# Durchführung von Konfigurations- und Administrationsaufgaben

## 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/concept-overview-of-the-configuration-sequence.html on October 23, 2024. Always check docs.netapp.com for the latest.

# Inhalt

Durchführung von Konfigurations- und Administrationsaufgaben . . . . . 1
Konfigurieren Von Unified Manager . . . . . 1

# Durchführung von Konfigurations- und Administrationsaufgaben

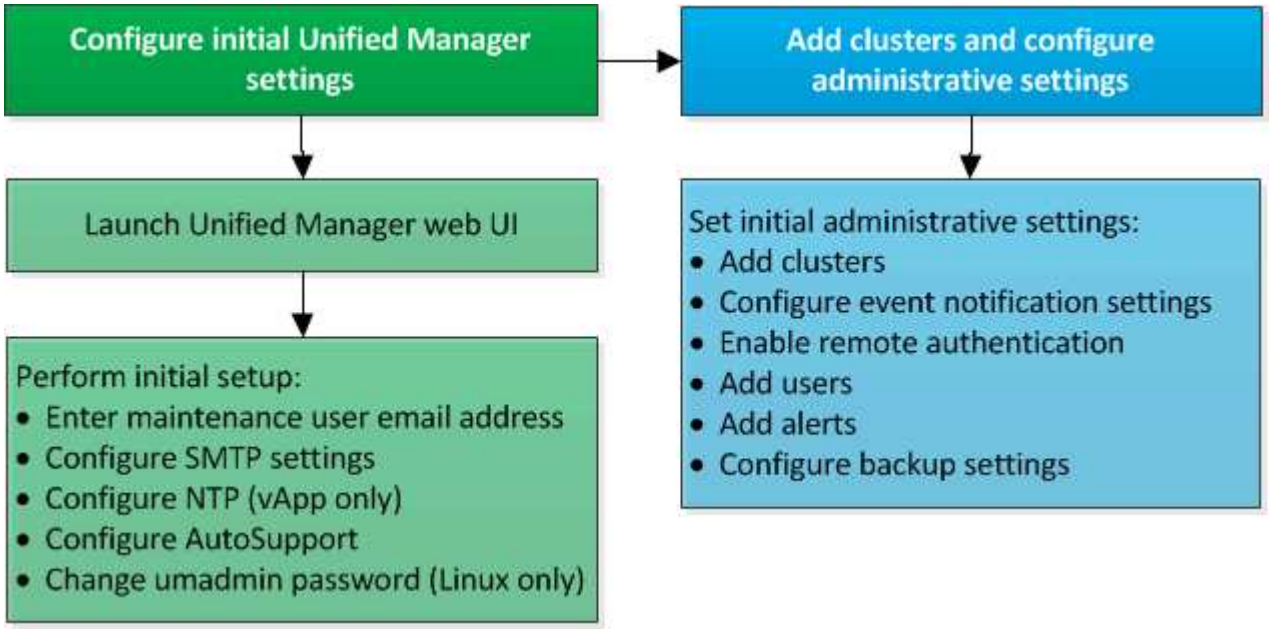
## Konfigurieren Von Unified Manager

Nach der Installation von Unified Manager müssen Sie die Ersteinrichtung (auch als Assistent für die erste Erfahrung bezeichnet) abschließen, um auf die Web-Benutzeroberfläche zuzugreifen. Anschließend können Sie weitere Konfigurationsaufgaben ausführen, wie beispielsweise das Hinzufügen von Clustern, die Konfiguration der Remote-Authentifizierung, das Hinzufügen von Benutzern und das Hinzufügen von Warnmeldungen.

Einige der in diesem Handbuch beschriebenen Verfahren sind erforderlich, um die Ersteinrichtung der Unified Manager-Instanz durchzuführen. Andere Verfahren empfehlen Konfigurationseinstellungen, die für die Einrichtung in der neuen Instanz hilfreich sind oder die gut zu wissen sind, bevor Sie mit dem regelmäßigen Monitoring Ihrer ONTAP Systeme beginnen.

### Überblick über die Konfigurationssequenz

Der Konfigurations-Workflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.




### Zugriff auf die Web-Benutzeroberfläche von Unified Manager

Nach der Installation von Unified Manager können Sie auf die Web-Benutzeroberfläche zugreifen, um Unified Manager einzurichten, damit Sie mit der Überwachung Ihrer ONTAP-Systeme beginnen können.

**Bevor Sie beginnen**

- Wenn Sie zum ersten Mal auf die Web-UI zugreifen, müssen Sie sich als Wartungbenutzer (oder umadmin-Benutzer für Linux-Installationen) einloggen.
- Wenn Sie Benutzern den Zugriff auf Unified Manager mit dem Kurznamen erlauben möchten, anstatt den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse zu verwenden, muss die Netzwerkkonfiguration diesen Kurznamen auf einen gültigen FQDN auflösen.
- Wenn der Server ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, dass der Zugriff fortgesetzt wird, oder ein Zertifikat einer Zertifizierungsstelle (CA) installieren, das digitale Zertifikat für die Serverauthentifizierung unterzeichnet hat.

**Schritte**

1. Starten Sie die Web-UI von Unified Manager über Ihren Browser, indem Sie die am Ende der Installation angezeigte URL verwenden. Die URL ist die IP-Adresse oder der vollqualifizierte Domain-Name (FQDN) des Unified Manager-Servers.

   Der Link hat das folgende Format: https://`URL`.

2. Melden Sie sich mit den Anmeldedaten der Wartungsbenutzer bei der Web-Benutzeroberfläche von Unified Manager an.

## Die Ersteinrichtung der Unified Manager-Weboberfläche durchführen

Um Unified Manager zu verwenden, müssen Sie zunächst die anfänglichen Setup-Optionen konfigurieren, einschließlich des NTP-Servers, der Wartungs-Benutzer-E-Mail-Adresse und des SMTP-Server-Host-Namens und -Optionen.

