Konfigurations- und Verwaltungsaufgaben durchführen

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

Konfigurations- und Verwaltungsaufgaben durchführen . . . 1
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
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. . . . 16
Der Hostname von Unified Manager kann geändert werden . . . 17
Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung in Active IQ Unified Manager . . . 21
Active IQ Unified Manager Sicherung konfigurieren . . . 22
Funktionseinstellungen managen . . . 22
Informationen zu Funktionseinstellungen in Active IQ Unified Manager . . . 22
Die richtlinienbasierte Speicherverwaltung in Active IQ Unified Manager kann aktiviert werden . . . 23
Informationen zur API Gateway Funktion in Active IQ Unified Manager . . . 23
Angeben der Zeitüberschreitung bei Inaktivität in Active IQ Unified Manager . . . 24
Aktivierung von Active IQ Portalereignissen in Active IQ Unified Manager . . . 24
Aktivieren und Deaktivieren von Sicherheitseinstellungen für die Compliance in Active IQ Unified Manager . . . 25
Aktivieren und Deaktivieren des Skript-Uploads in Active IQ Unified Manager . . . 26
Hinzufügen eines Anmeldebanners in Active IQ Unified Manager . . . 26
Verwendung der Managementplattform . . . 26
Informationen zur Wartungskonsole in Active IQ Unified Manager . . . 26
Informationen zum Wartungsbenutzer in Active IQ Unified Manager . . . 27
Diagnosefunktionen für Benutzer in Active IQ Unified Manager . . . 27
Zugriff auf die Wartungskonsole in Active IQ Unified Manager . . . 27
Zugriff auf die Wartungskonsole über die vSphere VM-Konsole in Active IQ Unified Manager . . . 28
Menüs der Managementplattform für die Wartung . . . 29
Das Kennwort des Wartungsbenutzers unter Windows in Active IQ Unified Manager ändern . . . 34
Ändern des Active IQ Unified Manager umadmin Passworts auf Linux Systemen . . . 34
Die von Active IQ Unified Manager für die HTTP- und HTTPS-Protokolle verwendeten Ports können geändert werden. . . . 35
Netzwerkschnittstellen zu Active IQ Unified Manager hinzufügen . . . 36
Das Clientzertifikat in Active IQ Unified Manager neu generieren . . . 36
Festplattenspeicher hinzufügen . . . 37
Benutzerzugriff verwalten . . . 40
Benutzer hinzufügen . . . 41
Benutzereinstellungen in Active IQ Unified Manager bearbeiten . . . 42
Benutzer in Active IQ Unified Manager anzeigen . . . 42
Löschen von Benutzern oder Gruppen in Active IQ Unified Manager . . . 43

Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager . . . 43
Informationen zu Benutzertypen in Active IQ Unified Manager . . . 44
Informationen zu Benutzerrollen in Active IQ Unified Manager . . . 44
Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager . . . 45
Verwalten der SAML-Authentifizierungseinstellungen . . . 47
SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 47
Verwendung eines Identitätsanbieters in Active IQ Unified Manager . . . 47
SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 49
Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager . . . 50
Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats . . . 51
SAML Authentifizierung in Active IQ Unified Manager deaktivieren . . . 52
Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert. . . . 53
Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden . . . 53
Authentifizierung verwalten . . . 54
Bearbeiten von Authentifizierungsservern in Active IQ Unified Manager . . . 54
Authentifizierungsserver in Active IQ Unified Manager löschen . . . 55
Authentifizierung mit Active Directory oder OpenLDAP in Active IQ Unified Manager . . . 55
Audit-Logging . . . 56
Die Seite „Remote-Authentifizierung“ in Active IQ Unified Manager . . . 58
Sicherheitszertifikate verwalten . . . 62
Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen . . . 62
Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager . . . 62
Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager . . . 63
Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden . . . 64
Seitenbeschreibungen für die Zertifikatsverwaltung . . . 66

Konfigurations- und Verwaltungsaufgaben durchführen

Konfigurieren von Active IQ Unified Manager

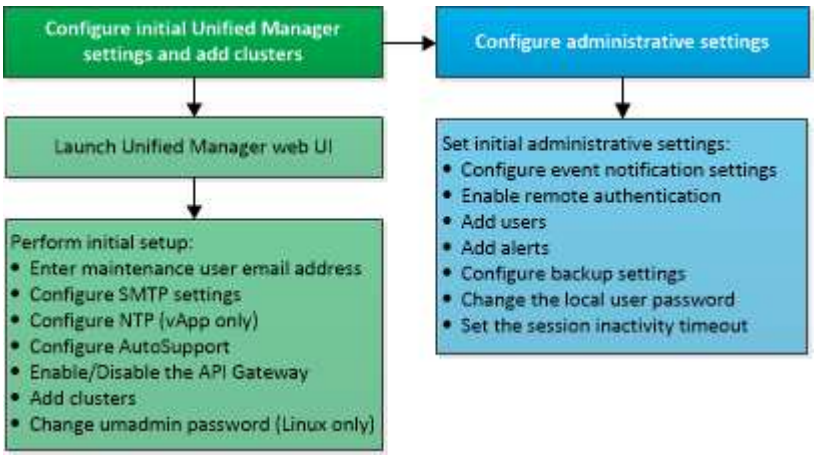
Informationen zur Konfiguration von Active IQ Unified Manager

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.

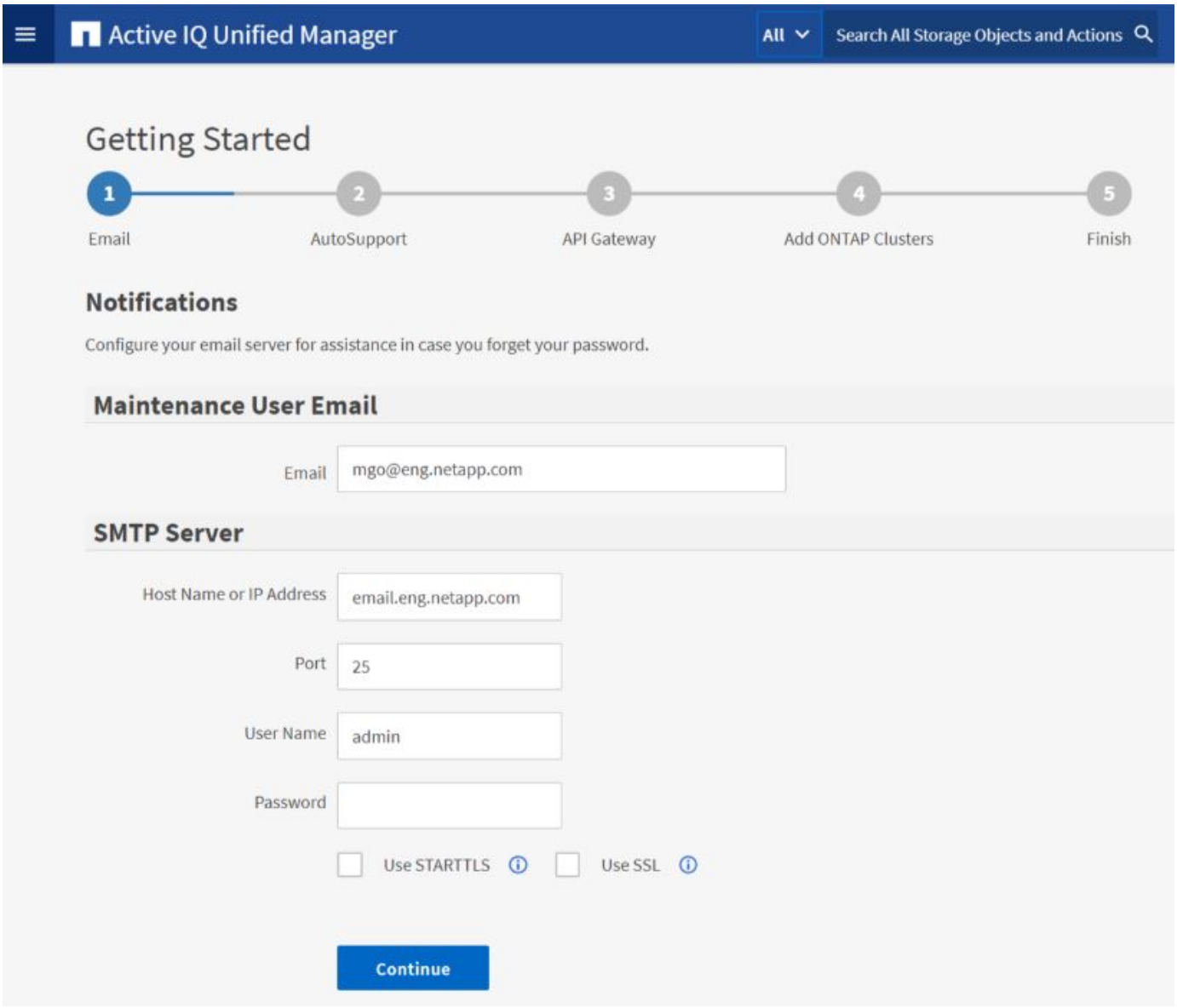
Um Unified Manager nutzen zu können, müssen Sie zunächst die Optionen für die Ersteinrichtung konfigurieren, einschließlich des NTP-Servers, der E-Mail-Adresse des Wartungsbenutzers, des SMTP-Server-Hosts und des Hinzufügens von ONTAP Clustern.

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**.

Wenn Sie auswählen…	Fahren Sie dann wie folgt fort…
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.
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.

Active IQ Unified Manager Sicherung konfigurieren

Die Backup-Funktion in Unified Manager lässt sich durch eine Reihe von Konfigurationsschritten auf den Hostsystemen und über die Managementplattform konfigurieren.

Informationen zu den Konfigurationsschritten finden Sie unter "Verwaltung von Sicherungs- und Wiederherstellungsvorgängen".

Funktionseinstellungen managen

Informationen zu Funktionseinstellungen in Active IQ Unified Manager

Die Seite „Funktionseinstellungen“ ermöglicht das Aktivieren und Deaktivieren bestimmter Funktionen in Active IQ Unified Manager. Dazu gehören das Erstellen und Managen von Storage-Objekten auf der Grundlage von Richtlinien, das Aktivieren von API Gateway und Login Banner, das Hochladen von Skripten zum Managen von Warnungen, die Zeitüberschreitung einer Web UI-Sitzung auf der Grundlage der Inaktivitätsdauer sowie das Deaktivieren des Empfangs von Plattformereignissen von Active IQ.

Die Seite „Feature Settings“ ist nur für Benutzer mit der Rolle „Application Administrator“

verfügbar.

Weitere Informationen zu Scripts Upload sind unter "Hochladen von Skripten aktivieren und deaktivieren" verfügbar.

Die richtlinienbasierte Speicherverwaltung in Active IQ Unified Manager kann aktiviert werden

Die Option **Richtlinienbasierte Storage Verwaltung** ermöglicht das Management von Storage auf Grundlage von Service Level Objectives (SLOs). Diese Option ist standardmäßig aktiviert.

Nach der Aktivierung dieser Funktion können Sie Storage Workloads auf den ONTAP Clustern provisionieren, die Ihrer Active IQ Unified Manager Instanz hinzugefügt wurden, und diese Workloads anhand der zugewiesenen Performance Service Levels und Storage Efficiency Policies managen.

Sie können diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **richtlinienbasierte Storage Verwaltung** aktivieren oder deaktivieren. Nach der Aktivierung dieser Funktion stehen die folgenden Seiten für Betrieb und Überwachung zur Verfügung:

- Provisionierung (Provisionierung von Storage Workloads)
- **Richtlinien** > **Performance Service Levels**
- **Richtlinien** > **Speichereffizienz**
- Workloads, die von der Spalte „Performance Service Level“ auf der Seite „Clusters Setup“ verwaltet werden
- Bereich „Workload Performance“ im **Dashboard**

Mithilfe der Bildschirme können Sie Performance Service Levels und Storage Efficiency Policies erstellen und Storage Workloads provisionieren. Sie können außerdem die Storage Workloads überwachen, die den zugewiesenen Performance Service Levels entsprechen, sowie diejenigen, die nicht entsprechen. Der Bereich „Workload Performance und Workload IOPS“ ermöglicht Ihnen außerdem, die Gesamt-, verfügbare und genutzte Kapazität sowie die Performance (IOPS) der Cluster in Ihrem Datacenter auf Grundlage der darauf provisionierten Storage Workloads zu bewerten.

Nach der Aktivierung dieser Funktion können Sie die Unified Manager REST APIs ausführen, um einige dieser Funktionen über **Menu Bar** > **Help button** > **API Documentation** > Kategorie **storage-provider** auszuführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL eingeben, um im Format https://<hostname>/docs/api/ auf die REST API-Seite zuzugreifen.

