Cluster und KMIP-Server authentifizieren sich gegenseitig

ONTAP 9

NetApp
September 12, 2024

Inhalt

Cluster und KMIP-Server authentifizieren sich gegenseitig

Die Authentifizierung des Clusters und eine Übersicht über KMIP-Server wurden gegenseitig überprüft

Durch die gegenseitige Authentifizierung des Clusters und eines externen Schlüsselmanagers wie einem KMIP-Server (Key Management Interoperability Protocol) kann der Schlüsselmanager mithilfe von KMIP über SSL mit dem Cluster kommunizieren. Sie tun dies, wenn eine Applikation oder eine bestimmte Funktion (z. B. die Storage-Verschlüsselung) sicheren Datenzugriff mit sicheren Schlüsseln erfordert.

Generieren Sie eine Anforderung zum Signieren eines Zertifikats für das Cluster

Sie können das Sicherheitszertifikat verwenden `generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Was Sie benötigen

Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritte

1. CSR erstellen:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size
   512|1024|1536|2048 -country country -state state -locality locality
   -organization organization -unit unit -email-addr email_of_contact -hash
   -function SHA1|SHA256|MD5
   ```

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Der folgende Befehl erzeugt einen CSR mit einem 2,048-bit privaten Schlüssel, der von der SHA256 Hashing-Funktion erzeugt wird, zur Verwendung durch die Software-Gruppe in der IT-Abteilung eines Unternehmens mit individuellem gemeinsamen Namen server1.companyname.com, mit Sitz in Sunnyvale, Kalifornien, USA. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet web@example.com. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Kopieren Sie die Zertifikatanforderung aus der CSR-Ausgabe, und senden Sie sie dann in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

Installieren Sie ein von einer Zertifizierungsstelle signiertes Serverzertifikat für das Cluster

Damit ein SSL-Server die Authentifizierung des Clusters oder der Storage Virtual Machine (SVM) als SSL-Client aktiviert, installieren Sie ein digitales Zertifikat mit dem Clienttyp auf dem Cluster oder der SVM. Anschließend stellen Sie dem SSL-Serveradministrator das Client-Ca-Zertifikat zur Installation auf dem Server zur Verfügung.

Was Sie benötigen

Sie müssen bereits das Stammzertifikat des SSL-Servers auf dem Cluster oder SVM mit dem installiert haben `server-ca` Zertifikatstyp.

Schritte

1. Um ein selbstsigniertes digitales Zertifikat für die Clientauthentifizierung zu verwenden, verwenden Sie das `security certificate create` Befehl mit dem `type client` Parameter.
2. Gehen Sie wie folgt vor, um ein von einer Zertifizierungsstelle signiertes digitales Zertifikat für die Clientauthentifizierung zu verwenden:

   a. Generieren Sie mithilfe des Sicherheitszertifikats eine digitale Zertifikatsignierungsanforderung (CSR) `generate-csr` Befehl.

      ONTAP zeigt die CSR-Ausgabe an, die eine Zertifikatanforderung und einen privaten Schlüssel enthält, und erinnert Sie daran, die Ausgabe in eine Datei zu kopieren, um sie später verwenden zu können.

   b. Senden Sie die Zertifikatsanforderung von der CSR-Ausgabe in einem elektronischen Formular (z. B. E-Mail) an eine vertrauenswürdige CA zum Signieren.

      Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten Zertifikats für zukünftige Referenz aufbewahren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat.

   a. Installieren Sie das CA-signierte Zertifikat mithilfe der `security certificate install` Befehl mit dem `-type client` Parameter.
   b. Geben Sie das Zertifikat und den privaten Schlüssel ein, wenn Sie dazu aufgefordert werden, und drücken Sie dann **Enter**.
   c. Geben Sie bei der Aufforderung zusätzliche Root- oder Zwischenzertifikate ein, und drücken Sie dann **Enter**.

      Sie installieren ein Zwischenzertifikat auf dem Cluster oder der SVM, wenn eine Zertifikatkette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt und mit dem Ihnen ausgestellten SSL-Zertifikat endet, die Zwischenzertifikate fehlen. Ein Zwischenzertifikat ist ein vom vertrauenswürdigen Stammverzeichnis herausgegebenem untergeordneten Zertifikat, das speziell für die Ausgabe von Serverzertifikaten der Endeinheit ausgegeben wird. Das Ergebnis ist eine Zertifikatskette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt, durch das Zwischenzertifikat geht und mit dem Ihnen ausgestellten SSL-Zertifikat endet.

3. Versorgen `client-ca` Zertifikat des Clusters oder der SVM an den Administrator des SSL-Servers zur Installation auf dem Server.

   Der Befehl zum Anzeigen des Sicherheitszertifikats mit dem `-instance` Und `-type client-ca` Parameter zeigt das an `client-ca` Zertifikatsinformationen

Installieren Sie ein CA-signiertes Client-Zertifikat für den KMIP-Server

Der Zertifikatsubtyp des Key Management Interoperability Protocol (KMIP) (der Parameter -subtype kmip-cert) legt gemeinsam mit den Client- und Server-Ca-Typen fest, dass das Zertifikat für die wechselseitige Authentifizierung des Clusters und einen externen Schlüsselmanager, z. B. einen KMIP-Server, verwendet wird.

Über diese Aufgabe

Installieren Sie ein KMIP-Zertifikat, um einen KMIP-Server als SSL-Server für das Cluster zu authentifizieren.

Schritte

1. Verwenden Sie die `security certificate install` Befehl mit dem `-type server-ca` Und `-subtype kmip-cert` Parameter zur Installation eines KMIP-Zertifikats für den KMIP-Server.
2. Wenn Sie aufgefordert werden, geben Sie das Zertifikat ein, und drücken Sie anschließend die Eingabetaste.

   ONTAP erinnert Sie daran, dass Sie eine Kopie des Zertifikats zur späteren Verwendung aufbewahren.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```