Konfigurieren Sie Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

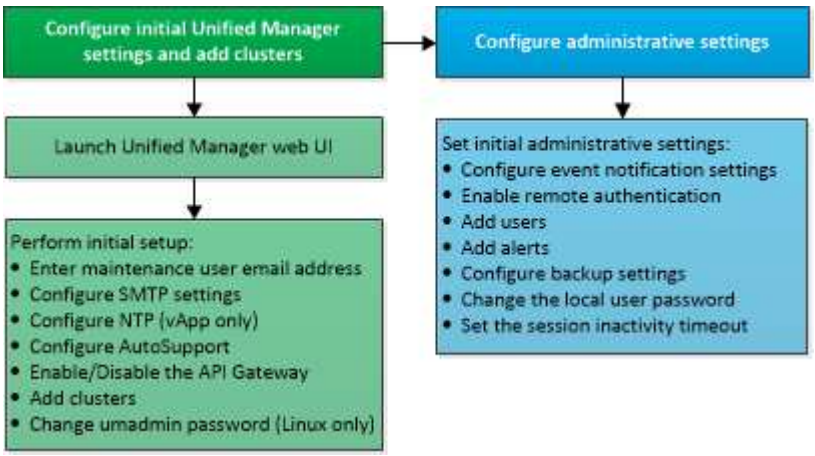
Konfigurieren Sie Active IQ Unified Manager

Nach der Installation von Active IQ Unified Manager (früher OnCommand Unified Manager) müssen Sie die Ersteinrichtung (auch „First Experience Wizard“ genannt) abschließen, um auf die Web-Benutzeroberfläche zuzugreifen. Anschließend können Sie zusätzliche Konfigurationsaufgaben ausführen, z. B. Cluster hinzufügen, Remote-Authentifizierung konfigurieren, Benutzer hinzufügen und Warnungen hinzufügen.

Einige der in diesem Handbuch beschriebenen Verfahren sind erforderlich, um die Ersteinrichtung Ihrer Unified Manager-Instanz abzuschließen. Bei anderen Verfahren handelt es sich um empfohlene Konfigurationseinstellungen, die für die Einrichtung Ihrer neuen Instanz hilfreich sind oder über die Sie Bescheid wissen sollten, bevor Sie mit der regelmäßigen Überwachung Ihrer ONTAP Systeme beginnen.

Übersicht über den Konfigurationsablauf

Der Konfigurationsworkflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Zugriff auf die Unified Manager-Web-Benutzeroberfläche

Nachdem Sie Unified Manager installiert haben, können Sie auf die Web-Benutzeroberfläche zugreifen, um Unified Manager einzurichten und mit der Überwachung Ihrer ONTAP -Systeme zu beginnen.

Bevor Sie beginnen

- Wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen, müssen Sie sich als Wartungsbenutzer (oder als Umadmin-Benutzer bei Linux-Installationen) anmelden.
- Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen statt über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in 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 akzeptieren, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat zur Serverauthentifizierung installieren.

Schritte

1. Starten Sie die Unified Manager-Web-Benutzeroberfläche von Ihrem Browser aus, indem Sie die URL verwenden, die am Ende der Installation angezeigt wird. Die URL ist die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Unified Manager-Servers.

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

2. Melden Sie sich mit Ihren Wartungsbenutzeranmeldeinformationen bei der Unified Manager-Web-Benutzeroberfläche an.

> Wenn Sie innerhalb einer Stunde drei erfolglose Anmeldeversuche bei der Web-Benutzeroberfläche unternehmen, werden Sie aus dem System ausgesperrt und müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Führen Sie die Ersteinrichtung der Unified Manager-Web-Benutzeroberfläche durch

Um Unified Manager zu verwenden, müssen Sie zunächst die anfänglichen Einrichtungsoptionen konfigurieren, einschließlich des NTP-Servers, der E-Mail-Adresse des Wartungsbenutzers, des SMTP-Serverhosts und des Hinzufügens von ONTAP Clustern.