Weitere Informationen zu den APIs sind unter "Erste Schritte mit Active IQ Unified Manager REST APIs" verfügbar.

Informationen zur API Gateway Funktion in Active IQ Unified Manager

Die API Gateway Funktion ermöglicht es, dass Active IQ Unified Manager als eine einzige Kontrollebene dient, über die Sie mehrere ONTAP Cluster managen können, ohne sich bei jedem einzelnen anmelden zu müssen.

Sie können diese Funktion auf den Konfigurationsseiten aktivieren, die bei der ersten Anmeldung bei Unified Manager angezeigt werden. Alternativ können Sie diese Funktion unter **General** > **Feature Settings** > **API Gateway** aktivieren oder deaktivieren.

Die Unified Manager REST APIs unterscheiden sich von den ONTAP REST APIs, und nicht alle Funktionen der ONTAP REST APIs können mit den Unified Manager REST APIs genutzt werden. Wenn jedoch eine spezifische geschäftliche Anforderung für den Zugriff auf die ONTAP APIs besteht, um bestimmte Funktionen zu managen, die in Unified Manager nicht verfügbar gemacht werden, kann die API Gateway Funktion aktiviert und die ONTAP APIs ausgeführt werden. Das Gateway fungiert als Proxy, um die API-Anfragen weiterzuleiten, wobei Header und Body der Anfragen im selben Format wie in den ONTAP APIs beibehalten werden. Sie können Ihre Unified Manager Anmeldeinformationen verwenden und die spezifischen APIs ausführen, um auf die ONTAP Cluster zuzugreifen und sie zu managen, ohne individuelle Anmeldeinformationen für Cluster übergeben zu müssen. Unified Manager fungiert als zentraler Managementpunkt für die Ausführung der APIs über die ONTAP Cluster hinweg, die von Ihrer Unified Manager Instanz gemanagt werden. Die von den APIs zurückgegebene Antwort ist dieselbe wie die Antwort, die von den jeweiligen ONTAP REST APIs zurückgegeben wird, wenn sie direkt über ONTAP ausgeführt werden.

Nach dem Aktivieren dieser Funktion können Sie die Unified Manager REST APIs über **Menüleiste** > **Hilfe** > **API-Dokumentation** > Kategorie **gateway** ausführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL eingeben, um im folgenden Format auf die REST API-Seite zuzugreifen `https://<hostname>/docs/api/`

Weitere Informationen zu den APIs sind unter "Erste Schritte mit Active IQ Unified Manager REST APIs" verfügbar.

Angeben der Zeitüberschreitung bei Inaktivität in Active IQ Unified Manager

Sie können den Wert für die Zeitüberschreitung bei Inaktivität für Active IQ Unified Manager festlegen. Nach der angegebenen Dauer der Inaktivität wird die Applikation automatisch abgemeldet. Diese Option ist standardmäßig aktiviert.

Sie können diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **Inaktivitäts-Timeout** deaktivieren oder die Zeit anpassen. Nach der Aktivierung sollten Sie im Feld **ABMELDEN NACH** die maximale Inaktivitätszeit (in Minuten) festlegen, nach der das System Sie automatisch abmeldet. Der Standardwert beträgt 4320 Minuten (72 Stunden).

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

Aktivierung von Active IQ Portalereignissen in Active IQ Unified Manager

Sie können festlegen, ob Ereignisse des Active IQ Portals aktiviert oder deaktiviert werden sollen. Diese Einstellung ermöglicht es dem Active IQ Portal, zusätzliche Ereignisse zur Systemkonfiguration, Verkabelung usw. zu identifizieren und anzuzeigen. Diese Option ist standardmäßig aktiviert.

Nach der Aktivierung dieser Funktion zeigt Active IQ Unified Manager Ereignisse an, die vom Active IQ Portal identifiziert wurden. Diese Ereignisse werden durch die Ausführung einer Reihe von Regeln auf AutoSupport Meldungen erstellt, die von allen überwachten Storage Systemen generiert werden. Diese Ereignisse unterscheiden sich von den anderen Unified Manager Ereignissen und identifizieren Vorfälle oder Risiken im Zusammenhang mit Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeitsproblemen.

Sie können diese Funktion unter **General** > **Feature Settings** > **Active IQ Portal Events** aktivieren oder deaktivieren. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell unter **Storage Management** > **Event Setup** > **Upload Rules** hochladen.

Diese Funktion ist standardmäßig aktiviert. Die Deaktivierung dieser Funktion bewirkt, dass Active IQ Ereignisse nicht mehr von Unified Manager identifiziert oder dort angezeigt werden. Wenn diese Funktion deaktiviert ist, kann Unified Manager nach ihrer Aktivierung Active IQ Ereignisse auf einem Cluster zu einer vordefinierten Zeit von 00:15 Uhr in der Zeitzone dieses Clusters empfangen.

Aktivieren und Deaktivieren von Sicherheitseinstellungen für die Compliance in Active IQ Unified Manager

Mithilfe der Schaltfläche **Anpassen** im Bereich **Sicherheits-Dashboard** der Seite „Funktionseinstellungen“ können Sie die Sicherheitsparameter für die Compliance-Überwachung in Unified Manager aktivieren oder deaktivieren.

Die auf dieser Seite aktivierten oder deaktivierten Einstellungen steuern den allgemeinen Compliance Status der Cluster und Storage VMs in Unified Manager. Je nach Auswahl sind die entsprechenden Spalten in der Ansicht **Security: All Clusters** auf der Cluster-Inventarseite und in der Ansicht **Security: All Storage VMs** auf der Storage VMs-Inventarseite sichtbar.

Nur Benutzer mit Administratorrolle können diese Einstellungen bearbeiten.

Die Sicherheitskriterien für Ihre ONTAP Cluster, Storage-VMs und Volumes werden anhand der in der "Leitfaden zur Sicherheitshärtung für NetApp ONTAP 9" definierten Empfehlungen bewertet. Im Sicherheitsbereich des Dashboard und auf der Seite Sicherheit wird der standardmäßige Sicherheits-Compliance-Status Ihrer Cluster, Storage-VMs und Volumes angezeigt. Für Cluster und Storage-VMs mit Sicherheitsverstößen werden außerdem Sicherheitsereignisse generiert und Managementaktionen aktiviert.

Sicherheitseinstellungen anpassen

Zur Anpassung der Einstellungen für die Compliance-Überwachung an Ihre ONTAP Umgebung sind die folgenden Schritte relevant:

Schritte

1. Die Auswahl erfolgt über **Allgemein > Funktionseinstellungen > Sicherheits-Dashboard > Anpassen**. Das Popup **Einstellungen für das Sicherheits-Dashboard anpassen** wird angezeigt.

   Die von Ihnen aktivierten oder deaktivierten Sicherheits-Compliance-Parameter können sich direkt auf die standardmäßigen Sicherheitsansichten, Berichte und geplanten Berichte in den Bildschirmen „Clusters“ und „Storage VMs“ auswirken. Wenn Sie vor der Änderung der Sicherheitsparameter einen Excel-Bericht aus diesen Bildschirmen hochgeladen hatten, könnten die heruntergeladenen Excel-Berichte fehlerhaft sein.

2. Das Aktivieren oder Deaktivieren der benutzerdefinierten Einstellungen für Ihre ONTAP Cluster erfolgt durch Auswahl der gewünschten allgemeinen Einstellung unter **Cluster**. Informationen zu den Optionen für die Anpassung der Cluster Compliance finden Sie unter "Compliance-Kategorien für Cluster".
3. Zum Aktivieren oder Deaktivieren der benutzerdefinierten Einstellungen für Ihre Storage VMs können Sie unter **Storage VM** die gewünschte allgemeine Einstellung auswählen. Informationen zu den Optionen zum Anpassen der Storage VM Compliance finden Sie unter "Compliance-Kategorien für Storage-VMs".

Anpassen von AutoSupport und Authentifizierungseinstellungen

Im Abschnitt **AutoSupport Settings** können Sie festlegen, ob HTTPS für das Senden von AutoSupport Nachrichten von ONTAP verwendet werden soll.

Im Abschnitt **Authentifizierungseinstellungen** können Sie aktivieren, dass Unified Manager Warnungen für den standardmäßigen ONTAP Administratorbenutzer ausgegeben werden.

Aktivieren und Deaktivieren des Skript-Uploads in Active IQ Unified Manager

Das Hochladen und Ausführen von Skripten in Unified Manager ist standardmäßig aktiviert. Wenn Ihr Unternehmen diese Aktivität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion deaktivieren.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

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

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Skripte deaktivieren	Im Bereich **Script Upload** lässt sich der Schieberegler nach links bewegen.
Aktivierung von Skripten	Im Bereich **Script Upload** den Schieberegler nach rechts stellen.

Hinzufügen eines Anmeldebanners in Active IQ Unified Manager

Durch das Hinzufügen eines Anmeldebanners kann Ihr Unternehmen beliebige Informationen anzeigen, z. B. wer Zugriff auf das System hat und welche Nutzungsbedingungen gelten, sowohl beim An- als auch beim Abmelden.

Jeder Benutzer, z. B. Storage Operatoren oder Administratoren, kann dieses Anmeldebanner-Popup bei der Anmeldung, Abmeldung und bei Zeitüberschreitung der Sitzung anzeigen.

Verwendung der Managementplattform

Informationen zur Wartungskonsole in Active IQ Unified Manager

Mit der Unified Manager Managementplattform für Wartung können Sie die Einstellungen auf Ihrem Unified Manager System managen und alle erforderlichen Änderungen vornehmen, um Probleme zu vermeiden.

Je nach dem Betriebssystem, auf dem Sie Unified Manager installiert haben, bietet die Managementplattform folgende Wartungsfunktionen:

- Fehlerbehebung bei Problemen mit Ihrer virtuellen Appliance, insbesondere wenn die Weboberfläche von Unified Manager nicht verfügbar ist
- Aktualisierung auf neuere Versionen von Unified Manager

- Support-Bundles für den Versand an den technischen Support generieren
- Netzwerkeinstellungen konfigurieren
- Passwort des Wartungsbenutzers ändern
- Verbindung zu einem externen Datenanbieter zum Senden von Performance Statistiken herstellen
- Änderung der internen Erfassung von Performance-Daten
- Wiederherstellung der Unified Manager Datenbank und der Konfigurationseinstellungen aus einer zuvor gesicherten Version.

Informationen zum Wartungsbenutzer in Active IQ Unified Manager

Der Wartungsbenutzer wird bei der Installation von Unified Manager auf einem Red Hat Enterprise Linux-System angelegt. Der Name des Wartungsbenutzers ist der Benutzer “umadmin”. Der Wartungsbenutzer hat in der web UI die Rolle Application Administrator und kann weitere Benutzer anlegen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder der umadmin Benutzer kann auch auf die Unified Manager Managementplattform zugreifen.

Diagnosefunktionen für Benutzer in Active IQ Unified Manager

Der Diagnosezugriff dient dazu, dass der technische Support Sie bei der Fehlersuche unterstützen kann, und Sie sollten ihn nur auf Anweisung des technischen Supports verwenden.

Der Diagnosebenutzer kann auf Anweisung des technischen Supports Befehle auf Betriebssystemebene zur Fehlerbehebung ausführen.

Zugriff auf die Wartungskonsole in Active IQ Unified Manager

Wenn die Unified Manager Benutzeroberfläche nicht in Betrieb ist oder wenn Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungs-Managementplattform zugreifen, um Ihr Unified Manager System zu managen.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität meldet die Wartungs-Managementplattform Sie ab.



Bei der Installation auf VMware ist eine gleichzeitige Anmeldung über Secure Shell nicht möglich, wenn Sie sich bereits als Wartungsbenutzer über die VMware Managementplattform angemeldet haben.

Schritt

1. Der Zugriff auf die Managementplattform erfolgt in den folgenden Schritten:

Auf diesem Betriebssystem…	Folgen Sie diesen Schritten…
VMware	a. Die Verbindung zur IP-Adresse oder zur vollqualifizierten Domain der virtuellen Unified Manager Appliance erfolgt mithilfe von Secure Shell. b. Zur Anmeldung bei der Managementplattform dienen Ihr Wartungsbenutzername und Ihr Passwort.
Linux	a. Die Verbindung mit der IP-Adresse oder dem vollqualifizierten Domainnamen des Unified Manager Systems erfolgt mithilfe von Secure Shell. b. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin). c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
Windows	a. Für die Anmeldung am Unified Manager System werden Administratoranmeldedaten verwendet. b. Starten von PowerShell als Windows-Administrator. c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.

Das Menü der Unified Manager Wartungs-Managementplattform wird angezeigt.