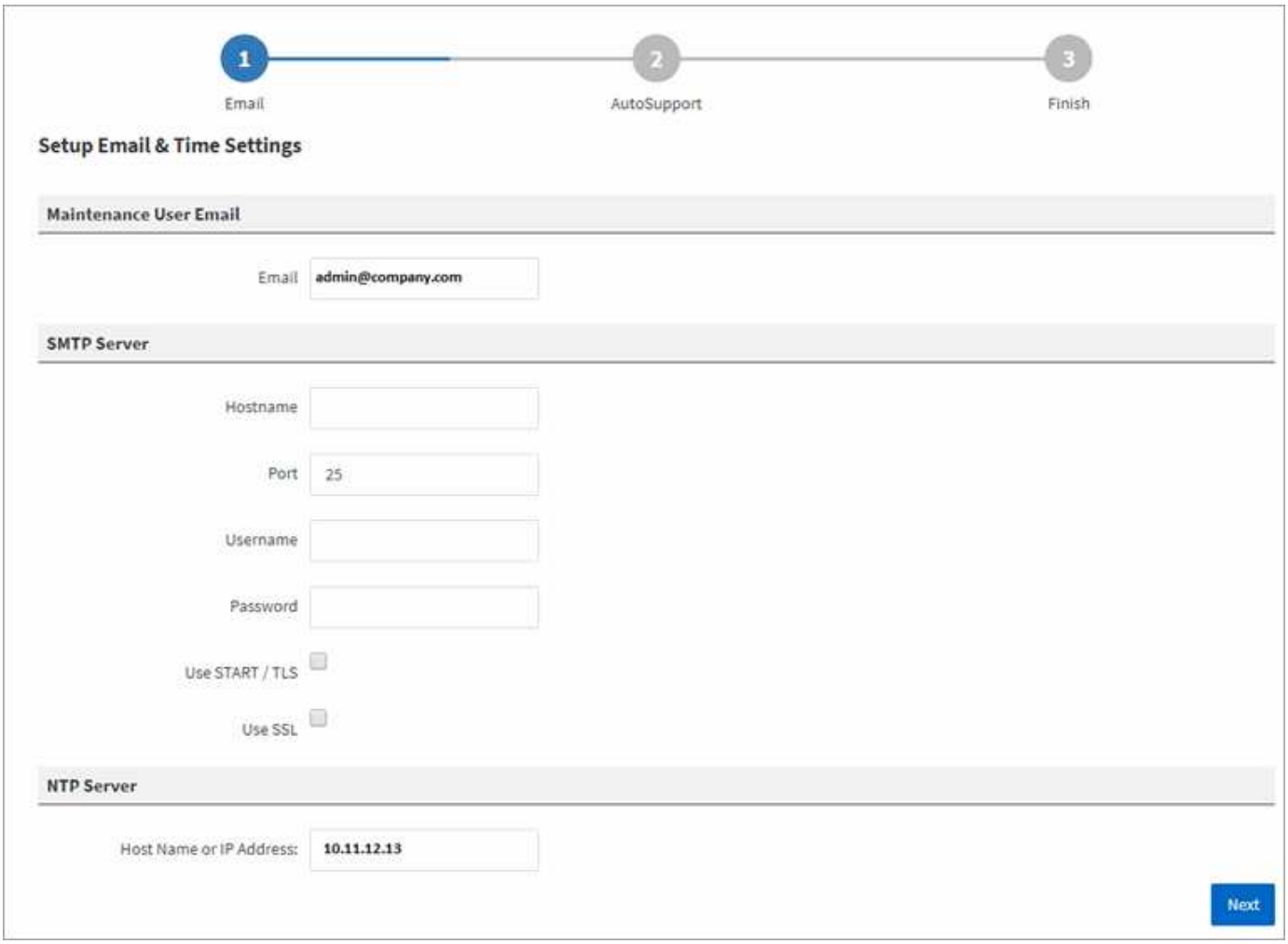
**Bevor Sie beginnen**

Sie müssen die folgenden Vorgänge durchgeführt haben:

- Die Web-UI von Unified Manager wurde über die nach der Installation bereitgestellte URL gestartet
- Sie sind mit dem während der Installation erstellten Wartungs-Benutzernamen und -Passwort (umadmin-Benutzer für Linux-Installationen) angemeldet

**Über diese Aufgabe**

Die Seite „Initial Setup“ von OnCommand Unified Manager wird nur angezeigt, wenn Sie das erste Mal auf die Web-Benutzeroberfläche zugreifen. Die folgende Seite ist von einer Installation auf VMware.




Wenn Sie später eine dieser Optionen ändern möchten, können Sie die Verwaltungsoptionen verwenden, auf die Sie zugreifen können, indem Sie auf die Schaltfläche * klicken* Aus der Symbolleiste von Unified Manager.

### Schritte

1. Geben Sie im Fenster **OnCommand Unified Manager Initial Setup** die E-Mail-Adresse des Wartungsbenutzers, den SMTP-Serverhostnamen und weitere SMTP-Optionen sowie den NTP-Server (nur VMware-Installationen) ein. Klicken Sie anschließend auf **Weiter**.
2. Klicken Sie auf der Seite **AutoSupport** auf **zustimmen und fortfahren**, um AutoSupport zu aktivieren.

   Wenn Sie einen Proxy für den Zugriff auf das Internet festlegen müssen, um AutoSupport-Inhalte an den Support zu senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Verwaltungsoptionen.

3. Auf Red hat- und CentOS-Systemen können Sie das umadmin-Benutzerpasswort von der standardmäßigen Zeichenfolge „`admin`“ in eine personalisierte Zeichenfolge ändern.

### Ergebnisse

Das anfängliche Setup-Fenster wird geschlossen, und die Unified Manager Web-Benutzeroberfläche wird angezeigt. Die Seite Configuration/Cluster Data Sources wird angezeigt, sodass Sie Cluster zu Ihrem System hinzufügen können.

## Hinzufügen von Clustern

Sie können OnCommand Unified Manager um ein Cluster erweitern, sodass Sie das Cluster überwachen können. Dazu gehört beispielsweise die Möglichkeit, Cluster-Informationen wie Systemzustand, Kapazität, Performance und Konfiguration des Clusters abzurufen, damit Sie etwaige auftretende Probleme finden und beheben können.

### Bevor Sie beginnen

- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die folgenden Informationen haben:
  - Host-Name oder Cluster-Management-IP-Adresse

    Der Hostname ist der FQDN oder der Kurzname, den Unified Manager zur Verbindung mit dem Cluster verwendet. Der Host-Name muss bis zur Cluster-Management-IP-Adresse aufgelöst werden.

    Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.
  - Benutzername und Passwort für den Data ONTAP-Administrator

    Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *ssh* und *http* eingestellt sein.
  - Typ des Protokolls (HTTP oder HTTPS), der auf dem Cluster konfiguriert werden kann und die Portnummer, die zum Herstellen einer Verbindung zum Cluster verwendet wird

    Sie können Cluster hinzufügen, die sich hinter einer NAT/Firewall befinden, indem Sie die Unified Manager NAT IP-Adresse verwenden. Alle angeschlossenen Workflow-Automatisierungs- oder SnapProtect-Systeme müssen sich auch hinter der NAT/Firewall befinden, und SnapProtect-API-Aufrufe müssen die NAT-IP-Adresse verwenden, um den Cluster zu identifizieren.
- Der FQDN des Unified Managers muss in der Lage sein, das ONTAP-System zu pingen.

  Sie können dies mit dem folgenden ONTAP-Befehl überprüfen: `ping -node node_name -destination Unified_Manager_FQDN`.
- Auf dem Unified Manager-Server muss ausreichend Speicherplatz vorhanden sein. Sie können dem Server kein Cluster hinzufügen, wenn mehr als 90 % des Speicherplatzes im Datenbankverzeichnis bereits belegt sind.

### Über diese Aufgabe

Für eine MetroCluster Konfiguration müssen Sie sowohl die lokalen als auch die Remote-Cluster hinzufügen, und die Cluster müssen korrekt konfiguriert sein.

Sie können ein einzelnes Cluster durch zwei Instanzen von Unified Manager überwachen, vorausgesetzt, Sie haben eine zweite Cluster-Management-LIF im Cluster konfiguriert, sodass jede Instanz von Unified Manager über eine andere LIF verbunden ist.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Cluster-Datenquellen**.
2. Klicken Sie auf der Seite **Konfiguration/Cluster-Datenquellen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Cluster hinzufügen** die erforderlichen Werte an, z. B. Hostname oder IP-Adresse des Clusters, Benutzername, Passwort, Protokoll für die Kommunikation und Portnummer.

   Standardmäßig sind das HTTPS-Protokoll und Port 443 ausgewählt.

   Sie können die Cluster-Management-IP-Adresse von IPv6 zu IPv4 oder von IPv4 zu IPv6 ändern. Die neue IP-Adresse wird im Cluster-Raster und die Seite der Cluster-Konfiguration nach Abschluss des nächsten Überwachungszyklus angezeigt.

4. Klicken Sie Auf **Absenden**.
5. Wenn HTTPS ausgewählt ist, führen Sie die folgenden Schritte aus:

   a. Klicken Sie im Dialogfeld **Autorisieren Host** auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.

   b. Klicken Sie Auf **Ja**.

      Unified Manager überprüft das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

   Wenn das Zertifikat abgelaufen ist, können Sie kein neues Cluster hinzufügen. Sie müssen zuerst das SSL-Zertifikat erneuern und dann den Cluster hinzufügen.

### Ergebnisse

Nachdem alle Objekte für ein neues Cluster erkannt wurden (ca. 15 Minuten), erfasst Unified Manager die historischen Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen. Wenn Sie Unified Manager während des Datenerfassungszeitraums neu starten, wird die Sammlung angehalten, und es werden für den fehlenden Zeitraum Lücken in den Leistungsdiagrammen angezeigt.

Wenn Sie eine Fehlermeldung erhalten, dass Sie das Cluster nicht hinzufügen können, prüfen Sie, ob die folgenden Probleme vorhanden sind:

- Wenn die Uhren auf den beiden Systemen nicht synchronisiert sind und das HTTPS-Zertifikat von Unified Manager nach dem Datum des Clusters liegt. Sie müssen sicherstellen, dass die Uhren mit NTP oder einem ähnlichen Dienst synchronisiert werden.
- Wenn der Cluster die maximale Anzahl von EMS-Benachrichtigungszielen erreicht hat, kann die Unified Manager-Adresse nicht hinzugefügt werden. Standardmäßig können nur 20 EMS-Benachrichtigungsziele auf dem Cluster definiert werden.

## Konfigurieren von Unified Manager zum Senden von Warnmeldungen

Sie können Unified Manager so konfigurieren, dass Sie Benachrichtigungen über Ereignisse in Ihrer Umgebung senden. Bevor Benachrichtigungen gesendet werden können, müssen Sie mehrere andere Unified Manager-Optionen konfigurieren.

### Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

### Über diese Aufgabe

Nach der Bereitstellung von Unified Manager und dem Abschluss der Erstkonfiguration sollten Sie Ihre Umgebung in Betracht ziehen, um Warnmeldungen auszulösen und auf der Grundlage des Eingangs von Ereignissen Benachrichtigungs-E-Mails oder SNMP-Traps zu generieren.

### Schritte

1. Konfigurieren Sie die Einstellungen für Ereignisbenachrichtigungen

   Wenn Sie Benachrichtigungen senden möchten, wenn bestimmte Ereignisse in Ihrer Umgebung auftreten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Benachrichtigung gesendet wird. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. Aktivieren Sie die Remote-Authentifizierung

   Wenn Remote-LDAP- oder Active Directory-Benutzer auf die Unified Manager-Instanz zugreifen und Warnmeldungen erhalten möchten, müssen Sie die Remote-Authentifizierung aktivieren.

3. Authentifizierungsserver hinzufügen

   Sie können Authentifizierungsserver hinzufügen, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

4. Benutzer hinzufügen

   Sie können mehrere verschiedene Typen von lokalen oder Remote-Benutzern hinzufügen und bestimmte Rollen zuweisen. Wenn Sie eine Warnmeldung erstellen, weisen Sie einen Benutzer zu, der die Benachrichtigungen erhält.

5. Warnmeldungen hinzufügen

   Nachdem Sie die E-Mail-Adresse zum Senden von Benachrichtigungen hinzugefügt haben, Benutzer hinzugefügt, um die Benachrichtigungen zu empfangen, Netzwerkeinstellungen konfiguriert und SMTP- und SNMP-Optionen konfiguriert, die für Ihre Umgebung erforderlich sind, können Sie Benachrichtigungen zuweisen.

### Konfigurieren von Einstellungen für Ereignisbenachrichtigungen

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder ein Ereignis einem Benutzer zugewiesen ist. Sie können den SMTP-Server konfigurieren, der zum Senden der Warnmeldung

verwendet wird, und Sie können verschiedene Benachrichtigungsmechanismen festlegen – beispielsweise können Alarmbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

#### Bevor Sie beginnen

Sie müssen die folgenden Informationen haben:

- E-Mail-Adresse, von der die Benachrichtigung gesendet wird

  Die E-Mail-Adresse wird im Feld „`von`“ in gesendeten Warnmeldungen angezeigt. Falls die E-Mail aus irgendeinem Grund nicht zugestellt werden kann, wird diese E-Mail-Adresse auch als Empfänger für nicht lieferbare E-Mails verwendet.

