Verifique a identidade de servidores remotos usando certificados

ONTAP 9

NetApp
January 17, 2025

Índice

Verifique a identidade de servidores remotos usando certificados

Verifique a identidade de servidores remotos usando a visão geral de certificados

O ONTAP suporta recursos de certificado de segurança para verificar a identidade de servidores remotos.

O software ONTAP permite conexões seguras usando esses recursos e protocolos de certificado digital:

- O OCSP (Online Certificate Status Protocol) valida o status de solicitações de certificados digitais de serviços ONTAP usando conexões SSL e TLS (Transport Layer Security). Esta funcionalidade está desativada por predefinição.
- Um conjunto padrão de certificados raiz confiáveis é incluído no software ONTAP.
- Os certificados KMIP (Key Management Interoperability Protocol) permitem a autenticação mútua de um cluster e de um servidor KMIP.

Verifique se os certificados digitais são válidos usando OCSP

A partir do ONTAP 9.2, o protocolo OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS (Transport Layer Security) recebam status de certificado digital quando o OCSP está ativado. Você pode ativar ou desativar verificações de status do certificado OCSP para aplicativos específicos a qualquer momento. Por padrão, a verificação do status do certificado OCSP está desativada.

O que você vai precisar

Você precisa de acesso avançado ao nível de privilégio para executar esta tarefa.

Sobre esta tarefa

O OCSP suporta as seguintes aplicações:

- AutoSupport
- Sistema de Gestão de Eventos (EMS)
- LDAP em TLS
- Key Management Interoperability Protocol (KMIP)
- Registo de auditoria
- FabricPool
- SSH (começando com ONTAP 9.13,1)

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`.

2. Para ativar ou desativar as verificações de status do certificado OCSP para aplicativos ONTAP específicos, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para alguns aplicativos sejam…	Use o comando…
Ativado	`security config ocsp enable -app app name`
Desativado	`security config ocsp disable -app app name`

O seguinte comando permite o suporte OCSP para AutoSupport e EMS.

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

Quando o OCSP está ativado, o aplicativo recebe uma das seguintes respostas:

- Bom - o certificado é válido e a comunicação prossegue.
- Revogado - o certificado é considerado permanentemente como não fidedigno pela Autoridade de Certificação de emissão e a comunicação não procede.
- Desconhecido - o servidor não tem nenhuma informação de estado sobre o certificado e a comunicação não consegue prosseguir.
- As informações do servidor OCSP estão ausentes no certificado - o servidor funciona como se o OCSP estivesse desativado e continua com a comunicação TLS, mas nenhuma verificação de status ocorre.
- Sem resposta do servidor OCSP - o aplicativo não consegue prosseguir.

3. Para ativar ou desativar as verificações de status do certificado OCSP para todos os aplicativos que usam comunicações TLS, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para todos os aplicativos sejam…	Use o comando…

Ativado	`security config ocsp enable`
	
	`-app all`

Desativado	`security config ocsp disable`
	
	`-app all`

Quando ativado, todos os aplicativos recebem uma resposta assinada, significando que o certificado especificado é bom, revogado ou desconhecido. No caso de um certificado revogado, o pedido não irá prosseguir. Se o aplicativo não receber uma resposta do servidor OCSP ou se o servidor estiver inacessível, o aplicativo não conseguirá prosseguir.

4. Use o `security config ocsp show` comando para exibir todos os aplicativos que suportam OCSP e seu status de suporte.

```
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.
```

Exibir certificados padrão para aplicativos baseados em TLS

A partir do ONTAP 9.2, o ONTAP fornece um conjunto padrão de certificados raiz confiáveis para aplicativos ONTAP usando a Segurança da camada de Transporte (TLS).

O que você vai precisar

Os certificados padrão são instalados somente no SVM do administrador durante sua criação ou durante uma atualização para o ONTAP 9.2.

Sobre esta tarefa

Os aplicativos atuais que atuam como cliente e exigem validação de certificado são AutoSupport, EMS, LDAP, Registro de auditoria, FabricPool e KMIP.

Quando os certificados expiram, é invocada uma mensagem EMS que solicita ao utilizador que elimine os certificados. Os certificados padrão só podem ser excluídos no nível avançado de privilégio.

> A exclusão dos certificados padrão pode resultar em alguns aplicativos do ONTAP não funcionarem como esperado (por exemplo, AutoSupport e Registro de auditoria).

Passo

1. Você pode exibir os certificados padrão instalados no SVM do administrador usando o comando show do certificado de segurança:

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

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

Informações sobre direitos autorais

Informações sobre marcas comerciais