Konfigurieren von Active IQ Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren von Active IQ Unified Manager . . . 1
- Informationen zur Konfiguration von Active IQ Unified Manager . . . 1
- Informationen zur Konfigurationsreihenfolge in Active IQ Unified Manager . . . 1
- Zugriff auf die Web-Benutzeroberfläche in Active IQ Unified Manager . . . 1
- Die Ersteinrichtung der Active IQ Unified Manager Weboberfläche wird durchgeführt. . . . 2
- Cluster zu Active IQ Unified Manager hinzufügen . . . 4
- Benachrichtigungen konfigurieren . . . 6
  - Active IQ Unified Manager wird so konfiguriert, dass Warnmeldungen gesendet werden. . . . 7
  - Konfiguration der Einstellungen für Ereignisbenachrichtigungen in Active IQ Unified Manager . . . 7
  - Remote Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 8
  - Verschachtelte Gruppen aus der Remote Authentifizierung in Active IQ Unified Manager sind deaktiviert . . . 10
  - Einrichtung von Authentifizierungsdiensten in Active IQ Unified Manager . . . 10
  - Hinzufügen von Authentifizierungsservern zu Active IQ Unified Manager . . . 11
  - Die Konfiguration der Authentifizierungsserver in Active IQ Unified Manager wird getestet . . . 13
  - Hinzufügen von Benachrichtigungen in Active IQ Unified Manager . . . 13
- Das lokale Benutzerkennwort in Active IQ Unified Manager kann geändert werden. . . . 15
- Die Zeitüberschreitung bei Sitzungsinaktivität in Active IQ Unified Manager festlegen . . . 16
- Die Zeitüberschreitung der Sitzung kann über die CLI in Active IQ Unified Manager festgelegt werden. . . . 17
- Der Hostname von Unified Manager kann geändert werden . . . 17
  - Der Hostname der virtuellen Active IQ Unified Manager Appliance kann geändert werden. . . . 17
  - In Active IQ Unified Manager kann ein HTTPS-Sicherheitszertifikat generiert werden . . . 18
  - Starten Sie die virtuelle Maschine Active IQ Unified Manager neu. . . . 20
  - Ändern des Hostnamens von Active IQ Unified Manager auf Linux Systemen . . . 20
- Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung in Active IQ Unified Manager . . . 21

Konfigurieren von Active IQ Unified Manager

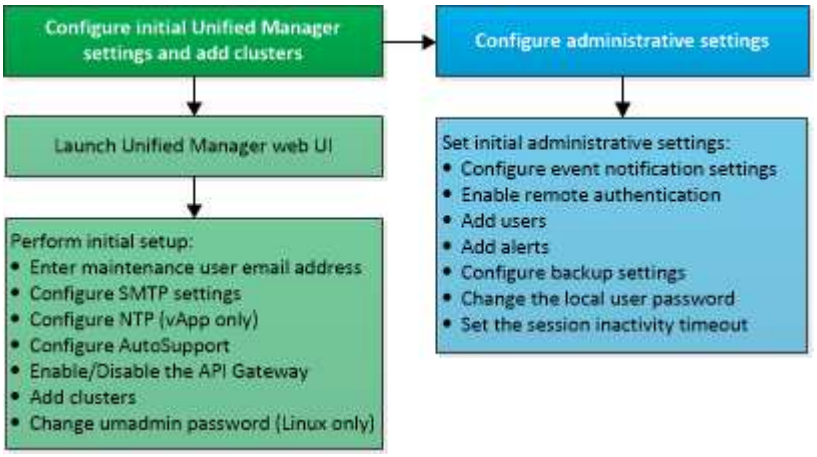
Informationen zur Konfiguration von Active IQ Unified Manager

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-UI zuzugreifen. Anschließend können Sie weitere Konfigurationsaufgaben durchführen, z. B. Cluster hinzufügen, die Remote-Authentifizierung konfigurieren, Benutzer hinzufügen und Warnungen hinzufügen.

Einige der in diesem Handbuch beschriebenen Verfahren sind für die Ersteinrichtung Ihrer Unified Manager Instanz erforderlich. Andere Verfahren sind empfohlene Konfigurationseinstellungen, die für Ihre neue Instanz hilfreich sind oder vor Beginn der regelmäßigen Überwachung Ihrer ONTAP Systeme wissenswert sind.

Informationen zur Konfigurationsreihenfolge in Active IQ Unified Manager

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



Zugriff auf die Web-Benutzeroberfläche in Active IQ Unified Manager

Nach der Installation von Unified Manager können Sie über die Web-Benutzeroberfläche Unified Manager einrichten, um 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 (bzw. als umadmin-Benutzer bei Linux-Installationen) anmelden.
- Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen anstelle des vollqualifizierten Domainnamens (FQDN) oder der 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 bestätigen, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat für die Serverauthentifizierung installieren.

Schritte

1. Der Aufruf der Unified Manager Weboberfläche im Browser erfolgt über die URL, die am Ende der Installation angezeigt wird. Die URL ist die IP-Adresse oder die vollqualifizierte Domain (FQDN) des Unified Manager Servers.

   Der Link hat folgendes Format: `https://URL`.

2. Für die Anmeldung bei der Unified Manager Weboberfläche verwenden Sie Ihre Wartungsbenutzerdaten.

   Wenn Sie innerhalb einer Stunde drei aufeinanderfolgende erfolglose Versuche unternehmen, sich bei der Web UI anzumelden, wird Ihr Zugriff auf das System gesperrt, und Sie müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Die Ersteinrichtung der Active IQ Unified Manager Weboberfläche wird durchgeführt.

