Der Hostname von Unified Manager kann geändert werden

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/config/task_change_unified_manager_host_name_on_vmware.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Der Hostname von Unified Manager kann geändert werden 1
Der Hostname der virtuellen Active IQ Unified Manager Appliance kann geändert werden. 1
In Active IQ Unified Manager kann ein HTTPS-Sicherheitszertifikat generiert werden 2
Starten Sie die virtuelle Maschine Active IQ Unified Manager neu. 4
Ändern des Hostnamens von Active IQ Unified Manager auf Linux Systemen 4

Der Hostname von Unified Manager kann geändert werden

Der Hostname der virtuellen Active IQ Unified Manager Appliance kann geändert werden.

Dem Netzwerkhost wird beim ersten Deployment der virtuellen Unified Manager Appliance ein Name zugewiesen. Sie können den Hostnamen nach dem Deployment ändern. Wenn Sie den Hostnamen ändern, müssen Sie auch das HTTPS-Zertifikat neu generieren.

Bevor Sie beginnen

Um diese Aufgaben ausführen zu können, müssen Sie bei Unified Manager als Wartungsbenutzer angemeldet sein oder Ihnen muss die Rolle Application Administrator zugewiesen sein.

Der Hostname (oder die Host-IP-Adresse) kann für den Zugriff auf die Unified Manager Web-Benutzeroberfläche verwendet werden. Wenn während des Deployment eine statisch IP-Adresse für Ihr Netzwerk konfiguriert wurde, wurde dem Netzwerkhost ein Name zugewiesen. Wenn das Netzwerk mit DHCP konfiguriert wurde, sollte der Hostname aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht ordnungsgemäß konfiguriert sind, wird der Hostname “Unified Manager” automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat generieren, wenn Sie den Hostnamen ändern und beabsichtigen, mit dem neuen Hostnamen auf die Unified Manager web UI zuzugreifen.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat mit dem tatsächlichen Hostnamen übereinstimmt.

Wenn Sie den Hostnamen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Hostname wird in WFA nicht automatisch aktualisiert.

Das neue Zertifikat tritt erst nach einem Neustart der virtuellen Maschine des Unified Manager in Kraft.

Schritte

1. Generierung eines HTTPS-Sicherheitszertifikats

   Wenn Sie den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es dem neuen Hostnamen zuzuordnen.

2. Neustart der virtuellen Maschine von Unified Manager

   Nach der Neugenerierung des HTTPS-Zertifikats ist ein Neustart der virtuellen Maschine von Unified Manager erforderlich.

In Active IQ Unified Manager kann ein HTTPS-Sicherheitszertifikat generiert werden

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein Standard HTTPS Zertifikat installiert. Es kann ein neues HTTPS Sicherheitszertifikat generiert werden, das das vorhandene Zertifikat ersetzt.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Es kann verschiedene Gründe für die Neugenerierung des Zertifikats geben, beispielsweise wenn Sie bessere Werte für den individuellen Namen (DN) wünschen, eine höhere Schlüssellänge oder eine längere Gültigkeitsdauer benötigen oder wenn das aktuelle Zertifikat abgelaufen ist.

Wenn Sie keinen Zugriff auf die Unified Manager Web-UI haben, können Sie das HTTPS-Zertifikat über die Managementplattform mit denselben Werten neu generieren. Beim Neugenerieren von Zertifikaten können Sie die Schlüssellänge und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie in der Managementplattform die Option `Reset Server Certificate` verwenden, wird ein neues HTTPS-Zertifikat mit einer Gültigkeit von 397 Tagen erstellt. Dieses Zertifikat verfügt über einen RSA-Schlüssel mit einer Länge von 2048 Bit.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. **Regenerate HTTPS Certificate** auswählen.

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

3. Je nachdem, wie das Zertifikat generiert werden soll, ist eine der folgenden Optionen auszuwählen:

Wenn Sie möchten…	Folgendes ist zu tun…
Neugenerierung des Zertifikats mit den aktuellen Werten	Die Option **Neu generieren mit aktuellen Zertifikatsattributen** auswählen.

