인증서를 사용하여 원격 서버의 ID를 확인합니다

ONTAP 9

NetApp
April 24, 2024

목차

인증서를 사용하여 원격 서버의 ID를 확인합니다 1
인증서 개요를 사용하여 원격 서버의 ID를 확인합니다 1
디지털 인증서가 OCSP를 사용하여 유효한지 확인합니다 1
TLS 기반 응용 프로그램에 대한 기본 인증서를 봅니다 3

인증서를 사용하여 원격 서버의 ID를 확인합니다

인증서 개요를 사용하여 원격 서버의 ID를 확인합니다

ONTAP는 보안 인증서 기능을 지원하여 원격 서버의 ID를 확인합니다.

ONTAP 소프트웨어는 다음과 같은 디지털 인증서 기능 및 프로토콜을 사용하여 보안 연결을 지원합니다.

- OCSP(온라인 인증서 상태 프로토콜)는 SSL 및 TLS(전송 계층 보안) 연결을 사용하여 ONTAP 서비스에서 디지털 인증서 요청 상태를 검증합니다. 이 기능은 기본적으로 비활성화되어 있습니다.
- 신뢰할 수 있는 루트 인증서의 기본 집합은 ONTAP 소프트웨어에 포함되어 있습니다.
- KMIP(Key Management Interoperability Protocol) 인증서를 통해 클러스터 및 KMIP 서버를 상호 인증할 수 있습니다.

디지털 인증서가 OCSP를 사용하여 유효한지 확인합니다

ONTAP 9.2부터 OCSP(온라인 인증서 상태 프로토콜)를 사용하면 ONTAP 응용 프로그램에서 TLS(전송 계층 보안) 통신을 사용하는 응용 프로그램이 OCSP가 활성화될 때 디지털 인증서 상태를 수신할 수 있습니다. 특정 애플리케이션에 대한 OCSP 인증서 상태 확인을 언제든지 활성화 또는 비활성화할 수 있습니다. 기본적으로 OCSP 인증서 상태 확인은 사용되지 않습니다.

필요한 것

이 작업을 수행하려면 고급 권한 수준 액세스 권한이 필요합니다.

이 작업에 대해

OCSP는 다음 애플리케이션을 지원합니다.

- AutoSupport
- EMS(이벤트 관리 시스템)
- TLS를 통한 LDAP
- 키 관리 상호 운용성 프로토콜(KMIP)
- 로깅 감사
- FabricPool
- SSH(ONTAP 9.13.1 로 시작)

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다.
2. 특정 ONTAP 응용 프로그램에 대한 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태를 통해 일부 응용 프로그램을 확인하려는 경우...	명령 사용...
활성화됨	`security config ocsp enable -app app name`
사용 안 함	`security config ocsp disable -app app name`

다음 명령을 실행하면 AutoSupport 및 EMS에 대한 OCSP 지원이 활성화됩니다.

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

OCSP가 활성화되면 애플리케이션은 다음 응답 중 하나를 수신합니다.

- 양호 - 인증서가 유효하며 통신이 진행됩니다.
- 해지 - 인증서는 발급 인증 기관에서 영구적으로 신뢰할 수 없는 것으로 간주되어 통신이 진행되지 않습니다.
- 알 수 없음 - 서버에 인증서에 대한 상태 정보가 없으며 통신이 진행되지 않습니다.
- OCSP 서버 정보가 인증서에 없습니다. 서버는 OCSP가 비활성화되어 TLS 통신을 계속하는 것처럼 작동하지만 상태 검사는 발생하지 않습니다.
- OCSP 서버의 응답이 없습니다. 응용 프로그램을 계속할 수 없습니다.

3. TLS 통신을 사용하는 모든 응용 프로그램에 대해 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태가 모든 응용 프로그램의 상태를 확인하려는 경우...	명령 사용...
활성화됨	'보안 구성 OCSP 활성화 '-APP ALL'
사용 안 함	보안 구성 OCSP 비활성화 '-APP ALL'

이 옵션을 활성화하면 모든 응용 프로그램은 지정된 인증서가 양호, 취소 또는 알 수 없다는 서명된 응답을 받습니다. 인증서가 해지된 경우 응용 프로그램을 계속 진행할 수 없습니다. 애플리케이션이 OCSP 서버로부터 응답을 수신하지 못하거나 서버에 연결할 수 없는 경우 응용 프로그램을 계속 진행할 수 없습니다.

4. 'Security config OCSP show' 명령어를 사용하면 OCSP를 지원하는 모든 애플리케이션과 지원 상태를 확인할 수 있다.

```
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.
```

TLS 기반 응용 프로그램에 대한 기본 인증서를 봅니다

ONTAP 9.2부터 ONTAP는 TLS(전송 계층 보안)를 사용하는 ONTAP 응용 프로그램에 대해 신뢰할 수 있는 루트 인증서 기본 집합을 제공합니다.

필요한 것

기본 인증서는 생성 중 또는 ONTAP 9.2로 업그레이드 도중에만 관리 SVM에 설치됩니다.

이 작업에 대해

현재 클라이언트 역할을 하고 인증서 검증이 필요한 애플리케이션은 AutoSupport, EMS, LDAP, 감사 로깅, FabricPool입니다. 및 KMIP

인증서가 만료되면 사용자에게 인증서 삭제를 요청하는 EMS 메시지가 호출됩니다. 기본 인증서는 고급 권한 수준에서만 삭제할 수 있습니다.

> 기본 인증서를 삭제하면 일부 ONTAP 응용 프로그램이 예상대로 작동하지 않을 수 있습니다(예: AutoSupport 및 감사 로깅).

단계

1. security certificate show 명령을 사용하여 admin SVM에 설치된 기본 인증서를 볼 수 있습니다.

   '* 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
```