Benachrichtigungen konfigurieren

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/task_configure_unified_manager_to_send_alert_notifications.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Benachrichtigungen konfigurieren . . . 1
- Active IQ Unified Manager wird so konfiguriert, dass Warnmeldungen gesendet werden. . . . 1
- Konfiguration der Einstellungen für Ereignisbenachrichtigungen in Active IQ Unified Manager . . . 2
- Remote Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 3
- Verschachtelte Gruppen aus der Remote Authentifizierung in Active IQ Unified Manager sind deaktiviert . . . 4
- Einrichtung von Authentifizierungsdiensten in Active IQ Unified Manager . . . 4
- Hinzufügen von Authentifizierungsservern zu Active IQ Unified Manager . . . 6
- Die Konfiguration der Authentifizierungsserver in Active IQ Unified Manager wird getestet . . . 7
- Hinzufügen von Benachrichtigungen in Active IQ Unified Manager . . . 8
  - Beispiel für das Hinzufügen einer Benachrichtigung . . . 9

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)

Für den Authentifizierungstyp…	Eingabe der folgenden Informationen…
OpenLDAP	• Bind individueller Name (in der entsprechenden LDAP-Notation) • Bind Passwort • Basisindividueller Name

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

Wenn für den Authentifizierungsserver die Option „Use Secure Connection“ ausgewählt ist, kommuniziert Unified Manager mit dem Authentifizierungsserver über das Secure Sockets Layer (SSL)-Protokoll.

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

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

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

Bevor Sie beginnen

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

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

Schritte

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

Einrichtung von Authentifizierungsdiensten in Active IQ Unified Manager

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

Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

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

Schritte

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

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

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

3. Auf **Speichern** klicken.

Hinzufügen von Authentifizierungsservern zu Active IQ Unified Manager

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

Bevor Sie beginnen

- Folgende Informationen müssen verfügbar sein:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie benötigen die Rolle des Anwendungsadministrators.

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

Schritte

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

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

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.