Bevor Sie beginnen

Sie müssen die folgenden Vorgänge ausgeführt haben:

- Die Unified Manager-Web-Benutzeroberfläche wurde über die nach der Installation bereitgestellte URL gestartet.
- Angemeldet mit dem Wartungsbenutzernamen und -kennwort (Umadmin-Benutzer für Linux-Installationen), die während der Installation erstellt wurden

Die Seite „Erste Schritte“ von Active IQ Unified Manager wird nur angezeigt, wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen. Die folgende Seite stammt aus einer Installation auf VMware.

Wenn Sie eine dieser Optionen später ändern möchten, können Sie Ihre Auswahl aus den allgemeinen Optionen im linken Navigationsbereich des Unified Managers treffen. Beachten Sie, dass die NTP-Einstellung nur für VMware-Installationen gilt und später über die Wartungskonsole von Unified Manager geändert werden kann.

Schritte

1. Geben Sie auf der Seite „Ersteinrichtung“ von Active IQ Unified Manager die E-Mail-Adresse des Wartungsbenutzers, den Hostnamen des SMTP-Servers und alle zusätzlichen SMTP-Optionen sowie den NTP-Server ein (nur VMware-Installationen). Klicken Sie dann auf **Weiter**.

> Wenn Sie die Option **STARTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatsseite angezeigt. Überprüfen Sie die Zertifikatdetails und akzeptieren Sie das Zertifikat, um mit den anfänglichen Einrichtungseinstellungen der Web-Benutzeroberfläche fortzufahren.

2. Klicken Sie auf der AutoSupport -Seite auf **Zustimmen und fortfahren**, um das Senden von AutoSupport -Nachrichten von Unified Manager an NetAppActive IQ zu aktivieren.

Wenn Sie einen Proxy für den Internetzugang festlegen müssen, um AutoSupport Inhalte zu senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Option **Allgemein** > * AutoSupport* in der Web-Benutzeroberfläche.

3. Ändern Sie auf Red Hat-Systemen das Umadmin-Benutzerkennwort von der Standardzeichenfolge „`admin`“ in eine personalisierte Zeichenfolge.
4. Wählen Sie auf der Seite „API-Gateway einrichten“ aus, ob Sie die API-Gateway-Funktion verwenden möchten, mit der Unified Manager die ONTAP Cluster verwalten kann, die Sie mithilfe von ONTAP REST-APIs überwachen möchten. Klicken Sie dann auf **Weiter**.

   Sie können diese Einstellung später in der Web-Benutzeroberfläche unter **Allgemein** > **Funktionseinstellungen** > **API-Gateway** aktivieren oder deaktivieren. Weitere Informationen zu den APIs finden Sie unter"Erste Schritte mit Active IQ Unified Manager REST-APIs" .

5. Fügen Sie die Cluster hinzu, die Unified Manager verwalten soll, und klicken Sie dann auf **Weiter**. Für jeden Cluster, den Sie verwalten möchten, benötigen Sie den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) für die Clusterverwaltung sowie den Benutzernamen und das Kennwort. Der Benutzer muss über die Rolle „admin“ verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche unter **Speicherverwaltung** > **Cluster-Setup** hinzufügen.

6. Überprüfen Sie auf der Seite „Zusammenfassung“, ob alle Einstellungen korrekt sind, und klicken Sie auf „Fertig stellen“.

Die Seite „Erste Schritte“ wird geschlossen und die Seite „Unified Manager Dashboard“ wird angezeigt.

Cluster hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dazu gehört die Möglichkeit, Clusterinformationen wie Zustand, Kapazität, Leistung und Konfiguration des Clusters abzurufen, sodass Sie eventuell auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen über die folgenden Informationen verfügen:
  - Unified Manager unterstützt lokale ONTAP -Cluster, ONTAP Select und Cloud Volumes ONTAP.
  - Hostname oder IP-Adresse zur Clusterverwaltung

    Der Hostname ist der FQDN oder Kurzname, den Unified Manager für die Verbindung mit dem Cluster verwendet. Der Hostname muss in die IP-Adresse der Clusterverwaltung aufgelöst werden.

    Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie ein Knotenverwaltungs-LIF verwenden, schlägt der Vorgang fehl.

  - Auf dem Cluster muss die ONTAP Softwareversion 9.1 oder höher ausgeführt werden.
  - ONTAP -Administratorbenutzername und -kennwort

Dieses Konto muss über die Rolle *admin* verfügen und der Anwendungszugriff muss auf *ontapi*, *console* und *http* eingestellt sein.

- Die Portnummer für die Verbindung mit dem Cluster über das HTTPS-Protokoll (normalerweise Port 443)
- Sie verfügen über die erforderlichen Zertifikate:

  SSL (HTTPS)-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Bei einer Neuinstallation von Unified Manager wird ein standardmäßiges selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, zur besseren Sicherheit ein Upgrade auf ein CA-signiertes Zertifikat durchzuführen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat integrieren. Weitere Informationen zum Neugenerieren von SSL-Zertifikaten finden Sie unter"Generieren eines HTTPS-Sicherheitszertifikats" .

  EMS-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Es wird während der Authentifizierung für von ONTAP empfangene EMS-Benachrichtigungen verwendet.

  Zertifikate für gegenseitige TLS-Kommunikation: Wird während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatsbasierte Authentifizierung ist für einen Cluster basierend auf der ONTAP -Version aktiviert. Wenn auf dem Cluster eine niedrigere ONTAP Version als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

  Die zertifikatbasierte Authentifizierung wird für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können es jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, sollten Sie es neu generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter"Cluster bearbeiten" .

  - Sie können einen Cluster über die Web-Benutzeroberfläche hinzufügen und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
  - Sie können einen Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mithilfe der Unified Manager-CLI hinzufügen, müssen Sie den Cluster mithilfe der Unified Manager-Benutzeroberfläche bearbeiten. Sie können sehen"Unterstützte Unified Manager CLI-Befehle" um einen Cluster mithilfe der Unified Manager CLI hinzuzufügen.
  - Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie die Sicherung von Unified Manager von einem Server nehmen und auf einem anderen Unified Manager-Server wiederherstellen, auf dem der Hostname oder die IP-Adresse geändert wurde, kann die Überwachung des Clusters fehlschlagen. Um den Fehler zu vermeiden, bearbeiten und speichern Sie die Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter"Cluster bearbeiten" .

+ **Cluster-Zertifikate**: Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager keinen Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatsgenerierung finden Sie im Knowledge Base-Artikel (KB). "So erneuern Sie ein selbstsigniertes ONTAP -Zertifikat in der System Manager-Benutzeroberfläche" .

- Sie müssen über ausreichend Speicherplatz auf dem Unified Manager-Server verfügen. Sie können dem Server keinen Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes im Datenbankverzeichnis belegt sind.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Klicken Sie auf der Seite „Cluster-Setup“ auf **Hinzufügen**.
3. Geben Sie im Dialogfeld „Cluster hinzufügen“ die erforderlichen Werte an, z. B. den Hostnamen oder die IP-Adresse des Clusters, den Benutzernamen, das Kennwort und die Portnummer.

   Sie können die IP-Adresse der Clusterverwaltung von IPv6 auf IPv4 oder von IPv4 auf IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Clusterraster und auf der Clusterkonfigurationsseite angezeigt.

4. Klicken Sie auf **Senden**.
5. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie auf **Ja**.

   Nachdem Sie die Clusterdetails gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster sehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn der Cluster zum ersten Mal hinzugefügt wird. Unified Manager überprüft das Zertifikat nicht bei jedem API-Aufruf an ONTAP.

Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines Clusters Leistungsinformationen für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.