Zugriff auf die Wartungskonsole über die vSphere VM-Konsole in Active IQ Unified Manager

Falls die Unified Manager Benutzeroberfläche nicht funktioniert oder falls Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Managementplattform zugreifen, um Ihre virtuelle Appliance neu zu konfigurieren.

Bevor Sie beginnen

- Sie müssen der Wartungsbenutzer sein.
- Die virtuelle Appliance muss eingeschaltet sein, um auf die Wartungs Managementplattform zuzugreifen.

Schritte

1. Die virtuelle Appliance Unified Manager befindet sich im vSphere Client.
2. Sie wählen die Registerkarte **Console** aus.
3. Zum Anmelden ist ein Klick in das Fenster der Managementplattform erforderlich.
4. Die Anmeldung bei der Managementplattform für die Wartung erfolgt mit Ihrem Benutzernamen und Passwort.

   Nach 15 Minuten Inaktivität meldet die Wartungs-Managementplattform Sie ab.

Menüs der Managementplattform für die Wartung

Informationen zu den Wartungskonsolenmenüs in Active IQ Unified Manager

Die Managementplattform besteht aus verschiedenen Menüs, die die Wartung und Verwaltung spezieller Funktionen und Konfigurationseinstellungen des Unified Manager Servers ermöglichen.

Je nach Betriebssystem, auf dem Sie Unified Manager installiert haben, besteht die Wartungs-Managementplattform aus den folgenden Menüs:

- Upgrade von Unified Manager (nur VMware)
- Netzwerkkonfiguration (nur VMware)
- Systemkonfiguration (nur VMware)
  a. Support/Diagnostik
  b. Serverzertifikat zurücksetzen
  c. Client Zertifikat neu generieren
  d. Backup-Wiederherstellung
  e. Externer Datenanbieter
  f. Konfiguration des Abfrageintervalls für die Performance
  g. SAML-Authentifizierung deaktivieren
  h. Applikationsports anzeigen/ändern
  i. Konfiguration des Debug-Protokolls
  j. Zugriff auf MySQL Port 3306 steuern
  k. Beenden

Sie wählen die Nummer aus der Liste aus, um auf die entsprechende Menüoption zuzugreifen. Beispielsweise wählen Sie für Backup und Wiederherstellung die Nummer 4.

Menü „Netzwerkkonfiguration“ in Active IQ Unified Manager

Über das Menü „Netzwerkkonfiguration“ können Sie die Netzwerkeinstellungen managen. Dieses Menü sollte verwendet werden, wenn die Benutzeroberfläche von Unified Manager nicht verfügbar ist.

Dieses Menü ist nicht verfügbar, wenn Unified Manager auf Red Hat Enterprise Linux oder auf Microsoft Windows installiert ist.

Folgende Menüoptionen stehen zur Verfügung.

- **Einstellungen für die Anzeige der IP-Adresse**

  Zeigt die aktuellen Netzwerkeinstellungen für die virtuelle Appliance an, einschließlich IP-Adresse, Netzwerk, Broadcast-Adresse, Netzmaske, Gateway und DNS-Server.

- **Ändern der IP-Adresseneinstellungen**

Damit können Sie alle Netzwerkeinstellungen der virtuellen Appliance ändern, einschließlich der IP-Adresse, der Netzmaske, des Gateways oder der DNS-Server. Wenn Sie Ihre Netzwerkeinstellungen über die Wartungs-Managementplattform von DHCP auf statische Netzwerkkonfiguration umstellen, können Sie den Hostnamen nicht bearbeiten. Damit die Änderungen wirksam werden, muss **Commit Changes** ausgewählt werden.

- **Einstellungen für die Domainnamensuche anzeigen**

  Zeigt die für die Auflösung von Hostnamen verwendete Suchliste für Domainnamen an.

- **Einstellungen für die Domainnamensuche ändern**

  Hiermit können Sie die Domänennamen ändern, nach denen bei der Auflösung von Hostnamen gesucht werden soll. Sie müssen **Commit Changes** auswählen, damit die Änderungen wirksam werden.

- **Anzeige statischer Routen**

  Zeigt die aktuellen statischen Netzwerkrouten an.

- **Statische Routen ändern**

  Ermöglicht das Hinzufügen oder Löschen statischer Netzwerkrouten. **Änderungen übernehmen** muss ausgewählt werden, damit die Änderungen wirksam werden.

  - **Route hinzufügen**

    Ermöglicht das Hinzufügen einer statischen Route.

  - **Route löschen**

    Ermöglicht das Löschen einer statischen Route.

  - **Zurück**

    Sie gelangen zurück zum **Main Menu**.

  - **Beenden**

    Beendet die Wartungs-Console.

- **Netzwerkschnittstelle deaktivieren**

  Deaktiviert alle verfügbaren Netzwerkschnittstellen. Wenn nur eine Netzwerkschnittstelle verfügbar ist, kann sie nicht deaktiviert werden. Damit die Änderungen wirksam werden, muss **Commit Changes** ausgewählt werden.

- **Netzwerkschnittstelle aktivieren**

  Aktiviert die verfügbaren Netzwerkschnittstellen. Sie müssen **Commit Changes** auswählen, damit die Änderungen wirksam werden.

- **Änderungen übernehmen**

  Wendet alle an den Netzwerkeinstellungen der virtuellen Appliance vorgenommenen Änderungen an. Diese Option muss ausgewählt werden, damit vorgenommene Änderungen wirksam werden, andernfalls treten die Änderungen nicht in Kraft.

- **Host anpingen**

  Dient zum Anpingen eines Zielhosts, um IP-Adressänderungen oder DNS-Konfigurationen zu bestätigen.

- **Auf Standardeinstellungen zurücksetzen**

  Setzt alle Einstellungen auf die Werkseinstellungen zurück. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

- **Zurück**

  Sie gelangen zurück zum **Main Menu**.

- **Beenden**

  Beendet die Wartungs-Console.

Im Active IQ Unified Manager steht das Menü „Systemkonfiguration“ zur Verfügung

Das Menü „Systemkonfiguration“ ermöglicht Ihnen das Managen Ihrer virtuellen Appliance mithilfe verschiedener Optionen, wie z. B. der Anzeige des Serverstatus sowie dem Neustarten und Herunterfahren der virtuellen Maschine.

Wenn Unified Manager auf einem Linux- oder Microsoft Windows-System installiert ist, steht in diesem Menü nur die Option „`Restore from a Unified Manager Backup`“ zur Verfügung.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverstatus anzeigen**

  Zeigt den aktuellen Serverstatus an. Zu den Statusoptionen gehören „Läuft“ und „Läuft nicht“.

  Falls der Server nicht läuft, müssen Sie sich möglicherweise an den technischen Support wenden.

- **Virtuelle Maschine neu starten**

  Die virtuelle Maschine wird neu gestartet, dabei werden alle Services beendet. Nach dem Neustart starten die virtuelle Maschine und die Services erneut.

- **Virtuelle Maschine herunterfahren**

  Fährt die virtuelle Maschine herunter und beendet alle Services.

  Diese Option steht nur in der Managementplattform der virtuellen Maschine zur Auswahl.

- **Änderung des <logged in user> Benutzerpassworts**

  Ändert das Passwort des aktuell angemeldeten Benutzers, bei dem es sich nur um den Wartungsbenutzer handeln kann.

- **Größe der Datenfestplatte erhöhen**

  Erhöht die Größe der Datenfestplatte (Festplatte 3) in der virtuellen Maschine.

- **Swap-Datenträgergröße erhöhen**

  Erhöht die Größe der Auslagerungsfestplatte (Festplatte 2) in der virtuellen Maschine.

- **Änderung der Zeitzone**

  Ändert die Zeitzone entsprechend Ihrem Standort.

- **NTP-Server ändern**

  Ändert die NTP-Servereinstellungen, wie z. B. die IP-Adresse oder die vollqualifizierte Domain (FQDN).

- **NTP-Service ändern**

  Wechselt zwischen den `ntp` und `systemd-timesyncd` Services.

- **Wiederherstellung aus einer Unified Manager Sicherung**

  Stellt die Unified Manager Datenbank und die Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

- **Serverzertifikat zurücksetzen**

  Setzt das Server-Sicherheitszertifikat zurück.

- **Hostname ändern**

  Ändert den Namen des Hosts, auf dem die virtuelle Appliance installiert ist.

- **Zurück**

  Verlassen des Menüs „Systemkonfiguration“ und Rückkehr zum Hauptmenü.

- **Beenden**

  Verlässt das Menü der Wartungs-Managementplattform.

Das Menü „Support und Diagnose“ in Active IQ Unified Manager kann verwendet werden

Über das Menü „Support und Diagnose“ können Sie ein Supportpaket erstellen, das Sie zur Fehlerbehebung an den technischen Support senden können.

Folgende Menüoptionen stehen zur Verfügung:

- **Light Support Bundle generieren**

  Ermöglicht die Erstellung eines schlanken Support-Bundles, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält; Performance-Daten, Erfassungsaufzeichnungsdateien und Server-Heap-Dump sind ausgeschlossen.

- **Support Bundle generieren**

  Ermöglicht das Erstellen eines vollständigen Support-Pakets (7-Zip-Datei) mit Diagnoseinformationen im Home-Verzeichnis des Diagnosebenutzers. Wenn Ihr System mit dem Internet verbunden ist, kann das Support-Paket auch auf NetApp hochgeladen werden.

Die Datei enthält Informationen, die durch eine AutoSupport Nachricht generiert werden, den Inhalt der Unified Manager Datenbank, detaillierte Daten über die Interna des Unified Manager Servers sowie ausführliche Protokolle, die normalerweise nicht in AutoSupport Nachrichten oder im Lightweight Support Bundle enthalten sind.

Zusätzliche Menüoptionen der Wartungskonsole in Active IQ Unified Manager

Die folgenden Menüoptionen ermöglichen Ihnen die Durchführung verschiedener administrativer Aufgaben auf dem Unified Manager Server.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverzertifikat zurücksetzen**

  Generiert das HTTPS-Serverzertifikat erneut.

  Sie können das Serverzertifikat in der Unified Manager GUI durch Klicken auf **General** > **HTTPS Certificates** > **Regenerate HTTPS Certificate** neu generieren.

- **SAML Authentifizierung deaktivieren**

  Deaktiviert die SAML Authentifizierung, sodass der Identitätsanbieter (IdP) keine Anmeldeauthentifizierung mehr für Benutzer bereitstellt, die auf die Unified Manager GUI zugreifen. Diese Managementplattform Option wird typischerweise verwendet, wenn ein Problem mit dem IdP-Server oder der SAML-Konfiguration den Zugriff von Benutzern auf die Unified Manager GUI verhindert.

- **Externer Datenanbieter**

  Bietet Optionen zum Verbinden von Unified Manager mit einem externen Datenanbieter. Nach dem Herstellen der Verbindung werden Performance-Daten an einen externen Server gesendet, sodass Storage-Performance-Experten die Performance-Kennzahlen mithilfe von Drittanbietersoftware grafisch darstellen können. Folgende Optionen werden angezeigt:

  - **Anzeigen der Serverkonfiguration**--Zeigt die aktuelle Verbindung und die Konfigurationseinstellungen für einen externen Datenanbieter an.
  - **Serververbindung hinzufügen / ändern** - ermöglicht die Eingabe neuer Verbindungseinstellungen für einen externen Datenanbieter oder die Änderung bestehender Einstellungen.
  - **Serverkonfiguration ändern** - Ermöglicht die Eingabe neuer Konfigurationseinstellungen für einen externen Datenanbieter oder die Änderung bestehender Einstellungen.
  - **Serververbindung löschen**--Löscht die Verbindung zu einem externen Datenanbieter.

    Nach dem Löschen der Verbindung verliert Unified Manager die Verbindung zum externen Server.

- **Backup-Wiederherstellung**

  Weitere Informationen finden Sie in den Themen unter "Verwaltung von Sicherungs- und Wiederherstellungsvorgängen".

- **Konfiguration des Performance-Abfrageintervalls**

  Stellt eine Option zum Konfigurieren der Häufigkeit bereit, mit der Unified Manager Performance-Statistikdaten von Clustern erfasst. Das Standarderfassungsintervall beträgt 5 Minuten.

  Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Datenerfassungen

großer Cluster nicht rechtzeitig abgeschlossen sind.

- **Anwendungsports anzeigen/ändern**

  Es besteht die Möglichkeit, die Standardports zu ändern, die Unified Manager für die HTTP- und HTTPS-Protokolle verwendet, falls dies aus Sicherheitsgründen erforderlich ist. Die Standardports sind 80 für HTTP und 443 für HTTPS.

