



Ändern des Unified Manager-Hostnamens

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

- Ändern des Unified Manager-Hostnamens 1
 - Ändern des Hostnamens der virtuellen Unified Manager-Appliance 1
 - Generieren Sie ein HTTPS-Sicherheitszertifikat 2
 - Starten Sie die virtuelle Unified Manager-Maschine neu 4
 - Ändern des Unified Manager-Hostnamens auf Linux-Systemen 4

Ändern des Unified Manager-Hostnamens

Irgendwann möchten Sie möglicherweise den Hostnamen des Systems ändern, auf dem Sie Unified Manager installiert haben. Beispielsweise möchten Sie den Host möglicherweise umbenennen, um Ihre Unified Manager-Server einfacher nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Die zum Ändern des Hostnamens erforderlichen Schritte unterscheiden sich, je nachdem, ob Unified Manager auf einem VMware ESXi-Server, einem Red Hat Linux-Server oder einem Microsoft Windows-Server ausgeführt wird.

Ändern des Hostnamens der virtuellen Unified Manager-Appliance

Dem Netzwerkhost wird bei der ersten Bereitstellung der virtuellen Unified Manager-Appliance ein Name zugewiesen. Sie können den Hostnamen nach der Bereitstellung 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 Wartungsb Benutzer angemeldet sein oder Ihnen die Rolle des Anwendungsadministrators zugewiesen sein.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht richtig konfiguriert sind, wird der Hostname „Unified Manager“ automatisch zugewiesen und mit dem Sicherheitszertifikat verknüpft.

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

Wenn Sie auf die Web-Benutzeroberfläche zugreifen, indem Sie die IP-Adresse des Servers anstelle des Hostnamens verwenden, 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 wird erst wirksam, wenn die virtuelle Unified Manager-Maschine neu gestartet wird.

Schritte

1. Generieren Sie ein HTTPS-Sicherheitszertifikat

Wenn Sie den neuen Hostnamen für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es mit dem neuen Hostnamen zu verknüpfen.

2. Starten Sie die virtuelle Unified Manager-Maschine neu

Nachdem Sie das HTTPS-Zertifikat neu generiert haben, müssen Sie die virtuelle Unified Manager-Maschine neu starten.

Generieren Sie ein HTTPS-Sicherheitszertifikat

Bei der ersten Installation von Active IQ Unified Manager wird ein Standard-HTTPS-Zertifikat installiert. Sie können ein neues HTTPS-Sicherheitszertifikat generieren, das das vorhandene Zertifikat ersetzt.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Es kann mehrere Gründe geben, das Zertifikat neu zu generieren, beispielsweise wenn Sie bessere Werte für den Distinguished Name (DN) wünschen, eine höhere Schlüsselgröße oder eine längere Ablaufdauer wünschen oder wenn das aktuelle Zertifikat abgelaufen ist.

Wenn Sie keinen Zugriff auf die Unified Manager-Web-Benutzeroberfläche haben, können Sie das HTTPS-Zertifikat mithilfe der Wartungskonsole mit denselben Werten neu generieren. Beim Neugenerieren von Zertifikaten können Sie die Schlüsselgröße und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie die `Reset Server Certificate Option` aus der Wartungskonsole, dann wird ein neues HTTPS-Zertifikat erstellt, das 397 Tage gültig ist. Dieses Zertifikat verfügt über einen RSA-Schlüssel mit einer Größe von 2048 Bit.

Schritte

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

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

3. Wählen Sie eine der folgenden Optionen, je nachdem, wie Sie das Zertifikat generieren möchten:

Wenn Sie wollen...	Machen Sie Folgendes...
Zertifikat mit den aktuellen Werten neu generieren	Klicken Sie auf die Option Mit aktuellen Zertifikatattributen neu generieren .

