Certificati

SANtricity 11.5

NetApp
February 12, 2024

Sommario

Certificati

Concetti

Come funzionano i certificati CA

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.

Quando si apre un browser e si tenta di connettersi a System Manager tramite la porta di gestione del controller, il browser tenta di verificare che il controller dell'array di storage sia un'origine attendibile. Se il browser non riesce a individuare un certificato digitale per il controller, avvisa l'utente che il certificato non è firmato da un'autorità riconosciuta e chiede se si desidera continuare. Se non si desidera più visualizzare questo avviso, è necessario ottenere un certificato digitale firmato da una CA.

Se si utilizza un server di gestione delle chiavi esterno con la funzione Drive Security, è anche possibile creare certificati per l'autenticazione tra il server e i controller oppure accettare i certificati autofirmati dall'array di storage.

Per utilizzare un certificato digitale di un'autorità fidata, è necessario attenersi alla seguente procedura:

1. Accedere al **Impostazioni › certificati**. L'accesso utente deve includere le autorizzazioni Security Admin; in caso contrario, **Certificates** non viene visualizzato nella pagina.
2. Creare una CSR (Certificate Signing Request) per ciascun controller o per un server di gestione delle chiavi.
3. Inviare i file .CSR a una CA, quindi attendere l'invio dei certificati.
4. Importare il certificato attendibile (intermedio e root) dalla CA. Questi certificati stabiliscono un punto di trust per una gerarchia CA.
5. Importare i certificati di gestione firmati per ciascun controller o server di gestione delle chiavi.

Terminologia del certificato

Scopri in che modo i termini del certificato si applicano al tuo array di storage.

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.

Termine	Descrizione
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.
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 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.
Certificato di gestione	Un certificato di gestione viene approvato da un'autorità di certificazione (CA) e consente un accesso sicuro all'applicazione Web. Definito anche "certificato firmato".
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 autofirmato	Un certificato autofirmato è precaricato sul controller. Se la connessione al sito è autofirmata, viene visualizzato un messaggio di avviso prima di procedere con l'applicazione Web.
Certificato attendibile	Un certificato attendibile di un'autorità di certificazione (CA) è un certificato noto nella parte superiore della gerarchia di certificati. Definito anche "certificato root".

Come fare

Completare una richiesta di firma del certificato CA (CSR) per i controller

Per ricevere un certificato di autorità di certificazione (CA) per i controller dell'array di storage, è necessario innanzitutto generare un file CSR (Certificate Signing Request) per ciascun controller dell'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.

A proposito di questa attività

Questa attività descrive come generare i file .CSR (richieste di firma del certificato) inviati a una CA per ricevere certificati di gestione firmati per i controller. È necessario fornire informazioni sull'organizzazione, oltre all'indirizzo IP o al nome DNS dei 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.

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

6. Inviare i file .CSR alla CA.

Al termine

Quando si ricevono i certificati digitali, importare i file di certificato appropriati inviati dalla CA.

Importazione di certificati attendibili per i controller

Dopo aver ricevuto i certificati digitali da un'autorità di certificazione (CA), è possibile importare la catena di certificati (intermedia e principale) per i controller.

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 stata generata una richiesta di firma del certificato (file CSR) e inviata alla CA.
- La CA ha restituito file di certificato attendibili.
- I file dei certificati vengono installati nel sistema locale.

A proposito di questa attività

Questa attività descrive come caricare i certificati attendibili per i controller dell'array di storage.

Fasi

1. Selezionare il **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.

Al termine

Importare il certificato di gestione.

Importare un certificato di gestione per i controller

Dopo aver importato la catena di certificati attendibili, viene importato un file di certificati di gestione (firmato) per ciascun controller nell'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.
- I certificati attendibili sono stati importati.
- La CA ha restituito un file di certificato di gestione per ciascun controller.
- I file dei certificati di gestione sono disponibili sul sistema locale.

A proposito di questa attività

Questa attività descrive come caricare i file dei certificati di gestione per l'autenticazione del controller.

