# 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

## 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 OCSP per applicazioni ONTAP specifiche, utilizzare il comando appropriato.

| Se si desidera che lo stato del certificato OCSP verifichi che alcune applicazioni siano… | Utilizzare il comando… |
|---|---|
| Attivato | `security config ocsp enable -app` app name |
| Disattivato | `security config ocsp disable -app` app name |

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

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

Quando OCSP 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 OCSP non sono presenti nel certificato - il server agisce come se OCSP sia disattivato e continui con la comunicazione TLS, ma non si verifica alcun controllo dello stato.
- Nessuna risposta dal server OCSP - l'applicazione non riesce a procedere.

3. Per attivare o disattivare i controlli dello stato dei certificati OCSP per tutte le applicazioni che utilizzano le comunicazioni TLS, utilizzare il comando appropriato.

| Se si desidera che lo stato del certificato OCSP verifichi che tutte le applicazioni siano… | Utilizzare il comando… |
|---|---|
| Attivato | `security config ocsp enable`<br><br>`-app all` |
| Disattivato | `security config ocsp disable`<br><br>`-app all` |

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 OCSP o se il server non è raggiungibile, l'applicazione non potrà procedere.

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

```
cluster::*> security config ocsp 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              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```