Wenn Sie möchten…	Folgendes ist zu tun…
Erzeugen des Zertifikats mit verschiedenen Werten	Auswahl der Option **Aktuelle Zertifikatsattribute aktualisieren**. Die Felder „Allgemeiner Name“ und „Alternative Namen“ verwenden die Werte des vorhandenen Zertifikats, 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 jedoch Werte eingeben, z. B. für E-MAIL, COMPANY, DEPARTMENT, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat eingetragen werden sollen. Außerdem kann aus der verfügbaren KEY SIZE (der Schlüsselalgorithmus ist „`RSA`“) und dem VALIDITY PERIOD ausgewählt werden. • Die zulässigen Werte für die Schlüssellänge sind `2048`, `3072` und `4096`. • Die Gültigkeitsdauer beträgt mindestens 1 Tag und maximal 36500 Tage. Obwohl eine Gültigkeitsdauer von 36.500 Tagen zulässig ist, empfiehlt sich eine Gültigkeitsdauer von maximal 397 Tagen bzw. 13 Monaten. Wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen wählen und planen, einen CSR für dieses Zertifikat zu exportieren und von einer bekannten CA signieren zu lassen, beträgt die Gültigkeit des von der CA zurückgegebenen signierten Zertifikats nur 397 Tage. • Sie können das Kontrollkästchen „Lokale Identifikationsinformationen ausschließen (z. B. localhost)“ aktivieren, wenn Sie die lokalen Identifikationsinformationen 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 Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld

4. Mit **Ja** kann das Zertifikat neu generiert werden.
5. Damit das neue Zertifikat wirksam wird, ist ein Neustart des Unified Manager Server erforderlich.
6. Die neuen Zertifikatsinformationen können durch Anzeige des HTTPS-Zertifikats überprüft werden.

Starten Sie die virtuelle Maschine Active IQ Unified Manager neu.

Sie können die virtuelle Maschine über die Managementplattform von Unified Manager neu starten. Ein Neustart ist erforderlich, nachdem ein neues Sicherheitszertifikat generiert wurde oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance ist eingeschaltet.

Sie sind bei der Managementplattform für die Wartung als Wartungsbenutzer angemeldet.

Sie können die virtuelle Maschine auch von vSphere aus mit der Option **Restart Guest** neu starten. Weitere Informationen finden Sie in der VMware-Dokumentation.

Schritte

1. Auf die Wartungskonsole zugreifen.
2. Für den Neustart der virtuellen Maschine ist **System Configuration** > **Reboot Virtual Machine** auszuwählen.

Ändern des Hostnamens von Active IQ Unified Manager auf Linux Systemen

Gegebenenfalls möchten Sie den Hostnamen des Red Hat Enterprise Linux Rechners ändern, auf dem Unified Manager installiert ist. Beispielsweise können Sie den Host umbenennen, um Ihre Unified Manager Server beim Auflisten Ihrer Linux Rechner leichter nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf das Linux-System, auf dem Unified Manager installiert ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web UI von Unified Manager zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname vom DNS-Server übernommen werden.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat generieren, wenn Sie den Hostnamen ändern und beabsichtigen, den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche zu verwenden.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche zugreifen, müssen Sie bei einer Änderung des Hostnamens kein neues Zertifikat generieren. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat mit dem tatsächlichen Hostnamen übereinstimmt. Das neue Zertifikat wird erst nach einem Neustart des Linux-Rechners wirksam.

Wenn Sie den Hostnamen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Hostname wird in WFA nicht automatisch aktualisiert.

Schritte

1. Sie melden sich als Root-Benutzer bei dem Unified Manager System an, das Sie ändern möchten.
2. Zum Beenden der Unified Manager Software und der zugehörigen MySQL Software ist der folgende Befehl einzugeben:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Die Änderung des Hostnamens erfolgt mit dem Linux `hostnamectl` Befehl:

   ```
   hostnamectl set-hostname new_FQDN

   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Das HTTPS-Zertifikat für den Server neu generieren:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Neustart des Netzwerkservice:

   ```
   systemctl restart NetworkManager.service
   ```

6. Nach dem Neustart des Dienstes sollte geprüft werden, ob der neue Hostname sich selbst anpingen kann:

   ```
   ping new_hostname

   ping nuhost
   ```

   Dieser Befehl sollte dieselbe IP-Adresse zurückgeben, die zuvor für den ursprünglichen Hostnamen festgelegt wurde.

7. Nachdem Sie die Änderung Ihres Hostnamens abgeschlossen und überprüft haben, muss Unified Manager mit dem folgenden Befehl neu gestartet werden:

   ```
   systemctl start mysqld ocie ocieau
   ```

Copyright-Informationen

Copyright © 2026 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, BEISPIELHAFTE 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 IRGENDEINER 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.