Verwalten von Clustern

Active IQ Unified Manager 9.12

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-912/storage-mgmt/concept_how_discovery_process_works.html on October 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten von Clustern 1
Funktionsweise der Cluster-Erkennung 1
Anzeigen der Liste der überwachten Cluster 2
Hinzufügen von Clustern 2
Cluster werden bearbeitet 4
Cluster werden entfernt 5
Cluster-Erkennung neu ermitteln 6

Verwalten von Clustern

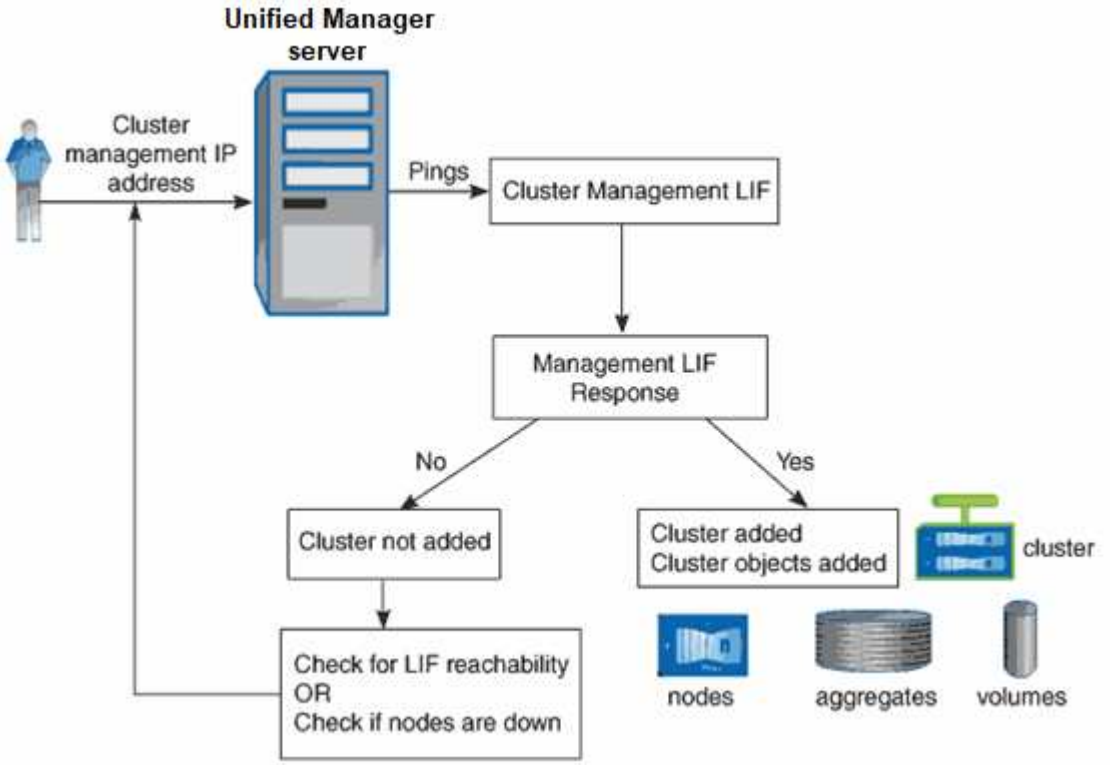
ONTAP-Cluster können mit Unified Manager gemanagt werden, um Cluster zu überwachen, hinzuzufügen, zu bearbeiten und zu entfernen.

Funktionsweise der Cluster-Erkennung

Nachdem Sie Unified Manager einen Cluster hinzugefügt haben, erkennt der Server die Cluster-Objekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsvorgang funktioniert, können Sie die Cluster und ihre Objekte im Unternehmen managen.