Da die Erfassung von 15 Tagen Leistungsdaten CPU-intensiv ist, wird empfohlen, das Hinzufügen neuer Cluster zu staffeln, damit Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden. Wenn Sie Unified Manager während des Datenkontinuitätserfassungszeitraums neu starten, wird die Erfassung angehalten und Sie sehen Lücken in den Leistungsdiagrammen für den fehlenden Zeitraum.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, überprüfen Sie, ob die Uhren auf den beiden Systemen nicht synchronisiert sind und das Startdatum des Unified Manager-HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Sie müssen sicherstellen, dass die Uhren über NTP oder einen ähnlichen Dienst synchronisiert werden.

Verwandte Informationen

"Installieren eines von einer Zertifizierungsstelle signierten und zurückgegebenen HTTPS-Zertifikats"

Konfigurieren Sie Unified Manager zum Senden von Warnbenachrichtigungen

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

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Nachdem Sie Unified Manager bereitgestellt und die Erstkonfiguration abgeschlossen haben, sollten Sie Ihre Umgebung so konfigurieren, dass basierend auf dem Empfang von Ereignissen Warnungen ausgelöst und Benachrichtigungs-E-Mails oder SNMP-Traps generiert werden.

Schritte

1. "Konfigurieren der Ereignisbenachrichtigungseinstellungen".

   Wenn Sie beim Auftreten bestimmter Ereignisse in Ihrer Umgebung Warnbenachrichtigungen erhalten möchten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Warnbenachrichtigung gesendet wird. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. "Remote-Authentifizierung aktivieren".

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

3. "Authentifizierungsserver hinzufügen".

   Sie können Authentifizierungsserver hinzufügen, sodass Remotebenutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

4. "Benutzer hinzufügen".

   Sie können verschiedene Arten von lokalen oder Remote-Benutzern hinzufügen und bestimmte Rollen zuweisen. Wenn Sie eine Warnung erstellen, weisen Sie einen Benutzer zu, der die Warnbenachrichtigungen erhalten soll.

5. "Benachrichtigungen hinzufügen".

   Nachdem Sie die E-Mail-Adresse zum Senden von Benachrichtigungen hinzugefügt, Benutzer zum Empfangen der Benachrichtigungen hinzugefügt, Ihre Netzwerkeinstellungen konfiguriert und die für Ihre Umgebung erforderlichen SMTP- und SNMP-Optionen konfiguriert haben, können Sie Warnungen zuweisen.

Konfigurieren der Ereignisbenachrichtigungseinstellungen

Sie können Unified Manager so konfigurieren, dass Warnbenachrichtigungen gesendet werden, wenn ein Ereignis generiert oder einem Benutzer zugewiesen wird. Sie können den SMTP-Server konfigurieren, der zum Senden der Warnung verwendet wird, und Sie

können verschiedene Benachrichtigungsmechanismen festlegen – beispielsweise können Warnbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Bevor Sie beginnen

Sie müssen über die folgenden Informationen verfügen:

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

  Die E-Mail-Adresse wird in gesendeten Warnbenachrichtigungen im Feld „Von“ angezeigt. Sollte die E-Mail aus irgendeinem Grund nicht zugestellt werden können, wird diese E-Mail-Adresse auch als Empfänger für unzustellbare E-Mails verwendet.

- Hostname des SMTP-Servers sowie Benutzername und Kennwort für den Zugriff auf den Server
- Hostname oder IP-Adresse des Trap-Zielhosts, der den SNMP-Trap empfängt, zusammen mit der SNMP-Version, dem ausgehenden Trap-Port, der Community und anderen erforderlichen SNMP-Konfigurationswerten

  Um mehrere Trap-Ziele anzugeben, trennen Sie jeden Host durch ein Komma. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie z. B. Version und ausgehender Trap-Port, für alle Hosts in der Liste gleich sein.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite „Benachrichtigungen“ die entsprechenden Einstellungen.