- **Zugriff auf MySQL Port 3306 kontrollieren**

  Steuert den Hostzugriff auf den Standard-MySQL-Port 3306. Aus Sicherheitsgründen ist der Zugriff über diesen Port bei einer Neuinstallation von Unified Manager auf Linux-, Windows- und VMware vSphere-Systemen nur auf localhost beschränkt. Mit dieser Option können Sie die Transparenz dieses Ports zwischen localhost und Remote-Hosts umschalten, das heißt, wenn er in Ihrer Umgebung nur für localhost aktiviert ist, können Sie diesen Port auch für Remote-Hosts verfügbar machen. Alternativ können Sie den Zugriff über diesen Port nur auf localhost beschränken, wenn er für alle Hosts aktiviert ist. Wenn der Zugriff zuvor auf Remote-Hosts aktiviert war, bleibt die Konfiguration bei einem Upgrade erhalten. Nach dem Umschalten der Port-Transparenz sollten die Firewall-Einstellungen auf Windows-Systemen überprüft und die Firewall-Einstellungen deaktiviert werden, wenn sie so konfiguriert sind, dass sie den Zugriff auf den MySQL-Port 3306 einschränken.

- **Beenden**

  Verlässt das Menü der Wartungs-Managementplattform.

Das Kennwort des Wartungsbenutzers unter Windows in Active IQ Unified Manager ändern

Sie können das Wartungsbenutzerkennwort von Unified Manager bei Bedarf ändern.

Schritte

1. Auf der Anmeldeseite der Unified Manager Web UI können Sie **Forgot Password** auswählen.

   Es wird eine Seite angezeigt, auf der Sie den Namen des Benutzers eingeben, dessen Passwort Sie zurücksetzen möchten.

2. Den Benutzernamen eingeben und auf **Submit** klicken.

   An die für diesen Benutzernamen definierte E-Mail-Adresse wird eine E-Mail mit einem Link zum Zurücksetzen des Passworts gesendet.

3. Das neue Passwort wird über den **Link zum Zurücksetzen des Passworts** in der E-Mail definiert.
4. Anschließend erfolgt die Anmeldung bei Unified Manager über die Web-Benutzeroberfläche mit dem neuen Passwort.

Ändern des Active IQ Unified Manager umadmin Passworts auf Linux Systemen

Aus Sicherheitsgründen müssen Sie das Standardpasswort für den Unified Manager-Benutzer „umadmin“ unmittelbar nach Abschluss der Installation ändern. Bei Bedarf können Sie das Passwort später jederzeit erneut ändern.

Bevor Sie beginnen

- Unified Manager muss auf einem Red Hat Enterprise Linux Linux System installiert sein.
- Sie benötigen die Root-Benutzer-Anmeldedaten für das Linux-System, auf dem Unified Manager installiert ist.

Schritte

1. Die Anmeldung als Root-Benutzer erfolgt auf dem Linux-System, auf dem Unified Manager ausgeführt wird.
2. Das Passwort des Benutzers umadmin ändern:

   ```
   passwd umadmin
   ```

   Das System fordert Sie auf, ein neues Passwort für den Benutzer umadmin einzugeben.

Die von Active IQ Unified Manager für die HTTP- und HTTPS-Protokolle verwendeten Ports können geändert werden.

Die von Unified Manager standardmäßig für HTTP- und HTTPS-Protokolle verwendeten Ports können nach der Installation bei Bedarf aus Sicherheitsgründen geändert werden. Die Standardports sind 80 für HTTP und 443 für HTTPS.

Bevor Sie beginnen

Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

> Bei der Verwendung von Mozilla Firefox oder Google Chrome gelten einige Ports als unsicher. Vor der Zuweisung einer neuen Portnummer für HTTP- und HTTPS-Datenverkehr ist eine Prüfung im Browser erforderlich. Die Auswahl eines unsicheren Ports kann dazu führen, dass das System nicht mehr erreichbar ist; in diesem Fall ist zur Behebung des Problems eine Kontaktaufnahme mit dem Kundensupport erforderlich.

Die Instanz von Unified Manager wird nach dem Ändern des Ports automatisch neu gestartet. Daher sollte dies ein geeigneter Zeitpunkt sein, um das System für kurze Zeit herunterzufahren.

1. Sie melden sich per SSH als Wartungsbenutzer am Unified Manager Host an.

   Die Eingabeaufforderungen der Unified Manager Wartungs-Managementplattform werden angezeigt.

2. Sie geben die Nummer der Menüoption mit der Bezeichnung **Anwendungsports anzeigen/ändern** ein und drücken anschließend die Eingabetaste.
3. Falls Sie dazu aufgefordert werden, geben Sie das Passwort des Wartungsbenutzers erneut ein.
4. Die neuen Portnummern für die HTTP- und HTTPS-Ports eingeben und anschließend die Eingabetaste drücken.

   Bleibt die Portnummer leer, wird der Standardport für das Protokoll verwendet.

   Die Abfrage lautet, ob Sie die Ports ändern und Unified Manager jetzt neu starten möchten.

5. Zum Ändern der Ports und zum Neustart von Unified Manager **y** eingeben.
6. Verlassen der Wartungskonsole.

Nach dieser Änderung müssen Benutzer die neue Portnummer in die URL einfügen, um auf die Unified

Manager Web-UI zuzugreifen, zum Beispiel https://host.company.com:1234, https://12.13.14.15:1122 oder https://[2001:db8:0:1]:2123.

Netzwerkschnittstellen zu Active IQ Unified Manager hinzufügen

Neue Netzwerkschnittstellen lassen sich hinzufügen, wenn eine Trennung des Netzwerkverkehrs erforderlich ist.

Bevor Sie beginnen

Sie müssen die Netzwerkschnittstelle mithilfe von vSphere zur virtuellen Appliance hinzugefügt haben.

Die virtuelle Appliance muss eingeschaltet sein.

Sie können diesen Vorgang nicht ausführen, wenn Unified Manager auf Red Hat Enterprise Linux oder Microsoft Windows installiert ist.

Schritte

1. Im Hauptmenü der vSphere Managementplattform **System Configuration** > **Reboot Operating System** auswählen.

   Nach dem Neustart kann die Wartungskonsole die neu hinzugefügte Netzwerkschnittstelle erkennen.

2. Auf die Wartungskonsole zugreifen.
3. Die Auswahl erfolgt über **Netzwerkkonfiguration** > **Netzwerkschnittstelle aktivieren**.
4. Anschließend die neue Netzwerkschnittstelle auswählen und die **Eingabetaste** drücken.

   eth1 wird ausgewählt und mit **Enter** bestätigt.

5. Zur Aktivierung der Netzwerkschnittstelle ist die Eingabe von **y** erforderlich.
6. Nun erfolgt die Eingabe der Netzwerkeinstellungen.

   Die Eingabe der Netzwerkeinstellungen ist erforderlich, wenn eine statische Schnittstelle verwendet wird oder DHCP nicht erkannt wird.

   Nach Eingabe der Netzwerkeinstellungen kehren Sie automatisch zum Menü **Netzwerkkonfiguration** zurück.

7. **Änderungen übernehmen** auswählen.

   Sie müssen die Änderungen übernehmen, um die Netzwerkschnittstelle hinzuzufügen.

Das Clientzertifikat in Active IQ Unified Manager neu generieren

Sie können die Managementplattform verwenden, um Ihr Unified Manager Client-Zertifikat neu zu generieren. Ihr Zertifikat hat eine verlängerte Gültigkeitsdauer von fünf Jahren.

Schritte

1. Melden Sie sich als Wartungsbenutzer an.
2. Wählen Sie **Regenerate Client Certificate** aus und drücken Sie **Enter**.

3. Falls das System eine Authentifizierung anfordert, müssen die erforderlichen Anmeldeinformationen eingegeben werden.
4. **Confirm Regeneration** wird ausgewählt und **Enter** wird gedrückt.
5. Nach der Neugenerierung des Zertifikats muss der Unified Manager Dienst neu gestartet werden, um die Änderungen anzuwenden.
6. Zur Überprüfung des aktualisierten Zertifikats ist eine Anmeldung bei ONTAP erforderlich. Der Status des Clientzertifikats und der Gültigkeitsstatus sind zu sehen.

Verwandte Informationen "ONTAP Zertifikate mit System Manager verwalten"

Festplattenspeicher hinzufügen

Dem Active IQ Unified Manager Datenbankverzeichnis Speicherplatz hinzufügen

Das Unified Manager Datenbankverzeichnis enthält alle von ONTAP Systemen erfassten Systemstatus- und Performance-Daten. Unter bestimmten Umständen kann es erforderlich sein, die Größe des Datenbankverzeichnisses zu erhöhen.

Das Datenbankverzeichnis kann beispielsweise voll werden, wenn Unified Manager Daten von einer großen Anzahl von Clustern erfasst, von denen jedes viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % gefüllt ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % gefüllt ist.

Sobald das Verzeichnis zu 95% gefüllt ist, werden keine zusätzlichen Daten mehr von Clustern erfasst.

Die erforderlichen Schritte zum Hinzufügen von Kapazität zum Datenverzeichnis unterscheiden sich je nachdem, ob Unified Manager auf einem VMware ESXi-Server, einem Red Hat-Server oder einem Microsoft Windows-Server ausgeführt wird.

Hinzufügen von Speicherplatz zum Datenverzeichnis auf einem Linux-Host in Active IQ Unified Manager

Falls Sie bei der ursprünglichen Einrichtung des Linux-Hosts dem `/opt/netapp/data` Verzeichnis nicht genügend Speicherplatz zur Unterstützung von Unified Manager zugewiesen und anschließend Unified Manager installiert haben, können Sie nach der Installation zusätzlichen Speicherplatz hinzufügen, indem Sie den Speicherplatz im `/opt/netapp/data` Verzeichnis erhöhen.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf den Red Hat Enterprise Linux Rechner, auf dem Unified Manager installiert ist.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Die Anmeldung als Root-Benutzer erfolgt auf dem Linux-Rechner, auf dem zusätzlicher Festplattenspeicher hinzugefügt werden soll.
2. Die Beendigung des Unified Manager Service und der zugehörigen MySQL Software erfolgt in der

angegebenen Reihenfolge:

```
systemctl stop ocieau ocie mysqld
```

3. Es wird ein temporärer Sicherungsordner (zum Beispiel `/backup-data`) mit ausreichendem Speicherplatz für die Daten im aktuellen `/opt/netapp/data` Verzeichnis benötigt.
4. Der Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data`Verzeichnisses sind in das Sicherungsdatenverzeichnis zu kopieren:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Wenn SE Linux aktiviert ist:

   a. SE Linux-Typ für Ordner in einem vorhandenen `/opt/netapp/data` Ordner:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Der Befehl chcon legt den SE Linux Typ für das Backup-Verzeichnis fest:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Entfernen des Inhalts des `/opt/netapp/data` Verzeichnisses:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Die Größe des `/opt/netapp/data` Verzeichnisses ist mithilfe von LVM-Befehlen oder durch Hinzufügen zusätzlicher Festplatten auf mindestens 150 GB zu erweitern.

   > Wenn Sie `/opt/netapp/data` von einer Festplatte erstellt haben, sollten Sie nicht versuchen, `/opt/netapp/data` sie als NFS- oder CIFS-Freigabe einzubinden. Denn in diesem Fall funktionieren einige LVM-Befehle, wie beispielsweise `resize` und `extend`, möglicherweise nicht wie erwartet, wenn Sie versuchen, den Speicherplatz zu erweitern.

8. Stellen Sie sicher, dass Eigentümer (mysql) und Gruppe (root) des `/opt/netapp/data`Verzeichnisses unverändert sind:

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. Bei aktiviertem SE Linux muss der Kontext für das `/opt/netapp/data`Verzeichnis weiterhin auf mysqld_db_t gesetzt sein:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Zum Vermeiden künftiger Datenbankfehler ist die überflüssige Datei abc zu löschen.
11. Kopieren des Inhalts von backup-data zurück in das erweiterte `/opt/netapp/data` Verzeichnis:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Wenn SE Linux aktiviert ist, ist der folgende Befehl auszuführen:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Start des MySQL-Dienstes:

```
systemctl start mysqld
```

14. Nach dem Start des MySQL-Service erfolgt der Start der Services ocie und ocieau in der angegebenen Reihenfolge:

```
systemctl start ocie ocieau
```

15. Nachdem alle Services gestartet sind, kann der Sicherungsordner `/backup-data` gelöscht werden:

```
rm -rf /backup-data
```

Hinzufügen von Speicherplatz zur Datenfestplatte auf einer VMware Virtual Machine in Active IQ Unified Manager

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Festplattenspeicher über die Unified Manager Wartungs-Managementplattform vergrößern.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere Client haben.
- Die virtuelle Maschine darf keine lokal gespeicherten Snapshots enthalten.
- Sie benötigen die Zugangsdaten für den Wartungsbenutzer.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe der virtuellen Festplatten erhöhen.

