Gestire i certificati

E-Series Systems

NetApp
March 22, 2024

Sommario

Gestire i certificati

Panoramica dei certificati

Gestione dei certificati nel plug-in di storage per vCenter consente di creare richieste di firma dei certificati (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Utilizzando Storage Plugin per vCenter, è possibile gestire i certificati per il browser su un sistema di gestione host e i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili.

Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

> Sebbene i certificati firmati dalla CA forniscano una migliore protezione di sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), richiedono anche tariffe che possono essere costose se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

Certificati firmati

Un certificato firmato viene convalidato da un'autorità di certificazione (CA), un'organizzazione di terze parti fidata. I certificati firmati includono i dettagli sul proprietario dell'entità (in genere, un server o un sito Web), la data di emissione e scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando si apre un browser e si inserisce un indirizzo Web, il sistema esegue un processo di verifica dei certificati in background per determinare se si sta effettuando la connessione a un sito Web che include un certificato valido firmato dalla CA. In genere, un sito protetto con un certificato firmato include un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se si tenta di connettersi a un sito Web che non contiene un certificato firmato dalla CA, il browser visualizza un avviso che indica che il sito non è sicuro.

La CA esegue le operazioni necessarie per verificare l'identità dell'utente durante il processo dell'applicazione. Potrebbero inviare un'e-mail all'azienda registrata, verificare l'indirizzo aziendale ed eseguire una verifica HTTP o DNS. Una volta completato il processo applicativo, la CA invia i file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di attendibilità, come segue:

- **Root** — nella parte superiore della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedio** — i certificati intermedi si disconnettono dalla radice. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.

- **Server** — nella parte inferiore della catena si trova il certificato del server, che identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di uno storage array richiede un certificato server separato.

Certificati autofirmati

Ogni controller dell'array di storage include un certificato preinstallato e autofirmato. Un certificato autofirmato è simile a un certificato firmato dalla CA, ad eccezione del fatto che è convalidato dal proprietario dell'entità anziché da una terza parte. Come un certificato firmato dalla CA, un certificato autofirmato contiene una propria chiave privata e garantisce inoltre che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client.

I certificati autofirmati non sono "attendibili" dai browser. Ogni volta che si tenta di connettersi a un sito Web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

Certificato di gestione

Quando si apre il plug-in, il browser tenta di verificare che l'host di gestione sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. È inoltre possibile ottenere certificati digitali firmati da una CA, in modo da non visualizzare più il messaggio di avviso.

Certificati attendibili

Durante una sessione di plug-in, potrebbero essere visualizzati ulteriori messaggi di sicurezza quando si tenta di accedere a un controller che non dispone di un certificato firmato dalla CA. In questo caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati dalla CA per i controller in modo che il plug-in possa autenticare le richieste dei client in entrata da questi controller.

USA certificati firmati dalla CA

È possibile ottenere e importare certificati con firma CA per un accesso sicuro al sistema di gestione che ospita lo Storage Plugin per vCenter.

L'utilizzo dei certificati firmati dalla CA è una procedura in tre fasi:

- Fase 1: Completare un file CSR.
- Fase 2: Inviare il file CSR.
- Fase 3: Importazione dei certificati di gestione.

Fase 1: Completare un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui è in esecuzione il plug-in. In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare il file CSR.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).

2. Dalla scheda **Gestione**, selezionare **completa CSR**.
3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città in cui si trova il sistema host o l'azienda.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova il sistema host o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.
4. Immettere le seguenti informazioni sul sistema host in cui è in esecuzione il plug-in:
   - **Nome comune** — l'indirizzo IP o il nome DNS del sistema host in cui è in esecuzione il plug-in. Assicurarsi che questo indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere al plug-in nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole.
   - **Nomi DNS alternativi** — se il nome comune è un nome DNS, immettere eventuali nomi DNS aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurarsi che le informazioni sull'host siano corrette. In caso contrario, i certificati restituiti dalla CA non avranno esito positivo quando si tenta di importarli.
6. Fare clic su **fine**.

Fase 2: Inviare il file CSR

Dopo aver creato un file CSR (Certificate Signing Request), il file CSR generato viene inviato a una CA per ricevere certificati di gestione firmati per il sistema che ospita il plug-in.

I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: .Pem, .crt, .cer o .key.

Fasi

1. Individuare il file CSR scaricato.

   La posizione della cartella del download dipende dal browser in uso.