- Hostname des SMTP-Servers sowie Benutzername und Kennwort für den Zugriff auf den Server
- SNMP-Version, Trap-Ziel-Host-IP-Adresse, Outbound-Trap-Port und die Community zum Konfigurieren des SNMP-Trap

Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

#### Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Setup-Menü auf **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite **Setup/Benachrichtigungen** die entsprechenden Einstellungen und klicken Sie auf **Speichern**.

   **Hinweise:**

   - Wenn die von-Adresse mit der Adresse „`OnCommand@localhost.com`“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich versendet werden.
   - Wenn der Hostname des SMTP-Servers nicht aufgelöst werden kann, können Sie anstelle des Host-Namens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.

### Aktivieren der Remote-Authentifizierung

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager-Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können auf die grafische Schnittstelle von Unified Manager zugreifen, um Storage-Objekte und Daten zu managen.

#### Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

> Der Unified Manager-Server muss direkt mit dem Authentifizierungsserver verbunden sein. Sie müssen alle lokalen LDAP-Clients wie SSSD (System Security Services Daemon) oder NSLCD (Name Service LDAP Caching Daemon) deaktivieren.

**Über diese Aufgabe**

Sie können die Remote-Authentifizierung entweder über Open LDAP oder Active Directory aktivieren. Wenn die Remote-Authentifizierung deaktiviert ist, können Remote-Benutzer nicht auf Unified Manager zugreifen.

Die Remote-Authentifizierung wird über LDAP und LDAPS (Secure LDAP) unterstützt. Unified Manager verwendet 389 als Standardport für nicht sichere Kommunikation und 636 als Standardport für sichere Kommunikation.

Das Zertifikat, das zur Authentifizierung von Benutzern verwendet wird, muss dem X.509-Format entsprechen.

**Schritte**

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Option **Remote-Authentifizierung aktivieren** aus.
3. Wählen Sie im Feld **Authentifizierungsdienst** den Diensttyp aus und konfigurieren Sie den Authentifizierungsdienst.

| Für Authentifizierungstyp… | Geben Sie die folgenden Informationen ein… |
|---|---|
| Active Directory | • Administratorname des Authentifizierungsservers in einem der folgenden Formate:<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name` (Mit der entsprechenden LDAP-Schreibweise)<br>• Administratorpasswort<br>• Basisname (unter Verwendung der entsprechenden LDAP-Notation) |
| Öffnen Sie LDAP | • Distinguished Name binden (in der entsprechenden LDAP-Notation)<br>• Kennwort binden<br>• Basisname mit Distinguished Name |

Wenn die Authentifizierung eines Active Directory-Benutzers sehr viel Zeit oder Zeit in Anspruch nimmt, benötigt der Authentifizierungsserver wahrscheinlich eine lange Zeit, um darauf zu reagieren. Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt.

Wenn Sie die Option Sichere Verbindung verwenden für den Authentifizierungsserver auswählen, kommuniziert Unified Manager mit dem Authentifizierungsserver über das SSL-Protokoll (Secure Sockets Layer).

4. Fügen Sie Authentifizierungsserver hinzu, und testen Sie die Authentifizierung.

5. Klicken Sie auf **Speichern und Schließen**.

### Deaktivieren verschachtelter Gruppen von der Remote-Authentifizierung

Wenn die Remote-Authentifizierung aktiviert ist, können Sie die verschachtelte Gruppenauthentifizierung deaktivieren, sodass sich nur einzelne Benutzer und nicht Gruppenmitglieder im Remote-Zugriff auf Unified Manager authentifizieren können. Sie können verschachtelte Gruppen deaktivieren, wenn Sie die Reaktionszeit der Active Directory-Authentifizierung verbessern möchten.

#### Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory anwendbar.

#### Über diese Aufgabe

Wenn Sie die Unterstützung für verschachtelte Gruppen in Unified Manager deaktivieren, wird die Authentifizierungszeit möglicherweise verkürzt. Wenn die Unterstützung verschachtelter Gruppen deaktiviert ist und eine Remote-Gruppe zu Unified Manager hinzugefügt wird, müssen einzelne Benutzer Mitglieder der Remote-Gruppe sein, um sich bei Unified Manager zu authentifizieren.

#### Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Aktivieren Sie auf der Seite **Setup/Authentifizierung** das Kontrollkästchen **Nested Group Lookup deaktivieren**.
3. Klicken Sie Auf **Speichern**.

### Hinzufügen von Authentifizierungsservern

Sie können Authentifizierungsserver hinzufügen und die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

#### Bevor Sie beginnen

- Folgende Informationen müssen zur Verfügung stehen:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

#### Über diese Aufgabe

Wenn der neue Authentifizierungsserver Teil eines Hochverfügbarkeitspaars (HA-Paar) ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann

der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

**Schritte**

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Management Server** > **Authentifizierung**.
3. Aktivieren oder Deaktivieren der Option * Sichere Verbindungsauthentifizierung verwenden*:

| Ihr Ziel ist | Dann tun Sie das… |
| --- | --- |
| Aktivieren Sie sie | a. Aktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**.<br>b. Klicken Sie im Bereich Authentication Servers auf **Add**.<br>c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen den Authentifizierungsnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein.<br>d. Klicken Sie im Dialogfeld Host autorisieren auf Zertifikat anzeigen.<br>e. Überprüfen Sie im Dialogfeld Zertifikat anzeigen die Zertifikatinformationen und klicken Sie dann auf **Schließen**.<br>f. Klicken Sie im Dialogfeld Host autorisieren auf **Ja**.<br>Wenn Sie die Option **Sichere Verbindungsauthentifizierung verwenden** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet 636 als Standardport für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation. |

| Ihr Ziel ist | Dann tun Sie das… |
| --- | --- |
| Deaktivieren | a. Deaktivieren Sie im Kontrollkästchen Remoteauthentifizierung aktivieren die Option **Sichere Verbindung verwenden**.<br>b. Klicken Sie im Bereich Authentication Servers auf **Add**.<br>c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers und die Portdetails an.<br>d. Klicken Sie Auf **Hinzufügen**. |

Der hinzugefügte Authentifizierungsserver wird im Bereich Server angezeigt.