   Anmerkungen:

   - Wenn die Absenderadresse bereits mit der Adresse „ActiveIQUnifiedManager@localhost.com“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.
   - Wenn der Hostname des SMTP-Servers nicht aufgelöst werden kann, können Sie anstelle des Hostnamens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.
3. Klicken Sie auf **Speichern**.
4. Wenn Sie die Option **STARTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatsseite angezeigt. Überprüfen Sie die Zertifikatsdetails und akzeptieren Sie das Zertifikat, um die Benachrichtigungseinstellungen zu speichern.

   Sie können auf die Schaltfläche **Zertifikatdetails anzeigen** klicken, um die Zertifikatsdetails anzuzeigen. Wenn das vorhandene Zertifikat abgelaufen ist, deaktivieren Sie das Kontrollkästchen **STARTLS verwenden** oder **SSL verwenden**, speichern Sie die Benachrichtigungseinstellungen und aktivieren Sie das Kontrollkästchen **STARTLS verwenden** oder **SSL verwenden** erneut, um ein neues Zertifikat anzuzeigen.

Remote-Authentifizierung aktivieren

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager-Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können auf die grafische Benutzeroberfläche des Unified

Managers zugreifen, um Speicherobjekte und Daten zu verwalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

> 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.

Sie können die Remote-Authentifizierung entweder mit 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 zur Authentifizierung der Benutzer verwendete Zertifikat muss dem X.509-Format entsprechen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Remote-Authentifizierung aktivieren…**.
3. Wählen Sie im Feld „Authentifizierungsdienst“ den Diensttyp aus und konfigurieren Sie den Authentifizierungsdienst.

Für den Authentifizierungstyp …	Geben Sie die folgenden Informationen ein …
Active Directory	• Name des Authentifizierungsserver-Administrators in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(unter Verwendung der entsprechenden LDAP-Notation) • Administratorkennwort • Basis-Distinguished Name (unter Verwendung der entsprechenden LDAP-Notation)
Öffnen Sie LDAP	• Bind-Distinguished Name (in der entsprechenden LDAP-Notation) • Bind-Passwort • Basis-Distinguished Name

Wenn die Authentifizierung eines Active Directory-Benutzers lange dauert oder ein Timeout auftritt, liegt das wahrscheinlich daran, dass der Authentifizierungsserver lange braucht, um zu antworten. Das Deaktivieren der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen.

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

4. **Optional:** Fügen Sie Authentifizierungsserver hinzu und testen Sie die Authentifizierung.
5. Klicken Sie auf **Speichern**.

Deaktivieren Sie verschachtelte Gruppen von der Remote-Authentifizierung

Wenn Sie die Remote-Authentifizierung aktiviert haben, können Sie die verschachtelte Gruppenauthentifizierung deaktivieren, sodass sich nur einzelne Benutzer und keine Gruppenmitglieder remote bei Unified Manager authentifizieren können. Sie können verschachtelte Gruppen deaktivieren, wenn Sie die Antwortzeit der Active Directory-Authentifizierung verbessern möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory möglich.

Das Deaktivieren der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen. 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 im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Verschachtelte Gruppensuche deaktivieren**.
3. Klicken Sie auf **Speichern**.

Einrichten von Authentifizierungsdiensten

Authentifizierungsdienste ermöglichen die Authentifizierung von Remote-Benutzern oder Remote-Gruppen in einem Authentifizierungsserver, bevor ihnen Zugriff auf Unified Manager gewährt wird. Sie können Benutzer authentifizieren, indem Sie vordefinierte Authentifizierungsdienste (wie Active Directory oder OpenLDAP) verwenden oder Ihren eigenen Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Wählen Sie einen der folgenden Authentifizierungsdienste aus:

Wenn Sie auswählen…	Dann tun Sie Folgendes …
Active Directory	a. Geben Sie den Administratornamen und das Kennwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Geben Sie den definierten Bind-Namen und das Bind-Passwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.
Sonstige	a. Geben Sie den definierten Bind-Namen und das Bind-Passwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**. c. Geben Sie die LDAP-Protokollversion an, die vom Authentifizierungsserver unterstützt wird. d. Geben Sie den Benutzernamen, die Gruppenmitgliedschaft, die Benutzergruppe und die Mitgliedsattribute ein.