Schritte

1. Im vSphere Client können Sie die virtuelle Maschine Unified Manager auswählen und dann die Festplattenkapazität für Daten `disk 3` erweitern. Einzelheiten sind der VMware Dokumentation zu entnehmen.

   In seltenen Fällen verwendet das Unified Manager Deployment „Festplatte 2“ statt „Festplatte 3“ als Datenfestplatte. Falls dies in Ihrem Deployment auftritt, empfiehlt sich eine Vergrößerung des Speicherplatzes der größeren Festplatte. Die Datenfestplatte verfügt stets über mehr Speicherplatz als die andere Festplatte.

2. Im vSphere Client werden die virtuelle Maschine Unified Manager und anschließend die Registerkarte **Console** ausgewählt.
3. Im Fenster der Managementplattform erfolgt anschließend die Anmeldung an der Wartungskonsole mit Ihrem Benutzernamen und Passwort.
4. Im Hauptmenü erfolgt die Eingabe der Nummer für die Option **Systemkonfiguration**.
5. Im Menü „Systemkonfiguration“ wird die Zahl für die Option **Datenträgergröße erhöhen** eingegeben.

Hinzufügen von Speicherplatz zum logischen Laufwerk auf einem Windows-Server in Active IQ Unified Manager

Wenn eine Vergrößerung des Speicherplatzes für die Unified Manager Datenbank erforderlich ist, kann die Kapazität des logischen Laufwerks erweitert werden, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie benötigen Windows-Administratorrechte.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Die Anmeldung als Administrator auf dem Windows-Server, dem zusätzlicher Festplattenspeicher hinzugefügt werden soll, ist erforderlich.
2. Im Folgenden ist der Schritt für die Methode zum Hinzufügen von mehr Platz aufgeführt:

Option	Beschreibung
Auf einem physischen Server sollte die Kapazität des logischen Laufwerks erhöht werden, auf dem der Unified Manager server installiert ist.	Die Schritte sind im Microsoft-Thema beschrieben: "Erweitern eines Basisvolumens"
Auf einem physischen Server wird eine Festplatte hinzugefügt.	Die Schritte sind im Microsoft-Thema beschrieben: "Hinzufügen von Festplatten"
Auf einer virtuellen Maschine die Größe einer Festplattenpartition erhöhen.	Die Schritte im VMware-Thema: "Vergrößern einer Festplattenpartition"

Benutzerzugriff verwalten

Benutzer hinzufügen

Hinzufügen von Benutzern in Active IQ Unified Manager

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite „Benutzer“ hinzufügen. Außerdem können Sie Remote-Benutzer oder Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Diesen Benutzern können Sie Rollen zuweisen, und auf Grundlage der Berechtigungen dieser Rollen können Benutzer mit Unified Manager die Storage Objekte und Daten managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Um einen Remote-Benutzer oder eine Remote-Gruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitätsanbieter (IdP) die Benutzer authentifiziert, die auf die grafische Benutzeroberfläche zugreifen, sollten Sie darauf achten, dass diese Benutzer als “remote” Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist für Benutzer vom Typ “local” oder “maintenance” nicht gestattet, wenn die SAML-Authentifizierung aktiviert ist.

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und verschachtelten Untergruppen bei Unified Manager authentifizieren, sofern verschachtelte Untergruppen nicht deaktiviert sind. Wenn Sie eine Gruppe aus OpenLDAP oder anderen Authentifizierungs-Services hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt ein Klick auf **Hinzufügen**.
3. Im Dialogfeld „Benutzer hinzufügen“ erfolgt die Auswahl des Benutzertyps, den Sie hinzufügen möchten, sowie die Eingabe der erforderlichen Informationen.

   Bei der Eingabe der erforderlichen Benutzerinformationen müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. E-Mail-Adressen, die von mehreren Benutzern gemeinsam genutzt werden, dürfen nicht angegeben werden.

4. Klicken Sie auf **Add**.

Erstellen eines Datenbankbenutzers in Active IQ Unified Manager

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie zunächst in der Unified Manager web UI einen Datenbankbenutzer mit der Rolle Integration Schema oder Report Schema erstellen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Datenbankbenutzer ermöglichen die Integration mit Workflow Automation und den Zugriff auf

berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Web-UI von Unified Manager oder die Wartungs-Managementplattform und können keine API-Aufrufe ausführen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ wählen Sie **Hinzufügen** aus.
3. Im Dialogfeld „Benutzer hinzufügen“ ist in der Dropdown-Liste „Typ“ die Option „Datenbankbenutzer“ auszuwählen.
4. Für den Datenbankbenutzer werden ein Name und ein Passwort eingegeben.
5. In der Dropdown-Liste **Rolle** wird die passende Rolle gewählt.

Wenn Sie…	Diese Rolle auswählen
Verbinden von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichte und andere Datenbankansichten	Berichtsschema

6. Klicken Sie auf **Add**.

Benutzereinstellungen in Active IQ Unified Manager bearbeiten

Sie können die Benutzereinstellungen, wie E-Mail-Adresse und Rolle, bearbeiten, die für jeden Benutzer festgelegt sind. Beispielsweise können Sie die Rolle eines Benutzers ändern, der ein Storage-Operator ist, und dem Benutzer Storage-Administratorrechte zuweisen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie die einem Benutzer zugewiesene Rolle ändern, werden die Änderungen übernommen, sobald eine der folgenden Aktionen eintritt:

- Der Benutzer meldet sich ab und wieder bei Unified Manager an.
- Die Sitzungszeitüberschreitung von 24 Stunden ist erreicht.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ den Benutzer auswählen, dessen Einstellungen bearbeitet werden sollen, und auf **Edit** klicken.
3. Im Dialogfeld „Benutzer bearbeiten“ können Sie die für den Benutzer festgelegten Einstellungen bearbeiten.
4. Auf **Speichern** klicken.

Benutzer in Active IQ Unified Manager anzeigen

Auf der Seite „Benutzer“ kann die Liste der Benutzer angezeigt werden, die Storage Objekte und Daten mit Unified Manager managen. Dort können Details zu den Benutzern

angezeigt werden, z. B. Benutzername, Benutzertyp, E-Mail-Adresse und die den Benutzern zugewiesene Rolle.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritt

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.

Löschen von Benutzern oder Gruppen in Active IQ Unified Manager

Sie können einen oder mehrere Benutzer aus der Datenbank des Managementservers löschen, um bestimmten Benutzern den Zugriff auf Unified Manager zu verweigern. Sie können auch Gruppen löschen, sodass alle Benutzer dieser Gruppe keinen Zugriff mehr auf den Managementserver haben.

Bevor Sie beginnen

- Wenn Sie Remote-Gruppen löschen, müssen Sie die den Benutzern der Remote-Gruppen zugewiesenen Ereignisse zuvor neu zugewiesen haben.

  Wenn Sie lokale Benutzer oder Remote-Benutzer löschen, wird die Zuweisung der diesen Benutzern zugewiesenen Ereignisse automatisch aufgehoben.

- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt die Auswahl der Benutzer oder Gruppen, die gelöscht werden sollen; anschließend erfolgt ein Klick auf **Löschen**.
3. Zum Bestätigen der Löschung auf **Ja** klicken.

Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen auf dem Active IQ Unified Manager Server hat. RBAC ermöglicht Administratoren die Verwaltung von Benutzergruppen durch die Definition von Rollen. Wenn der Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränkt werden muss, müssen für diese Administratorkonten eingerichtet werden. Wenn die Informationen, die Administratoren anzeigen können, und die Vorgänge, die sie ausführen können, eingeschränkt werden sollen, müssen den erstellten Administratorkonten Rollen zugewiesen werden.

Der Verwaltungsserver verwendet rollenbasierte Zugriffskontrolle (RBAC) für die Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Verwaltungsservers für den administrativen Benutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um diese anzuzeigen.

Wenn Sie einen Vorgang initiieren, der bestimmte Berechtigungen erfordert, fordert der Managementserver Sie zur Anmeldung auf. Um beispielsweise Administratorkonten zu erstellen, müssen Sie sich mit einem Konto mit Zugriff als Application Administrator anmelden.

Informationen zu Benutzertypen in Active IQ Unified Manager

Ein Benutzertyp legt die Art des Benutzerkontos fest und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungsbenutzer. Jeder dieser Typen hat eine eigene Rolle, die ein Benutzer mit der Rolle „Administrator“ zuweist.

Die Unified Manager Benutzertypen sind wie folgt:

- **Wartungsbenutzer**

  Wird bei der Erstkonfiguration von Unified Manager erstellt. Der Wartungsbenutzer erstellt anschließend weitere Benutzer und weist ihnen Rollen zu. Der Wartungsbenutzer ist außerdem der einzige Benutzer mit Zugriff auf die Managementplattform. Wenn Unified Manager auf einem Red Hat Enterprise Linux-System installiert wird, erhält der Wartungsbenutzer den Benutzernamen “umadmin.”

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt je nach der vom Wartungsbenutzer oder von einem Benutzer mit der Rolle "Application Administrator" zugewiesenen Rolle Funktionen aus.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldedaten auf die Unified Manager UI zugreifen. Der Name dieses Kontos sollte mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Alle Benutzer innerhalb der Remote-Gruppe erhalten mit ihren individuellen Benutzeranmeldeinformationen Zugriff auf die Unified Manager UI. Remote-Gruppen können entsprechend ihren zugewiesenen Rollen Funktionen ausführen.

- **Remote-Benutzer**

  Der Zugriff auf die Unified Manager UI erfolgt mithilfe der Anmeldedaten, die auf dem Authentifizierungsserver gespeichert sind. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die ihm vom Wartungsbenutzer oder von einem Benutzer mit der Rolle „Application Administrator“ zugewiesen wurde.

- **Datenbankbenutzer**

  Verfügt über Lesezugriff auf Daten in der Unified Manager Datenbank, hat keinen Zugriff auf die Unified Manager Weboberfläche oder die Wartungsmanagementplattform und kann keine API-Aufrufe ausführen.

Informationen zu Benutzerrollen in Active IQ Unified Manager

Der Wartungsbenutzer oder Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle beinhaltet bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie im Unified Manager ausführen können, hängt von Ihrer zugewiesenen Rolle und den damit verbundenen Berechtigungen ab.

Unified Manager umfasst die folgenden vordefinierten Benutzerrollen:

- **Operator**

  Zeigt Storage-Systeminformationen und andere von Unified Manager erfasste Daten an, einschließlich

Verlaufsdaten und Kapazitätstrends. Diese Rolle ermöglicht dem Storage-Operator, Ereignisse anzuzeigen, zuzuweisen, zu bestätigen, zu beheben und mit Notizen zu versehen.

- **Storage-Administrator**

  Konfiguriert Storage-Managementvorgänge in Unified Manager. Diese Rolle ermöglicht dem Storage-Administrator die Konfiguration von Schwellenwerten sowie die Erstellung von Warnungen und anderen spezifischen Optionen und Richtlinien für das Storage-Management.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die nicht mit dem Storage-Management zusammenhängen. Diese Rolle ermöglicht die Verwaltung von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und administrativen Optionen, einschließlich Authentifizierung, SMTP, Netzwerk und AutoSupport.

  Bei der Installation von Unified Manager auf Linux-Systemen erhält der erste Benutzer mit der Rolle des Anwendungsadministrators automatisch den Namen “umadmin”.

- **Integrationsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Unified Manager Datenbankansichten zur Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Berichtsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Berichte und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Zu den einsehbaren Datenbanken gehören:

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager

Anhand Ihrer zugewiesenen Benutzerrolle können Sie ermitteln, welche Operationen Sie im Unified Manager durchführen können.

Die folgende Tabelle zeigt die Funktionen, die jede Benutzerrolle ausführen kann:

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Anzeigen von Informationen zum Storage-System	•	•	•	•	•

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Andere Daten wie z. B. Verläufe und Kapazitätstrends lassen sich anzeigen.	•	•	•	•	•
Ereignisse anzeigen, zuweisen und beheben	•	•	•		
Storage-Service-Objekte wie SVM-Zuordnungen und Ressourcenpools anzeigen	•	•	•		
Anzeige von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Warnmeldungen definieren		•	•		
Storage-Managementoptionen managen		•	•		
Storage-Managementrichtlinien managen		•	•		
Benutzer verwalten			•		
Administrative Optionen managen			•		
Definition von Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Integration mit WFA managen und Zugriff auf die Datenbankansichten gewähren				•	
Berichte planen und speichern		•	•		
Ausführung von “Fix It”-Vorgängen über Management Actions		•	•		
Bereitstellung von schreibgeschütztem Zugriff auf Datenbankansichten					•

Verwalten der SAML-Authentifizierungseinstellungen

SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Nachdem Sie die Einstellungen für die Remote-Authentifizierung konfiguriert haben, können Sie die Authentifizierung mit Security Assertion Markup Language (SAML) aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Web-Benutzeroberfläche von Unified Manager zugreifen können.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform für die Wartung zugreifen.