4. Führen Sie eine Testauthentifizierung durch, um zu bestätigen, dass Sie Benutzer im hinzugefügten Authentifizierungsserver authentifizieren können.

### Die Konfiguration der Authentifizierungsserver wird getestet

Sie können die Konfiguration Ihrer Authentifizierungsserver überprüfen, um sicherzustellen, dass der Verwaltungsserver mit diesen Servern kommunizieren kann. Sie können die Konfiguration validieren, indem Sie von Ihren Authentifizierungsservern nach einem Remote-Benutzer oder einer Remotegruppe suchen und diese unter Verwendung der konfigurierten Einstellungen authentifizieren.

#### Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe authentifizieren kann.
- Sie müssen Ihre Authentifizierungsserver hinzugefügt haben, damit der Verwaltungsserver von diesen Servern nach dem Remote-Benutzer oder der Remote-Gruppe suchen und diese authentifizieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

#### Über diese Aufgabe

Wenn der Authentifizierungsservice auf Active Directory festgelegt ist und Sie die Authentifizierung von Remote-Benutzern validieren, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

#### Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Klicken Sie auf der Seite **Setup/Authentifizierung** auf **Testauthentifizierung**.
3. Geben Sie im Dialogfeld **Testbenutzer** den Benutzernamen und das Kennwort des Remote-Benutzers oder den Benutzernamen der Remote-Gruppe an und klicken Sie dann auf **Test**.

Wenn Sie eine Remote-Gruppe authentifizieren, müssen Sie das Kennwort nicht eingeben.

### Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Verwaltung/Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

#### Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

#### Über diese Aufgabe

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

#### Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/Benutzer** auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld **Benutzer hinzufügen** den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

### Hinzufügen von Meldungen

Sie können Benachrichtigungen konfigurieren, um Sie über die Erzeugung eines bestimmten Ereignisses zu benachrichtigen. Sie können Meldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse mit einem bestimmten Schweregrad konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und ein Skript der Warnmeldung zuordnen.

**Bevor Sie beginnen**

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, SMTP-Server und SNMP-Trap-Host konfiguriert haben, damit der Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript basierend auf dem Ereignis ausführen möchten, müssen Sie das Skript mithilfe der Seite Management/Scripts zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.

**Über diese Aufgabe**

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite Konfiguration/Warnmeldungen erstellen, wie hier beschrieben.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Alerting**.
2. Klicken Sie auf der Seite **Konfiguration/Alarmfunktionen** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen**, und wählen Sie die Ressourcen aus, die in die Warnung aufgenommen oder von ihr ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Die Liste der verfügbaren Ressourcen zeigt auf der Grundlage der angegebenen Textzeichenfolge nur die Ressourcen an, die der Filterregel entsprechen. Die von Ihnen angegebene Textzeichenfolge ist die Groß-/Kleinschreibung.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschl- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschließregel, und die Warnung wird nicht für Ereignisse generiert, die sich auf die ausgeschlossene Ressource beziehen.

5. Klicken Sie auf **Events** und wählen Sie die Ereignisse basierend auf dem Ereignisnamen oder dem Schweregrad aus, für den Sie eine Warnung auslösen möchten.

   Um mehrere Ereignisse auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Actions**, und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit aus, wählen Sie aus, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung erzeugt wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnmeldung zur Bearbeitung erneut öffnen, erscheint das Feld Name leer, da die geänderte E-Mail-Adresse dem zuvor ausgewählten Benutzer nicht mehr zugeordnet ist. Wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite Verwaltung/Benutzer geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

#### Beispiel für das Hinzufügen einer Meldung

Dieses Beispiel zeigt, wie eine Warnung erstellt wird, die die folgenden Anforderungen erfüllt:

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse
- Aktionen: Enthält “sample@domain.com”, ein Skript “Test”, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein `HealthTest` Im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Eingabe `abc` Im Feld **Name enthält** werden die Volumes angezeigt, deren Name „`abc`“ enthält.
   b. Wählen Sie im Bereich Verfügbare Ressourcen **<<All Volumes whose name contains 'abc'>>** aus, und verschieben Sie sie in den Bereich Ausgewählte Ressourcen.
   c. Klicken Sie auf **Ausschließe**, und geben Sie ein `xyz` Klicken Sie im Feld **Name enthält** auf **Hinzufügen**.
3. Klicken Sie auf **Events** und wählen Sie im Feld Ereignis Severity * die Option **kritisch** aus.
4. Wählen Sie im Bereich passende Ereignisse die Option * Alle kritischen Ereignisse* aus, und verschieben Sie sie in den Bereich Ausgewählte Ereignisse.
5. Klicken Sie auf **Aktionen** und geben Sie ein `sample@domain.com` Im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **alle 15 Minuten**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können eine Warnung konfigurieren, um wiederholt Benachrichtigungen an die Empfänger für eine bestimmte Zeit zu senden. Legen Sie fest, zu welchem Zeitpunkt die Ereignisbenachrichtigung für die Warnmeldung aktiv ist.

7. Wählen Sie im Menü Skript zum Ausführen auswählen die Option **Test** Skript .
8. Klicken Sie Auf **Speichern**.

## EMS-Ereignisse, die automatisch dem Unified Manager hinzugefügt werden

Bei der Verwendung von Unified Manager 9.4 oder höher werden die folgenden ONTAP EMS-Ereignisse automatisch dem Unified Manager hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf jedem Cluster ausgelöst werden, das Unified Manager überwacht.

