Verwalten von Sicherheitszertifikaten

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

Inhalt

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.

Bevor Sie beginnen

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

Über diese Aufgabe

Durch das Anzeigen des Zertifikats können Sie den Inhalt eines neu erstellten Zertifikats oder alternative URL-Namen anzeigen, von denen aus Sie auf Unified Manager zugreifen können.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Nachdem Sie fertig sind

Wenn Sie ausführlichere Informationen zum Sicherheitszertifikat als auf der Seite HTTPS-Zertifikat anzeigen müssen, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Erstellen eines HTTPS-Sicherheitszertifikats

Sie können aus mehreren Gründen ein neues HTTPS-Sicherheitszertifikat generieren, z. B. wenn Sie mit einer anderen Zertifizierungsstelle signieren möchten oder wenn das aktuelle Sicherheitszertifikat abgelaufen ist. Das neue Zertifikat ersetzt das vorhandene Zertifikat.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

Wenn Sie keinen Zugriff auf die Web-UI von Unified Manager haben, können Sie mithilfe der Wartungskonsole das HTTPS-Zertifikat mit den gleichen Werten neu generieren.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

   Das Dialogfeld „HTTPS-Zertifikat neu erstellen“ wird angezeigt.

3. Wählen Sie je nach Erstellung des Zertifikats eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.
Generieren Sie das Zertifikat mithilfe anderer Werte	`Click the *Update the Current Certificate Attributes* option. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Die anderen Felder benötigen keine Werte, aber Sie können Werte eingeben, z. B. für Stadt, Bundesland und Land, wenn diese Werte in das Zertifikat eingetragen werden sollen.`  Sie können das Kontrollkästchen „`lokale Identifizierungsdaten ausschließen (z. B. localhost)`“ aktivieren, 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.

4. Klicken Sie auf **Ja**, um das Zertifikat erneut zu generieren.
5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.

Nachdem Sie fertig sind

Überprüfen Sie die neuen Zertifikatinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

Starten Sie die Virtual Machine von Unified Manager neu

Sie können die virtuelle Maschine von der Wartungskonsole von Unified Manager aus neu starten. Sie müssen neu starten, nachdem Sie ein neues Sicherheitszertifikat erstellt haben oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance wird eingeschaltet.

Sie sind als Maintenance-Benutzer bei der Wartungskonsole angemeldet.

Über diese Aufgabe

Sie können die virtuelle Maschine von vSphere auch mit der Option **Neustart Gast** neu starten. Weitere Informationen finden Sie in der VMware Dokumentation.

Schritte

1. Öffnen Sie die Wartungskonsole.
2. Wählen Sie **Systemkonfiguration** > **Virtuelle Maschine Neu Starten**.

Herunterladen einer Anforderung zum Signieren eines HTTPS-Zertifikats

Sie können eine Zertifizierungsanfrage für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, so dass Sie die Datei einer Zertifizierungsstelle zum Signieren bereitstellen 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.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikatsignierungsanforderung herunterladen**.
3. Speichern Sie die `<hostname>.csr` Datei:

Nachdem Sie fertig sind

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

Installieren eines HTTPS-Sicherheitszertifikats

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.

Bevor Sie beginnen

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 die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf  , und klicken Sie dann im Menü **Setup** auf **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.

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-----
```

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 Anforderung zum Signieren von Zertifikaten herunterladen, ein neues HTTPS-Zertifikat erstellen oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues 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. Sie werden vom Browser aufgefordert, das zu speichern `<hostname>.csr` Datei so, dass Sie die Datei an eine 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 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.