Gestione dei certificati di sicurezza

Active IQ Unified Manager 9.9

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-99/online-help/task-viewing-the-https-security-certificate-ocf.html on January 31, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestione dei certificati di sicurezza 1
Visualizzazione del certificato di protezione HTTPS 1
Generazione di un certificato di protezione HTTPS 1
Download di una richiesta di firma del certificato HTTPS 3
Installazione di un certificato HTTPS firmato e restituito dalla CA 4
Installazione di un certificato HTTPS generato utilizzando strumenti esterni 5
Descrizioni delle pagine per la gestione dei certificati 7

Gestione dei certificati di sicurezza

È possibile configurare HTTPS nel server Unified Manager per monitorare e gestire i cluster su una connessione sicura.

Visualizzazione del certificato di protezione HTTPS

È possibile confrontare i dettagli del certificato HTTPS con il certificato recuperato nel browser per garantire che la connessione crittografata del browser a Unified Manager non venga intercettata.

Prima di iniziare

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

A proposito di questa attività

La visualizzazione del certificato consente di verificare il contenuto di un certificato rigenerato o di visualizzare i nomi Alt (SAN) del soggetto da cui è possibile accedere a Unified Manager.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.

   Il certificato HTTPS viene visualizzato nella parte superiore della pagina

Al termine

Per visualizzare informazioni più dettagliate sul certificato di protezione rispetto a quelle visualizzate nella pagina del certificato HTTPS, è possibile visualizzare il certificato di connessione nel browser.

Generazione di un certificato di protezione HTTPS

Quando Active IQ Unified Manager viene installato per la prima volta, viene installato un certificato HTTPS predefinito. È possibile generare un nuovo certificato di protezione HTTPS che sostituisce il certificato esistente.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Possono esserci diversi motivi per rigenerare il certificato, ad esempio se si desidera ottenere valori migliori per Nome distinto (DN) o se si desidera una dimensione della chiave più elevata o un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non si dispone dell'accesso all'interfaccia utente Web di Unified Manager, è possibile rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, è

possibile definire la dimensione della chiave e la durata della validità della chiave. Se si utilizza `Reset Server Certificate` Dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo certificato avrà una chiave RSA di 2048 bit.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Rigenera certificato HTTPS**.

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Selezionare una delle seguenti opzioni a seconda della modalità di generazione del certificato:

Se si desidera…	Eseguire questa operazione…
Rigenera il certificato con i valori correnti	Fare clic sull'opzione **Rigenera using Current Certificate Attributes**.
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione **Update the Current Certificate Attributes** (Aggiorna attributi del certificato corrente). I campi Nome comune e nomi alternativi utilizzano i valori del certificato esistente se non vengono immessi nuovi valori. Il campo "Common Name" deve essere impostato sull'FQDN dell'host. Gli altri campi non richiedono valori, ma è possibile inserire valori, ad esempio, per L'EMAIL, LA SOCIETÀ, IL REPARTO, Città, Stato e Paese se si desidera inserire tali valori nel certificato. È inoltre possibile selezionare una DELLE DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA"). E PERIODO di validità. • I valori consentiti per la dimensione della chiave sono `2048`, `3072` e. `4096`. • I periodi di validità vanno da un minimo di 1 giorno a un massimo di 36500 giorni. Anche se è consentito un periodo di validità di 36500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se si seleziona un periodo di validità superiore a 397 giorni e si prevede di esportare una CSR per questo certificato e di ottenerla firmata da una CA nota, la validità del certificato firmato restituito dalla CA sarà ridotta a 397 giorni. • Selezionare la casella di controllo "Escludi informazioni di identificazione locali" se si desidera rimuovere le informazioni di identificazione locali dal campo dei nomi alternativi del certificato. Quando questa casella di controllo è selezionata, nel campo nomi alternativi viene utilizzato solo il valore immesso nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

1. Fare clic su **Sì** per rigenerare il certificato.

2. Riavviare il server Unified Manager in modo che il nuovo certificato abbia effetto.

Al termine

Verificare le informazioni sul nuovo certificato visualizzando il certificato HTTPS.

Riavvio della macchina virtuale di Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. Riavviare dopo aver generato un nuovo certificato di protezione o in caso di problemi con la macchina virtuale.

Prima di iniziare

L'appliance virtuale è accesa.

Si è connessi alla console di manutenzione come utente di manutenzione.

A proposito di questa attività

È inoltre possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione **Restart Guest**. Per ulteriori informazioni, consultare la documentazione di VMware.

Fasi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione del sistema** > **riavvio della macchina virtuale**.

Download di una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per il certificato di protezione HTTPS corrente in modo da fornire il file a un'autorità di certificazione da firmare. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Scarica richiesta firma certificato HTTPS**.
3. Salvare `<hostname>.csr` file.

Al termine

È possibile fornire il file a un'autorità di certificazione per firmare e installare il certificato firmato.

Installazione di un certificato HTTPS firmato e restituito dalla CA

È possibile caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il file caricato e installato deve essere una versione firmata del certificato autofirmato esistente. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Prima di iniziare

È necessario aver completato le seguenti operazioni:

- Il file Certificate Signing Request è stato scaricato e firmato da un'autorità di certificazione
- La catena di certificati è stata salvata in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma root, inclusi eventuali certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Se la validità del certificato per il quale è stata creata una CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima della firma e della restituzione del certificato

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Installa certificato HTTPS**.
3. Nella finestra di dialogo visualizzata, fare clic su **Scegli file…** per individuare il file da caricare.
4. Selezionare il file, quindi fare clic su **Installa** per installarlo.

