Ändern des Unified Manager-Host-Namens

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

This PDF was generated from https://docs.netapp.com/de-de/oncommand-unified-manager-95/config/task-generating-an-https-security-certificate-ocf.html on October 23, 2024. Always check docs.netapp.com for the latest.

Inhalt

Ändern des Unified Manager-Host-Namens 1
Ändern des Host-Namens der virtuellen Unified Manager-Appliance 1
Ändern des Unified Manager Host-Namens auf Linux-Systemen 4

Ändern des Unified Manager-Host-Namens

Irgendwann möchten Sie möglicherweise den Host-Namen des Systems ändern, auf dem Unified Manager installiert ist. Beispielsweise möchten Sie den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren.

Je nachdem, ob Unified Manager auf einem VMware ESXi Server, auf einem Red hat oder CentOS Linux Server oder auf einem Microsoft Windows Server ausgeführt wird, sind die zum Ändern des Host-Namens erforderlichen Schritte unterschiedlich.

Ändern des Host-Namens der virtuellen Unified Manager-Appliance

Dem Netzwerk-Host wird ein Name zugewiesen, wenn die virtuelle Unified Manager-Appliance zuerst bereitgestellt wird. Sie können den Host-Namen nach der Bereitstellung ändern. Wenn Sie den Hostnamen ändern, müssen Sie auch das HTTPS-Zertifikat neu generieren.

Bevor Sie beginnen

Sie müssen bei Unified Manager als Wartungbenutzer angemeldet sein oder Ihnen die Rolle „OnCommand Administrator“ zugewiesen haben, um diese Aufgaben ausführen zu können.

Über diese Aufgabe

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

Unabhängig davon, wie der Hostname zugewiesen wurde, wenn Sie den Host-Namen ändern und beabsichtigen, den neuen Hostnamen zum Zugriff auf die Unified Manager Web-UI zu verwenden, müssen Sie ein neues Sicherheitszertifikat generieren.

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat so zu aktualisieren, dass der Hostname im Zertifikat dem tatsächlichen Hostnamen entspricht.

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

Das neue Zertifikat wird erst wirksam, wenn die virtuelle Unified Manager-Maschine neu gestartet wird.

Schritte

1. Generieren eines HTTPS-Sicherheitszertifikats

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

2. Starten Sie die Virtual Machine von Unified Manager neu

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

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**.

Ihr Ziel ist	Tun Sie das…
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**.

Ändern des Unified Manager Host-Namens auf Linux-Systemen

Irgendwann möchten Sie den Host-Namen von Red hat Enterprise Linux oder CentOS Rechner ändern, auf dem Unified Manager installiert ist. Sie möchten beispielsweise den Host umbenennen, um Ihre Unified Manager-Server nach Typ, Arbeitsgruppe oder überwachten Cluster-Gruppen einfacher zu identifizieren, wenn Sie Ihre Linux-Maschinen auflisten.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Wenn Sie über die IP-Adresse des Servers und nicht über den Hostnamen auf die Web-Benutzeroberfläche 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 dem tatsächlichen Hostnamen entspricht. Das neue Zertifikat wird erst wirksam, wenn der Linux-Rechner neu gestartet wird.

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

Schritte

1. Melden Sie sich als Root-Benutzer beim Unified Manager-System an, das Sie ändern möchten.

2. Beenden Sie die Unified Manager Software und die zugehörige MySQL Software, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben:
3. Ändern Sie den Host-Namen mit Linux `hostnamectl` Befehl: `hostnamectl set-hostname new_FQDN`

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

4. Generieren Sie das HTTPS-Zertifikat für den Server erneut:`/opt/netapp/essentials/bin/cert.sh create`
5. Netzwerkdienst neu starten: `service network restart`
6. Überprüfen Sie nach dem Neustart des Dienstes, ob der neue Hostname selbst pingen 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 Host-Namens abgeschlossen und überprüft haben, starten Sie Unified Manager neu, indem Sie in der angezeigten Reihenfolge die folgenden Befehle eingeben:

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, 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.