Wenn Sie den Authentifizierungsdienst ändern möchten, müssen Sie alle vorhandenen Authentifizierungsserver löschen und dann neue Authentifizierungsserver hinzufügen.

3. Klicken Sie auf **Speichern**.

Authentifizierungsserver hinzufügen

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 vorliegen:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst konfiguriert haben, damit der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn der Authentifizierungsserver, den Sie hinzufügen, Teil eines Hochverfügbarkeitspaars (HA) ist (das dieselbe Datenbank verwendet), können Sie auch den Partnerauthentifizierungsserver hinzufügen. Dadurch kann der Verwaltungsserver mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren oder deaktivieren Sie die Option **Sichere Verbindung verwenden**:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Aktivieren Sie es	a. Wählen Sie die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich „Authentifizierungsserver“ auf **Hinzufügen**. c. Geben Sie im Dialogfeld „Authentifizierungsserver hinzufügen“ den Authentifizierungsnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein. d. Klicken Sie im Dialogfeld „Host autorisieren“ auf „Zertifikat anzeigen“. e. Überprüfen Sie im Dialogfeld „Zertifikat anzeigen“ die Zertifikatsinformationen und klicken Sie dann auf **Schließen**. f. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Ja**. Wenn Sie die Option **Authentifizierung für sichere Verbindung 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.
Deaktivieren Sie es	a. Deaktivieren Sie die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich „Authentifizierungsserver“ auf **Hinzufügen**. c. Geben Sie im Dialogfeld „Authentifizierungsserver hinzufügen“ entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers sowie die Portdetails an. d. Klicken Sie auf **Hinzufügen**.

Der von Ihnen hinzugefügte Authentifizierungsserver wird im Bereich „Server“ angezeigt.

3. Führen Sie eine Testauthentifizierung durch, um zu bestätigen, dass Sie Benutzer auf dem von Ihnen hinzugefügten Authentifizierungsserver authentifizieren können.

Testen Sie die Konfiguration der Authentifizierungsserver

Sie können die Konfiguration Ihrer Authentifizierungsserver validieren, um sicherzustellen, dass der Verwaltungsserver mit ihnen kommunizieren kann. Sie können die Konfiguration validieren, indem Sie auf Ihren Authentifizierungsservern nach einem Remotebenutzer oder einer Remotegruppe suchen und diese mithilfe der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst konfiguriert haben, damit 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 aus nach dem Remotebenutzer oder der Remotegruppe suchen und sie authentifizieren kann.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn der Authentifizierungsdienst auf Active Directory eingestellt ist und Sie die Authentifizierung von Remotebenutzern validieren, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Klicken Sie auf **Authentifizierung testen**.
3. Geben Sie im Dialogfeld „Testbenutzer“ den Benutzernamen und das Kennwort des Remotebenutzers oder den Benutzernamen der Remotegruppe an und klicken Sie dann auf **Test**.

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

Benachrichtigungen hinzufügen

Sie können Warnmeldungen konfigurieren, die Sie benachrichtigen, wenn ein bestimmtes Ereignis generiert wird. Sie können Warnungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse eines bestimmten Schweregrads konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und der Warnung ein Skript zuordnen.

