Active IQ Unified Manager wird konfiguriert

Active IQ Unified Manager 9.14

NetApp
November 11, 2024

Inhalt

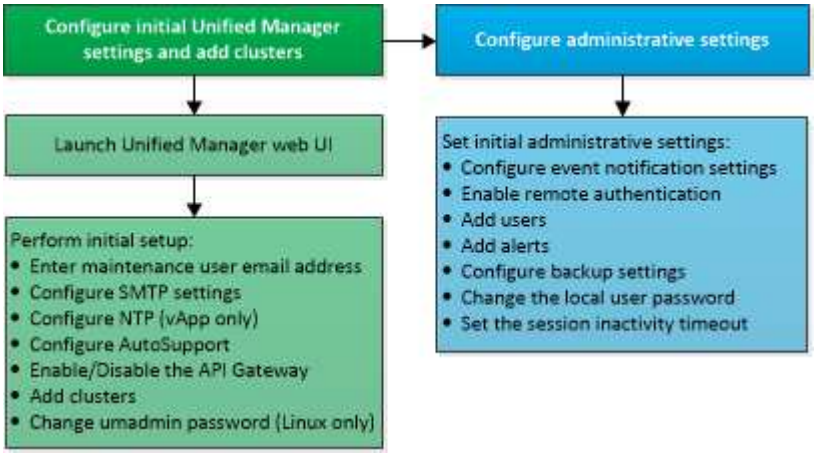
Active IQ Unified Manager wird konfiguriert

Nach der Installation von Active IQ Unified Manager (früher OnCommand 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.

Was Sie brauchen

- 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.

   Wenn Sie innerhalb einer Stunde drei aufeinanderfolgende erfolglose Versuche zur Anmeldung bei der Web-Benutzeroberfläche vornehmen, werden Sie aus dem System gesperrt und müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Die Ersteinrichtung der Unified Manager-Weboberfläche durchführen

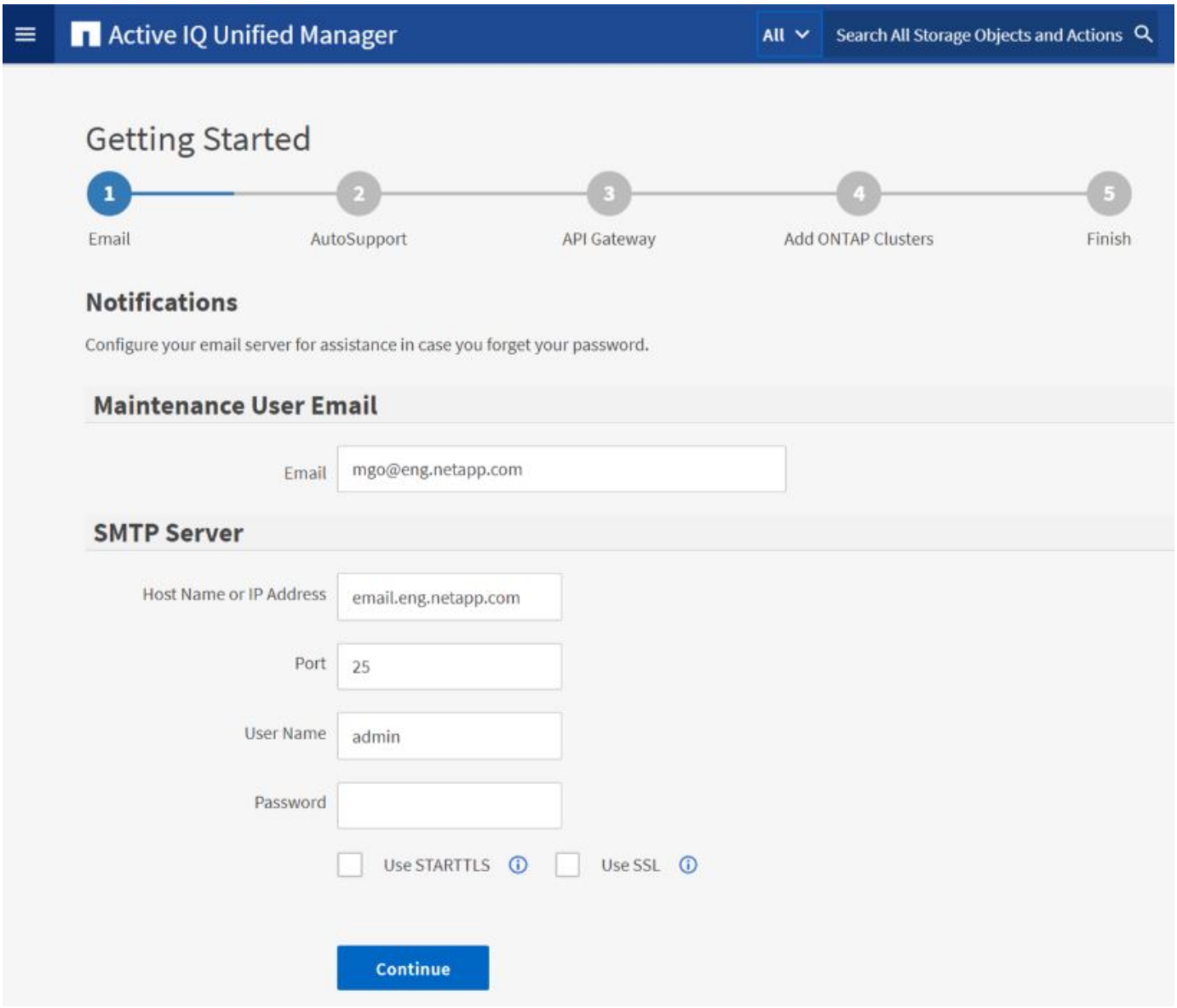
Um Unified Manager zu verwenden, müssen Sie zuerst die anfänglichen Setup-Optionen konfigurieren, einschließlich des NTP-Servers, der Wartungs-Benutzer-E-Mail-Adresse, des SMTP-Server-Hosts und des Hinzufügens von ONTAP-Clustern.