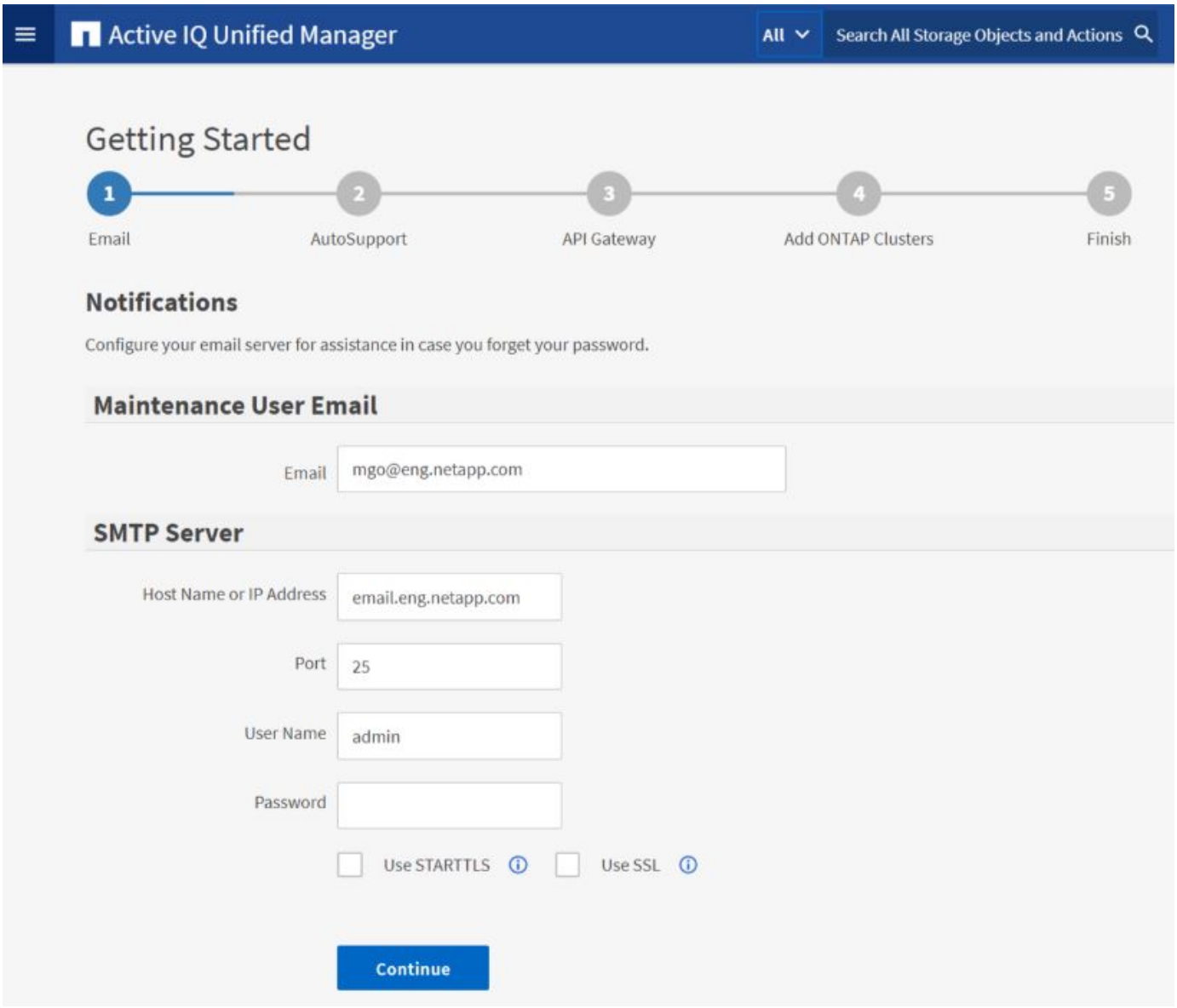
Um Unified Manager nutzen zu können, müssen Sie zunächst die Optionen für die Ersteinrichtung konfigurieren, einschließlich des NTP-Servers, der E-Mail-Adresse des Wartungsbenutzers, des SMTP-Server-Hosts und des Hinzufügens von ONTAP Clustern.

Bevor Sie beginnen

Sie müssen folgende Vorgänge durchgeführt haben:

- Start der Unified Manager Web-UI über die nach der Installation bereitgestellte URL
- Angemeldet mit dem während der Installation erstellten Wartungsbenutzernamen und -passwort (Benutzer umadmin bei Linux-Installationen)

Die Seite „Erste Schritte“ von Active IQ Unified ManagerGetting wird nur angezeigt, wenn Sie erstmals auf die Web-Benutzeroberfläche zugreifen. Die unten stehende Seite stammt aus einer Installation auf VMware.



Wenn Sie eine dieser Optionen später ändern möchten, können Sie Ihre Auswahl im linken Navigationsbereich von Unified Manager unter „Allgemeine Optionen“ treffen. Die NTP-Einstellung gilt nur für VMware-Installationen und kann später über die Unified Manager Managementplattform geändert werden.

Schritte

1. Auf der Seite „Ersteinrichtung“ von Active IQ Unified Manager werden die E-Mail-Adresse des Wartungsbenutzers, der Hostname des SMTP-Servers, alle zusätzlichen SMTP-Optionen sowie der NTP-Server (nur bei VMware Installationen) eingegeben. Danach folgt ein Klick auf **Continue**.

   Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatsseite angezeigt. Anschließend können Sie mit den Einstellungen der Ersteinrichtung der Web-Benutzeroberfläche fortfahren, indem Sie die Zertifikatsdetails überprüfen und das Zertifikat akzeptieren.

2. Auf der Seite AutoSupport können Sie **Agree and Continue** auswählen, um das Senden von AutoSupport Nachrichten von Unified Manager an NetAppActive IQ zu aktivieren.

   Wenn ein Proxy für den Internetzugang zum Senden von AutoSupport Inhalten festgelegt werden muss oder wenn AutoSupport deaktiviert werden soll, steht in der Web-Benutzeroberfläche die Option **Allgemein**

> **AutoSupport** zur Verfügung.

3. Auf Red Hat Systemen erfolgt die Änderung des Passworts des Benutzers umadmin von der Standardzeichenfolge “admin” zu einer personalisierten Zeichenfolge.
4. Auf der Seite „API Gateway einrichten“ wählen Sie aus, ob Sie die API Gateway Funktion verwenden möchten, mit der Unified Manager die ONTAP Cluster managen kann, die Sie mithilfe von ONTAP REST APIs überwachen möchten. Anschließend klicken Sie 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. Die Cluster, die von Unified Manager gemanagt werden sollen, werden hinzugefügt, und anschließend wird auf **Weiter** geklickt. Für jeden Cluster, der gemanagt werden soll, müssen der Hostname oder die Clusterverwaltungs-IP-Adresse (IPv4 oder IPv6) sowie die Anmeldedaten aus Benutzername und Passwort vorliegen - der Benutzer muss über die Rolle “admin” verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche unter **Speicherverwaltung** > **Cluster-Einrichtung** hinzufügen.
6. Auf der Übersichtsseite können Sie überprüfen, ob alle Einstellungen korrekt sind, und anschließend auf **Finish** klicken.

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

Cluster zu Active IQ Unified Manager hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dies umfasst die Möglichkeit, Clusterinformationen wie den Systemstatus, die Kapazität, die Performance und die Konfiguration des Clusters abzurufen, damit Sie auftretende Probleme erkennen und beheben können.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie benötigen folgende Informationen:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select, Cloud Volumes ONTAP.
  - Hostname oder Cluster-Management-IP-Adresse

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

    Die Clusterverwaltungs-IP-Adresse muss die Clusterverwaltungs-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn eine Knotenverwaltungs-LIF verwendet wird, schlägt der Vorgang fehl.
  - Auf dem Cluster muss mindestens die ONTAP Softwareversion 9.1 oder höher ausgeführt werden.
  - ONTAP Administrator-Benutzername und Passwort

    Dieses Konto muss die Rolle *admin* besitzen, wobei der Anwendungszugriff auf *ontapi*, *amqp*, *console* und *http* festgelegt sein muss.

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

  SSL-Zertifikat (HTTPS): Dieses Zertifikat gehört Unified Manager. Bei einer Neuinstallation von Unified Manager wird standardmäßig ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, es für mehr Sicherheit auf ein von einer Zertifizierungsstelle signiertes Zertifikat umzustellen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Services das neue Zertifikat übernehmen. Weitere Informationen zum Regenerieren von SSL-Zertifikaten enthält "Generieren eines HTTPS-Sicherheitszertifikats".

  EMS-Zertifikat: Dieses Zertifikat gehört dem Unified Manager. Es dient zur Authentifizierung von EMS-Benachrichtigungen, die von ONTAP empfangen werden.

  Zertifikate für die gegenseitige TLS-Kommunikation: Werden während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist für einen Cluster abhängig von der ONTAP Version aktiviert. Wenn auf einem Cluster eine ONTAP Version niedriger als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

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

  - Über die Web-Benutzeroberfläche lässt sich ein Cluster hinzufügen, und die zertifikatbasierte Authentifizierung wird dabei automatisch aktiviert.
  - Sie können einen Cluster über Unified Manager CLI hinzufügen, die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mit Unified Manager CLI hinzufügen, müssen Sie den Cluster anschließend über Unified Manager UI bearbeiten. Unter "Unterstützte Unified Manager CLI-Befehle" finden Sie Informationen zum Hinzufügen eines Clusters mit Unified Manager CLI.
  - Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie das Backup von Unified Manager auf einem Server erstellen und es auf einem anderen Unified Manager Server wiederherstellen, bei dem Hostname oder IP-Adresse geändert wurden, kann die Überwachung des Clusters fehlschlagen. Zur Vermeidung dieses Fehlers empfiehlt sich das Bearbeiten und Speichern der Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter "Cluster bearbeiten".

  + **Clusterzertifikate**: Dieses Zertifikat gehört ONTAP. Sie können keinen Cluster mit einem abgelaufenen Zertifikat zu Unified Manager hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, müssen Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatserstellung finden Sie im entsprechenden Knowledge-Base-Artikel "Erneuern eines ONTAP selbstsignierten Zertifikats in der System Manager Benutzeroberfläche".

- Auf dem Unified Manager Server muss ausreichend Speicherplatz vorhanden sein. Ein Cluster kann dem Server nicht hinzugefügt werden, wenn bereits mehr als 90 % des Speicherplatzes im Datenbankverzeichnis belegt sind.

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

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ ist **Add** auszuwählen.
3. Im Dialogfeld „Cluster hinzufügen“ werden die erforderlichen Werte wie Hostname oder IP-Adresse des Clusters, Benutzername, Kennwort und Portnummer angegeben.