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ 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 Warnung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie möchten, dass basierend auf dem Ereignis ein Skript ausgeführt wird, müssen Sie das Skript über die Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können nach dem Empfang eines Ereignisses direkt auf der Seite „Ereignisdetails“ eine Warnung erstellen. Außerdem können Sie eine Warnung auch auf der Seite „Warnungseinrichtung“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite „Alarm-Setup“ auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld „Warnung hinzufügen“ auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie die Ressourcen aus, die in die Warnung einbezogen oder davon ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Basierend auf der von Ihnen angegebenen Textzeichenfolge zeigt die Liste der verfügbaren Ressourcen nur die Ressourcen an, die der Filterregel entsprechen. Bei der von Ihnen angegebenen Textzeichenfolge wird zwischen Groß- und Kleinschreibung unterschieden.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel und für Ereignisse im Zusammenhang mit der ausgeschlossenen Ressource wird keine Warnung generiert.

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

   Um mehr als ein Ereignis auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

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

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

   Sie können Benutzer auch über SNMP-Traps benachrichtigen.

7. Klicken Sie auf **Speichern**.

Beispiel für das Hinzufügen einer Warnung

Dieses Beispiel zeigt, wie Sie eine Warnung erstellen, die die folgenden Anforderungen erfüllt:

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

Führen Sie im Dialogfeld „Warnung hinzufügen“ die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name** und geben Sie **HealthTest** in das Feld **Alert Name** ein.
2. Klicken Sie auf **Ressourcen** und wählen Sie auf der Registerkarte „Einschließen“ aus der Dropdownliste **Volumes** aus.
   a. Geben Sie **abc** in das Feld **Name enthält** ein, um die Volumes anzuzeigen, deren Name „`abc`“ enthält.
   b. Wählen Sie **+[All Volumes whose name contains 'abc'] +** aus dem Bereich „Verfügbare Ressourcen“ und verschieben Sie es in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **Ausschließen**, geben Sie **xyz** in das Feld **Name enthält** ein und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie auf **Ereignisse** und wählen Sie im Feld „Ereignisschweregrad“ die Option **Kritisch** aus.
4. Wählen Sie im Bereich „Übereinstimmende Ereignisse“ die Option „Alle kritischen Ereignisse“ aus und verschieben Sie sie in den Bereich „Ausgewählte Ereignisse“.
5. Klicken Sie auf **Aktionen** und geben Sie **sample@domain.com** in das Feld „Diese Benutzer benachrichtigen“ ein.
6. Wählen Sie **Alle 15 Minuten erinnern**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können einen Alarm so konfigurieren, dass den Empfängern für einen bestimmten Zeitraum wiederholt Benachrichtigungen gesendet werden. Sie sollten den Zeitpunkt ermitteln, ab dem die Ereignisbenachrichtigung für den Alarm aktiv ist.
7. Wählen Sie im Menü „Auszuführendes Skript auswählen“ die Option „Skript **Test**“ aus.
8. Klicken Sie auf **Speichern**.

Ändern des lokalen Benutzerkennworts

Sie können Ihr lokales Benutzeranmeldekennwort ändern, um potenziellen Sicherheitsrisiken vorzubeugen.

Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Um das Kennwort eines Remote-Benutzers zu ändern, wenden Sie sich an Ihren Kennwortadministrator. Informationen zum Ändern des Wartungsbenutzerkennworts 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 und das neue Passwort ein.
4. Klicken Sie auf **Speichern**.

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

Festlegen des Sitzungs-Inaktivitäts-Timeouts

Sie können den Inaktivitäts-Timeout-Wert für Unified Manager angeben, sodass die Sitzung nach einer bestimmten Zeit der Inaktivität automatisch beendet wird. Standardmäßig ist das Timeout auf 4.320 Minuten (72 Stunden) eingestellt.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Diese Einstellung wirkt sich auf alle angemeldeten Benutzersitzungen aus.

