. Dies kann aus einem der folgenden Gründe auftreten:
  - Ein ungültiger oder kein syslog_Host ist konfiguriert.
  - Ein ungültiges Protokoll außer UDP oder TCP ist konfiguriert.
  - Eine Portnummer ist ungültig.
- Bei einer TCP- oder TLS-über-TCP-Konfiguration schlägt die Verbindung fehl, wenn der Server den IP-Port nicht abhört, und der Dienst wird heruntergefahren.

Konfigurieren Sie die Authentifizierung des gegenseitigen X.509-Zertifikats

X.509-zertifikatbasierte gegenseitige Authentifizierung ist für die SSL-Kommunikation (Secure Sockets Layer) zwischen dem Antivirus Connector und ONTAP im Verwaltungspfad möglich. Wenn der EO-Modus aktiviert ist und das Zertifikat nicht gefunden wird, wird der AV-Connector beendet. Führen Sie die folgenden Schritte auf dem Antivirus Connector durch:

Schritte

1. Der Antivirus Connector sucht nach dem Clientzertifikat des Virenschutzanschlusses und dem Zertifikat der Zertifizierungsstelle (CA) für den NetApp-Server im Verzeichnispfad, von dem aus der Virenschutzanschlussanschluss das Installationsverzeichnis ausführt. Kopieren Sie die Zertifikate in diesen festen Verzeichnispfad.
2. Betten Sie das Clientzertifikat und seinen privaten Schlüssel in das PKCS12-Format ein und benennen Sie

es mit „AV_Client.P12“.

3. Stellen Sie sicher, dass das zum Signieren des Zertifikats für den NetApp-Server verwendete Zertifizierungsstellenzertifikat (zusammen mit jeder Zwischenzertifizierungsstelle bis zur Stammzertifizierungsstelle) im PEM-Format (Privacy Enhanced Mail) mit dem Namen „ONTAP_CA.pem“ vorliegt. Platzieren Sie es im Installationsverzeichnis des Antivirus Connectors. Installieren Sie auf dem NetApp ONTAP-System das CA-Zertifikat (zusammen mit einer Zwischenzertifikationsberechtigung bis zur Stammzertifizierungsstelle), mit dem das Clientzertifikat für den Antivirus-Connector unter „ONTAP“ als Zertifikat vom Typ „Client-CA“ signiert wird.