   Sie können die Cluster-Management-IP-Adresse von IPv6 auf IPv4 oder von IPv4 auf IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Cluster-Raster und auf der Seite zur Cluster-Konfiguration angezeigt.
4. Anschließend **Absenden** auswählen.
5. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
6. Klicken Sie auf **Ja**.

   Nach dem Speichern der Clusterdetails können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster einsehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, prüft Unified Manager das Zertifikat nur beim erstmaligen Hinzufügen des Clusters. Unified Manager prüft 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 Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

Da die Erfassung von 15 Tagen an Performance-Daten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit Abfragen zur Erfassung der Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden. Außerdem wird die Erfassung angehalten, wenn Unified Manager während des Zeitraums der Erfassung der Datenkontinuität neu gestartet wird, und in den Performance-Diagrammen sind für den fehlenden Zeitraum Lücken zu sehen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, ist zu prüfen, ob die Uhren der beiden Systeme nicht synchronisiert sind und ob das Startdatum des Unified Manager HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Es muss sichergestellt werden, dass die Uhren mithilfe von NTP oder einem ähnlichen Service synchronisiert sind.

Verwandte Informationen

"Installation eines von einer CA signierten und zurückgegebenen HTTPS-Zertifikats"

Benachrichtigungen konfigurieren

Active IQ Unified Manager wird so konfiguriert, dass Warnmeldungen gesendet werden.

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

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Nach dem Deployment von Unified Manager und dem Abschluss der Erstkonfiguration sollte die Konfiguration Ihrer Umgebung so erfolgen, dass beim Empfang von Ereignissen Warnmeldungen ausgelöst und Benachrichtigungs-E-Mails oder SNMP-Traps generiert werden.

Schritte

1. "Konfiguration der Einstellungen für Ereignisbenachrichtigungen".

   Wenn Sie bei bestimmten Ereignissen in Ihrer Umgebung Benachrichtigungen erhalten möchten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Benachrichtigungen gesendet werden sollen. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. "Remote-Authentifizierung aktivieren".

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

3. "Authentifizierungsserver hinzufügen".

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

4. "Benutzer hinzufügen".

   Sie können verschiedene Arten von lokalen oder Remote-Benutzern hinzufügen und ihnen spezifische Rollen zuweisen. Beim Erstellen einer Warnung weisen Sie einen Benutzer zu, der die Warnungsbenachrichtigungen erhalten soll.

5. "Benachrichtigungen hinzufügen".

   Nachdem Sie die E-Mail-Adresse für den Versand 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.

Konfiguration der Einstellungen für Ereignisbenachrichtigungen in Active IQ Unified Manager

Sie können Unified Manager so konfigurieren, dass Alarmbenachrichtigungen gesendet werden, sobald ein Ereignis generiert oder einem Benutzer zugewiesen wird. Sie können den SMTP-Server konfigurieren, der zum Senden der Alarmbenachrichtigung verwendet

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

Bevor Sie beginnen

Sie benötigen folgende Informationen:

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

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

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

  Zur Angabe mehrerer Trap-Ziele dienen Kommas als Trennzeichen zwischen den einzelnen Hosts. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie Version und ausgehender Trap-Port, für alle Hosts in der Liste identisch sein.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benachrichtigungen**.
2. Auf der Seite „Benachrichtigungen“ können Sie die entsprechenden Einstellungen konfigurieren.

   Anmerkungen:

   - Wenn die Absenderadresse mit der Adresse "ActiveIQUnifiedManager@localhost.com" vorausgefüllt ist, sollte sie in eine echte, funktionierende E-Mail-Adresse geändert werden, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.
   - Kann der Hostname des SMTP-Servers nicht aufgelöst werden, können Sie anstelle des Hostnamens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.
3. Auf **Speichern** klicken.
4. Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatsseite angezeigt. Zum Speichern der Benachrichtigungseinstellungen ist eine Überprüfung der Zertifikatsdetails sowie die Annahme des Zertifikats erforderlich.

   Über die Schaltfläche **View Certificate Details** können die Zertifikatsdetails angezeigt werden. Wenn das vorhandene Zertifikat abgelaufen ist, kann die Markierung im Kontrollkästchen **Use STARTTLS** oder **Use SSL** entfernt, die Benachrichtigungseinstellungen gespeichert und anschließend das Kontrollkästchen **Use STARTTLS** oder **Use SSL** erneut aktiviert werden, um ein neues Zertifikat anzuzeigen.

Remote Authentifizierung in Active IQ Unified Manager ist aktiviert

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

Manager auf Storage-Objekte und Daten zugreifen und diese managen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

> 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 Port 389 als Standardport für ungesicherte Kommunikation und Port 636 als Standardport für gesicherte Kommunikation.

> Das zur Authentifizierung von Benutzern verwendete Zertifikat muss dem X.509-Format entsprechen.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen für **Remote-Authentifizierung…** aktivieren.
3. Im Feld „Authentifizierungsdienst“ erfolgen die Auswahl des Diensttyps und die Konfiguration des Authentifizierungsdiensts.

Für den Authentifizierungstyp…	Eingabe der folgenden Informationen…
Active Directory	• Name des Administrators des Authentifizierungsservers in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (unter Verwendung der entsprechenden LDAP-Notation) • Administratorpasswort • Basis individueller Name (unter Verwendung der entsprechenden LDAP-Notation)
OpenLDAP	• Bind individueller Name (in der entsprechenden LDAP-Notation) • Bind Passwort • Basisindividueller Name

Wenn die Authentifizierung eines Active Directory-Benutzers lange dauert oder eine Zeitüberschreitung auftritt, benötigt der Authentifizierungsserver wahrscheinlich lange für eine Antwort. Das Deaktivieren der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen.