Was Sie brauchen

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

Die Seite Active IQ Unified ManagerGetting Started 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 Ihre Auswahl aus den Optionen Allgemein im linken Navigationsbereich von Unified Manager auswählen. Beachten Sie, dass die NTP-Einstellung nur für VMware Installationen gilt. Die Einstellung kann später mithilfe der Unified Manager Wartungskonsole geändert werden.

Schritte

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

   Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatseite angezeigt. Überprüfen Sie die Zertifikatdetails, und akzeptieren Sie das Zertifikat, um mit den anfänglichen Setup-Einstellungen 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 Zugriff auf das Internet festlegen müssen, um AutoSupport-Inhalte zu

senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Option **Allgemein** > **AutoSupport** von der Web-Benutzeroberfläche.

3. Ändern Sie auf Red hat- und CentOS-Systemen das umadmin-Benutzerpasswort von der standardmäßigen Zeichenfolge „`admin`“ in eine personalisierte Zeichenfolge.
4. Wählen Sie auf der Seite API-Gateway einrichten, ob Sie die API-Gateway-Funktion verwenden möchten, mit der Unified Manager die ONTAP-Cluster verwalten kann, die Sie mit ONTAP REST-APIs überwachen möchten. Klicken Sie dann auf **Weiter**.

   Sie können diese Einstellung später in der Web-Benutzeroberfläche über **Allgemein** > **Feature-Einstellungen** > **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, müssen Sie den Host-Namen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und die Kennwort-Anmeldedaten haben. Der Benutzer muss über die Rolle „`admin`“ verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche von **Storage Management** > **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.

Hinzufügen von Clustern

Sie können Active IQ Unified Manager ein Cluster hinzufügen, 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.

Was Sie brauchen

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

  - Der Cluster muss die ONTAP Version 9.1 oder höher ausführen.
  - Benutzername und Passwort für den ONTAP-Administrator

    Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *Console* und *http*

eingestellt sein.

- Die Port-Nummer für die Verbindung zum Cluster mithilfe des HTTPS-Protokolls (normalerweise Port 443)
- Sie verfügen über die erforderlichen Zertifikate:

  SSL (HTTPS) Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Bei einer neuen Installation von Unified Manager wird ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt ein Upgrade auf ein Zertifikat, das von einer Zertifizierungsstelle unterzeichnet wurde, um die Sicherheit zu erhöhen. Wenn das Serverzertifikat abgelaufen ist, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat aufnehmen können. Weitere Informationen zur Neugenerierung von SSL-Zertifikaten finden Sie unter "Erstellen eines HTTPS-Sicherheitszertifikats".

  EMS-Zertifikat: Dieses Zertifikat ist im Besitz von Unified Manager. Es wird bei der Authentifizierung für EMS-Benachrichtigungen verwendet, die von ONTAP empfangen werden.

  Zertifikate für gegenseitige TLS-Kommunikation: Wird bei der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist auf Grundlage der Version von ONTAP für ein Cluster aktiviert. Wenn das Cluster mit der Version ONTAP niedriger als die Version 9.5 ist, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

  Die zertifikatbasierte Authentifizierung wird für ein Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Allerdings können Sie die Aktivierung durch Ändern und Speichern der Cluster-Details aktivieren. Wenn das Zertifikat abgelaufen ist, sollten Sie es erneut generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter "Cluster werden bearbeitet".

