Utilizzare i certificati

SANtricity 11.8

NetApp
April 05, 2024

Sommario

Utilizzare i certificati . . . 1
USA certificati firmati CA per i controller . . . 1
Reimpostare i certificati di gestione . . . 3
Visualizzare le informazioni sul certificato importato . . . 4
Importare i certificati per i controller quando agiscono come client . . . 5
Attiva il controllo della revoca del certificato . . . 6
Eliminare i certificati attendibili . . . 6
Utilizzare i certificati firmati CA per l’autenticazione con un server di gestione delle chiavi . . . 7
Esportare i certificati del server di gestione delle chiavi . . . 9

Utilizzare i certificati

USA certificati firmati CA per i controller

È possibile ottenere certificati con firma CA per comunicazioni sicure tra i controller e il browser utilizzato per l'accesso a System Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o i nomi DNS di ciascun controller.

A proposito di questa attività

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

Fase 1: Completare gli CSR per i controller

È necessario innanzitutto generare un file CSR (Certificate Signing Request) per ciascun controller dell'array di storage.

A proposito di questa attività

Questa attività descrive come generare un file CSR da System Manager. La CSR fornisce informazioni sull'organizzazione e sull'indirizzo IP o il nome DNS del controller. Durante questa attività, viene generato un file CSR se l'array di storage ha un controller e due file CSR se ha due controller.

> In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare i file CSR.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Array Management (Gestione array), selezionare **complete CSR** (completa CSR).

   > Se viene visualizzata una finestra di dialogo che richiede di accettare un certificato autofirmato per il secondo controller, fare clic su **Accetta certificato autofirmato** per continuare.

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 tuo storage array o il tuo business.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova lo storage array o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.

> Alcuni campi potrebbero essere precompilati con le informazioni appropriate, ad esempio l'indirizzo IP del controller. Non modificare i valori prepopolati a meno che non si sia certi che siano errati. Ad esempio, se non è stata ancora completata una CSR, l'indirizzo IP del controller viene impostato su "localhost". In questo caso, è necessario modificare "localhost" con il nome DNS o l'indirizzo IP del controller.

4. Verificare o inserire le seguenti informazioni sul controller A nell'array di storage:
   - **Controller A common name** — per impostazione predefinita viene visualizzato l'indirizzo IP o il nome DNS del controller A. Assicurarsi che l'indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere a System Manager nel browser. Il nome DNS non può iniziare con un carattere jolly.
   - **Controller A alternate IP addresses** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il controller A. Per più voci, utilizzare un formato delimitato da virgole.
   - **Controller A alternate DNS Names** — se il nome comune è un nome DNS, inserire eventuali nomi DNS aggiuntivi per il controller A. 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. Se lo storage array dispone di un solo controller, il pulsante **Finish** è disponibile.

     Se lo storage array ha due controller, il pulsante **Next** (Avanti) è disponibile.

> Non fare clic sul collegamento **Ignora questo passaggio** quando si crea una richiesta CSR. Questo collegamento viene fornito in situazioni di ripristino degli errori. In rari casi, una richiesta CSR potrebbe non riuscire su un controller, ma non sull'altro. Questo collegamento consente di saltare la fase per la creazione di una richiesta CSR sul controller A, se già definita, e passare alla fase successiva per la creazione di una richiesta CSR sul controller B.

5. Se è presente un solo controller, fare clic su **fine**. Se sono presenti due controller, fare clic su **Avanti** per immettere le informazioni relative al controller B (come sopra), quindi fare clic su **fine**.

   Per un singolo controller, un file CSR viene scaricato nel sistema locale. Per i controller doppi, vengono scaricati due file CSR. La posizione della cartella del download dipende dal browser in uso.

6. Passare a. Fase 2: Inviare i file CSR.

Fase 2: Inviare i file CSR

Dopo aver creato i file CSR (Certificate Signing Request), inviare i file a un'autorità di certificazione (CA). 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 i file CSR scaricati.
2. Inviare i 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.

3. Quando la CA restituisce i certificati firmati, passare a. Fase 3: Importazione dei certificati firmati per i controller.

Fase 3: Importazione dei certificati firmati per i controller

Una volta ricevuti i certificati firmati dall'autorità di certificazione (CA), importare i file per i controller.