Wenn für den Authentifizierungsserver die Option „Use Secure Connection“ ausgewählt ist, kommuniziert

Unified Manager mit dem Authentifizierungsserver über das Secure Sockets Layer (SSL)-Protokoll.

4. **Optional:** Authentifizierungsserver hinzufügen und die Authentifizierung testen.
5. Auf **Speichern** klicken.

Verschachtelte Gruppen aus der Remote Authentifizierung in Active IQ Unified Manager sind deaktiviert

Wenn die Remote-Authentifizierung aktiviert ist, kann die Authentifizierung verschachtelter Gruppen deaktiviert werden, sodass sich nur einzelne Benutzer und nicht Gruppenmitglieder remote bei Unified Manager authentifizieren können. Verschachtelte Gruppen können deaktiviert werden, wenn die Antwortzeit der Active Directory-Authentifizierung verbessert werden soll.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Die Deaktivierung verschachtelter Gruppen gilt nur bei Verwendung von Active Directory.

Die Deaktivierung der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen. Wenn die Unterstützung für verschachtelte Gruppen deaktiviert ist und eine Remote-Gruppe zu Unified Manager hinzugefügt wird, müssen die einzelnen Benutzer Mitglieder der Remote-Gruppe sein, um sich bei Unified Manager zu authentifizieren.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen für **Verschachtelte Gruppensuche deaktivieren** muss aktiviert sein.
3. Auf **Speichern** klicken.

Einrichtung von Authentifizierungsdiensten in Active IQ Unified Manager

Authentifizierungs Services ermöglichen die Authentifizierung von Remote-Benutzern oder Remote-Gruppen auf einem Authentifizierungsserver, bevor sie Zugriff auf Unified Manager erhalten. Sie können Benutzer mithilfe vordefinierter Authentifizierungs Services (wie Active Directory oder OpenLDAP) authentifizieren oder einen eigenen Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

- Die Remote-Authentifizierung muss aktiviert sein.
- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Auswahl eines der folgenden Authentifizierung Services:

Wenn Sie auswählen…	Fahren Sie dann wie folgt fort…
Active Directory	a. Administratorname und Passwort eingeben. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Sie geben den individuellen Namen für Bind und das Passwort für Bind ein. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**.
Andere	a. Sie geben den individuellen Namen für Bind und das Passwort für Bind ein. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**. c. Die vom Authentifizierungsserver unterstützte LDAP Protokollversion. d. Einzugeben sind Benutzername, Gruppenzugehörigkeit, Benutzergruppe und Mitgliedsattribute.

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

3. Auf **Speichern** klicken.

Hinzufügen von Authentifizierungsservern zu Active IQ Unified Manager

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 verfügbar sein:

- 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 benötigen die Rolle des Anwendungsadministrators.

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

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Die Option **Sichere Verbindung verwenden** lässt sich aktivieren oder deaktivieren:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Aktivierung	a. Die Option **Sichere Verbindung verwenden** wird ausgewählt. b. Im Bereich „Authentifizierungsserver“ ist auf **Hinzufügen** zu klicken. c. Im Dialogfeld „Authentifizierungsserver hinzufügen“ ist der Authentifizierungsname oder die IP-Adresse (IPv4 oder IPv6) des Servers einzugeben. d. Im Dialogfeld „Host autorisieren“ auf „Zertifikat anzeigen“ klicken. e. Im Dialogfeld „Zertifikat anzeigen“ können Sie die Zertifikatsinformationen überprüfen und anschließend auf **Schließen** klicken. f. Im Dialogfeld „Host autorisieren“ erfolgt die Auswahl von **Ja**. Wenn Sie die Option **Use Secure Connection authentication** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet standardmäßig Port 636 für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation.

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Deaktivieren	a. Die Option **Sichere Verbindung verwenden** darf nicht aktiviert sein. b. Im Bereich „Authentifizierungsserver“ ist auf **Hinzufügen** zu klicken. c. Im Dialogfeld „Authentifizierungsserver hinzufügen“ erfolgt die Angabe entweder des Hostnamens oder der IP-Adresse (IPv4 oder IPv6) des Servers sowie der Portdetails. d. Klicken Sie auf **Add**.

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

3. Eine Testauthentifizierung bestätigt, dass Benutzer auf dem hinzugefügten Authentifizierungsserver authentifiziert werden können.

Die Konfiguration der Authentifizierungsserver in Active IQ Unified Manager wird getestet

Sie können die Konfiguration Ihrer Authentifizierungsserver überprüfen, um sicherzustellen, dass der Management Server mit ihnen kommunizieren kann. Sie können die Konfiguration überprüfen, indem Sie auf Ihren Authentifizierungsservern nach einem Remote-Benutzer oder einer Remote-Gruppe suchen und diese mithilfe der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsservice 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 Managementserver auf diesen Servern nach dem Remote-Benutzer oder der Remote-Gruppe suchen und diese authentifizieren kann.
- Sie benötigen die Rolle des Anwendungsadministrators.

Wenn der Authentifizierungsdienst auf Active Directory eingestellt ist und die Authentifizierung von Remote-Benutzern validiert wird, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Dann folgt ein Klick auf **Authentifizierung testen**.
3. Im Dialogfeld „Test User“ geben Sie den Benutzernamen und das Kennwort des Remote-Benutzers oder den Benutzernamen der Remote-Gruppe an und klicken anschließend auf **Test**.

