Certificati

SANtricity 11.6

NetApp
February 12, 2024

Sommario

Certificati

Concetti

Come funzionano i certificati

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet.

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con System Manager è possibile gestire i certificati tra il browser di un sistema di gestione host (che funge da client) e i controller di un sistema storage (che funge da server).

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 diramano 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. Tuttavia, un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA.

I certificati autofirmati non sono "trusted" 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.

Certificati utilizzati per il server di gestione delle chiavi

Se si utilizza un server di gestione delle chiavi esterno con la funzione Drive Security, è anche possibile gestire i certificati per l'autenticazione tra il server e i controller.

Terminologia del certificato

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per il rilascio di un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
Catena di certificati	Gerarchia di file che aggiunge un livello di protezione ai certificati. In genere, la catena include un certificato root nella parte superiore della gerarchia, uno o più certificati intermedi e i certificati server che identificano le entità.
Certificato del client	Per la gestione delle chiavi di sicurezza, un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa fidarsi dei propri indirizzi IP.
Certificato intermedio	Uno o più certificati intermedi si diramano dalla directory principale nella catena di certificati. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.

Termine	Descrizione
Certificato del server di gestione delle chiavi	Per la gestione delle chiavi di sicurezza, un certificato del server di gestione delle chiavi convalida il server, in modo che lo storage array possa fidarsi del proprio indirizzo IP.
Archivio chiavi	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle chiavi pubbliche e ai certificati corrispondenti. Queste chiavi e certificati identificano le proprie entità, ad esempio i controller.
Server OCSP	Il server OCSP (Online Certificate Status Protocol) determina se l'autorità di certificazione (CA) ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un server se il certificato viene revocato.
Certificato root	Il certificato root si trova nella parte superiore della gerarchia nella catena del certificato e 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.
Certificato firmato	Certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include i dettagli relativi al proprietario dell'entità (in genere, un server o un sito Web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di trust e quindi viene utilizzato più spesso negli ambienti di produzione. Definito anche "certificato firmato da CA" o "certificato di gestione".
Certificato autofirmato	Un certificato autofirmato viene validato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA e, di conseguenza, viene spesso utilizzato negli ambienti di test. Detto anche certificato "preinstallato".
Certificato del server	Il certificato del server si trova nella parte inferiore della catena di certificati. Identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di un sistema storage richiede un certificato server separato.

Come fare

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.

A proposito di questa attività

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

Fase 1: Completare e inviare una CSR per i controller

È necessario innanzitutto generare un file CSR (Certificate Signing Request) per ciascun controller nell'array di storage, quindi inviare i file a un'autorità di certificazione (CA).

Prima di iniziare

- È necessario conoscere l'indirizzo IP o il nome DNS di ciascun controller.

A proposito di questa attività

La CSR fornisce informazioni sull'organizzazione, l'indirizzo IP o il nome DNS del controller e una coppia di chiavi che identifica il server Web nel controller. Durante questa attività, viene generato un file CSR se nell'array di storage è presente un solo controller e due file CSR se sono presenti due controller.

> Non generare una nuova CSR dopo l'invio alla CA. Quando si genera una CSR, il sistema crea una coppia di chiavi private e pubbliche. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi. Quando si ricevono i certificati firmati e li si importano nel keystore, il sistema garantisce che sia le chiavi private che quelle pubbliche siano la coppia originale. Pertanto, non è necessario generare una nuova CSR dopo averla inoltrata alla CA. In tal caso, i controller generano nuove chiavi e i certificati ricevuti dalla CA non funzioneranno.

Fasi

1. Selezionare **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.

- **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. 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. Individuare i file CSR scaricati. La posizione della cartella dipende dal browser.
7. Inviare i file CSR a una CA e richiedere i certificati firmati in formato PEM.
8. Attendere che la CA restituisca i certificati, quindi passare a. Fase 2: Importazione dei certificati firmati per i controller.

Fase 2: Importazione dei certificati firmati per i controller

Una volta ricevuti i certificati firmati, vengono importati i file per i controller.

Prima di iniziare

- La CA ha restituito file di certificato firmati.
- I file sono disponibili sul sistema locale.
- Se la CA ha fornito un 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 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 **tutte le attività › Esporta**). Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.