Prima di iniziare

- La CA ha restituito file di certificato firmati. Questi file includono il certificato root, uno o più certificati intermedi e i certificati 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 i certificati del server che identificano i controller. È possibile utilizzare Windows `certmgr` Utility per disimballare 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.
- I file dei certificati sono stati copiati nel sistema host in cui si accede a System Manager.

Fasi

1. Selezionare il **Impostazioni › certificati**
2. Dalla scheda Array Management (Gestione array), selezionare **Import** (Importa).

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

3. Fare clic sui pulsanti **Browse** per selezionare prima i file dei certificati principali e intermedi, quindi selezionare ciascun certificato server per i controller. I file root e intermedi sono gli stessi per entrambi i controller. Solo i certificati server sono univoci per ciascun controller. 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**.

   I file vengono caricati e validati.

Risultato

La sessione viene terminata automaticamente. Per rendere effettive le certificazioni, è necessario effettuare nuovamente l'accesso. Quando si effettua nuovamente l'accesso, vengono utilizzati i nuovi certificati firmati dalla CA per la sessione.

Reimpostare i certificati di gestione

È possibile ripristinare i certificati sui controller dall'utilizzo dei certificati firmati dalla CA ai

certificati autofirmati impostati in fabbrica.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati con FIRMA CA devono essere importati in precedenza.

A proposito di questa attività

La funzione Reset elimina i file di certificato firmati dalla CA corrente da ciascun controller. I controller torneranno quindi a utilizzare certificati autofirmati.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Array Management (Gestione array), selezionare **Reset** (Ripristina).

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

3. Tipo `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.

Risultati

I controller tornano a utilizzare certificati autofirmati. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Visualizzare le informazioni sul certificato importato

Dalla pagina certificati, è possibile visualizzare il tipo di certificato, l'autorità di emissione e l'intervallo di date valido dei certificati per l'array di storage.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare una delle schede per visualizzare le informazioni relative ai certificati.

Scheda	Descrizione
Gestione degli array	Visualizzare le informazioni sui certificati firmati dalla CA importati per ciascun controller, inclusi il file root, i file intermedi e i file server.

Scheda	Descrizione
Affidabile	Visualizza le informazioni su tutti gli altri tipi di certificati importati per i controller. Utilizzare il campo del filtro sotto **Mostra certificati…** per visualizzare i certificati installati dall'utente o preinstallati. • **Installato dall'utente** — certificati caricati da un utente nell'array di storage, che possono includere certificati attendibili quando il controller agisce come client (anziché come server), certificati LDAPS e certificati Identity Federation. • **Preinstallati** — certificati autofirmati inclusi con lo storage array.
Gestione delle chiavi	Consente di visualizzare informazioni sui certificati firmati dalla CA importati per un server di gestione delle chiavi esterno.

Importare i certificati per i controller quando agiscono come client

Se il controller rifiuta una connessione perché non è in grado di convalidare la catena di trust per un server di rete, è possibile importare un certificato dalla scheda Trusted che consente al controller (che agisce come client) di accettare le comunicazioni da quel server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I file dei certificati vengono installati nel sistema locale.

A proposito di questa attività

Se si desidera consentire a un altro server di contattare i controller (ad esempio, un server LDAP o un server syslog che utilizza TLS), potrebbe essere necessario importare i certificati dalla scheda Trusted.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Trusted (attendibile), selezionare **Import** (Importa).

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

3. Fare clic su **Browse** (Sfoglia) per selezionare i file di certificato per i controller.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultati

I file vengono caricati e validati.

Attiva il controllo della revoca del certificato

È possibile attivare i controlli automatici dei certificati revocati, in modo che un server OCSP (Online Certificate Status Protocol) blocchi gli utenti da connessioni non sicure.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Su entrambi i controller viene configurato un server DNS, che consente di utilizzare un nome di dominio completo per il server OCSP. Questa attività è disponibile nella pagina hardware.
- Se si desidera specificare il proprio server OCSP, è necessario conoscere l'URL di tale server.

A proposito di questa attività

Il controllo automatico della revoca è utile nei casi in cui la CA ha emesso un certificato in modo errato o una chiave privata è compromessa.

Durante questa attività, è possibile configurare un server OCSP o utilizzare il server specificato nel file del certificato. Il server OCSP determina se la CA ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un sito se il certificato viene revocato.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   È inoltre possibile attivare il controllo delle revoche dalla scheda **Gestione chiavi**.

