



Funktionseinstellungen verwalten

Active IQ Unified Manager

NetApp

October 15, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-916/config/concept_policy_based_storage_management.html on October 15, 2025. Always check docs.netapp.com for the latest.

Inhalt

- Funktionseinstellungen verwalten 1
 - Aktivieren Sie die richtlinienbasierte Speicherverwaltung 1
 - API-Gateway aktivieren 2
 - Inaktivitäts-Timeout angeben 2
 - Aktivieren von Active IQ Portalereignissen 2
 - Aktivieren und Deaktivieren von Sicherheitseinstellungen zur Einhaltung der Vorschriften 3
 - Sicherheitseinstellungen anpassen 3
 - Passen Sie AutoSupport und Authentifizierungseinstellungen an 4
 - Aktivieren und Deaktivieren des Skript-Uploads 4
 - Login-Banner hinzufügen 4

Funktionseinstellungen verwalten

Auf der Seite „Funktionseinstellungen“ können Sie bestimmte Funktionen in Active IQ Unified Manager aktivieren und deaktivieren. Dazu gehören das Erstellen und Verwalten von Speicherobjekten basierend auf Richtlinien, das Aktivieren des API-Gateways und des Anmeldebanners, das Hochladen von Skripten zum Verwalten von Warnungen, das Timeout einer Web-UI-Sitzung basierend auf der Inaktivitätszeit und das Deaktivieren des Empfangs von Active IQ Plattformereignissen.



Die Seite „Funktionseinstellungen“ ist nur für Benutzer mit der Rolle „Anwendungsadministrator“ verfügbar.

Informationen zum Hochladen von Skripten finden Sie unter ["Aktivieren und Deaktivieren des Skript-Uploads"](#) .

Aktivieren Sie die richtlinienbasierte Speicherverwaltung

Die Option **Richtlinienbasiertes Speichermanagement** ermöglicht ein Speichermanagement basierend auf Service Level Objectives (SLOs). Diese Option ist standardmäßig aktiviert.

Wenn Sie diese Funktion aktivieren, können Sie Speicher-Workloads auf den ONTAP -Clustern bereitstellen, die Ihrer Active IQ Unified Manager Instanz hinzugefügt wurden, und diese Workloads basierend auf den zugewiesenen Performance Service Levels und Speichereffizienzrichtlinien verwalten.

Sie können diese Funktion unter **Allgemein > Funktionseinstellungen > Richtlinienbasierte Speicherverwaltung** aktivieren oder deaktivieren. Nach Aktivierung dieser Funktion stehen folgende Seiten zur Bedienung und Überwachung zur Verfügung:

- Bereitstellung (Speicher-Workload-Bereitstellung)
- **Richtlinien > Leistungs-Service-Levels**
- **Richtlinien > Speichereffizienz**
- Spalte „Vom Leistungsservicelevel verwaltete Workloads“ auf der Seite „Cluster-Setup“
- Workload-Performance-Panel auf dem **Dashboard**

Sie können die Bildschirme verwenden, um Leistungsservicelevel und Speichereffizienzrichtlinien zu erstellen und Speicher-Workloads bereitzustellen. Sie können auch die Speicherarbeitslasten überwachen, die den zugewiesenen Leistungsserviceleveln entsprechen, sowie die nicht konformen. Über die Bedienfelder „Workload-Leistung“ und „Workload-IOPS“ können Sie außerdem die gesamte, verfügbare und genutzte Kapazität und Leistung (IOPS) der Cluster in Ihrem Rechenzentrum basierend auf den darauf bereitgestellten Speicher-Workloads bewerten.

Nachdem Sie diese Funktion aktiviert haben, können Sie die Unified Manager REST-APIs ausführen, um einige dieser Funktionen über **Menüleiste > Hilfe-Schaltfläche > API-Dokumentation > Kategorie Speicheranbieter** auszuführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format `https://<hostname>/docs/api/` eingeben.

Weitere Informationen zu den APIs finden Sie unter ["Erste Schritte mit Active IQ Unified Manager REST-APIs"](#) .

API-Gateway aktivieren

Die API-Gateway-Funktion ermöglicht es Active IQ Unified Manager , eine einzige Steuerebene zu sein, von der aus Sie mehrere ONTAP Cluster verwalten können, ohne sich einzeln bei ihnen anmelden zu müssen.