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 su **Browse** (Sfoglia) per selezionare il file per il controller A. Se sono presenti due controller, fare clic sul secondo pulsante **Sfoglia** per selezionare il file per il controller B.

   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.

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 importati in precedenza.

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 visualizzare le informazioni relative ai certificati installati dall'utente o preinstallati.

Fasi

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

2. Selezionare una delle schede per visualizzare informazioni sui certificati di gestione per i controller, i certificati attendibili e i certificati per un server di gestione delle chiavi.

Scheda	Descrizione
Gestione degli array	Visualizza informazioni su tutti i certificati server importati per i controller.
Affidabile	Visualizza informazioni su tutti i certificati attendibili (root) 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 (inclusi certificati attendibili, certificati LDAPS e certificati Identity Federation). • **Preinstallato**. Certificati inclusi con lo storage array.
Gestione delle chiavi	Visualizza informazioni su tutti i certificati di gestione (firmati) importati per un server di gestione delle chiavi esterno.

Eliminare i certificati attendibili

È possibile eliminare qualsiasi certificato importato dall'utente.

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.

> Se si elimina un certificato utilizzato per autenticare i certificati di gestione dell'array di storage o il server LDAP, si potrebbe perdere l'accesso al sistema prima di importare un certificato sostitutivo.

A proposito di questa attività

Questa attività descrive come eliminare i certificati importati dall'utente. Impossibile eliminare i certificati predefiniti.

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).

Reimpostare i certificati di gestione

È possibile riportare i certificati di gestione sull'array di storage allo stato autofirmato di 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 devono essere importati in precedenza.

A proposito di questa attività

La reimpostazione dei certificati di gestione sullo storage array elimina i certificati di gestione correnti da ciascuno dei controller. Una volta ripristinati i certificati, i controller tornano 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 e fare clic su **Reset**.

Risultati

Dopo l'aggiornamento del browser, i controller tornano a utilizzare certificati autofirmati. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Completare la richiesta di firma del certificato CA (CSR) per un server delle chiavi

Per ricevere un certificato di autorità di certificazione (CA) per un server di gestione delle chiavi, è necessario innanzitutto generare un file CSR (Certificate Signing Request).

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 i file .CSR (richieste di firma del certificato) inviati a una CA per ricevere i certificati firmati per un server di gestione delle chiavi. Durante questa attività, è necessario fornire informazioni sull'organizzazione.

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. Inviare i file .CSR alla CA.

Al termine

Quando si ottengono i certificati client e server dal server di gestione delle chiavi, importarli per l'autenticazione con i controller degli array di storage.

Importazione dei certificati del server di gestione delle chiavi

Per la gestione esterna delle chiavi, si importano 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. Esistono due tipi di certificati: Il certificato client convalida i controller, 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.
- È disponibile un certificato client per lo storage array.

  Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili i propri indirizzi IP. Per ottenere un certificato client, è necessario completare una CSR per l'array di storage e caricarla sul server di gestione delle chiavi. Dal server, generare un certificato client.

- Il certificato del server di gestione delle chiavi è disponibile.

  Un certificato del server di gestione delle chiavi convalida il server, in modo che lo storage array possa fidarsi del proprio indirizzo IP. Per ottenere un certificato del server di gestione delle chiavi, è necessario generarlo dal 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.

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. Fare clic sui pulsanti **Browse** per selezionare i file.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. 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).

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. Il controllo automatico della revoca è utile nei casi in cui l'autorità di certificazione (CA) ha emesso un certificato in modo errato o se una chiave privata è compromessa.

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

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 Key Management (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).

Risultato

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

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, 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 i propri indirizzi IP. Per ottenere un certificato client, è necessario completare una CSR per l'array di storage e caricarla sul server di gestione delle chiavi. Dal server, generare un certificato client, quindi utilizzare System Manager per importarlo.

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 ottenere un certificato del server di gestione delle chiavi, è necessario generarlo dal server di gestione delle chiavi.

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.