3. Fare clic su **attività non comuni**, quindi selezionare **attiva verifica revoca** dal menu a discesa.
4. Selezionare **i want to enable revocation checking**, in modo che nella casella di controllo venga visualizzato un segno di spunta e che nella finestra di dialogo vengano visualizzati altri campi.
5. Nel campo **OCSP responder address** (Indirizzo responder OCSP), è possibile inserire un URL per un server responder OCSP. Se non si immette un indirizzo, il sistema utilizza l'URL del server OCSP dal file del certificato.
6. Fare clic su **Test Address** per verificare che il sistema possa stabilire una connessione all'URL specificato.
7. Fare clic su **Save** (Salva).

Risultati

Se lo storage array tenta di connettersi a un server con un certificato revocato, la connessione viene negata e viene registrato un evento.

Eliminare i certificati attendibili

È possibile eliminare i certificati installati dall'utente precedentemente importati dalla scheda Trusted.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

- Se si sta aggiornando un certificato attendibile con una nuova versione, il certificato aggiornato deve essere importato prima di eliminare il vecchio certificato.

> Prima di importare un certificato sostitutivo, si potrebbe perdere l'accesso a un sistema se si elimina un certificato utilizzato per autenticare i controller e un altro server, ad esempio un server LDAP.

A proposito di questa attività

Questa attività descrive come eliminare i certificati installati dall'utente. I certificati autofirmati preinstallati non possono essere cancellati.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   La tabella mostra i certificati attendibili dell'array di storage.

3. Nella tabella, selezionare il certificato che si desidera rimuovere.
4. Fare clic sul **attività non comuni › Elimina**.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

5. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

Utilizzare i certificati firmati CA per l'autenticazione con un server di gestione delle chiavi

Per comunicazioni sicure tra un server di gestione delle chiavi e i controller degli array di storage, è necessario configurare i set di certificati appropriati.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

L'autenticazione tra i controller e un server di gestione delle chiavi è una procedura in due fasi.

Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi

È necessario innanzitutto generare un file CSR (Certificate Signing Request), quindi utilizzare la CSR per richiedere un certificato client firmato a un'autorità di certificazione (CA) attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).

Fasi

1. Selezionare il **Impostazioni › certificati**.

2. Dalla scheda Key Management (Gestione chiavi), selezionare **complete CSR** (completa CSR).
3. Inserire le seguenti informazioni:
   - **Nome comune** — un nome che identifica questa CSR, ad esempio il nome dell'array di storage, che verrà visualizzato nei file di certificato.
   - **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 o la località in cui si trova l'organizzazione.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova l'organizzazione.
   - **Codice ISO Paese** — Codice ISO (International Organization for Standardization) a due cifre, ad esempio USA, in cui si trova l'organizzazione.
4. Fare clic su **Download**.

   Un file CSR viene salvato nel sistema locale.

5. Richiedere un certificato client firmato a una CA attendibile dal server di gestione delle chiavi.
6. Se si dispone di un certificato client, visitare il sito Web all'indirizzo Fase 2: Importazione dei certificati per il server di gestione delle chiavi.

Fase 2: Importazione dei certificati per il server di gestione delle chiavi

Come fase successiva, importare i certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Esistono due tipi di certificati: Il certificato client convalida i controller dello storage array, mentre il certificato del server di gestione delle chiavi convalida il server. È necessario caricare sia il file di certificato del client per i controller che il file di certificato del server per il server di gestione delle chiavi.

Prima di iniziare

- Si dispone di un file di certificato client firmato (vedere Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi) Ed è stato copiato sull'host in cui si accede a System Manager. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al server di gestione delle chiavi.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Key Management (Gestione chiavi), selezionare **Import** (Importa).

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

3. Accanto a **Select client certificate** (Seleziona certificato client), fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato client per i controller dell'array di storage.

Il nome del file viene visualizzato nella finestra di dialogo.

4. Accanto a **Select key management server's server certificate**, fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato del server per il server di gestione delle chiavi. È possibile scegliere un certificato root, intermedio o server per il server di gestione delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

5. Fare clic su **Importa**.

   I file vengono caricati e validati.

Esportare i certificati del server di gestione delle chiavi

È possibile salvare un certificato per un server di gestione delle chiavi nel computer locale.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati devono essere importati in precedenza.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Key Management** (Gestione chiavi).
3. Dalla tabella, selezionare il certificato che si desidera esportare, quindi fare clic su **Esporta**.

   Viene visualizzata la finestra di dialogo Save (Salva).

4. Inserire un nome file e fare clic su **Save** (Salva).