Sie können diese Funktion auf den Konfigurationsseiten aktivieren, die angezeigt werden, wenn Sie sich zum ersten Mal bei Unified Manager anmelden. Alternativ können Sie diese Funktion unter **Allgemein > Funktionseinstellungen > API-Gateway** aktivieren oder deaktivieren.

Unified Manager REST-APIs unterscheiden sich von ONTAP REST-APIs und nicht alle Funktionen von ONTAP REST-APIs können durch die Verwendung der Unified Manager REST-APIs genutzt werden. Wenn Sie jedoch aus geschäftlichen Gründen auf die ONTAP -APIs zugreifen müssen, um bestimmte Funktionen zu verwalten, die nicht für Unified Manager verfügbar sind, können Sie die API-Gateway-Funktion aktivieren und die ONTAP -APIs ausführen. Das Gateway fungiert als Proxy zum Tunneln der API-Anfragen, indem es die Header- und Body-Anfragen im gleichen Format wie in den ONTAP -APIs verwaltet. Sie können Ihre Unified Manager-Anmeldeinformationen verwenden und die spezifischen APIs ausführen, um auf die ONTAP -Cluster zuzugreifen und sie zu verwalten, ohne einzelne Cluster-Anmeldeinformationen weiterzugeben. Unified Manager fungiert als zentraler Verwaltungspunkt für die Ausführung der APIs in den ONTAP Clustern, die von Ihrer Unified Manager-Instanz verwaltet werden. Die von den APIs zurückgegebene Antwort ist dieselbe wie die Antwort, die von den jeweiligen ONTAP REST-APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

Nachdem Sie diese Funktion aktiviert haben, können Sie die Unified Manager REST-APIs über **Menüleiste > Hilfe-Schaltfläche > API-Dokumentation > Kategorie Gateway** ausführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format <https://<hostname>/docs/api/>

Weitere Informationen zu den APIs finden Sie unter "[Erste Schritte mit Active IQ Unified Manager REST-APIs](#)".

Inaktivitäts-Timeout angeben

Sie können den Inaktivitäts-Timeout-Wert für Active IQ Unified Manager angeben. Nach einer Inaktivität der angegebenen Zeit wird die Anwendung automatisch abgemeldet. Diese Option ist standardmäßig aktiviert.

Sie können diese Funktion deaktivieren oder die Zeit unter **Allgemein > Funktionseinstellungen > Inaktivitäts-Timeout** ändern. Sobald Sie diese Funktion aktivieren, sollten Sie im Feld **ABMELDEN NACH** das Zeitlimit der Inaktivität (in Minuten) angeben, nach dem sich das System automatisch abmeldet. Der Standardwert beträgt 4320 Minuten (72 Stunden).



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

Aktivieren von Active IQ Portalereignissen

Sie können angeben, ob Sie Active IQ Portalereignisse aktivieren oder deaktivieren möchten. Diese Einstellung ermöglicht es dem Active IQ Portal, zusätzliche Ereignisse zur Systemkonfiguration, Verkabelung usw. zu erkennen und anzuzeigen. Diese Option ist standardmäßig aktiviert.

Wenn Sie diese Funktion aktivieren, zeigt Active IQ Unified Manager Ereignisse an, die vom Active IQ Portal erkannt wurden. Diese Ereignisse werden erstellt, indem ein Satz von Regeln für AutoSupport -Nachrichten ausgeführt wird, die von allen überwachten Speichersystemen 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 **Allgemein > Funktionseinstellungen > * Active IQ Portalereignisse*** aktivieren oder deaktivieren. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Speicherverwaltung > Ereigniseinrichtung > Regeln hochladen** hochladen.

Diese Funktion ist standardmäßig aktiviert. Durch Deaktivieren dieser Funktion werden Active IQ -Ereignisse nicht mehr erkannt oder im Unified Manager angezeigt. Wenn diese Funktion deaktiviert ist, kann Unified Manager die Active IQ -Ereignisse auf einem Cluster zu einer vordefinierten Zeit von 00:15 Uhr für die Zeitzone dieses Clusters empfangen.

