Konfigurieren von Unified Manager zum Senden von Warnmeldungen

Active IQ Unified Manager 9.14

NetApp
November 11, 2024

Inhalt

Konfigurieren von Unified Manager zum Senden von Warnmeldungen

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

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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

Schritte

1. "Konfigurieren Sie die Einstellungen für Ereignisbenachrichtigungen".

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

2. "Aktivieren Sie die Remote-Authentifizierung".

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

3. "Authentifizierungsserver hinzufügen".

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

4. "Benutzer hinzufügen".

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

5. "Warnmeldungen hinzufügen".

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

Konfigurieren von Einstellungen für Ereignisbenachrichtigungen

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet werden, wenn ein Ereignis generiert wird oder ein Ereignis einem Benutzer zugewiesen

ist. Sie können den SMTP-Server konfigurieren, der zum Senden der Warnmeldung verwendet wird, und Sie können verschiedene Benachrichtigungsmechanismen festlegen – beispielsweise können Alarmbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Was Sie brauchen

Sie müssen die folgenden Informationen haben:

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

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

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

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

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

Schritte

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

   Hinweise:

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

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

Aktivieren der Remote-Authentifizierung

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

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

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

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

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

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

Schritte

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

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

Für Authentifizierungstyp…	Geben Sie die folgenden Informationen ein…
Öffnen Sie LDAP	• Distinguished Name binden (in der entsprechenden LDAP-Notation) • Kennwort binden • Basisname mit Distinguished Name

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

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

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

Deaktivieren verschachtelter Gruppen von der Remote-Authentifizierung

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

Was Sie brauchen

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

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

Schritte

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

Einrichten von Authentifizierungsservices

Authentifizierungsservices ermöglichen die Authentifizierung von Remote-Benutzern oder Remotegruppen in einem Authentifizierungsserver, bevor sie ihnen den Zugriff auf Unified

Manager gewähren. Sie können Benutzer mithilfe von vordefinierten Authentifizierungsdiensten (z. B. Active Directory oder OpenLDAP) authentifizieren, oder indem Sie Ihren eigenen Authentifizierungsmechanismus konfigurieren.

Was Sie brauchen

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

Schritte

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

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

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

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

3. Klicken Sie Auf **Speichern**.

Hinzufügen von Authentifizierungsservern

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

Was Sie brauchen

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

Wenn der neue Authentifizierungsserver Teil eines Hochverfügbarkeitspaars (HA-Paar) ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

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

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

Der hinzugefügte Authentifizierungsserver wird im Bereich Server angezeigt.

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

Die Konfiguration der Authentifizierungsserver wird getestet

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

Was Sie brauchen

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

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

Schritte

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

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

Hinzufügen von Meldungen

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

Was Sie brauchen

- Sie müssen Benachrichtigungseinstellungen wie die Benutzer-E-Mail-Adresse, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager-Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Meldung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie ein Skript auf der Grundlage des Ereignisses ausführen möchten, müssen Sie das Skript mithilfe der Seite „Skripte“ zu Unified Manager hinzugefügt haben.

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

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

Schritte

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

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

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

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

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

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

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

   Sie können auch Benutzer über SNMP-Traps benachrichtigen.

7. Klicken Sie Auf **Speichern**.

Beispiel für das Hinzufügen einer Meldung

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

- Alarmname: HealthTest
- Ressourcen: Enthält alle Volumes, deren Name „`abc`“ enthält und schließt alle Volumes aus, deren Name „`xyz`“ enthält
- Ereignisse: Umfasst alle kritischen Systemzustandsereignisse

- Aktionen: Enthält „sample@domain.com“, ein „`Test`“-Skript, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Führen Sie im Dialogfeld Alarm hinzufügen die folgenden Schritte aus:

Schritte

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

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

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