Die folgenden EMS-Ereignisse stehen zur Verfügung, wenn Cluster mit ONTAP 9.5 oder höher überwacht werden:

| Name des Unified Manager Events | EMS-Ereignisname | Betroffene Ressource | Schweregrad der ONTAP |
|---|---|---|---|
| Objektspeicherzugriff für Aggregatverschiebung verweigert | arl.netra.ca.check.failed | Aggregat | Fehler |
| Objektspeicherzugriff während eines Storage Failover für Aggregatverschiebung verweigert | gb.netra.ca.check.failed | Aggregat | Fehler |
| FabricPool Speicherplatz fast voll | Fabricpool.Fast.full | Cluster | Fehler |
| Beginn des NVMe-of-Grace-Zeitraums | nvmf.graceperiod.start | Cluster | Warnung |
| NVMe-of-Grace-Zeitraum aktiv | nvmf.graceperiod.active | Cluster | Warnung |
| NVMe-of-Grace-Zeitraum abgelaufen | nvmf.graceperiod.expired | Cluster | Warnung |
| LUN wurde zerstört | lun.destroy | LUN | Informationsdaten |
| Cloud AWS MetaDataConnFail | Cloud.aws.metadataConnFail | Knoten | Fehler |
| Cloud AWS IAMCredsExpired – Cloud | Cloud.aws.iamCredsExpired | Knoten | Fehler |
| Cloud AWS IAMCredsungültig | Cloud.aws.iamCredsungültig | Knoten | Fehler |
| Cloud AWS IAMCredsNotFound | Cloud.aws.iamCredsNotFound | Knoten | Fehler |
| Cloud AWS IAMCredsNotinitialisiert | Cloud.aws.iamNotinitialisiert | Knoten | Informationsdaten |
| Cloud AWS IAMRoleInvalid | Cloud.AWS.iamRoleIngültig | Knoten | Fehler |
| Cloud AWS IAMRoleNotFound | Cloud.aws.iamRoleNotFound | Knoten | Fehler |

| Name des Unified Manager Events | EMS-Ereignisname | Betroffene Ressource | Schweregrad der ONTAP |
|---|---|---|---|
| Objstore Host Unlösbar | Objstore.Host.unlösbar | Knoten | Fehler |
| Objstore InterClusterLifDown | objstore.interclusterlifDown | Knoten | Fehler |
| Signatur des Objektspeichers mit Nichtübereinschrift anfordern | osc.signatureMismatch | Knoten | Fehler |
| Einer der NFSv4-Pools ist erschöpft | Nblade.nfsV4PoolAust | Knoten | Kritisch |
| QoS Monitor Memory-Besteuerung | qos.Monitor.Memory.maxed | Knoten | Fehler |
| QoS Monitor Memory nicht gespeichert | qos.Monitor.Memory.abgenutzt | Knoten | Informationsdaten |
| NVMeNS zerstören | NVMeNS.destroy | Namespace | Informationsdaten |
| NVMeNS Online | NVMeNS.offline | Namespace | Informationsdaten |
| NVMeNS Offline | NVMeNS.online | Namespace | Informationsdaten |
| NVMe Out of Space | NVMeNS.out.of.space | Namespace | Warnung |
| Synchrone Replizierung Aus Sync Heraus | sms.Status.out.of.Sync | SnapMirror Beziehung | Warnung |
| Synchrone Replizierung Wiederhergestellt | sms.status.in.sync | SnapMirror Beziehung | Informationsdaten |
| Fehler Bei Der Automatischen Synchronisierung Der Replikation | sms.Resync.Versuch.failed | SnapMirror Beziehung | Fehler |
| Viele CIFS-Verbindungen | Nblade.cifsManyAuths | SVM | Fehler |
| Max. CIFS-Verbindung überschritten | Nblade.cifsMaxOpenSameFile | SVM | Fehler |

| Name des Unified Manager Events | EMS-Ereignisname | Betroffene Ressource | Schweregrad der ONTAP |
|---|---|---|---|
| Max. Anzahl der CIFS-Verbindung pro Benutzer überschritten | Nblade.cifsMaxSessPerUsrConn | SVM | Fehler |
| CIFS NetBIOS-Namenskonflikt | Nblade.cifsNbNameConflict | SVM | Fehler |
| Versucht, eine nicht existierende CIFS-Freigabe zu verbinden | Nblade.cifsNoPrivShare | SVM | Kritisch |
| Fehler beim CIFS Shadow Copy-Vorgang | cifs.shadowcopy.Failure | SVM | Fehler |
| Vom AV-Server gefundener Virus | Nblade.vscanVirusDetected | SVM | Fehler |
| Keine AV-Server-Verbindung für Virus Scan | Nblade.vscanNoScannerKonn | SVM | Kritisch |
| Kein AV-Server registriert | Nblade.vscanNoRegdScanner | SVM | Fehler |
| Keine reaktionsfähige AV-Server-Verbindung | Nblade.vscanConnInaktiv | SVM | Informationsdaten |
| AV-Server ist zu beschäftigt, um neue Scananforderung zu akzeptieren | Nblade.vscanConnBackPressure | SVM | Fehler |
| Nicht autorisierter Benutzer versucht, AV-Server zu verwenden | Nblade.vscanBadUserPrivAccess | SVM | Fehler |
| FlexGroup-Komponenten haben Platzprobleme | Flexgroup.debestandals.have.space.Issues | Datenmenge | Fehler |
| FlexGroup-Komponenten-Space-Status alles OK | Flexgroup.Komponenten.space.Status.all.ok | Datenmenge | Informationsdaten |
| FlexGroup-Komponenten haben Inodes-Probleme | flexgroup.constituents.have.inodes.issues | Datenmenge | Fehler |

| Name des Unified Manager Events | EMS-Ereignisname | Betroffene Ressource | Schweregrad der ONTAP |
|---|---|---|---|
| FlexGroup-Komponenten inodes Status Alle OK | flexgroup.constituents.inodes.status.all.ok | Datenmenge | Informationsdaten |
| Logischer Volume-Speicherplatz Fast Voll | Monitor.vol.nearFull | Datenmenge | Warnung |
| Logischer Speicherplatz Des Volume Voll | Monitor.vol.voll | Datenmenge | Fehler |
| Logischer Speicherplatz Des Volume Ist Normal | Monitor.vol.one.ok | Datenmenge | Informationsdaten |
| Fehler bei der automatischen WAFL-Volume-Größe | wafl.vol.autoSize.fail | Datenmenge | Fehler |
| Die automatische WAFL-Volume-Größe ist abgeschlossen | wafl.vol.autoSize.done | Datenmenge | Informationsdaten |

## Abonnieren von ONTAP EMS-Veranstaltungen

Sie können EMS-Ereignisse (Event Management System) abonnieren, die von Systemen generiert werden, die mit ONTAP Software installiert sind. Eine Untermenge von EMS-Ereignissen wird automatisch an Unified Manager gemeldet. Weitere EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie sich für diese Ereignisse angemeldet haben.

### Bevor Sie beginnen

Abonnieren Sie keine EMS-Ereignisse, die bereits Unified Manager hinzugefügt wurden, da dies zu Verwirrung führen kann, wenn Sie zwei Ereignisse für dasselbe Problem erhalten.