Wenn Sie wollen...	Machen Sie Folgendes...
Generieren Sie das Zertifikat mit unterschiedlichen Werten	Klicken Sie auf die Option Aktuelle Zertifikatattribute aktualisieren. Wenn Sie keine neuen Werte eingeben, werden in den Feldern „Allgemeiner Name“ und „Alternative Namen“ die Werte aus dem vorhandenen Zertifikat verwendet. Der „Common Name“ sollte auf den FQDN des Hosts eingestellt werden. Für die anderen Felder sind keine Werte erforderlich, Sie können jedoch beispielsweise Werte für E-MAIL, FIRMA, ABTEILUNG, Stadt, Bundesland und Land eingeben, wenn diese Werte im Zertifikat eingetragen werden sollen. Sie können auch aus der verfügbaren SCHLÜSSELGRÖSSE (der Schlüsselalgorithmus ist „RSA“) und der GÜLTIGKEITSDAUER auswählen.

4. Klicken Sie auf **Ja**, um das Zertifikat neu zu generieren.

5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.

6. Überprüfen Sie die neuen Zertifikatsinformationen, indem Sie das HTTPS-Zertifikat anzeigen. Die zulässigen Werte für die Schlüsselgröße sind 2048, 3072 und 4096.

Starten Sie die virtuelle Unified Manager-Maschine neu

Sie können die virtuelle Maschine über die Wartungskonsole von Unified Manager neu starten. Nach der Generierung eines neuen Sicherheitszertifikats oder bei einem Problem mit der virtuellen Maschine ist ein Neustart erforderlich.

Bevor Sie beginnen

Die virtuelle Appliance ist eingeschaltet.

Sie sind als Wartungsbenutzer bei der Wartungskonsole angemeldet.

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

Schritte

1. Greifen Sie auf die Wartungskonsole zu.
2. Wählen Sie **Systemkonfiguration > Virtuelle Maschine neu starten**.

Ändern des Unified Manager-Hostnamens auf Linux-Systemen

Irgendwann möchten Sie möglicherweise den Hostnamen der Red Hat Enterprise Linux-Maschine ändern, auf der Sie Unified Manager installiert haben. Beispielsweise möchten Sie möglicherweise den Host umbenennen, um Ihre Unified Manager-Server beim Auflisten Ihrer Linux-Computer einfacher nach Typ, Arbeitsgruppe oder Clustergruppe zu identifizieren.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf das Linux-System verfügen, auf dem Unified Manager installiert ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. 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 den neuen Hostnamen für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwenden möchten.

Wenn Sie auf die Web-Benutzeroberfläche zugreifen, indem Sie die IP-Adresse des Servers anstelle des Hostnamens verwenden, 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. Das neue Zertifikat wird erst nach einem Neustart der Linux-Maschine 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.

Die Gültigkeitsdauer beträgt mindestens 1 Tag und höchstens 36500 Tage.

Obwohl eine Gültigkeitsdauer von 36.500 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 von einer bekannten Zertifizierungsstelle signieren zu lassen, wird die Gültigkeit des signierten Zertifikats, das Ihnen von der Zertifizierungsstelle zurückgegeben wird, auf 397 Tage reduziert.

- Sie können das Kontrollkästchen **Lokale Identifizierungsinformationen ausschließen** (z. B. localhost) aktivieren, 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 **Identifizierungsinformationen** eingeben. Wenn dieses Feld leer gelassen wird, enthält das resultierende Zertifikat überhaupt kein Feld für alternative Namen.

Schritte

1. Melden Sie sich als Root-Benutzer beim Unified Manager-System an, das Sie ändern möchten.
2. Stoppen Sie die Unified Manager-Software und die zugehörige MySQL-Software, indem Sie den folgenden Befehl eingeben:

```
systemctl stop ocieau ocie mysqld
```

3. Ändern Sie den Hostnamen mit dem Linux `hostnamectl` Befehl:

```
hostnamectl set-hostname new_FQDN
```

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

4. Generieren Sie das HTTPS-Zertifikat für den Server neu:

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

5. Starten Sie den Netzwerkdienst neu:

```
systemctl restart NetworkManager.service
```

6. Überprüfen Sie nach dem Neustart des Dienstes, ob der neue Hostname in der Lage ist, sich selbst anzupingen:

```
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, starten Sie Unified Manager neu, indem Sie den folgenden Befehl eingeben:

```
systemctl start mysqld ocie ocieau
```

Copyright-Informationen

Copyright © 2025 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 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.