



Verifique a identidade de servidores remotos usando certificados

ONTAP 9

NetApp
January 17, 2025

Índice

Verifique a identidade de servidores remotos usando certificados	1
Verifique a identidade de servidores remotos usando a visão geral de certificados	1
Verifique se os certificados digitais são válidos usando OCSP	1
Exibir certificados padrão para aplicativos baseados em TLS	3

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	<code>security config ocsf enable -app app name</code>
Desativado	<code>security config ocsf disable -app app name</code>

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

```
cluster::*> security config ocsf 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	<code>security config ocsf enable</code> <code>-app all</code>
Desativado	<code>security config ocsf disable</code> <code>-app all</code>

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.

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

```
cluster::*> security config oosp 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

- 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

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.