Das Monitoring-Intervall zum Erfassen von Cluster-Konfigurationsinformationen beträgt 15 Minuten. Beispielsweise dauert es nach dem Hinzufügen eines Clusters 15 Minuten, bis die Cluster-Objekte in der UI von Unified Manager angezeigt werden. Dieser Zeitrahmen trifft auch zu, wenn Sie die Änderungen an einem Cluster vornehmen. Wenn Sie beispielsweise einer SVM in einem Cluster zwei neue Volumes hinzufügen, werden diese neuen Objekte in der UI nach dem nächsten Abfrageintervall bis zu 15 Minuten angezeigt.

Das folgende Image veranschaulicht den Erkennungsvorgang:



Nachdem alle Objekte für ein neues Cluster erkannt wurden, sammelt Unified Manager historische Performance-Daten für die letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen.

Anzeigen der Liste der überwachten Cluster

Mithilfe der Seite Cluster Setup können Sie das Inventar der Cluster anzeigen. Sie können Details zu den Clustern anzeigen, z. B. ihren Namen oder ihre IP-Adresse und ihren Kommunikationsstatus.

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**. + Alle vom Unified Manager gemanagten Cluster in Ihrer Storage-Umgebung werden angezeigt. Die Liste der Cluster wird nach der Spalte „Sammlungsstatus“ sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach unterschiedlichen Spalten zu sortieren.

Hinzufügen von Clustern

Sie können Active IQ Unified Manager ein Cluster hinzufügen, sodass Sie das Cluster überwachen können. Dazu gehört beispielsweise die Möglichkeit, Cluster-Informationen wie Systemzustand, Kapazität, Performance und Konfiguration des Clusters abzurufen, damit Sie etwaige auftretende Probleme finden und beheben können.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.
- Sie müssen den Host-Namen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) für das Cluster haben.

  Bei Verwendung des Host-Namens muss dieser für die Cluster-Management-IP-Adresse für die Cluster-Management-LIF aufgelöst werden. Wenn Sie eine Node-Management-LIF verwenden, schlägt der Vorgang fehl.

- Sie müssen Benutzername und Passwort besitzen, um auf das Cluster zugreifen zu können.

  Für dieses Konto muss die Rolle *admin* mit dem Anwendungszugriff auf *ontapi*, *Console* und *http* eingestellt sein.

- Sie müssen die Port-Nummer kennen, um eine Verbindung zum Cluster mithilfe des HTTPS-Protokolls (normalerweise Port 443) herzustellen.
- Der Cluster muss die ONTAP Version 9.1 oder höher ausführen.
- Auf dem Unified Manager-Server muss ausreichend Speicherplatz vorhanden sein. Sie können dem Server kein Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.
- Sie verfügen über die erforderlichen Zertifikate. Unified Manager installiert Sicherheitszertifikate beim Hinzufügen eines Clusters:

Server-Zertifikate: Dieses Zertifikat ist Eigentum von Unified Manager. Bei einer neuen Installation von Unified Manager wird ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt ein Upgrade auf ein Zertifikat, das von einer Zertifizierungsstelle unterzeichnet wurde, um die Sicherheit zu erhöhen. Wenn das Serverzertifikat abgelaufen ist, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat aufnehmen können. Weitere Informationen zum erneuten Generieren eines SSL-Zertifikats finden Sie unter "Erstellen eines HTTPS-Sicherheitszertifikats".

Zertifikate für gegenseitige TLS-Kommunikation: Wird bei der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist auf Grundlage der Version von ONTAP für ein Cluster aktiviert. Wenn das Cluster mit der Version ONTAP niedriger als die Version 9.5 ist, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

Die zertifikatbasierte Authentifizierung wird für ein Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager auf Unified Manager 9.12 aktualisieren. Allerdings können Sie die Aktivierung durch Ändern und Speichern der Cluster-Details aktivieren. Wenn das Zertifikat abgelaufen ist, sollten Sie es erneut generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und erneuten Generieren des Zertifikats finden Sie unter "Cluster werden bearbeitet".