A proposito di questa attività

Questa attività descrive come caricare i file dei certificati.

Fasi

1. Selezionare **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 root 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.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

   I file vengono caricati e validati.

Risultati

La sessione viene terminata automaticamente. È necessario effettuare nuovamente l'accesso affinché i certificati abbiano effetto. Quando si effettua nuovamente l'accesso, per la sessione viene utilizzato il nuovo certificato firmato dalla CA.

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

   Viene visualizzata la finestra di dialogo Conferma **Ripristina 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.
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. • **Preinstallato**. 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 **Impostazioni › certificati**.
2. Dalla scheda **Trusted**, 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 **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 **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 su **operazioni 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.

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

Questa attività descrive come generare il file CSR, che verrà utilizzato per richiedere un certificato client firmato a una CA attendibile dal server di gestione delle chiavi. 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). Durante questa attività, è necessario fornire informazioni sull'organizzazione.

Fasi

1. Selezionare **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.

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.
- 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 il file di certificato del server 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.

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

A proposito di questa attività

Questa attività descrive come caricare i file di certificato per l'autenticazione tra i controller degli array di storage e il server di gestione delle chiavi. 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.

Fasi

1. Selezionare **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.

   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 **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).

FAQ

Perché viene visualizzata la finestra di dialogo Impossibile accedere ad altri controller?

Quando si eseguono determinate operazioni relative ai certificati CA (ad esempio, l'importazione di un certificato), potrebbe essere visualizzata una finestra di dialogo che richiede di accettare un certificato autofirmato per il secondo controller.

Negli array di storage con due controller (configurazioni duplex), questa finestra di dialogo viene talvolta visualizzata se Gestione sistema SANtricity non riesce a comunicare con il secondo controller o se il browser non può accettare il certificato durante un determinato momento di un'operazione.

Se viene visualizzata questa finestra di dialogo, fare clic su **Accetta certificato autofirmato** per continuare. Se viene richiesta una password da un'altra finestra di dialogo, immettere la password dell'amministratore utilizzata per accedere a System Manager.

Se questa finestra di dialogo viene visualizzata di nuovo e non è possibile completare un'attività di certificazione, provare una delle seguenti procedure:

- Utilizzare un tipo di browser diverso per accedere a questo controller, accettare il certificato e continuare.
- Accedere al secondo controller con System Manager, accettare il certificato autofirmato, quindi tornare al primo controller e continuare.

Come è possibile sapere quali certificati devono essere caricati in System Manager per la gestione esterna delle chiavi?

Per la gestione esterna delle chiavi, vengono importati due tipi di certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi in modo che le due entità possano fidarsi l'una dell'altra.

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). Per ottenere un certificato client, utilizzare System Manager per completare una CSR per lo storage array. È quindi possibile caricare la CSR su un server di gestione delle chiavi e generare un certificato client da tale server. Una volta ottenuto un certificato client, copiare il file 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. Recuperare il file di certificato del server dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager.

Cosa devo sapere sulla verifica della revoca dei certificati?

System Manager consente di controllare i certificati revocati utilizzando un server OCSP (Online Certificate Status Protocol), invece di caricare gli elenchi di revoca dei certificati (CRL).

I certificati revocati non devono più essere attendibili. Un certificato potrebbe essere revocato per diversi motivi; ad esempio, se l'autorità di certificazione (CA) ha emesso il certificato in modo errato, una chiave privata è stata compromessa o l'entità identificata non è conforme ai requisiti dei criteri.

Dopo aver stabilito una connessione a un server OCSP in Gestione sistema, lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog. Lo storage array tenta di validare i certificati di questi server per assicurarsi che non siano stati revocati. Il server restituisce quindi il valore "buono", "revocato" o "sconosciuto" per il certificato. Se il certificato viene revocato o l'array non riesce a contattare il server OCSP, la connessione viene rifiutata.

> Se si specifica un indirizzo del responder OCSP in System Manager o nell'interfaccia della riga di comando (CLI), l'indirizzo OCSP trovato nel file del certificato viene sovrascritta.

Per quali tipi di server verrà attivato il controllo delle revoche?

Lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog.