



Verificare l'identità dei server remoti utilizzando i certificati

ONTAP 9

NetApp
April 24, 2024

Sommario

- Verificare l'identità dei server remoti utilizzando i certificati 1
 - Verificare l'identità dei server remoti utilizzando la panoramica dei certificati 1
 - Verificare che i certificati digitali siano validi utilizzando OCSP 1
 - Visualizza i certificati predefiniti per le applicazioni basate su TLS 3

Verificare l'identità dei server remoti utilizzando i certificati

Verificare l'identità dei server remoti utilizzando la panoramica dei certificati

ONTAP supporta le funzionalità dei certificati di sicurezza per verificare l'identità dei server remoti.

Il software ONTAP consente connessioni sicure utilizzando le seguenti funzionalità e protocolli di certificazione digitale:

- Il protocollo OCSP (Online Certificate Status Protocol) convalida lo stato delle richieste di certificati digitali dai servizi ONTAP utilizzando connessioni SSL e TLS (Transport Layer Security). Questa funzione è disattivata per impostazione predefinita.
- Il software ONTAP include un set predefinito di certificati root attendibili.
- I certificati KMIP (Key Management Interoperability Protocol) consentono l'autenticazione reciproca di un cluster e di un server KMIP.

Verificare che i certificati digitali siano validi utilizzando OCSP

A partire da ONTAP 9.2, il protocollo OCSP (Online Certificate Status Protocol) consente alle applicazioni ONTAP che utilizzano le comunicazioni TLS (Transport Layer Security) di ricevere lo stato del certificato digitale quando OCSP è attivato. È possibile attivare o disattivare i controlli dello stato dei certificati OCSP per applicazioni specifiche in qualsiasi momento. Per impostazione predefinita, il controllo dello stato del certificato OCSP è disattivato.

Di cosa hai bisogno

Per eseguire questa attività, è necessario disporre di un accesso avanzato a livello di privilegi.

A proposito di questa attività

OCSP supporta le seguenti applicazioni:

- AutoSupport
- Sistema di gestione degli eventi (EMS)
- LDAP su TLS
- Protocollo KMIP (Key Management Interoperability Protocol)
- Registrazione dell'audit
- FabricPool
- SSH (a partire da ONTAP 9.13.1)

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`.
2. Per attivare o disattivare i controlli dello stato dei certificati OSCP per applicazioni ONTAP specifiche, utilizzare il comando appropriato.

Se si desidera che lo stato del certificato OSCP verifichi che alcune applicazioni siano...	Utilizzare il comando...
Attivato	<code>security config ocsd enable -app app name</code>
Disattivato	<code>security config ocsd disable -app app name</code>

Il seguente comando abilita il supporto OSCP per AutoSupport e EMS.

```
cluster::*> security config ocsd enable -app asup,ems
```

Quando OSCP è attivato, l'applicazione riceve una delle seguenti risposte:

- Buono - il certificato è valido e la comunicazione procede.
 - Revocato - il certificato viene considerato permanentemente come non attendibile dall'autorità di certificazione di emissione e la comunicazione non riesce.
 - Sconosciuto - il server non dispone di informazioni sullo stato del certificato e la comunicazione non riesce.
 - Le informazioni del server OSCP non sono presenti nel certificato - il server agisce come se OSCP sia disattivato e continui con la comunicazione TLS, ma non si verifica alcun controllo dello stato.
 - Nessuna risposta dal server OSCP - l'applicazione non riesce a procedere.
3. Per attivare o disattivare i controlli dello stato dei certificati OSCP per tutte le applicazioni che utilizzano le comunicazioni TLS, utilizzare il comando appropriato.

Se si desidera che lo stato del certificato OSCP verifichi che tutte le applicazioni siano...	Utilizzare il comando...
Attivato	<code>security config ocsd enable</code> <code>-app all</code>
Disattivato	<code>security config ocsd disable</code> <code>-app all</code>

Quando questa opzione è attivata, tutte le applicazioni ricevono una risposta firmata che indica che il certificato specificato è valido, revocato o sconosciuto. In caso di certificato revocato, l'applicazione non potrà procedere. Se l'applicazione non riesce a ricevere una risposta dal server OSCP o se il server non è raggiungibile, l'applicazione non potrà procedere.

4. Utilizzare `security config ocsf show` Per visualizzare tutte le applicazioni che supportano OCSP e il relativo stato di supporto.

```
cluster::*> security config ocsf show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

Visualizza i certificati predefiniti per le applicazioni basate su TLS

A partire da ONTAP 9.2, ONTAP fornisce un set predefinito di certificati root attendibili per le applicazioni ONTAP che utilizzano TLS (Transport Layer Security).

Di cosa hai bisogno

I certificati predefiniti vengono installati solo sulla SVM amministrativa durante la creazione o durante un aggiornamento a ONTAP 9.2.

A proposito di questa attività

Le applicazioni correnti che agiscono come client e richiedono la convalida dei certificati sono AutoSupport, EMS, LDAP, registrazione degli audit, FabricPool, E KMIP.

Quando i certificati scadono, viene richiamato un messaggio EMS che richiede all'utente di eliminarli. I certificati predefiniti possono essere eliminati solo al livello di privilegio avanzato.



L'eliminazione dei certificati predefiniti potrebbe causare il mancato funzionamento di alcune applicazioni ONTAP (ad esempio, AutoSupport e registrazione audit).

Fase

1. È possibile visualizzare i certificati predefiniti installati sulla SVM amministrativa utilizzando il comando `show` del certificato di protezione:

```
security certificate show -vserver -type server-ca
```

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01                AACertificateServices
server-ca
  Certificate Authority: AAA Certificate Services
    Expiration Date: Sun Dec 31 18:59:59 2028
```

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.