Verwendung eines Identitätsanbieters in Active IQ Unified Manager

Wenn Unified Manager so konfiguriert wird, dass ein Identitätsanbieter (IdP) die SAML-Authentifizierung für alle Remote-Benutzer durchführt, müssen einige erforderliche Konfigurationseinstellungen beachtet werden, damit die Verbindung zu Unified Manager erfolgreich hergestellt werden kann.

Sie müssen die Unified Manager URI und die Metadaten in den IdP-Server eingeben. Diese Informationen können Sie auf der Unified Manager SAML-Authentifizierungsseite kopieren. Unified Manager gilt im Standard Security Assertion Markup Language (SAML) als Serviceprovider (SP).

Unterstützte Verschlüsselungsstandards

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

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS Konfigurationsanforderungen

- Sie müssen drei Anspruchsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauensstellungseintrag der vertrauenden Seite analysieren kann.

Claim-Regel	Wert
SAM-Kontoname	Name-ID
SAM-Kontoname	urn:oid:0.9.2342.19200300.100.1.1
Tokengruppen — Unqualifizierter Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Sie müssen das Authentifizierungsverfahren auf “Forms Authentication” festlegen, da Benutzer sonst beim Abmelden von Unified Manager eine Fehlermeldung erhalten können. Die folgenden Schritte sind erforderlich:
  a. Die ADFS Management Console wird geöffnet.
  b. In der linken Baumansicht den Ordner „Authentifizierungsrichtlinien“ auswählen.
  c. Rechts unter „Aktionen“ befindet sich die Option „Globale primäre Authentifizierungsrichtlinie bearbeiten“.
  d. Als Authentifizierungsverfahren für das Intranet wird statt der Standardeinstellung “Windows Authentication” die Option “Forms Authentication” verwendet.
- In einigen Fällen wird die Anmeldung über den IdP abgelehnt, wenn das Sicherheitszertifikat des Unified Manager CA-signiert ist. Es gibt zwei Lösungsansätze für dieses Problem:
  - Im Link finden Sie Anweisungen zum Deaktivieren der Widerrufsprüfung auf dem ADFS-Server für verkettete CA-Zertifikate der zugeordneten Relying Party:

    "Widerrufsprüfung pro Relying Party Trust deaktivieren"

  - Der CA-Server muss sich innerhalb des ADFS-Servers befinden, um die Zertifikatsanforderung des Unified Manager Servers zu signieren.

Weitere Konfigurationsanforderungen

- Die Taktabweichung von Unified Manager ist auf 5 Minuten eingestellt, daher darf die Zeitdifferenz zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen, da die Authentifizierung sonst fehlschlägt.

SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Sie können die Security Assertion Markup Language (SAML) Authentifizierung aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Unified Manager Weboberfläche zugreifen können.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung konfiguriert und überprüft haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote User oder eine Remote Group mit der Rolle Application Administrator erstellt haben.
- Der Identitätsanbieter (IdP) muss von Unified Manager unterstützt werden und konfiguriert sein.
- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den IdP-Server.

Nachdem Sie die SAML-Authentifizierung in Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn der IdP mit den Hostinformationen des Unified Manager Servers konfiguriert wurde. Daher ist es erforderlich, beide Teile der Verbindung abzuschließen, bevor der Konfigurationsprozess gestartet wird. Der IdP kann vor oder nach der Konfiguration von Unified Manager eingerichtet werden.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche des Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform, die Unified Manager-Befehle oder die ZAPIs zugreifen.

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

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Kontrollkästchen **SAML-Authentifizierung aktivieren** ist auszuwählen.

   Die für die Konfiguration der IdP-Verbindung erforderlichen Felder werden angezeigt.

3. Einzugeben sind die IdP URI und die IdP Metadaten, die für die Verbindung des Unified Manager Servers mit dem IdP Server erforderlich sind.

   Wenn der IdP-Server direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URI auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch zu füllen.

4. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.

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

5. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der IdP-Anmeldeseite anstatt auf der Unified Manager-Anmeldeseite eingeben.

Falls dies noch nicht geschehen ist, sind für den Abschluss der Konfiguration der Zugriff auf Ihren IdP sowie die Eingabe der URI und der Metadaten des Unified Manager Servers erforderlich.



Wenn Sie ADFS als Identitätsanbieter verwenden, beachtet die Unified Manager GUI die ADFS-Zeitüberschreitung nicht und funktioniert weiter, bis die Unified Manager Sitzungs-Zeitüberschreitung erreicht ist. Die Zeitüberschreitung der GUI-Sitzung kann durch Klicken auf **General** > **Feature Settings** > **Inactivity Timeout** geändert werden.

Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager

Sie können den Identitätsanbieter (IdP) ändern, den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet.

Bevor Sie beginnen

- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den Identitätsanbieter (IdP).

Der neue IdP lässt sich vor oder nach der Konfiguration von Unified Manager konfigurieren.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Einzugeben sind die neue IdP URI sowie die IdP-Metadaten, die für die Verbindung des Unified Manager server mit dem IdP erforderlich sind.

   Wenn der IdP direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URL auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch auszufüllen.

3. Sie können den Unified Manager Metadaten-URI kopieren oder die Metadaten in einer XML-Textdatei speichern.
4. Im nächsten Schritt erfolgt die Auswahl von **Konfiguration speichern**.

   Ein Meldungsfeld wird angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

5. Klicken Sie auf **OK**.

Zum Abschließen der Konfiguration auf den neuen IdP zugreifen und die Unified Manager Server-URI sowie die Metadaten eingeben.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der neuen IdP-Anmeldeseite anstatt auf der alten IdP-Anmeldeseite eingeben.

Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats

Jede Änderung des auf dem Unified Manager Server installierten HTTPS-Sicherheitszertifikats erfordert eine Aktualisierung der SAML Authentifizierungskonfigurationseinstellungen. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, ihm eine neue IP-Adresse zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager Servers funktioniert die SAML Authentifizierung nicht mehr, und Benutzer können nicht auf die grafische Benutzeroberfläche des Unified Manager zugreifen. Um den Zugriff auf die Benutzeroberfläche wiederherzustellen, müssen Sie die SAML Authentifizierungseinstellungen sowohl auf dem IdP Server als auch auf dem Unified Manager Server aktualisieren.

Schritte

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Die Unified Manager Benutzeroberfläche kann über den aktualisierten FQDN oder die IP-Adresse aufgerufen werden. Dabei wird das aktualisierte Serverzertifikat im Browser akzeptiert, und die Anmeldung erfolgt mit den Anmeldedaten des Wartungsbenutzers.
4. Die Konfiguration der IdP-Verbindung erfolgt auf der Seite **Setup/Authentifizierung** über die Registerkarte **SAML-Authentifizierung**.
5. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.
6. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.
8. Zum Abschluss der Konfiguration erfolgt auf dem IdP-Server die Eingabe der URI des Unified Manager-Servers und der Metadaten.

Identitätsanbieter	Konfigurationsschritte
ADFS	a. In der ADFS-Management-GUI erfolgt das Löschen des vorhandenen Eintrags für die Vertrauensstellung der vertrauenden Seite. b. Das Hinzufügen eines neuen Eintrags für die Vertrauensstellung der vertrauenden Seite erfolgt mithilfe des `saml_sp_metadata.xml` aktualisierten Unified Manager Servers. c. Definition der drei Anspruchsregeln, die Unified Manager benötigt, um ADFS SAML-Antworten für diesen Eintrag der Vertrauensstellung der vertrauenden Seite zu analysieren. d. Ein Neustart des ADFS Windows Service ist erforderlich.
Shibboleth	a. Der neue FQDN des Unified Manager Servers ist in den `attribute-filter.xml` und `relying-party.xml` Dateien zu aktualisieren. b. Nach dem Neustart des Apache Tomcat Webservers ist zu warten, bis Port 8005 online ist.

9. Nach der Anmeldung bei Unified Manager sollte überprüft werden, ob die SAML-Authentifizierung über Ihren IdP wie erwartet funktioniert.

SAML Authentifizierung in Active IQ Unified Manager deaktivieren

Sie können die SAML Authentifizierung deaktivieren, wenn die Authentifizierung von Remote-Benutzern über einen sicheren Identitätsanbieter (IdP) beendet werden soll, bevor sie sich bei der Unified Manager Weboberfläche anmelden können. Wenn die SAML Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter, wie z. B. Active Directory oder LDAP, die Anmeldeauthentifizierung.

Nach der Deaktivierung der SAML-Authentifizierung können neben den konfigurierten Remote-Benutzern auch lokale Benutzer und Wartungsbenutzer auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager Managementplattform deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Häkchen im Kontrollkästchen **SAML-Authentifizierung aktivieren** wird entfernt.
3. Auf **Speichern** klicken.

Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

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

Sie greifen auf Ihren IdP zu und löschen die Unified Manager Server URI und die Metadaten.

Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert.

Möglicherweise ist es erforderlich, die SAML Authentifizierung über die Managementplattform zu deaktivieren, wenn kein Zugriff auf die Unified Manager GUI besteht. Dies kann bei Fehlkonfigurationen oder wenn der Identitätsanbieter (IdP) nicht erreichbar ist, der Fall sein.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Managementplattform haben.

Wenn die SAML-Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP die Anmeldeauthentifizierung. Lokale Benutzer und Wartungsbenutzer können dann zusätzlich zu den konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML Authentifizierung auch auf der Seite „Setup/Authentication“ in der UI deaktivieren.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

Schritte

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Nach Eingabe von **y** und Drücken der Eingabetaste wird Unified Manager neu gestartet.

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

Falls erforderlich, können Sie auf Ihren IdP zugreifen und die Unified Manager Server-URL sowie die Metadaten löschen.

Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden

Auf der Seite „SAML-Authentifizierung“ können Sie Unified Manager so konfigurieren, dass Remote-Benutzer mithilfe von SAML über einen sicheren Identitätsanbieter (IdP)

authentifiziert werden, bevor sie sich bei der Unified Manager Weboberfläche anmelden können.

- Sie müssen über die Rolle „Application Administrator“ verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.
- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Mindestens ein Remote-Benutzer oder eine Remote-Gruppe muss konfiguriert sein.

Nachdem die Remote-Authentifizierung und die Remote-Benutzer konfiguriert wurden, können Sie durch Aktivieren des Kontrollkästchens „SAML-Authentifizierung aktivieren“ die Authentifizierung mithilfe eines sicheren Identitätsanbieters aktivieren.

- **IdP-URI**

  Die URI für den Zugriff auf den IdP vom Unified Manager Server. Beispiel-URIs sind unten aufgeführt.

  ADFS Beispiel-URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth Beispiel-URI:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP-Metadaten**

  Die IdP-Metadaten im XML-Format.

  Wenn die IdP-URL vom Unified Manager Server aus erreichbar ist, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Hostsystem (FQDN)**

  Der FQDN des Unified Manager Hostsystems, wie er während der Installation definiert wurde. Sie können diesen Wert bei Bedarf ändern.

- **Host-URI**

  Die URI für den Zugriff auf das Unified Manager Hostsystem vom IdP aus.

- **Host-Metadaten**

  Die Metadaten des Hostsystems im XML-Format.

Authentifizierung verwalten

Bearbeiten von Authentifizierungsservern in Active IQ Unified Manager

Sie können den Port ändern, den der Unified Manager Server für die Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen **Verschachtelte Gruppensuche deaktivieren** muss aktiviert sein.
3. Im Bereich **Authentifizierungsserver** den Authentifizierungsserver auswählen, der bearbeitet werden soll, und anschließend auf **Bearbeiten** klicken.
4. Im Dialogfeld **Authentifizierungsserver bearbeiten** können Sie die Portdetails bearbeiten.
5. Auf **Speichern** klicken.

Authentifizierungsserver in Active IQ Unified Manager löschen

Sie können einen Authentifizierungsserver löschen, wenn Sie verhindern möchten, dass der Unified Manager Server mit dem Authentifizierungsserver kommuniziert. Wenn Sie beispielsweise einen Authentifizierungsserver ändern möchten, mit dem der Verwaltungsserver kommuniziert, können Sie den Authentifizierungsserver löschen und einen neuen Authentifizierungsserver hinzufügen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie einen Authentifizierungsserver löschen, können Remote-Benutzer oder -Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Einen oder mehrere Authentifizierungsserver, die gelöscht werden sollen, auswählen und anschließend auf **Löschen** klicken.
3. Mit **Ja** wird die Löschanfrage bestätigt.