   Bei der Authentifizierung einer Remote-Gruppe dürfen Sie das Passwort nicht eingeben.

Hinzufügen von Benachrichtigungen in Active IQ Unified Manager

Sie können Warnmeldungen so konfigurieren, dass Sie benachrichtigt werden, wenn ein

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

Bevor Sie beginnen

- Es müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, der SMTP-Server und der SNMP-Trap-Host konfiguriert sein, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Benachrichtigung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn ein Skript basierend auf dem Ereignis ausgeführt werden soll, muss das Skript zuvor über die Seite „Skripte“ zu Unified Manager hinzugefügt worden sein.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Es besteht die Möglichkeit, eine Benachrichtigung direkt auf der Seite „Ereignisdetails“ nach dem Empfang eines Ereignisses zu erstellen, zusätzlich zur Erstellung einer Benachrichtigung über die Seite „Benachrichtigungseinrichtung“, wie hier beschrieben.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite „Benachrichtigungseinstellungen“ erfolgt ein Klick auf **Hinzufügen**.
3. Im Dialogfeld „Warnung hinzufügen“ wird auf **Name** geklickt und ein Name sowie eine Beschreibung für die Warnung eingegeben.
4. **Ressourcen** auswählen und die Ressourcen bestimmen, die in die Benachrichtigung einbezogen oder von ihr ausgeschlossen werden.

   Ein Filter kann festgelegt werden, indem im Feld **Name enthält** ein Text-String angegeben wird, um eine Gruppe von Ressourcen auszuwählen. Basierend auf dem angegebenen Text-String werden in der Liste der verfügbaren Ressourcen nur die Ressourcen angezeigt, die der Filterregel entsprechen. Der angegebene Text-String ist Groß-/Kleinschreibungs-empfindlich.

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

5. Auf **Ereignisse** klicken und die Ereignisse anhand des Ereignisnamens oder des Typs des Schweregrads auswählen, für die ein Alarm ausgelöst werden soll.

   Um mehr als ein Ereignis auszuwählen, die Strg-Taste gedrückt halten, während die Auswahl getroffen wird.

6. Auf **Aktionen** klicken, die Benutzer auswählen, die benachrichtigt werden sollen, die Benachrichtigungshäufigkeit festlegen, auswählen, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und ein Skript zuweisen, das ausgeführt wird, wenn eine Warnung generiert wird.

   Wenn die für den Benutzer angegebene E-Mail-Adresse geändert und die Benachrichtigung erneut zum Bearbeiten geöffnet wird, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert wurde, wird

die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

Alternativ ist es möglich, die Benutzer auch über SNMP-Traps zu benachrichtigen.

7. Auf **Speichern** klicken.

Beispiel für das Hinzufügen einer Benachrichtigung

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

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

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

Schritte

1. Unter **Name** erfolgt die Eingabe von **HealthTest** in das Feld **Alarmname**.
2. **Ressourcen** auswählen und im Tab „Einschließen“ **Volumes** aus der Dropdown-Liste wählen.
   a. Durch Eingabe von **abc** in das Feld **Name enthält** werden die Volumes angezeigt, deren Name “abc” enthält.
   b. **<<All Volumes whose name contains 'abc'>>** im Bereich „Verfügbare Ressourcen“ auswählen und in den Bereich „Ausgewählte Ressourcen“ verschieben.
   c. Nach Auswahl von **Exclude** erfolgt die Eingabe von **xyz** in das Feld **Name contains**; anschließend wird **Add** ausgewählt.
3. Auf **Ereignisse** klicken und im Feld **Ereignisschweregrad Kritisch** auswählen.
4. Im Bereich „Übereinstimmende Ereignisse“ **Alle kritischen Ereignisse** auswählen und in den Bereich „Ausgewählte Ereignisse“ verschieben.
5. Unter **Actions** wird im Feld **Alert these users sample@domain.com** eingetragen.
6. **Alle 15 Minuten erinnern** benachrichtigt den Benutzer alle 15 Minuten.

   Sie können eine Benachrichtigung so konfigurieren, dass sie über einen festgelegten Zeitraum wiederholt an die Empfänger gesendet wird. Es sollte der Zeitpunkt festgelegt werden, ab dem die Ereignisbenachrichtigung für die Benachrichtigung aktiv ist.

7. Im Menü „Auszuführendes Skript auswählen“ das Skript **Test** auswählen.
8. Auf **Speichern** klicken.

Das lokale Benutzerkennwort in Active IQ Unified Manager kann geändert werden.

Sie können Ihr Passwort für die Anmeldung als lokaler Benutzer 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. Die Änderung eines Remote-Benutzerpassworts erfolgt über Ihren Passwortadministrator. Informationen zum Ändern des Passworts des Wartungsbenutzers enthält "Verwenden der Managementplattform".

Schritte

1. Sie sind bei Unified Manager angemeldet.
2. In der oberen Menüleiste erfolgt die Auswahl zunächst über das Benutzersymbol und anschließend über **Passwort ändern**.

   Bei Remote-Benutzern ist die Option **Passwort ändern** nicht verfügbar.

3. Im Dialogfeld „Passwort ändern“ erfolgt die Eingabe des aktuellen Passworts und des neuen Passworts.
4. Auf **Speichern** klicken.

