Verwalten von Sicherheitszertifikaten

Active IQ Unified Manager 9.12

NetApp
March 22, 2023

Inhaltsverzeichnis

Verwalten von Sicherheitszertifikaten

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

Anzeigen des HTTPS-Sicherheitszertifikats

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

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Durch das Anzeigen des Zertifikats können Sie den Inhalt eines neu erstellten Zertifikats überprüfen oder die entsprechenden Alt-Namen (SAN) anzeigen, auf die 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 als auf der Seite HTTPS-Zertifikat anzeigen müssen, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Herunterladen einer Anforderung zum Signieren eines HTTPS-Zertifikats

Sie können eine Zertifizierungssignierungsanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, so dass Sie die Datei einer Zertifizierungsstelle zum Signieren zur Verfügung stellen können. Ein von einer Zertifizierungsstelle signiertes Zertifikat hilft bei der Verhinderung von man-in-the-Middle-Angriffen und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

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

Sie können die Datei einer Zertifizierungsstelle zum Signieren bereitstellen und dann das signierte Zertifikat installieren.

Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem eine Zertifizierungsstelle unterschrieben und zurückgesendet wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein CA-signiertes Zertifikat hilft bei der Verhinderung von man-in-the-Middle-Angriffen und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Was Sie brauchen

Sie müssen die folgenden Aktionen durchgeführt haben:

- Laden Sie die Zertifikatsignierungsanforderungsdatei herunter und lassen Sie sie von einer Zertifizierungsstelle signiert werden
- Die Zertifikatskette wurde im PEM-Format gespeichert
- Alle Zertifikate in der Kette enthalten, vom Unified Manager-Serverzertifikat bis zum Stammzertifikat, einschließlich aller vorhandenen Zwischenzertifikate

Sie müssen über die Anwendungsadministratorrolle verfügen.

> Wenn die Gültigkeit des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage beträgt, wird die Gültigkeit von der Zertifizierungsstelle vor dem Signieren und Zurücksenden des Zertifikats auf 397 Tage reduziert

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 HTTPS-Zertifikats, das mit externen Tools generiert wurde".

Beispiel für eine Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatkettendatei angezeigt werden kann:

```
-----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 eines HTTPS-Zertifikats, das mit externen Tools generiert wurde

Sie können Zertifikate installieren, die selbst signiert sind oder CA-signiert sind und mit einem externen Tool wie OpenSSL, BoringSSL, LetsEncrt generiert werden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette laden, da diese Zertifikate extern öffentlich-private Schlüsselpaare sind. Die zulässigen Schlüssel-Paar-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 aufweisen.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager-Host gehört
2. Zertifikat des Servers, das mit dem privaten Schlüssel übereinstimmt
3. Zertifikat der CAS in umgekehrter Reihenfolge bis zum Root, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC-Schlüsselpaar

Die zulässigen Kurven sind „`prime256v1`“ und „`secp384r1`“. Beispiel eines Zertifikats mit einem extern generierten 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 RSA-Schlüsselpaar, das zum Host-Zertifikat gehört, 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.

Überprüft beim Hochladen extern generierter Zertifikate

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

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

- Der allgemeine Name (CN) im Hostzertifikat wird mit dem FQDN des Hosts überprüft.
- Der allgemeine Name (CN) des Host-Zertifikats sollte nicht leer oder leer sein und nicht auf localhost gesetzt werden.
- Das Startdatum der Gültigkeit darf nicht in der Zukunft liegen und das Gültigkeitsdatum des Zertifikats sollte nicht in der Vergangenheit liegen.
- Wenn Intermediate CA oder CA vorhanden ist, sollte das Startdatum des Zertifikats nicht in der Zukunft liegen und das Gültigkeitsdatum sollte nicht in der Vergangenheit liegen.

Der private Schlüssel in der Eingabe sollte nicht verschlüsselt werden. Wenn private Schlüssel verschlüsselt sind, werden sie 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-----
```

Seitenbeschreibungen zur Zertifikatverwaltung

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

Seite „HTTPS-Zertifikat“

Auf der Seite HTTPS-Zertifikat können Sie das aktuelle Sicherheitszertifikat anzeigen, eine Anfrage zum Signieren von Zertifikaten herunterladen, ein neues selbstsigniertes HTTPS-Zertifikat erstellen oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat generiert haben, wird auf dieser Seite das Zertifikat angezeigt, das während der Installation generiert wurde.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Vorgänge ausführen:

- **HTTPS-Zertifikatsignierungsanforderung herunterladen**

  Lädt eine Zertifizierungsanfrage 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 zur Verfügung stellen können.

- **HTTPS-Zertifikat installieren**

  Ermöglicht es Ihnen, ein Sicherheitszertifikat hochzuladen und zu installieren, nachdem eine Zertifizierungsstelle unterschrieben und zurückgesendet wurde. Das neue Zertifikat wird wirksam, nachdem Sie den Verwaltungsserver neu gestartet haben.

- **HTTPS-Zertifikat neu erstellen**

  Ermöglicht Ihnen das Generieren eines neuen selbstsignierten HTTPS-Zertifikats, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat wird wirksam, nachdem Sie Unified Manager neu gestartet haben.

Dialogfeld „HTTPS-Zertifikat neu erstellen“

Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ ermöglicht Ihnen, die Sicherheitsinformationen anzupassen und anschließend ein neues HTTPS-Zertifikat mit diesen Informationen zu erstellen.

Die aktuellen Zertifikatinformationen werden auf dieser Seite angezeigt.

Mit der Auswahl „`regenerieren mit aktuellen Zertifikatattributen`“ und „`Aktuellen Zertifikatattributen aktualisieren`“ können Sie das Zertifikat mit den aktuellen Informationen neu generieren oder ein Zertifikat mit neuen Informationen generieren.

- **Gemeinsamer Name**

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

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

- **E-Mail**

  Optional Eine E-Mail-Adresse, an die Sie sich mit Ihrem Unternehmen wenden können, in der Regel die E-Mail-Adresse des Zertifikatadministrators oder DER IT-Abteilung.

- **Unternehmen**

  Optional In der Regel wird der Name Ihres Unternehmens eingetragen.

- **Abteilung**

  Optional Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

Optional Der Standort der Stadt Ihrer Firma.

- **Bundesland**

  Optional Der Ort des Staates oder der Provinz, nicht abgekürzt, Ihrer Firma.

- **Land**

  Optional Der Standort Ihres Unternehmens in Ihrem Land. Dies ist in der Regel ein zweistelliger ISO-Code des Landes.

- **Alternative Namen**

  Erforderlich. Zusätzliche, nicht primäre Domain-Namen, die verwendet werden können, um auf diesen Server zusätzlich zu den vorhandenen localhost oder anderen Netzwerkadressen zugreifen. Trennen Sie jeden alternativen Namen durch ein Komma.

  Aktivieren Sie das Kontrollkästchen „`lokale Identifizierungsdaten ausschließen (z. B. localhost)`“, wenn Sie die lokalen Identifizierungsdaten aus dem Feld Alternative Namen im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, werden nur die Daten verwendet, die Sie in das Feld Alternative Namen eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

- **SCHLÜSSELGRÖSSE (SCHLÜSSELALGORITHMUS: RSA)**

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

- **GÜLTIGKEITSZEITRAUM**

  Die standardmäßige Gültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, wird die vorherige Zertifikatsgültigkeit möglicherweise nicht geändert.

Weitere Informationen finden Sie unter "HTTPS-Zertifikate werden generiert".