### Über diese Aufgabe

Sie können eine beliebige Anzahl von EMS-Veranstaltungen abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert. Nur die validierten Ereignisse werden auf die in Unified Manager überwachten Cluster angewendet. Der *ONTAP 9 EMS Ereigniskatalog* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite ONTAP 9 Produktdokumentation die entsprechende Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Veranstaltungen zu finden.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die von Ihnen abonnierenden ONTAP EMS-Ereignisse konfigurieren und benutzerdefinierte Skripts für die Ausführung dieser Ereignisse erstellen.

Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, kann es möglicherweise ein Problem mit der DNS-Konfiguration des Clusters geben, was verhindert, dass das Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Cluster-Administrator die DNS-Konfiguration des Clusters korrigieren und dann Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server gespült.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Konfiguration** > **Ereignisse verwalten**.
2. Klicken Sie auf der Seite **Konfiguration/Ereignisse verwalten** auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld * EMS-Ereignisse abonnieren* den Namen des ONTAP EMS-Events ein, zu dem Sie abonnieren möchten.

   Um die Namen der EMS-Ereignisse anzuzeigen, die Sie in der ONTAP Cluster Shell abonnieren können, können Sie die verwenden `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher).

   "So konfigurieren Sie ONTAP EMS-Ereignisabonnements in OnCommand Unified Manager / Active IQ Unified Manager"

4. Klicken Sie Auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste der abonnierten EMS-Ereignisse hinzugefügt, aber in der Spalte „Cluster anwendbar“ wird für das hinzugefügte EMS-Ereignis der Status als „`Unbekannt`“ angezeigt.

5. Klicken Sie auf **Speichern und Schließen**, um das EMS-Ereignisabonnement mit dem Cluster zu registrieren.
6. Klicken Sie erneut auf **EMS-Events abonnieren**.

   Der Status „`ja`“ wird in der Spalte „gilt für Cluster“ für das EMS-Ereignis, das Sie hinzugefügt haben, angezeigt.

   Wenn der Status nicht „`ja`“ lautet, überprüfen Sie die Schreibweise des EMS-Ereignisnamens von ONTAP. Wenn der Name falsch eingegeben wird, müssen Sie das falsche Ereignis entfernen und das Ereignis erneut hinzufügen.

**Nachdem Sie fertig sind**

Wenn das ONTAP EMS-Ereignis auftritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um Details zum EMS-Ereignis auf der Seite Ereignisdetails anzuzeigen. Sie können auch das Ergebnis des Ereignisses verwalten oder Alarme für das Ereignis erstellen.

## Verwalten von SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem sicheren Identitäts-Provider (IdP) authentifiziert werden, bevor sie auf die Unified Manager Web-UI zugreifen können.

Beachten Sie, dass nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager haben, nachdem die SAML-Authentifizierung aktiviert wurde. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole zugreifen.

### Anforderungen an Identitätsanbieter

Wenn Sie Unified Manager für die Verwendung eines Identitäts-Providers (IdP) konfigurieren, um die SAML-Authentifizierung für alle Remote-Benutzer durchzuführen, müssen Sie einige erforderliche Konfigurationseinstellungen beachten, damit die Verbindung zu Unified Manager erfolgreich hergestellt wird.

Sie müssen die Unified Manager-URI und die Metadaten im IdP-Server eingeben. Sie können diese Informationen von der Seite Unified ManagerSAML Authentication kopieren. Unified Manager gilt im SAML-Standard (Security Assertion Markup Language) als Service Provider (SP).

#### Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

#### Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

#### ADFS-Konfigurationsanforderungen

- Sie müssen drei Antragsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauenseintrag der Treuhandgesellschaft analysieren kann.

| Forderungsregel | Wert |
|---|---|
| SAM-Account-Name | Name-ID |
| SAM-Account-Name | Urne:oid:0.9.2342.19200300.100.1.1 |
| Token-Gruppen — Unqualifizierter Name | Urne:oid:1.3.6.1.4.1.5923.1.5.1.1 |

- Sie müssen die Authentifizierungsmethode auf „`Forms Authentication`“ festlegen, oder Benutzer erhalten möglicherweise einen Fehler beim Abmelden von Unified Manager, wenn Sie Internet Explorer verwenden. Führen Sie hierzu folgende Schritte aus:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Strukturansicht auf den Ordner Authentication Policies.
  c. Klicken Sie unter Aktionen auf der rechten Seite auf Globale primäre Authentifizierungsrichtlinie bearbeiten.
  d. Setzen Sie die Intranet-Authentifizierungsmethode auf „`Forms Authentication`“ anstatt auf die Standardauthentifizierung „`Windows Authentication`“.
- In einigen Fällen wird die Anmeldung über das IdP abgelehnt, wenn das Unified Manager-

Sicherheitszertifikat CA-signiert ist. Es gibt zwei Problemumgehungen zur Lösung dieses Problems:

- Befolgen Sie die Anweisungen im Link, um die Widerrufs-Prüfung auf dem ADFS-Server für verkettete CA-Zertifikat zugeordnete abhängige Partei zu deaktivieren:

  http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

- Der CA-Server befindet sich im ADFS-Server, um die Zertifiktanforderung des Unified Manager-Servers zu signieren.

**Sonstige Konfigurationsanforderungen**

- Die Unified Manager-Taktskew ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann oder die Authentifizierung fehlschlägt.
- Wenn Benutzer versuchen, mit Internet Explorer auf Unified Manager zuzugreifen, wird möglicherweise die Meldung angezeigt **die Webseite kann die Seite nicht anzeigen**. Stellen Sie in diesem Fall sicher, dass diese Benutzer die Option „`Sso freundliche HTTP-Fehlermeldungen`“ in **Tools** > **Internetoptionen** > **Erweitert** deaktivieren.

### Aktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remote-Benutzer von einem Secure Identity Provider (IdP) authentifiziert werden, bevor sie auf die Web-UI von Unified Manager zugreifen können.

**Bevor Sie beginnen**

- Sie müssen die Remote-Authentifizierung konfiguriert und bestätigt haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe mit der Rolle „OnCommand-Administrator“ erstellt haben.
- Der Identitäts-Provider (IdP) muss von Unified Manager unterstützt und konfiguriert werden.
- Sie müssen über die IdP-URL und die Metadaten verfügen.
- Sie müssen Zugriff auf den IdP-Server haben.