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

Die Zeitüberschreitung bei Sitzungsinaktivität in Active IQ Unified Manager festlegen

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

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Diese Einstellung betrifft alle angemeldeten Benutzersitzungen.

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

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Feature Settings** können Sie die Inaktivitäts-Zeitüberschreitung festlegen, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Es ist keine Zeitüberschreitung festgelegt, sodass die Sitzung niemals automatisch geschlossen wird.	Im Bereich **Inactivity Timeout** den Schieberegler nach links (aus) verschieben und auf **Apply** klicken.
Festlegen einer bestimmten Anzahl von Minuten als Wert für die Zeitüberschreitung	Im Bereich **Inactivity Timeout** den Schieberegler nach rechts (Ein) bewegen, den Wert für die Inaktivitäts-Zeitüberschreitung in Minuten angeben und **Apply** auswählen.

Die Zeitüberschreitung der Sitzung kann über die CLI in Active IQ Unified Manager festgelegt werden.

Über die Befehlszeilenschnittstelle (CLI) kann für Unified Manager ein maximaler Wert für die Sitzungs-Zeitüberschreitung festgelegt werden, sodass die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist die Sitzungs-Zeitüberschreitung auf den Maximalwert von 4.320 Minuten (72 Stunden) eingestellt. Das bedeutet, dass Ihre Sitzung nach 72 Stunden automatisch endet, selbst wenn Sie angemeldet sind und Unified Manager aktiv nutzen.

Über diese Aufgabe

Sie benötigen die Rolle des Anwendungsadministrators.

Die Einstellung für die Zeitüberschreitung von Sitzungen betrifft alle angemeldeten Benutzersitzungen.

Schritte

1. Die Anmeldung bei der Unified Manager CLI erfolgt durch Eingabe des `um cli login` Befehls. Für die Authentifizierung werden ein gültiger Benutzername und ein gültiges Passwort benötigt.
2. Der `um option set max.session.timeout.value=<in mins>` Befehl dient zum Ändern des Werts der Sitzungs-Zeitüberschreitung.

Der Hostname von Unified Manager kann geändert werden

Der Hostname der virtuellen Active IQ Unified Manager Appliance kann geändert werden.

Dem Netzwerkhost wird beim ersten Deployment der virtuellen Unified Manager Appliance ein Name zugewiesen. Sie können den Hostnamen nach dem Deployment 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 muss die Rolle Application Administrator zugewiesen sein.

Der Hostname (oder die Host-IP-Adresse) kann für den Zugriff auf die Unified Manager Web-Benutzeroberfläche verwendet werden. Wenn während des Deployment eine statisch IP-Adresse für Ihr Netzwerk konfiguriert wurde, wurde dem Netzwerkhost ein Name zugewiesen. Wenn das Netzwerk mit DHCP konfiguriert wurde, sollte der Hostname aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht ordnungsgemäß konfiguriert sind, wird der Hostname “Unified Manager” automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat generieren, wenn Sie den Hostnamen ändern und beabsichtigen, mit dem neuen Hostnamen auf die Unified Manager web UI zuzugreifen.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche 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 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 tritt erst nach einem Neustart der virtuellen Maschine des Unified Manager in Kraft.

Schritte

1. Generierung eines HTTPS-Sicherheitszertifikats

   Wenn Sie den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es dem neuen Hostnamen zuzuordnen.

2. Neustart der virtuellen Maschine von Unified Manager

   Nach der Neugenerierung des HTTPS-Zertifikats ist ein Neustart der virtuellen Maschine von Unified Manager erforderlich.

In Active IQ Unified Manager kann ein HTTPS-Sicherheitszertifikat generiert werden

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein Standard HTTPS Zertifikat installiert. Es kann ein neues HTTPS Sicherheitszertifikat generiert werden, das das vorhandene Zertifikat ersetzt.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Es kann verschiedene Gründe für die Neugenerierung des Zertifikats geben, beispielsweise wenn Sie bessere Werte für den individuellen Namen (DN) wünschen, eine höhere Schlüssellänge oder eine längere Gültigkeitsdauer benötigen oder wenn das aktuelle Zertifikat abgelaufen ist.

Wenn Sie keinen Zugriff auf die Unified Manager Web-UI haben, können Sie das HTTPS-Zertifikat über die Managementplattform mit denselben Werten neu generieren. Beim Neugenerieren von Zertifikaten können Sie die Schlüssellänge und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie in der Managementplattform die Option `Reset Server Certificate` verwenden, wird ein neues HTTPS-Zertifikat mit einer Gültigkeit von 397 Tagen erstellt. Dieses Zertifikat verfügt über einen RSA-Schlüssel mit einer Länge von 2048 Bit.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. **Regenerate HTTPS Certificate** auswählen.

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

3. Je nachdem, wie das Zertifikat generiert werden soll, ist eine der folgenden Optionen auszuwählen:

Wenn Sie möchten…	Folgendes ist zu tun…
Neugenerierung des Zertifikats mit den aktuellen Werten	Die Option **Neu generieren mit aktuellen Zertifikatsattributen** auswählen.

