Sicherheitszertifikate verwalten

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

Sicherheitszertifikate verwalten

Sie können HTTPS im Unified Manager-Server konfigurieren, um Ihre Cluster über eine sichere Verbindung zu überwachen und zu verwalten.

Zeigen Sie das HTTPS-Sicherheitszertifikat an

Sie können die HTTPS-Zertifikatdetails mit dem abgerufenen Zertifikat in Ihrem Browser vergleichen, um sicherzustellen, dass die verschlüsselte Verbindung Ihres Browsers zu Unified Manager nicht abgefangen wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Durch Anzeigen des Zertifikats können Sie den Inhalt eines neu generierten Zertifikats überprüfen oder Subject Alt Names (SAN) anzeigen, von denen aus Sie auf Unified Manager zugreifen können.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Wenn Sie ausführlichere Informationen zum Sicherheitszertifikat benötigen als die, die auf der Seite „HTTPS-Zertifikat“ angezeigt werden, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Laden Sie eine HTTPS-Zertifikatsignieranforderung herunter

Sie können eine Zertifizierungssignaturanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, sodass Sie die Datei einer Zertifizierungsstelle zur Signierung vorlegen können. Ein von einer Zertifizierungsstelle signiertes Zertifikat trägt dazu bei, Man-in-the-Middle-Angriffe zu verhindern und bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikatsignieranforderung herunterladen**.
3. Speichern Sie die `<hostname>.csr` Datei.

Sie können die Datei einer Zertifizierungsstelle zur Signierung vorlegen und anschließend das signierte Zertifikat installieren.

Installieren Sie ein von einer CA signiertes und zurückgegebenes HTTPS-Zertifikat

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem es von einer Zertifizierungsstelle signiert und zurückgegeben wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein von einer Zertifizierungsstelle signiertes Zertifikat trägt dazu bei, Man-in-the-Middle-Angriffe zu verhindern und bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

*Was .Bevor Sie beginnen

Sie müssen die folgenden Aktionen abgeschlossen haben:

- Die Certificate Signing Request-Datei heruntergeladen und von einer Zertifizierungsstelle signieren lassen
- Die Zertifikatskette wurde im PEM-Format gespeichert
- Alle Zertifikate in der Kette eingeschlossen, vom Unified Manager-Serverzertifikat bis zum Stammsignaturzertifikat, einschließlich aller vorhandenen Zwischenzertifikate

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn die Gültigkeit des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage beträgt, wird die Gültigkeit von der Zertifizierungsstelle vor der Unterzeichnung und Rücksendung des Zertifikats auf 397 Tage verkürzt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat installieren**.
3. Klicken Sie im angezeigten Dialogfeld auf **Datei auswählen…**, um die hochzuladende Datei zu suchen.
4. Wählen Sie die Datei aus und klicken Sie dann auf **Installieren**, um die Datei zu installieren.

   Weitere Informationen finden Sie unter"Installieren eines mit externen Tools generierten HTTPS-Zertifikats" .

Beispiel einer Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatskettendatei aussehen könnte:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Installieren Sie ein mit externen Tools generiertes HTTPS-Zertifikat

Sie können selbstsignierte oder von einer Zertifizierungsstelle signierte Zertifikate installieren, die mit einem externen Tool wie OpenSSL, BoringSSL oder LetsEncrypt generiert wurden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette laden, da es sich bei diesen Zertifikaten um extern generierte öffentlich-private Schlüsselpaare handelt. Die zulässigen Schlüsselpaar-Algorithmen sind „`RSA`“ und „`EC`“. Die Option **HTTPS-Zertifikat installieren** ist auf der Seite „HTTPS-Zertifikate“ im Abschnitt „Allgemein“ verfügbar. Die Datei, die Sie hochladen, sollte das folgende Eingabeformat haben.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager Host gehört
2. Zertifikat des Servers, das zum privaten Schlüssel passt
3. Zertifikat der CAs in umgekehrter Reihenfolge bis zur Wurzel, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC-Schlüsselpaar

Die zulässigen Kurven sind „prime256v1“ und „secp384r1“. Musterzertifikat mit extern generiertem EC-Paar:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar

Die zulässigen Schlüsselgrößen für das zum Host-Zertifikat gehörende RSA-Schlüsselpaar sind 2048, 3072 und 4096. Zertifikat mit einem extern generierten **RSA-Schlüsselpaar**:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Nachdem das Zertifikat hochgeladen wurde, sollten Sie die Active IQ Unified Manager Instanz neu starten, damit die Änderungen wirksam werden.

Prüfungen beim Hochladen extern erstellter Zertifikate

Das System führt beim Hochladen eines mit externen Tools erstellten Zertifikats Prüfungen durch. Wenn eine der Prüfungen fehlschlägt, wird das Zertifikat abgelehnt. Es ist auch eine Validierung für die Zertifikate enthalten, die aus der CSR innerhalb des Produkts generiert werden, und für Zertifikate, die mit externen Tools generiert werden.

- Der private Schlüssel in der Eingabe wird anhand des Host-Zertifikats in der Eingabe validiert.