Aktivieren und Deaktivieren von Sicherheitseinstellungen zur Einhaltung der Vorschriften

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

Die Einstellungen, die auf dieser Seite aktiviert oder deaktiviert werden, regeln den allgemeinen Compliance-Status der Cluster und Speicher-VMs auf Unified Manager. Basierend auf den Auswahlen sind die entsprechenden Spalten in der Ansicht **Sicherheit: Alle Cluster** der Cluster-Inventarseite und in der Ansicht **Sicherheit: Alle Storage-VMs** der Storage-VM-Inventarseite sichtbar.



Nur Benutzer mit Administratorrolle können diese Einstellungen bearbeiten.

Die Sicherheitskriterien für Ihre ONTAP Cluster, Storage-VMs und Volumes werden anhand der Empfehlungen bewertet, die in der ["Leitfaden zur Sicherheitshärtung für NetApp ONTAP 9"](#) . Das Sicherheitsfenster auf dem Dashboard und die Sicherheitsseite zeigen den Standard-Sicherheitskonformitätsstatus Ihrer Cluster, Speicher-VMs und Volumes an. Außerdem werden Sicherheitsereignisse generiert und Verwaltungsaktionen für Cluster und Speicher-VMs aktiviert, bei denen Sicherheitsverletzungen vorliegen.

Sicherheitseinstellungen anpassen

Um die Einstellungen für die Compliance-Überwachung entsprechend Ihrer ONTAP Umgebung anzupassen, führen Sie die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Allgemein > Funktionseinstellungen > Sicherheits-Dashboard > Anpassen**. Das Popup **Einstellungen des Sicherheits-Dashboards anpassen** wird angezeigt.



Die Sicherheitskonformitätsparameter, die Sie aktivieren oder deaktivieren, können sich direkt auf die Standardsicherheitsansichten, Berichte und geplanten Berichte auf den Bildschirmen „Cluster“ und „Speicher-VMs“ auswirken. Wenn Sie vor der Änderung der Sicherheitsparameter einen Excel-Bericht von diesen Bildschirmen hochgeladen haben, sind die heruntergeladenen Excel-Berichte möglicherweise fehlerhaft.

2. Um die benutzerdefinierten Einstellungen für Ihre ONTAP Cluster zu aktivieren oder zu deaktivieren,

wählen Sie unter **Cluster** die gewünschte allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Cluster-Compliance finden Sie unter "[Cluster-Compliance-Kategorien](#)".

- Um die benutzerdefinierten Einstellungen für Ihre Speicher-VMs zu aktivieren oder zu deaktivieren, wählen Sie unter **Speicher-VM** die gewünschte allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Storage-VM-Compliance finden Sie unter "[Storage-VM-Compliance-Kategorien](#)".

Passen Sie AutoSupport und Authentifizierungseinstellungen an

Im Abschnitt * AutoSupport -Einstellungen* können Sie angeben, ob zum Senden von AutoSupport -Nachrichten von ONTAP der HTTPS-Transport verwendet werden soll.

Im Abschnitt **Authentifizierungseinstellungen** können Sie die Ausgabe von Unified Manager-Warnungen für den standardmäßigen ONTAP Administratorbenutzer aktivieren.

Aktivieren und Deaktivieren des Skript-Uploads

Die Möglichkeit, Skripte in Unified Manager hochzuladen und auszuführen, ist standardmäßig aktiviert. Wenn Ihre Organisation diese Aktivität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion deaktivieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

- Klicken Sie im linken Navigationsbereich auf **Allgemein > Funktionseinstellungen**.
- Deaktivieren oder aktivieren Sie auf der Seite „Funktionseinstellungen“ die Skripterstellung, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen...	Dann tun Sie Folgendes ...
Skripte deaktivieren	Bewegen Sie im Bereich Skript-Upload den Schieberegler nach links.
Aktivieren von Skripten	Bewegen Sie im Bereich Skript-Upload den Schieberegler nach rechts.

Login-Banner hinzufügen

Durch das Hinzufügen eines Anmeldebanners kann Ihre Organisation beim An- und Abmelden beliebige Informationen anzeigen, beispielsweise wer auf das System zugreifen darf und welche Nutzungsbedingungen gelten.

Jeder Benutzer, beispielsweise Speicherbetreiber oder Administratoren, kann dieses Anmeldebanner-Popup während der Anmeldung, Abmeldung und Sitzungs-Timeout sehen.

Copyright-Informationen

Copyright © 2025 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, BEISPIELHAFT 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 IRGEND EINER 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.