   Per ulteriori informazioni, vedere "Installazione di un certificato HTTPS generato utilizzando strumenti esterni"

Esempio di catena di certificati

Nell'esempio seguente viene illustrato come potrebbe essere visualizzato il file di catena del certificato:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Installazione di un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare i certificati autofirmati o con firma CA e generati utilizzando uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

È necessario caricare la chiave privata insieme alla catena di certificati, poiché questi certificati sono coppia di chiavi pubbliche e private generate esternamente. Gli algoritmi di coppia di chiavi consentiti sono “RSA” e “EC”. L’opzione **Installa certificato HTTPS** è disponibile nella pagina certificati HTTPS nella sezione Generale. Il file caricato deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all’host Active IQ UM
2. Certificato del server che corrisponde alla chiave privata
3. Certificato delle CA invertito fino alla root, che vengono utilizzate per firmare il certificato di cui sopra

Formato per il caricamento di un certificato con una coppia di chiavi EC

Le curve consentite sono “prime256v1” e “secp384r1”. Esempio di certificato con una coppia EC generata esternamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Formato per il caricamento di un certificato con una coppia di chiavi RSA

Le dimensioni delle chiavi consentite per la coppia di chiavi RSA appartenente al certificato host sono 2048, 3072 e 4096. Certificato con una coppia di chiavi * RSA generata esternamente*:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Una volta caricato il certificato, riavviare l'istanza di Active IQ Unified Manager per rendere effettive le modifiche.

Verifica durante il caricamento dei certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato mediante strumenti esterni. Se uno dei controlli non riesce, il certificato viene rifiutato. Sono incluse anche le validazioni per i certificati generati dalla CSR all'interno del prodotto e per i certificati generati utilizzando strumenti esterni.

- La chiave privata nell'input viene convalidata in base al certificato host nell'input.
- Il nome comune (CN) nel certificato host viene verificato in base all'FQDN dell'host.

- Il nome comune (CN) del certificato host non deve essere vuoto o vuoto e non deve essere impostato su localhost.
- La data di inizio della validità non deve essere futura e la data di scadenza del certificato non deve essere passata.
- Se esiste una CA o una CA intermedia, la data di inizio della validità del certificato non deve essere futura e la data di scadenza della validità non deve essere passata.

La chiave privata nell'input non deve essere crittografata. Se sono presenti chiavi private crittografate, queste vengono rifiutate dal sistema.

Esempio 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Esempio 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Esempio 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina HTTPS Certificate (certificato HTTPS) per visualizzare i certificati di protezione correnti e generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

La pagina HTTPS Certificate (certificato HTTPS) consente di visualizzare il certificato di protezione corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS o installare un nuovo certificato HTTPS.

Se non è stato generato un nuovo certificato HTTPS, il certificato visualizzato in questa pagina corrisponde al certificato generato durante l'installazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica richiesta firma certificato HTTPS**

  Scarica una richiesta di certificazione per il certificato HTTPS attualmente installato. Il browser richiede di salvare `<hostname>.csr` In modo da poter fornire il file a un'autorità di certificazione da firmare.

- **Installare il certificato HTTPS**

  Consente di caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il nuovo certificato è in vigore dopo il riavvio del server di gestione.

- **Rigenera certificato HTTPS**

  Consente di generare un certificato HTTPS, che sostituisce il certificato di protezione corrente. Il nuovo certificato è in vigore dopo il riavvio di Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS

La finestra di dialogo Rigenera certificato HTTPS consente di personalizzare le informazioni di protezione e generare un nuovo certificato HTTPS con tali informazioni.

In questa pagina vengono visualizzate le informazioni sul certificato corrente.

La selezione "Regenerate using Current Certificate Attributes" e "Update the Current Certificate Attributes" consente di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

  Obbligatorio. Il nome di dominio completo (FQDN) che si desidera proteggere.

  Nelle configurazioni ad alta disponibilità di Unified Manager, utilizzare l'indirizzo IP virtuale.

- **E-mail**

  Opzionale. Un indirizzo e-mail per contattare l'organizzazione, in genere l'indirizzo e-mail dell'amministratore dei certificati o del reparto IT.

- **Azienda**

  Opzionale. In genere, il nome della società.

- **Reparto**

  Opzionale. Il nome del reparto della società.

- **Città**

  Opzionale. La località della tua azienda.

- **Stato**

Opzionale. L’ubicazione dello stato o della provincia, non abbreviata, dell’azienda.

- **Paese**

  Opzionale. L’ubicazione del paese dell’azienda. Si tratta in genere di un codice ISO di due lettere del paese.

- **Nomi alternativi**

  Obbligatorio. Nomi di dominio aggiuntivi non primari che possono essere utilizzati per accedere a questo server oltre all’host locale o ad altri indirizzi di rete esistenti. Separare ciascun nome alternativo con una virgola.

  Selezionare la casella di controllo “Exclude local identifying information (e.g. localhost)” (Escludi informazioni di identificazione locale) se si desidera rimuovere le informazioni di identificazione locale dal campo dei nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, solo i dati immessi nel campo vengono utilizzati nel campo nomi alternativi. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

- **DIMENSIONE DELLA CHIAVE (ALGORITMO CHIAVE: RSA)**

  L’algoritmo delle chiavi è impostato su RSA. È possibile selezionare una delle dimensioni delle chiavi: 2048, 3072 o 4096 bit. La dimensione predefinita della chiave è impostata su 2048 bit.

- **PERIODO DI VALIDITÀ**

  Il periodo di validità predefinito è 397 giorni. Se è stato eseguito l’aggiornamento da una versione precedente, la validità del certificato precedente potrebbe essere invariata.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.