   Wenn die Option **Sichere Verbindung verwenden** aktiviert ist, werden die mit dem Authentifizierungsserver verknüpften Zertifikate zusammen mit dem Authentifizierungsserver gelöscht.

Authentifizierung mit Active Directory oder OpenLDAP in Active IQ Unified Manager

Sie können die Remote Authentifizierung auf dem Management-Server aktivieren und den Management-Server so konfigurieren, dass er mit Ihren Authentifizierungsservern kommuniziert, sodass Benutzer innerhalb der Authentifizierungsserver auf Unified Manager zugreifen können.

Sie können einen der folgenden vordefinierten Authentifizierungsservices verwenden oder Ihren eigenen Authentifizierungsservice angeben:

- Microsoft Active Directory

  Sie können Microsoft Lightweight Directory Services nicht verwenden.

- OpenLDAP

Sie können den erforderlichen Authentifizierungsservice auswählen und die entsprechenden Authentifizierungsserver hinzufügen, um den Remote-Benutzern im Authentifizierungsserver den Zugriff auf Unified Manager zu ermöglichen. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet. Der Managementserver verwendet das Lightweight Directory Access Protocol (LDAP), um Remote-Benutzer innerhalb des konfigurierten Authentifizierungsservers zu authentifizieren.

Für lokale Benutzer, die im Unified Manager angelegt werden, verwaltet der Verwaltungsserver eine eigene Datenbank mit Benutzernamen und Passwörtern. Der Verwaltungsserver führt die Authentifizierung durch und verwendet weder Active Directory noch OpenLDAP für die Authentifizierung.

Audit-Logging

Informationen zu Audit-Protokollen in Active IQ Unified Manager

Mithilfe von Revisionsprotokollen lässt sich feststellen, ob die Revisionsprotokolle manipuliert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Revisionsprotokollen protokolliert. Die Audits werden für alle Funktionen der Benutzeroberfläche und der öffentlich zugänglichen APIs von Active IQ Unified Manager durchgeführt.

Mit der **Audit Log: File View** können Sie alle in Ihrem Active IQ Unified Manager verfügbaren Revisionsprotokolldateien anzeigen und darauf zugreifen. Die Dateien in der **Audit Log: File View** sind nach ihrem Erstellungsdatum aufgelistet. Diese Ansicht zeigt Informationen zu allen Revisionsprotokollen an, die seit der Installation oder dem Upgrade bis zum aktuellen Zeitpunkt im System erfasst wurden. Wenn Sie im Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und sind in den Protokollen verfügbar. Der Status jeder Protokolldatei wird mithilfe des Attributs “File Integrity Status” erfasst, das aktiv überwacht wird, um Manipulationen oder das Löschen der Protokolldatei zu erkennen. Die Revisionsprotokolle können einen der folgenden Status aufweisen, wenn sie im System verfügbar sind:

Status	Beschreibung
AKTIV	Datei, in der Protokolle derzeit protokolliert werden.
NORMAL	Eine inaktive, komprimierte und im System gespeicherte Datei.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUAL_DELETE	Datei, die ein autorisierter Benutzer gelöscht hat.
ROLLOVER_DELETE	Datei, die aufgrund des auf der Rolling Configuration Policy basierenden Entfernens gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Revisionsprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht „Audit Logs“ aufgeführten Revisionsprotokolle löschen. Sie können ein Revisionsprotokoll löschen und optional einen Grund für das Löschen der Datei angeben, was künftig dabei hilft, eine gültige Löschung nachzuvollziehen. In der Spalte REASON werden der Grund zusammen mit dem Namen des Benutzers aufgeführt, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt dazu, dass die Datei aus dem System gelöscht wird, der Eintrag in der DB-Tabelle jedoch nicht.

Sie können die Revisionsprotokolle aus Active IQ Unified Manager über die Schaltfläche **HERUNTERLADEN** im Bereich „Audit Logs“ herunterladen und die Revisionsprotokolldateien exportieren. Die Dateien, die als „`NORMAL`“ oder „`TAMPERED`“ gekennzeichnet sind, werden in einem komprimierten `.gzip` Format heruntergeladen.

Die Revisionsprotokoll-Dateien werden regelmäßig archiviert und zur späteren Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Revisionsprotokolle digital signiert, um die Sicherheit und Integrität zu wahren.

Wenn ein vollständiges AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Revisionsprotokolldateien. Wenn jedoch ein kompaktes Support Bundle generiert wird, enthält es nur die aktiven Revisionsprotokolle. Die archivierten Revisionsprotokolle sind nicht enthalten.

Konfiguration der Audit-Protokolle von Active IQ Unified Manager

Mit der Schaltfläche **Configure** im Abschnitt „Revisionsprotokolle“ lässt sich die Rotationsrichtlinie für Revisionsprotokolldateien konfigurieren und außerdem die Remote Protokollierung für die Revisionsprotokolle aktivieren.

Sie können die Werte in **MAX FILE SIZE** und **AUDIT LOG RETENTION DAYS** entsprechend der gewünschten Datenmenge und -häufigkeit festlegen, die Sie im System speichern möchten. Der Wert im Feld **TOTAL AUDIT LOG SIZE** ist die Größe der gesamten im System vorhandenen Revisionsprotokolldaten. Die Rotationsrichtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe der Revisionsprotokoll-Sicherung den in **TOTAL AUDIT LOG SIZE** konfigurierten Wert erreicht, wird die Datei gelöscht, die zuerst archiviert wurde. Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag bleibt jedoch weiterhin in der Datenbank verfügbar und ist als “Rollover Delete” gekennzeichnet. Der Wert **AUDIT LOG RETENTION DAYS** steht für die Anzahl der Tage, für die die Revisionsprotokolldateien aufbewahrt werden. Jede Datei, die älter ist als der in diesem Feld festgelegte Wert, wird rotiert.

Schritte

1. **Revisionsprotokolle** > > **Konfigurieren** auswählen.
2. Werte für **MAXIMALE DATEIGRÖSSE**, **GESAMTGRÖSSE DES REVISIONSPROTOKOLLS** und **AUFBEWAHRUNGSTAGE DES REVISIONSPROTOKOLLS** werden eingegeben.

   Die Aktivierung der Remote-Protokollierung erfolgt über **Enable Remote Logging**.

Die Remote-Protokollierung von Audit-Protokollen in Active IQ Unified Manager kann aktiviert werden

Sie können im Dialogfeld „Revisionsprotokolle konfigurieren“ das Kontrollkästchen „Remote-Protokollierung aktivieren“ auswählen, um die Remote-Revisionsprotokollierung zu aktivieren. Mit dieser Funktion können Sie Revisionsprotokolle an einen Remote-Syslog-Server übertragen. Dies ermöglicht Ihnen, Ihre Revisionsprotokolle auch bei begrenztem Speicherplatz zu managen.

Die Remote-Protokollierung von Revisionsprotokollen bietet eine manipulationssichere Sicherung für den Fall, dass die Revisionsprotokoll-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Im Dialogfeld **Revisionsprotokolle konfigurieren** kann das Kontrollkästchen **Remote-Protokollierung aktivieren** ausgewählt werden.

   Es werden zusätzliche Felder zum Konfigurieren der Remote-Protokollierung angezeigt.

2. Für die Verbindung mit dem gewünschten Remote-Server werden **HOSTNAME** und **PORT** eingegeben.
3. Im Feld **SERVER CA CERTIFICATE** erfolgt die Auswahl eines öffentlichen Zertifikats des Zielservers über **BROWSE**.

   Das Zertifikat sollte im `.pem` Format hochgeladen werden. Dieses Zertifikat sollte vom Ziel Syslog-Server bezogen werden und darf nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten “hostname” als Teil des `SubjectAltName`(SAN)-Attributs enthalten.

4. Einzugeben sind die Werte für die folgenden Felder: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Die Werte sollten für diese Felder in Millisekunden angegeben werden.

5. Die Auswahl des gewünschten Syslog-Formats und der TLS Protokollversion erfolgt in den Feldern **FORMAT** und **PROTOCOL**.
6. Wenn der Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erfordert, ist das Kontrollkästchen **Client-Authentifizierung aktivieren** auszuwählen.

   Sie müssen das Zertifikat für die Client-Authentifizierung herunterladen und vor dem Speichern der Konfiguration des Revisionsprotokolls auf den Syslog-Server hochladen, andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Zertifikats für die Client-Authentifizierung erstellen.

   Beispiel: syslog-ng erfordert, dass ein <hash> des Zertifikats mit dem Befehl `openssl x509 -noout -hash -in cert.pem` erstellt wird. Anschließend sollten Sie das Client-Authentifizierungs-Zertifikat symbolisch mit einer Datei verknüpfen, die nach dem <hash> .0 benannt ist.

7. **Speichern** konfiguriert die Verbindung mit Ihrem Server und aktiviert die Remote-Protokollierung.

   Sie werden zur Seite „Revisionsprotokolle“ weitergeleitet.

> Der Wert für **Verbindungs-Zeitüberschreitung** kann sich auf die Konfiguration auswirken. Wenn die Konfiguration länger für eine Antwort benötigt als der definierte Wert, kann dies aufgrund eines Verbindungsfehlers zu einem Konfigurationsfehler führen. Für den Aufbau einer erfolgreichen Verbindung sollte der Wert für **Verbindungs-Zeitüberschreitung** erhöht und die Konfiguration erneut versucht werden.

Die Seite „Remote-Authentifizierung“ in Active IQ Unified Manager

Auf der Seite „Remote-Authentifizierung“ kann Unified Manager so konfiguriert werden, dass es mit Ihrem Authentifizierungsserver kommuniziert, um Remote-Benutzer zu authentifizieren, die versuchen, sich bei der Unified Manager Web-Benutzeroberfläche anzumelden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Nachdem Sie das Kontrollkästchen „Enable remote authentication“ aktiviert haben, können Sie die Remote-Authentifizierung mithilfe eines Authentifizierungsservers aktivieren.

- **Authentifizierungsdienst**

  Ermöglicht die Konfiguration des Verwaltungsservers zur Authentifizierung von Benutzern bei Verzeichnisdienstanbietern wie Active Directory oder OpenLDAP oder zur Angabe eines eigenen Authentifizierungsverfahrens. Die Angabe eines Authentifizierungsdienstes ist nur möglich, wenn die Remote-Authentifizierung aktiviert wurde.

  - **Active Directory**
    - Administratorname

      Gibt den Administratornamen des Authentifizierungsservers an.

    - Passwort

      Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

    - Basis-individueller Name

      Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

    - Verschachtelte Gruppensuche deaktivieren

      Legt fest, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Bei Verwendung von Active Directory können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

    - Sichere Verbindung verwenden

      Gibt den Authentifizierungsdienst an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

  - **OpenLDAP**
    - Bind individueller Name

      Gibt den Bind-individuellen Namen an, der zusammen mit dem Basis-individuellen Namen verwendet wird, um Remote-Benutzer auf dem Authentifizierungsserver zu finden.

    - Bind Passwort

      Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

    - Basis-individueller Name

      Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

- Sichere Verbindung verwenden

  Gibt an, dass Secure LDAP für die Kommunikation mit LDAP-Authentifizierungsservern verwendet wird.

- **Andere**

  - Bind individueller Name

    Gibt den Bind individueller Name an, der zusammen mit dem Basis individueller Name verwendet wird, um Remote-Benutzer auf dem von Ihnen konfigurierten Authentifizierungsserver zu finden.

  - Bind Passwort

    Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

  - Basis-individueller Name

    Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

  - Protokollversion

    Gibt die vom Authentifizierungsserver unterstützte Version des Lightweight Directory Access Protocol (LDAP) an. Sie können festlegen, ob die Protokollversion automatisch erkannt werden soll oder ob die Version auf 2 oder 3 gesetzt werden soll.

  - Attribut für den Benutzernamen

    Gibt den Namen des Attributs auf dem Authentifizierungsserver an, das die Benutzeranmeldenamen enthält, die der Verwaltungsserver authentifiziert.

  - Attribut der Gruppenzugehörigkeit

    Gibt einen Wert an, der Remote-Benutzern die Mitgliedschaft in der Management Servergruppe basierend auf einem Attribut und einem Wert zuweist, die im Authentifizierungsserver des Benutzers angegeben sind.

  - UGID

    Wenn die Remote-Benutzer als Mitglieder eines GroupOfUniqueNames-Objekts im Authentifizierungsserver enthalten sind, können Sie mit dieser Option den Remote-Benutzern die Mitgliedschaft in der Managementservergruppe basierend auf einem bestimmten Attribut in diesem GroupOfUniqueNames-Objekt zuweisen.