  - Sie können ein Cluster über die Web-Benutzeroberfläche hinzufügen, und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
  - Sie können ein Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie ein Cluster mit der Unified Manager CLI hinzufügen, muss das Cluster über die Unified Manager UI bearbeitet werden. Es wird angezeigt"Unterstützte CLI-Befehle von Unified Manager", wie Sie mithilfe der Unified Manager CLI einen Cluster hinzufügen.
  - Wenn die zertifikatbasierte Authentifizierung für ein Cluster aktiviert ist und Sie das Backup von Unified Manager von einem Server aus erstellen und auf einen anderen Unified Manager Server wiederherstellen. Hier wird der Hostname oder die IP-Adresse geändert, dann kann das Monitoring des Clusters fehlschlagen. Um den Ausfall zu vermeiden, bearbeiten und speichern Sie die Cluster-Details. Weitere Informationen zum Bearbeiten von Cluster-Details finden Sie unter "Cluster werden bearbeitet".

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

- 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.

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 **Storage-Management** > **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. Hostname oder IP-Adresse des Clusters, Benutzername, Passwort und Portnummer.

   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. Klicken Sie im Dialogfeld Host autorisieren auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie Auf **Ja**.

   Nachdem Sie die Cluster-Details gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für ein Cluster anzeigen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

Nachdem alle Objekte für ein neues Cluster erkannt wurden, sammelt Unified Manager historische Performance-Daten für die 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, überprüfen Sie, ob die Uhren auf den beiden Systemen nicht synchronisiert sind und das HTTPS-Zertifikat von Unified Manager nach dem Startdatum des Clusters liegt. Sie müssen sicherstellen, dass die Uhren mit NTP oder einem ähnlichen Dienst synchronisiert werden.

Verwandte Informationen

"Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat"

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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.

Was Sie brauchen

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
- Hostname oder IP-Adresse für den Trap-Ziel-Host, der den SNMP-Trap empfängt, zusammen mit der SNMP-Version, dem Outbound-Trap-Port, der Community und anderen erforderlichen SNMP-Konfigurationswerten

  Um mehrere Trap-Ziele festzulegen, trennen Sie jeden Host durch ein Komma. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie Version und Outbound-Trap-Port, für alle Hosts in der Liste identisch 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.

   Hinweise:

   - Wenn die von-Adresse 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 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.
3. Klicken Sie Auf **Speichern**.
4. Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatseite angezeigt. Überprüfen Sie die Zertifikatdetails, und akzeptieren Sie das Zertifikat, um die Benachrichtigungseinstellungen zu speichern.

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

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.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle 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 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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie das Kontrollkästchen für **Remote-Authentifizierung aktivieren…**.
3. Wählen Sie im Feld Authentifizierungsdienst den Diensttyp aus, und konfigurieren Sie den Authentifizierungsservice.

Für Authentifizierungstyp…	Geben Sie die folgenden Informationen ein…
Active Directory	• Administratorname des Authentifizierungsservers in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Mit der entsprechenden LDAP-Notation) • Administratorpasswort • Basisname (unter Verwendung der entsprechenden LDAP-Notation)
Öffnen Sie LDAP	• Distinguished Name binden (in der entsprechenden LDAP-Notation) • Kennwort binden • 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. **Optional:** Fügen Sie Authentifizierungsserver hinzu, und testen Sie die Authentifizierung.
5. Klicken Sie Auf **Speichern**.

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.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory anwendbar.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie das Kontrollkästchen für **Suche nach verschachtelter Gruppe deaktivieren**.
3. Klicken Sie Auf **Speichern**.

Einrichten von Authentifizierungsservices

Authentifizierungsservices ermöglichen die Authentifizierung von Remote-Benutzern oder Remotegruppen in einem Authentifizierungsserver, bevor sie ihnen den Zugriff auf Unified Manager gewähren. Sie können Benutzer mithilfe von vordefinierten Authentifizierungsdiensten (z. B. Active Directory oder OpenLDAP) authentifizieren, oder indem Sie Ihren eigenen Authentifizierungsmechanismus konfigurieren.

Was Sie brauchen

- Sie müssen die Remote-Authentifizierung aktiviert haben.
- Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

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

Wenn Sie die Option…	Dann tun Sie das…
Active Directory	a. Geben Sie den Administratornamen und das Kennwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.
OpenLDAP	a. Geben Sie den Distinguished Name und das Bind-Passwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.
Andere	a. Geben Sie den Distinguished Name und das Bind-Passwort ein. b. Geben Sie den Basisnamen des Authentifizierungsservers an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**. c. Geben Sie die vom Authentifizierungsserver unterstützte LDAP-Protokollversion an. 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**.