Diese Option ist nicht verfügbar, wenn Sie die SAML-Authentifizierung (Security Assertion Markup Language) aktiviert haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Geben Sie auf der Seite **Funktionseinstellungen** das Inaktivitäts-Timeout an, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Legen Sie kein Timeout fest, sodass die Sitzung nie automatisch geschlossen wird	Bewegen Sie im Bereich **Inaktivitäts-Timeout** den Schieberegler nach links (Aus) und klicken Sie auf **Übernehmen**.
Legen Sie eine bestimmte Anzahl von Minuten als Timeout-Wert fest	Bewegen Sie im Bereich **Inaktivitäts-Timeout** den Schieberegler nach rechts (Ein), geben Sie den Wert für das Inaktivitäts-Timeout in Minuten an und klicken Sie auf **Übernehmen**.

Legen Sie das Sitzungs-Timeout über die CLI fest

Sie können mithilfe der CLI einen maximalen Sitzungs-Timeout-Wert für Unified Manager festlegen, sodass die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist Ihr Sitzungs-Timeout auf den Maximalwert von 4.320 Minuten (72 Stunden) eingestellt. Dies bedeutet, dass Ihre Sitzung nach 72 Stunden automatisch endet, auch wenn Sie angemeldet sind und Unified Manager aktiv verwenden.

Informationen zu diesem Vorgang

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Die Einstellung für das Sitzungs-Timeout wirkt sich auf alle angemeldeten Benutzersitzungen aus.

Schritte

1. Melden Sie sich bei der Unified Manager CLI an, indem Sie den `um cli login` Befehl. Verwenden Sie zur Authentifizierung einen gültigen Benutzernamen und ein gültiges Passwort.
2. Geben Sie den `um option set max.session.timeout.value=<in mins>` Befehl zum Ändern des

Sitzungs-Timeout-Werts.

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 Wartungsbenutzer 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` .
- 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 auf dem Zertifikat (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 eingeben. Wenn dieses Feld leer gelassen wird, enthält das resultierende Zertifikat überhaupt kein Feld für alternative Namen.

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 **Gast 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 überwachter 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.

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
   ```

Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung

Ab Unified Manager 9.7 können Sie Speicher-Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern bereitstellen und diese Workloads basierend auf zugewiesenen Leistungsserviceleveln verwalten. Diese Funktionalität ähnelt dem Erstellen von Workloads im ONTAP System Manager und dem Anhängen von QoS-Richtlinien. Bei Anwendung mit Unified Manager können Sie jedoch Workloads über alle Cluster hinweg bereitstellen und verwalten, die Ihre Unified Manager-Instanz überwacht.

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Diese Option ist standardmäßig aktiviert, Sie können sie jedoch deaktivieren, wenn Sie Workloads nicht mit Unified Manager bereitstellen und verwalten möchten.

Wenn diese Option aktiviert ist, werden in der Benutzeroberfläche viele neue Elemente bereitgestellt:

Neue Inhalte	Standort
Eine Seite zum Bereitstellen neuer Workloads	Verfügbar unter **Allgemeine Aufgaben** > **Bereitstellung**
Eine Seite zum Erstellen von Richtlinien für Leistungsservicelevel	Verfügbar unter **Einstellungen** > **Richtlinien** > **Leistungs-Servicelevel**
Eine Seite zum Erstellen von Richtlinien zur Leistungsspeichereffizienz	Verfügbar unter **Einstellungen** > **Richtlinien** > **Speichereffizienz**
Panels, die Ihre aktuelle Workload-Leistung und Workload-IOPS beschreiben	Verfügbar über das Dashboard

Weitere Informationen zu diesen Seiten und dieser Funktionalität finden Sie in der Online-Hilfe des Produkts.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Funktionseinstellungen** die richtlinienbasierte Speicherverwaltung, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Deaktivieren Sie die richtlinienbasierte Speicherverwaltung	Bewegen Sie im Bereich **Richtlinienbasierte Speicherverwaltung** den Schieberegler nach links.
Aktivieren Sie die richtlinienbasierte Speicherverwaltung	Bewegen Sie im Bereich **Richtlinienbasierte Speicherverwaltung** den Schieberegler nach rechts.