- Der Common Name (CN) im Host-Zertifikat wird mit dem FQDN des Hosts abgeglichen.
- Der allgemeine Name (CN) des Hostzertifikats darf nicht leer sein und darf nicht auf „localhost“ gesetzt werden.
- Das Gültigkeitsbeginndatum sollte nicht in der Zukunft und das Gültigkeitsablaufdatum des Zertifikats nicht in der Vergangenheit liegen.
- Wenn eine Zwischenzertifizierungsstelle oder Zertifizierungsstelle vorhanden ist, darf das Gültigkeitsbeginndatum des Zertifikats nicht in der Zukunft und das Gültigkeitsablaufdatum nicht in der Vergangenheit liegen.

Der private Schlüssel in der Eingabe sollte nicht verschlüsselt sein. Wenn verschlüsselte private Schlüssel vorhanden sind, werden diese vom System abgelehnt.

Beispiel 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Beispiel 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Beispiel 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Wenn die Installation des Zertifikats fehlschlägt, lesen Sie den folgenden Knowledge Base-Artikel (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"^]

Seitenbeschreibungen zur Zertifikatsverwaltung

Auf der Seite „HTTPS-Zertifikat“ können Sie die aktuellen Sicherheitszertifikate anzeigen und neue HTTPS-Zertifikate generieren.

HTTPS-Zertifikatseite

Auf der Seite „HTTPS-Zertifikat“ können Sie das aktuelle Sicherheitszertifikat anzeigen,

eine Zertifikatsignieranforderung herunterladen, ein neues selbstsigniertes HTTPS-Zertifikat generieren oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat generiert haben, handelt es sich bei dem auf dieser Seite angezeigten Zertifikat um das Zertifikat, das während der Installation generiert wurde.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Vorgänge ausführen:

- **HTTPS-Zertifikatsignieranforderung herunterladen**

  Lädt eine Zertifizierungsanforderung für das aktuell installierte HTTPS-Zertifikat herunter. Ihr Browser fordert Sie auf, die Datei <hostname>.csr zu speichern, damit Sie die Datei einer Zertifizierungsstelle zum Signieren vorlegen können.

- **HTTPS-Zertifikat installieren**

  Ermöglicht Ihnen das Hochladen und Installieren eines Sicherheitszertifikats, nachdem es von einer Zertifizierungsstelle signiert und zurückgegeben wurde. Das neue Zertifikat ist nach dem Neustart des Verwaltungsservers wirksam.

- **HTTPS-Zertifikat neu generieren**

  Ermöglicht Ihnen, ein neues selbstsigniertes HTTPS-Zertifikat zu generieren, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat ist nach dem Neustart von Unified Manager wirksam.

Dialogfeld „HTTPS-Zertifikat neu generieren“

Im Dialogfeld „HTTPS-Zertifikat neu generieren“ können Sie die Sicherheitsinformationen anpassen und dann mit diesen Informationen ein neues HTTPS-Zertifikat generieren.

Auf dieser Seite werden die aktuellen Zertifikatsinformationen angezeigt.

Mit der Auswahl „Mithilfe der aktuellen Zertifikatsattribute neu generieren“ und „Aktualisieren der aktuellen Zertifikatsattribute“ können Sie das Zertifikat mit den aktuellen Informationen neu generieren oder ein Zertifikat mit neuen Informationen erstellen.

- **Allgemeiner Name**

  Erforderlich. Der vollqualifizierte Domänenname (FQDN), den Sie sichern möchten.

  Verwenden Sie in Hochverfügbarkeitskonfigurationen von Unified Manager die virtuelle IP-Adresse.

- **E-Mail**

  Optional. Eine E-Mail-Adresse zur Kontaktaufnahme mit Ihrer Organisation; normalerweise die E-Mail-Adresse des Zertifikatadministrators oder der IT-Abteilung.

- **Unternehmen**

  Optional. Normalerweise der eingetragene Name Ihres Unternehmens.

- **Abteilung**

Optional. Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional. Der Stadtstandort Ihres Unternehmens.

- **Zustand**

  Optional. Der Bundesstaat oder die Provinz, in der sich Ihr Unternehmen befindet (nicht abgekürzt).

- **Land**

  Optional. Der Standort Ihres Unternehmens. Dies ist normalerweise ein zweistelliger ISO-Code des Landes.

- **Alternative Namen**

  Erforderlich. Zusätzliche, nicht primäre Domänennamen, die zusätzlich zu den vorhandenen Localhost- oder anderen Netzwerkadressen für den Zugriff auf diesen Server verwendet werden können. Trennen Sie jeden alternativen Namen durch ein Komma.

  Aktivieren Sie das Kontrollkästchen „Lokale Identifizierungsinformationen ausschließen (z. B. localhost)“, wenn Sie die lokalen Identifizierungsinformationen aus dem Feld „Alternative Namen“ im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, wird im Feld „Alternative Namen“ nur das verwendet, was Sie in das Feld eingeben. Wenn dieses Feld leer gelassen wird, enthält das resultierende Zertifikat überhaupt kein Feld für alternative Namen.

- **SCHLÜSSELGRÖSSE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA eingestellt. Sie können eine der Schlüsselgrößen auswählen: 2048, 3072 oder 4096 Bit. Die Standardschlüsselgröße ist auf 2048 Bit eingestellt.

- **GÜLTIGKEITSDAUER**

  Die Standardgültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, bleibt die Gültigkeit des vorherigen Zertifikats möglicherweise unverändert.

Weitere Informationen finden Sie unter "Generieren von HTTPS-Zertifikaten".