Wenn Sie möchten…	Folgendes ist zu tun…
Erzeugen des Zertifikats mit verschiedenen Werten	Auswahl der Option **Aktuelle Zertifikatsattribute aktualisieren**. Die Felder „Allgemeiner Name“ und „Alternative Namen“ verwenden die Werte des vorhandenen Zertifikats, 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 jedoch Werte eingeben, z. B. für E-MAIL, COMPANY, DEPARTMENT, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat eingetragen werden sollen. Außerdem kann aus der verfügbaren KEY SIZE (der Schlüsselalgorithmus ist „`RSA`“) und dem VALIDITY PERIOD ausgewählt werden. • Die zulässigen Werte für die Schlüssellänge sind `2048`, `3072` und `4096`. • Die Gültigkeitsdauer beträgt mindestens 1 Tag und maximal 36500 Tage. Obwohl eine Gültigkeitsdauer von 36.500 Tagen zulässig ist, empfiehlt sich eine Gültigkeitsdauer von maximal 397 Tagen bzw. 13 Monaten. Wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen wählen und planen, einen CSR für dieses Zertifikat zu exportieren und von einer bekannten CA signieren zu lassen, beträgt die Gültigkeit des von der CA zurückgegebenen signierten Zertifikats nur 397 Tage. • Sie können das Kontrollkästchen „Lokale Identifikationsinformationen ausschließen (z. B. localhost)“ aktivieren, wenn Sie die lokalen Identifikationsinformationen 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 Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld

4. Mit **Ja** kann das Zertifikat neu generiert werden.
5. Damit das neue Zertifikat wirksam wird, ist ein Neustart des Unified Manager Server erforderlich.
6. Die neuen Zertifikatsinformationen können durch Anzeige des HTTPS-Zertifikats überprüft werden.

Starten Sie die virtuelle Maschine Active IQ Unified Manager neu.

Sie können die virtuelle Maschine über die Managementplattform von Unified Manager neu starten. Ein Neustart ist erforderlich, nachdem ein neues Sicherheitszertifikat generiert wurde oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance ist eingeschaltet.

Sie sind bei der Managementplattform für die Wartung als Wartungsbenutzer angemeldet.

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

Schritte

1. Auf die Wartungskonsole zugreifen.
2. Für den Neustart der virtuellen Maschine ist **System Configuration** > **Reboot Virtual Machine** auszuwählen.

Ändern des Hostnamens von Active IQ Unified Manager auf Linux Systemen

Gegebenenfalls möchten Sie den Hostnamen des Red Hat Enterprise Linux Rechners ändern, auf dem Unified Manager installiert ist. Beispielsweise können Sie den Host umbenennen, um Ihre Unified Manager Server beim Auflisten Ihrer Linux Rechner leichter nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf das Linux-System, auf dem Unified Manager installiert ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web UI von Unified Manager zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen 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 generieren, wenn Sie den Hostnamen ändern und beabsichtigen, den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche zu verwenden.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche zugreifen, müssen Sie bei einer Änderung des Hostnamens kein neues Zertifikat generieren. 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 des Linux-Rechners 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. Sie melden sich als Root-Benutzer bei dem Unified Manager System an, das Sie ändern möchten.
2. Zum Beenden der Unified Manager Software und der zugehörigen MySQL Software ist der folgende Befehl einzugeben:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Die Änderung des Hostnamens erfolgt mit dem Linux `hostnamectl` Befehl:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Das HTTPS-Zertifikat für den Server neu generieren:

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

5. Neustart des Netzwerkservice:

   ```
   systemctl restart NetworkManager.service
   ```

6. Nach dem Neustart des Dienstes sollte geprüft werden, ob der neue Hostname sich selbst anpingen kann:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Dieser Befehl sollte dieselbe IP-Adresse zurückgeben, die zuvor für den ursprünglichen Hostnamen festgelegt wurde.

7. Nachdem Sie die Änderung Ihres Hostnamens abgeschlossen und überprüft haben, muss Unified Manager mit dem folgenden Befehl neu gestartet werden:

   ```
   systemctl start mysqld ocie ocieau
   ```

Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung in Active IQ Unified Manager

Ab Unified Manager 9.7 können Sie Storage Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern provisionieren und diese Workloads anhand zugewiesener Performance Service Levels managen. Diese Funktionalität ähnelt der Erstellung von Workloads in ONTAP System Manager und dem Anhängen von QoS Richtlinien, bei der Verwendung von Unified Manager können Sie Workloads jedoch clusterübergreifend auf allen Clustern provisionieren und managen, die von Ihrer Unified Manager Instanz überwacht werden.

Sie benötigen die Rolle des Anwendungsadministrators.

Diese Option ist standardmäßig aktiviert, kann jedoch deaktiviert werden, wenn Sie Workloads nicht mit Unified Manager provisionieren und managen möchten.

Wenn diese Option aktiviert ist, stehen viele neue Elemente in der Benutzeroberfläche zur Verfügung:

Neue Inhalte	Standort
Eine Seite zum Provisionieren neuer Workloads	Verfügbar unter **Allgemeine Aufgaben** > **Provisionierung**
Eine Seite zum Erstellen von Performance Service Level-Richtlinien	Verfügbar unter **Einstellungen** > **Richtlinien** > **Performance Service Levels**
Eine Seite zum Erstellen von Performance Storage Effizienzrichtlinien	Verfügbar unter **Einstellungen** > **Richtlinien** > **Speichereffizienz**
Bereiche, die Ihre aktuelle Workload Performance und Workload IOPS beschreiben	Im Dashboard verfügbar

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

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Funktionseinstellungen** können Sie die richtlinienbasierte Storage-Verwaltung deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Deaktivierung der richtlinienbasierten Storage-Verwaltung	Im Bedienfeld **Policy-based storage management** den Schieberegler nach links verschieben.
Aktivierung der richtlinienbasierten Storage-Verwaltung	Im Bedienfeld **Policy-based storage management** lässt sich der Schieberegler nach rechts verschieben.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.