



# **Erstellen eines HTTPS-Sicherheitszertifikats**

## **Active IQ Unified Manager 9.9**

NetApp  
April 05, 2024

This PDF was generated from <https://docs.netapp.com/de-de/active-iq-unified-manager-99/online-help/task-restarting-the-unified-manager-virtual-machine.html> on April 05, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Erstellen eines HTTPS-Sicherheitszertifikats. . . . . 1
  - Bevor Sie beginnen . . . . . 1
  - Über diese Aufgabe . . . . . 1
  - Schritte . . . . . 1
  - Nachdem Sie fertig sind . . . . . 2
  - Starten Sie die Virtual Machine von Unified Manager neu. . . . . 2

# Erstellen eines HTTPS-Sicherheitszertifikats

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein HTTPS-Standardzertifikat installiert. Sie können ein neues HTTPS-Sicherheitszertifikat generieren, das das vorhandene Zertifikat ersetzt.

## Bevor Sie beginnen

Sie müssen über die Anwendungsadministratorrolle verfügen.

## Über diese Aufgabe

Es kann mehrere Gründe geben, das Zertifikat neu zu generieren, z. B. wenn Sie bessere Werte für Distinguished Name (DN) haben möchten oder wenn Sie eine höhere Schlüsselgröße oder einen längeren Ablaufzeitraum wünschen oder wenn das aktuelle Zertifikat abgelaufen ist.

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. Beim erneuten Generieren von Zertifikaten können Sie die Schlüsselgröße und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie den verwenden `Reset Server Certificate Option` von der Wartungskonsole aus, wird dann ein neues HTTPS-Zertifikat erstellt, das 397 Tage lang gültig ist. Dieses Zertifikat hat einen RSA-Schlüssel der Größe 2048 Bit.


## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein > 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 <b>regenerieren mit aktuellen Zertifikatattributen</b> .

Ihr Ziel ist	Tun Sie das...
Generieren Sie das Zertifikat mithilfe anderer Werte	<p>Klicken Sie auf die Option <b>Aktuellen Zertifikatattributen aktualisieren</b>.</p> <p>Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Der „Common Name“ sollte auf den FQDN des Hosts gesetzt werden. Die anderen Felder erfordern keine Werte, Sie können aber Werte eingeben, beispielsweise FÜR E-MAIL, FIRMA, ABTEILUNG, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat ausgefüllt werden sollen. Sie können auch aus der verfügbaren SCHLÜSSEGRÖSSE (der Schlüsselalgorithmus lautet „RSA“) und DER GÜLTIGKEITSDAUER auswählen.</p> <div data-bbox="440 850 493 905">  </div> <ul style="list-style-type: none"> <li>• Die zulässigen Werte für die Schlüsselgröße sind 2048, 3072 Und 4096.</li> <li>• Die Gültigkeitsdauer beträgt mindestens 1 Tag bis maximal 36500 Tage.</li> </ul> <p>Auch wenn eine Gültigkeitsdauer von 36500 Tagen zulässig ist, wird empfohlen, eine Gültigkeitsdauer von nicht mehr als 397 Tagen oder 13 Monaten zu verwenden. Denn wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen auswählen und planen, eine CSR für dieses Zertifikat zu exportieren und es von einer bekannten Zertifizierungsstelle unterschrieben zu lassen, wird die Gültigkeit des von der Zertifizierungsstelle zurückgegebenen signierten Zertifikats auf 397 Tage reduziert.</p> <ul style="list-style-type: none"> <li>• 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, wird im Feld Alternative Namen nur das verwendet, was Sie in das Feld eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.</li> </ul>

1. Klicken Sie auf **Ja**, um das Zertifikat erneut zu generieren.
2. 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**.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.