2. Inviare il file CSR a una CA (ad esempio, VeriSign o DigiCert) e richiedere certificati firmati in formato PEM.

> Dopo aver inviato un file CSR alla CA, NON rigenerare un altro file CSR.

Ogni volta che si genera una CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi del sistema. Quando si ricevono i certificati firmati e li si importano, il sistema garantisce che sia la chiave privata che la chiave pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno ed è necessario richiedere nuovi certificati alla CA.

Fase 3: Importazione dei certificati di gestione

Una volta ricevuti i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui è installato il plug-in.

Prima di iniziare

- È necessario disporre dei certificati firmati dalla CA. Questi file includono il certificato di origine, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: Il certificato root, uno o più certificati intermedi e il certificato del server. È possibile utilizzare l'utility Windows certmgr per decomprimere i file (fare clic con il pulsante destro del mouse e selezionare **All Tasks › Export**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- È necessario copiare i file dei certificati nel sistema host in cui è in esecuzione il plug-in.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **Importa**.

   Viene visualizzata una finestra di dialogo per l'importazione dei file dei certificati.

3. Fare clic su **Browse** (Sfoglia) per selezionare prima i file dei certificati root e intermedi, quindi selezionare il certificato del server. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultato

I file vengono caricati e validati. Le informazioni sul certificato vengono visualizzate nella pagina Gestione certificati.

Reimpostare i certificati di gestione

Per il sistema di gestione che ospita lo Storage Plugin per vCenter, è possibile riportare il certificato di gestione allo stato originale autofirmato.

A proposito di questa attività

Questa attività elimina il certificato di gestione corrente dal sistema host in cui è in esecuzione Storage Plugin per vCenter. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Management**, selezionare **Reset**.

   Viene visualizzata la finestra di dialogo Conferma ripristino certificato di gestione.

3. Digitare reset nel campo, quindi fare clic su **Reset**.

   Dopo l'aggiornamento del browser, il browser potrebbe bloccare l'accesso al sito di destinazione e

segnalare che il sito utilizza HTTP Strict Transport Security. Questa condizione si verifica quando si torna ai certificati autofirmati. Per eliminare la condizione che sta bloccando l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultato

Il sistema torna a utilizzare il certificato autofirmato dal server. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Importare certificati per gli array

Se necessario, è possibile importare i certificati per gli array di storage in modo che possano autenticarsi con il sistema che ospita lo Storage Plugin per vCenter. I certificati possono essere firmati da un'autorità di certificazione (CA) o autofirmati.

Prima di iniziare

Se si importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.
4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

   Il certificato viene caricato e validato.

Visualizzare i certificati

È possibile visualizzare informazioni riepilogative per un certificato, che includono l'organizzazione che utilizza il certificato, l'autorità che ha emesso il certificato, il periodo di validità e le impronte digitali (identificatori univoci).

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.

3. Per visualizzare ulteriori informazioni su un certificato, selezionare la relativa riga, selezionare i puntini di sospensione alla fine della riga, quindi fare clic su **Visualizza** o **Esporta**.

Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

Prima di iniziare

Per aprire il file esportato, è necessario disporre di un'applicazione per il visualizzatore dei certificati.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Selezionare un certificato dalla pagina, quindi fare clic sui puntini di sospensione alla fine della riga.
4. Fare clic su **Esporta**, quindi salvare il file del certificato.
5. Aprire il file nell'applicazione di visualizzazione dei certificati.

Eliminare i certificati attendibili

È possibile eliminare uno o più certificati non più necessari, ad esempio un certificato scaduto.

Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.

> Tenere presente che l'eliminazione di un certificato root o intermedio può influire su più array di storage, poiché questi array possono condividere gli stessi file di certificato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.
3. Selezionare uno o più certificati nella tabella, quindi fare clic su **Elimina**.

   > La funzione Elimina non è disponibile per i certificati preinstallati.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

4. Confermare l'eliminazione, quindi fare clic su **Delete** (Elimina).

   Il certificato viene rimosso dalla tabella.

Risolvi i certificati non attendibili

Dalla pagina Certificate (certificato), è possibile risolvere i certificati non attendibili importando un certificato autofirmato dall'array di storage o importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

Prima di iniziare

Se si intende importare un certificato firmato dalla CA, assicurarsi che:

- È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
- La CA ha restituito file di certificato attendibili.
- I file dei certificati sono disponibili nel sistema locale.

A proposito di questa attività

I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura al plug-in, ma la connessione non viene confermata come sicura. Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti o revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.
4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

   Il certificato viene caricato e validato.