  - Verschachtelte Gruppensuche deaktivieren

    Legt fest, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Bei Verwendung von Active Directory können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

  - Mitglied

    Gibt den Attributnamen an, den Ihr Authentifizierungsserver verwendet, um Informationen über die

einzelnen Mitglieder einer Gruppe zu speichern.

- Benutzerobjektklasse

  Gibt die Objektklasse eines Benutzers auf dem Remote-Authentifizierungsserver an.

- Gruppenobjektklasse

  Gibt die Objektklasse aller Gruppen auf dem Remote-Authentifizierungsserver an.

> Die Werte, die Sie für die Attribute „Member“, „User Object Class“ und „Group Object Class“ eingeben, müssen mit den Werten übereinstimmen, die in Ihren Active Directory-, OpenLDAP- und LDAP-Konfigurationen hinzugefügt wurden. Andernfalls kann die Authentifizierung fehlschlagen.

- Sichere Verbindung verwenden

  Gibt den Authentifizierungsdienst an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

> Wenn Sie den Authentifizierungsservice ändern möchten, ist es erforderlich, alle vorhandenen Authentifizierungsserver zu löschen und neue Authentifizierungsserver hinzuzufügen.

Bereich der Authentifizierungsserver

Im Bereich „Authentifizierungsserver“ sind die Authentifizierungsserver aufgeführt, mit denen der Verwaltungsserver kommuniziert, um Remote-Benutzer zu finden und zu authentifizieren. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet.

- **Befehlsschaltflächen**

  Ermöglicht das Hinzufügen, Bearbeiten oder Löschen von Authentifizierungsservern.

  - Hinzufügen

    Ermöglicht das Hinzufügen eines Authentifizierungsservers.

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

  - Bearbeiten

    Hier können Sie die Einstellungen für einen ausgewählten Authentifizierungsserver bearbeiten.

  - Löschen

    Löscht die ausgewählten Authentifizierungsserver.

- **Name oder IP-Adresse**

  Zeigt den Hostnamen oder die IP-Adresse des Authentifizierungsservers an, der zur Authentifizierung des Benutzers auf dem Managementserver verwendet wird.

- **Port**

  Zeigt die Portnummer des Authentifizierungsservers an.

- **Authentifizierungstest**

  Mit dieser Schaltfläche können Sie die Konfiguration Ihres Authentifizierungsservers überprüfen, indem Sie einen Remote-Benutzer oder eine Remote-Gruppe authentifizieren.

  Wenn Sie beim Testen nur den Benutzernamen angeben, sucht der Verwaltungsserver den Remote-Benutzer auf dem Authentifizierungsserver, authentifiziert ihn aber nicht. Wenn Sie sowohl den Benutzernamen als auch das Passwort angeben, sucht der Verwaltungsserver den Remote-Benutzer und authentifiziert ihn.

  Sie können die Authentifizierung nicht testen, wenn die Remote-Authentifizierung deaktiviert ist.

Sicherheitszertifikate verwalten

Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen

Sie können die Details des HTTPS-Zertifikats mit dem abgerufenen Zertifikat in Ihrem Browser vergleichen, um sicherzustellen, dass die verschlüsselte Verbindung Ihres Browsers zu Unified Manager nicht abgefangen wird.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die Anzeige des Zertifikats ermöglicht die Überprüfung des Inhalts eines neu generierten Zertifikats oder die Anzeige von Subject Alt Names (SAN), über die auf Unified Manager zugegriffen werden kann.

Schritt

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

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Falls Sie detailliertere Informationen zum Sicherheitszertifikat benötigen, als auf der Seite HTTPS Certificate angezeigt werden, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager

Sie können eine Zertifikatssignierungsanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, um die Datei einer Zertifizierungsstelle zur Signierung vorzulegen. Ein von einer Zertifizierungsstelle signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

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

2. Sie können auf **Download HTTPS Certificate Signing Request** klicken.
3. Die `<hostname>.csr` Datei speichern.

Sie können die Datei einer Zertifizierungsstelle zum Signieren vorlegen und anschließend das signierte Zertifikat installieren.

Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem es von einer Certificate Authority signiert und zurückgegeben wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein CA-signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

*Was Sie vor Beginn beachten sollten

Sie müssen die folgenden Aktionen abgeschlossen haben:

- Die Datei mit der Zertifikatsignierungsanforderung wurde heruntergeladen und durch eine Zertifizierungsstelle signiert.
- Zertifikatskette im PEM-Format gespeichert
- Die Kette umfasste alle Zertifikate, vom Unified Manager Serverzertifikat bis zum Stamm-Signaturzertifikat, einschließlich aller vorhandenen Zwischenzertifikate.

Sie benötigen die Rolle des Anwendungsadministrators.

Beträgt die Gültigkeitsdauer des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage, wird sie von der CA vor der Unterzeichnung und Rücksendung des Zertifikats auf 397 Tage verkürzt.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. Anschließend wählen Sie **HTTPS-Zertifikat installieren** aus.
3. In dem angezeigten Dialogfeld kann über **Datei auswählen…** die hochzuladende Datei gesucht werden.
4. Nach dem Auswählen der Datei installiert ein Klick auf **Install** die Datei.

   Informationen finden sich unter "Installation eines mit externen Tools generierten HTTPS-Zertifikats".

Beispiel einer Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatskettendatei aussehen könnte:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden

Sie können selbstsignierte oder CA-signierte Zertifikate installieren, die mit einem externen Tool wie OpenSSL, BoringSSL oder LetsEncrypt generiert wurden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette hochladen, da diese Zertifikate extern generierte Paare aus öffentlichem und privatem Schlüssel sind. Die zulässigen Schlüsselpaaralgorithmen sind „`RSA`“ und „`EC`“. Die Option „Install HTTPS Certificate“ ist auf der Seite „HTTPS Certificates“ im Abschnitt „General“ verfügbar. Die hochgeladene Datei sollte das folgende Eingabeformat aufweisen.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager Host gehört
2. Zertifikat des Servers, das zum privaten Schlüssel passt
3. Zertifikate der Zertifizierungsstellen in umgekehrter Reihenfolge bis zur Root-CA, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC Schlüsselpaar

Zulässige Kurven sind „`prime256v1`“ und „`secp384r1`“. Beispiel eines Zertifikats mit einem extern generierten EC-Paar:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar

Die zulässigen Schlüssellängen für das zum Host-Zertifikat gehörende RSA-Schlüsselpaar sind 2048, 3072 und 4096. Zertifikat mit einem extern generierten **RSA-Schlüsselpaar**:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Nach dem Hochladen des Zertifikats sollte die Active IQ Unified Manager Instanz neu gestartet werden, damit die Änderungen wirksam werden.

Prüfungen beim Hochladen extern generierter Zertifikate

Das System führt beim Hochladen eines mit externen Tools erstellten Zertifikats Prüfungen durch. Wenn eine dieser Prüfungen fehlschlägt, lehnt das System das Zertifikat ab. Die Validierung umfasst auch Zertifikate, die innerhalb des Produkts aus dem CSR generiert werden, sowie Zertifikate, die mit externen Tools erstellt werden.

- Der private Schlüssel in den Eingabedaten wird mit dem Host-Zertifikat in den Eingabedaten validiert.
- Der Common Name (CN) im Hostzertifikat wird mit dem FQDN des Hosts verglichen.
- Der Common Name (CN) des Hostzertifikats darf nicht leer sein oder nur Leerzeichen enthalten und darf nicht auf localhost gesetzt sein.
- Das Gültigkeitsbeginndatum sollte nicht in der Zukunft liegen, und das Gültigkeitsablaufdatum des Zertifikats sollte nicht in der Vergangenheit liegen.
- Falls Intermediate CA oder CA vorhanden ist, sollte das Gültigkeitsbeginn-Datum des Zertifikats nicht in der Zukunft liegen und das Gültigkeitsablaufdatum nicht in der Vergangenheit liegen.



Der private Schlüssel in den Eingabedaten darf nicht verschlüsselt sein. Falls private Schlüssel verschlüsselt sind, lehnt das System sie ab.

Beispiel 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
```

```
-----END ENCRYPTED PRIVATE KEY-----
```

Beispiel 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Beispiel 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Falls die Zertifikatsinstallation fehlschlägt, finden Sie weitere Informationen im Wissensdatenbank-Artikel (KB): "ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"

Seitenbeschreibungen für die Zertifikatsverwaltung

Informationen zur HTTPS-Zertifikatsseite in Active IQ Unified Manager

Die Seite „HTTPS-Zertifikat“ ermöglicht das Anzeigen des aktuellen Sicherheitszertifikats, das Herunterladen einer Anforderung zur Zertifikatsignierung, das Generieren eines neuen selbstsignierten HTTPS-Zertifikats oder das Installieren eines neuen HTTPS-Zertifikats.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat erstellt haben, wird auf dieser Seite das Zertifikat angezeigt, das während der Installation generiert wurde.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die folgenden Vorgänge durchführen:

- **HTTPS-Zertifikatsignierungsanforderung herunterladen**

  Lädt eine Zertifikatanforderung für das derzeit installierte HTTPS-Zertifikat herunter. Ihr Browser fordert Sie auf, die <hostname>.csr-Datei zu speichern, damit Sie die Datei einer Zertifizierungsstelle zum Signieren bereitstellen können.

- **Installation des HTTPS-Zertifikats**

  Ermöglicht das Hochladen und Installieren eines Sicherheitszertifikats, nachdem dieses von einer Zertifizierungsstelle signiert und zurückgesendet wurde. Das neue Zertifikat ist nach einem Neustart des Verwaltungsservers wirksam.

- **HTTPS-Zertifikat neu generieren**

Ermöglicht die Generierung eines neuen selbstsignierten HTTPS-Zertifikats, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat ist nach einem Neustart des Unified Manager gültig.

Dialogfeld „HTTPS-Zertifikat in Active IQ Unified Manager neu generieren“

Im Dialogfeld „HTTPS-Zertifikat neu generieren“ können Sie die Sicherheitsinformationen anpassen und anschließend ein neues HTTPS-Zertifikat mit diesen Informationen generieren.

Auf dieser Seite erscheinen die aktuellen Zertifikatsinformationen.

Die Auswahlmöglichkeiten “Regenerate Using Current Certificate Attributes” und “Update the Current Certificate Attributes” ermöglichen es Ihnen, das Zertifikat mit den aktuellen Informationen neu zu generieren oder ein Zertifikat mit neuen Informationen zu erstellen.

- **Allgemeiner Name**

  Erforderlich. Der vollqualifizierte Domain-Name (FQDN), den Sie sichern möchten.

  In Hochverfügbarkeitskonfigurationen von Unified Manager kommt die virtuelle IP-Adresse zum Einsatz.

- **E-Mail**

  Optional. Eine E-Mail-Adresse zur Kontaktaufnahme mit Ihrem Unternehmen; in der Regel die E-Mail-Adresse des Zertifikatsadministrators oder der IT-Abteilung.

- **Unternehmen**

  Optional. In der Regel der eingetragene Name Ihres Unternehmens.

- **Abteilung**

  Optional. Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional. Der Ort Ihres Unternehmens.

- **Zustand**

  Optional. Das Bundesland oder die Provinz Ihres Unternehmens, nicht abgekürzt.

- **Land**

  Optional. Der Länderstandort Ihres Unternehmens. Dies ist normalerweise ein zweistelliger ISO-Code des Landes.

- **Alternative Bezeichnungen**

  Erforderlich. Zusätzliche, nicht primäre Domänennamen, die zusätzlich zu localhost oder anderen Netzwerkadressen für den Zugriff auf diesen Server verwendet werden können. Als Trennzeichen zwischen den einzelnen alternativen Namen dienen Kommas.

  Das Kontrollkästchen „`Lokale Identifikationsinformationen ausschließen (z. B. localhost)`“ wird ausgewählt, wenn die lokalen Identifikationsinformationen aus dem Feld „Alternative

Namen“ im Zertifikat entfernt werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, werden im Feld „Alternative Namen“ nur die Daten verwendet, die in das Feld eingegeben werden. Wenn das Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld „Alternative Namen“.

- **SCHLÜSSELLÄNGE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA eingestellt. Sie können zwischen den Schlüssellängen 2048, 3072 oder 4096 Bit wählen. Die Standardschlüssellänge beträgt 2048 Bit.

- **GÜLTIGKEITSDAUER**

  Die Standardgültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, bleibt die Gültigkeit des vorherigen Zertifikats möglicherweise unverändert.

Weitere Informationen sind unter "Generierung von HTTPS-Zertifikaten" verfügbar.

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.