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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren oder Deaktivieren der Option * Sichere Verbindung verwenden*:

Ihr Ziel ist	Dann tun Sie das…
Aktivieren Sie sie	a. Wählen Sie die Option * Sichere Verbindung verwenden* aus. b. Klicken Sie im Bereich Authentication Servers auf **Add**. 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 Zertifikatinformationen und klicken Sie dann auf **Schließen**. f. Klicken Sie im Dialogfeld Host autorisieren auf **Ja**. 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.
Deaktivieren	a. Deaktivieren Sie die Option * Sichere Verbindung verwenden*. b. Klicken Sie im Bereich Authentication Servers auf **Add**. c. Geben Sie im Dialogfeld Authentifizierungsserver hinzufügen entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers und die Portdetails an. d. Klicken Sie Auf **Hinzufügen**.

Der hinzugefügte Authentifizierungsserver wird im Bereich Server angezeigt.

3. 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.

Was Sie brauchen

- 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 über die Anwendungsadministratorrolle verfügen.

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 im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Klicken Sie Auf **Authentifizierung Testen**.
3. Geben Sie im Dialogfeld Testbenutzer den Benutzernamen und das Kennwort des Remote-Benutzers oder des Benutzernamens der Remote-Gruppe ein, und klicken Sie dann auf **Test**.

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

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.

Was Sie brauchen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, 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 Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript auf der Grundlage des Ereignisses ausführen möchten, müssen Sie das Skript mithilfe der Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können eine Warnmeldung direkt auf der Seite Ereignisdetails erstellen, nachdem Sie ein Ereignis empfangen haben. Zusätzlich können Sie eine Warnung auf der Seite „Alarmkonfiguration“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Klicken Sie auf der Seite Alarmkonfiguration 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 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 „`Test`“-Skript, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name**, und geben Sie **HealthTest** in das Feld **Alarmname** ein.
2. Klicken Sie auf **Ressourcen**, und wählen Sie in der Einschließen-Registerkarte **Volumes** aus der Dropdown-Liste aus.
   a. Geben Sie in das Feld **Name enthält abc** ein, um die Volumes anzuzeigen, deren Name „`abc`“ enthält.
   b. Wählen Sie[All Volumes whose name contains 'abc'] im Bereich „Verfügbare Ressourcen“ die Option **++** aus, und verschieben Sie sie in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **exclude**, und geben Sie **xyz** in das Feld **Name enthält** ein, und klicken Sie dann 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 **sample@domain.com** in das Feld Diese Benutzer benachrichtigen ein.
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 aus.
8. Klicken Sie Auf **Speichern**.

Ändern des lokalen Benutzerpassworts

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

Was Sie brauchen

Sie müssen als lokaler Benutzer angemeldet sein.

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 Benutzerpassworts für die Wartung 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**.

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.

Einstellen des Timeout für die Inaktivität der Sitzung

Sie können für Unified Manager den Wert für Inaktivitätszeitüberschreitung festlegen, damit die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist das Timeout auf 4,320 Minuten (72 Stunden) eingestellt.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Diese Einstellung betrifft alle angemeldeten Benutzersitzungen.

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 **Feature Settings** das Inaktivitätszeitlimit an, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Haben Sie keine Zeitüberschreitung gesetzt, so dass die Sitzung nie automatisch geschlossen wird	Bewegen Sie im Fenster **Inaktivität Timeout** den Schieberegler nach links (aus) und klicken Sie auf **Apply**.
Legen Sie eine bestimmte Anzahl von Minuten als Zeitwert fest	Bewegen Sie im Fenster **Inaktivität Timeout** die Schieberegler-Taste nach rechts (ein), geben Sie den Wert für Inaktivität in Minuten an und klicken Sie auf **Apply**.

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.

Was Sie brauchen

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

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 „`Unified Manager`“ 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

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein HTTPS-Standardzertifikat installiert. Sie können ein neues HTTPS-Sicherheitszertifikat generieren, das das vorhandene Zertifikat ersetzt.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Es kann mehrere Gründe geben, das Zertifikat neu zu generieren, z. B. wenn Sie bessere Werte für Distinguished Name (DN) haben möchten oder wenn Sie eine höhere Schlüsselgröße oder einen längeren Ablaufzeitraum wünschen oder wenn das aktuelle Zertifikat abgelaufen ist.