**Über diese Aufgabe**

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn das IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Daher müssen Sie darauf vorbereitet sein, beide Teile der Verbindung abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Das IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Nach Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Wartungskonsole, die Unified Manager-Befehle oder Zapis zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

**Schritte**

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Einrichtungsmenü auf **Authentifizierung**.
2. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML Authentication** aus.
3. Aktivieren Sie das Kontrollkästchen * SAML-Authentifizierung aktivieren*.

   Die Felder, die zum Konfigurieren der IdP-Verbindung erforderlich sind, werden angezeigt.

4. Geben Sie die IdP-URI und die IdP-Metadaten ein, die erforderlich sind, um den Unified Manager-Server mit dem IdP-Server zu verbinden.

   Wenn der IdP-Server direkt über den Unified Manager-Server erreichbar ist, können Sie nach Eingabe der IdP-URI auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld IdP-Metadaten automatisch zu füllen.

5. Kopieren Sie den Unified Manager-Host-Metadaten-URI, oder speichern Sie die Host-Metadaten in eine XML-Textdatei.

   Sie können den IdP-Server derzeit mit diesen Informationen konfigurieren.

6. Klicken Sie Auf **Speichern**.

   Es wird ein Meldungsfeld angezeigt, um zu bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

**Ergebnisse**

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldedaten auf der Anmeldeseite IdP statt auf der Anmeldeseite von Unified Manager ein.

**Nachdem Sie fertig sind**

Wenn noch nicht abgeschlossen ist, greifen Sie auf Ihr IdP zu, und geben Sie den URI und die Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

> Wenn Sie ADFS als Identitäts-Provider verwenden, wird die Unified Manager-GUI nicht das ADFS-Timeout-Timeout erfüllt und funktioniert weiter, bis das Timeout der Unified Manager-Sitzung erreicht ist. Wenn Unified Manager auf Windows, Red hat oder CentOS bereitgestellt wird, kann das Timeout der GUI-Sitzung mit dem folgenden Unified Manager CLI-Befehl geändert werden: `um option set absolute.session.timeout=00:15:00`Mit diesem Befehl wird das Zeitlimit für die Unified Manager GUI-Sitzung auf 15 Minuten festgelegt.

## Konfigurieren von Backup-Einstellungen für Datenbanken

Sie können die Backup-Einstellungen für die Unified Manager Datenbank so konfigurieren, dass der Datenbank-Backup-Pfad, die Aufbewahrungsanzahl und der Backup-Zeitplan festgelegt werden. Sie können tägliche oder wöchentliche geplante Backups aktivieren. Standardmäßig sind geplante Backups deaktiviert.

**Bevor Sie beginnen**

- Sie müssen über die Rolle „Operator“, „OnCommand Administrator“ oder „Storage Administrator“ verfügen.
- Sie müssen mindestens 150 GB Speicherplatz an dem Speicherort haben, den Sie als Backup-Pfad definieren.

  Es wird empfohlen, einen externen Standort zu verwenden, der sich außerhalb des Unified Manager-Hostsystems befindet.

- Wenn Unified Manager auf einem Linux-System installiert ist, stellen Sie sicher, dass der Benutzer „`jboss`“ über Schreibberechtigungen in das Backup-Verzeichnis verfügt.
- Sie sollten Backup-Vorgänge nicht so planen, dass sie unmittelbar nach dem Hinzufügen eines neuen Clusters ausgeführt werden, während Unified Manager historische Performance-Daten von 15 Tagen erfasst.

**Über diese Aufgabe**

Mehr Zeit wird bei der ersten Durchführung eines Backups als bei nachfolgenden Backups benötigt, da es sich bei dem ersten Backup um ein Vollbackup handelt. Ein vollständiges Backup kann über 1 GB dauern und kann drei bis vier Stunden dauern. Nachfolgende Backups sind inkrementell und erfordern weniger Zeit.

**Schritte**

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann auf **Verwaltung** > **Datenbank-Backup**.
2. Klicken Sie auf der Seite **Management/Datenbank-Backup** auf **Aktionen** > **Einstellungen für die Datenbanksicherung**.
3. Konfigurieren Sie die entsprechenden Werte für einen Backup-Pfad und die Anzahl der Aufbewahrung.

   Der Standardwert für die Aufbewahrungsanzahl ist 10; Sie können 0 verwenden, um unbegrenzte Backups zu erstellen.

4. Wählen Sie im Abschnitt **Terminhäufigkeit** das Kontrollkästchen **Aktivieren** aus, und geben Sie dann einen täglichen oder wöchentlichen Zeitplan an.
   - * Daily*

     Wenn Sie diese Option auswählen, müssen Sie eine Zeit im 24-Stunden-Format eingeben, um das Backup zu erstellen. Wenn Sie beispielsweise 18:30 angeben, wird täglich um 6:30 Uhr ein Backup erstellt.

   - **Wöchentlich**

     Wenn Sie diese Option auswählen, müssen Sie die Uhrzeit und den Tag für die Erstellung des Backups angeben. Wenn Sie beispielsweise den Tag als Montag und die Zeit als 16:30 angeben, wird jeden Montag um 4:30 Uhr ein wöchentliches Backup erstellt.

5. Klicken Sie auf **Speichern und Schließen**.

## Ändern des lokalen Benutzerpassworts

Sie können Ihr lokales Benutzeranmeldeswort ändern, um potenzielle Sicherheitsrisiken zu vermeiden.

### Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

### Über diese Aufgabe

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Wenden Sie sich an Ihren Passwortadministrator, um ein Kennwort für Remote-Benutzer zu ändern. Informationen zum Ändern des Wartungs-Benutzerpassworts finden Sie unter "Verwenden der Wartungskonsole".

### Schritte

1. Melden Sie sich bei Unified Manager an.
2. Klicken Sie in der oberen Menüleiste auf das Benutzersymbol und dann auf **Passwort ändern**.

   Die Option **Passwort ändern** wird nicht angezeigt, wenn Sie ein Remote-Benutzer sind.

3. Geben Sie im Dialogfeld **Passwort ändern** das aktuelle Passwort und das neue Passwort ein.
4. Klicken Sie Auf **Speichern**.

### Nachdem Sie fertig sind

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration konfiguriert ist, müssen Sie das Passwort auf dem zweiten Node des Setup ändern. Beide Instanzen müssen dasselbe Passwort haben.

## 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**. |
| 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.`<br><br>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.<br><br>+ |

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.