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. Beim erneuten Generieren von Zertifikaten können Sie die Schlüsselgröße und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie die Option aus

der Wartungskonsole verwenden `Reset Server Certificate`, wird ein neues HTTPS-Zertifikat erstellt, das 397 Tage gültig ist. Dieses Zertifikat hat einen RSA-Schlüssel der Größe 2048 Bit.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

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

3. Wählen Sie je nach Erstellung des Zertifikats eine der folgenden Optionen aus:

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mit den aktuellen Werten neu	Klicken Sie auf die Option **regenerieren mit aktuellen Zertifikatattributen**.

Ihr Ziel ist	Tun Sie das…
Generieren Sie das Zertifikat mithilfe anderer Werte	Klicken Sie auf die Option **Aktuellen Zertifikatattributen aktualisieren**. Die Felder allgemeiner Name und Alternative Namen verwenden die Werte aus dem vorhandenen Zertifikat, wenn Sie keine neuen Werte eingeben. Der „`Common Name`“ sollte auf den FQDN des Hosts gesetzt werden. Die anderen Felder erfordern keine Werte, Sie können aber Werte eingeben, beispielsweise FÜR E-MAIL, FIRMA, ABTEILUNG, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat ausgefüllt werden sollen. Sie können auch aus der verfügbaren SCHLÜSSEGRÖSSE (der Schlüsselalgorithmus lautet „`RSA`“.) und DER GÜLTIGKEITSDAUER auswählen.

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.
6. Überprüfen Sie die neuen Zertifikatinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

- Die zulässigen Werte für die Schlüsselgröße sind `2048`, `3072` und `4096`.
- Die Gültigkeitsdauer beträgt mindestens 1 Tag bis maximal 36500 Tage.

Auch wenn eine Gültigkeitsdauer von 36500 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 es von einer bekannten Zertifizierungsstelle unterschrieben zu lassen, wird die Gültigkeit des von der Zertifizierungsstelle zurückgegebenen signierten Zertifikats auf 397 Tage reduziert.

- 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, wird im Feld Alternative Namen nur das verwendet, was Sie in das Feld eingeben. Wenn das Zertifikat leer gelassen wird, hat das resultierende Zertifikat überhaupt kein Feld alternativer Namen.

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.

Was Sie brauchen

Die virtuelle Appliance wird eingeschaltet.

Sie sind als Maintenance-Benutzer bei der Wartungskonsole angemeldet.

Sie können die virtuelle Maschine auch von vSphere 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.

Was Sie brauchen

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

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 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 erneut:

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

5. Netzwerkdienst neu starten:

   ```
   systemctl restart NetworkManager.service
   ```

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. Starten Sie Unified Manager neu, indem Sie den folgenden Befehl eingeben, nachdem Sie die Änderung Ihres Host-Namens abgeschlossen und überprüft haben:

   ```
   systemctl start mysqld ocie ocieau
   ```

Aktivieren und Deaktivieren des richtlinienbasierten Storage-Managements

Ab Unified Manager 9.7 können Sie Storage-Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern bereitstellen und diese Workloads auf Basis zugewiesener Performance-Service-Level managen. Diese Funktion ähnelt dem Erstellen von Workloads in ONTAP System Manager und dem Anbinden von QoS-Richtlinien. Bei Anwendung mit Unified Manager können Sie Workloads jedoch über alle Cluster bereitstellen und managen, von denen Ihre Unified Manager Instanz überwacht wird.

Sie müssen über die Anwendungsadministratorrolle verfügen.

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

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

Neuer Inhalt	Standort
Eine Seite für die Bereitstellung neuer Workloads	Verfügbar über **Allgemeine Aufgaben** > **Provisioning**
Eine Seite zum Erstellen von Service-Level-Richtlinien für die Performance	Verfügbar über **Einstellungen** > **Richtlinien** > **Leistungsstufen**
Eine Seite, um Richtlinien zur Performance-Storage-Effizienz zu erstellen	Erhältlich über **Einstellungen** > **Richtlinien** > **Storage-Effizienz**
Panels zur Beschreibung Ihrer aktuellen Workload-Performance und Workload-IOPS	Verfügbar über das Dashboard

Weitere Informationen zu diesen Seiten und zu dieser Funktion 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 **Feature Settings** die richtlinienbasierte Speicherverwaltung, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren Sie das richtlinienbasierte Storage-Management	Bewegen Sie im Fenster **Policy-based Storage Management** die Schieberegler-Taste nach links.
Richtlinienbasiertes Storage-Management	Bewegen Sie im Fenster **Policy-based Storage Management** die Schieberegler-Taste nach rechts.

Copyright-Informationen

Markeninformationen