- Die zertifikatbasierte Authentifizierung wird automatisch aktiviert, wenn Sie ein Cluster aus der Web-Benutzeroberfläche hinzufügen. Wenn Sie ein Cluster aus der Wartungskonsole hinzufügen, ist die zertifikatbasierte Authentifizierung nicht aktiviert.
- Wenn die zertifikatbasierte Authentifizierung für ein Cluster aktiviert ist und Sie das Backup von Unified Manager von einem Server aus erstellen und auf einen anderen Unified Manager Server wiederherstellen. Hier wird der Hostname oder die IP-Adresse geändert, dann kann das Monitoring des Clusters fehlschlagen. Um den Ausfall zu vermeiden, bearbeiten und speichern Sie die Cluster-Details. Weitere Informationen über das Bearbeiten von Cluster-Details finden Sie unter "Cluster werden bearbeitet".

Clientzertifikate: Wird bei der Authentifizierung für EMS-Nachrichten verwendet, die von ONTAP empfangen wurden. Das Zertifikat ist im Besitz von ONTAP und erforderlich, wenn Sie einem ONTAP Cluster zu Unified Manager hinzufügen. Sie können ein Cluster nicht zu Unified Manager mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Client-Zertifikat bereits abgelaufen ist, sollten Sie es vor dem Hinzufügen des Clusters neu generieren. Wenn dieses Zertifikat jedoch für einen Cluster abläuft, der bereits hinzugefügt wurde und von Unified Manager verwendet wird, funktioniert EMS Messaging weiterhin mit dem abgelaufenen Zertifikat. Informationen zur Erstellung von Zertifikaten finden Sie im Artikel Knowledge Base (KB) "So erneuern Sie ein selbstsigniertes ONTAP-Zertifikat in der System Manager-Benutzeroberfläche".

- Eine einzelne Instanz von Unified Manager kann eine bestimmte Anzahl Nodes unterstützen. Wenn Sie eine Umgebung überwachen müssen, die die Anzahl der unterstützten Nodes überschreitet, müssen Sie eine zusätzliche Instanz von Unified Manager installieren, um einige der Cluster zu überwachen. Informationen zur Liste der unterstützten Node-Anzahl finden Sie im "Unified Manager Best Practices-Leitfaden".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Klicken Sie auf der Seite Cluster Setup auf **Hinzufügen**.
3. Geben Sie im Dialogfeld Cluster hinzufügen die Werte nach Bedarf an, und klicken Sie dann auf **Absenden**.
4. Klicken Sie im Dialogfeld Host autorisieren auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.

5. Klicken Sie Auf **Ja**.

   In Unified Manager 9.12 finden Sie nach dem Speichern der Cluster-Details das Zertifikat für eine gegenseitige TLS-Kommunikation für einen Cluster.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn das Cluster zunächst hinzugefügt wird. Unified Manager überprüft nicht das Zertifikat für jeden API-Aufruf an ONTAP.

Nachdem alle Objekte für ein neues Cluster erkannt wurden, sammelt Unified Manager historische Performance-Daten für die letzten 15 Tage. Diese Statistiken werden mithilfe der Funktionalität zur Datenerfassung erfasst. Diese Funktion bietet Ihnen sofort nach dem Hinzufügen mehr als zwei Wochen Performance-Informationen für einen Cluster. Nach Abschluss des Datenerfassungszyklus werden Cluster-Performance-Daten in Echtzeit standardmäßig alle fünf Minuten erfasst.

Da die Sammlung von 15 Tagen Leistungsdaten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zu staffeln, so dass Datenkontinuitätssammlung nicht auf zu vielen Clustern zur gleichen Zeit laufen. Wenn Sie Unified Manager während des Datenerfassungszeitraums neu starten, wird die Sammlung angehalten, und es werden für den fehlenden Zeitraum Lücken in den Leistungsdiagrammen angezeigt.

Wenn Sie eine Fehlermeldung erhalten, dass Sie das Cluster nicht hinzufügen können, prüfen Sie, ob die folgenden Probleme vorhanden sind:

- Wenn die Uhren auf den beiden Systemen nicht synchronisiert sind und das HTTPS-Zertifikat von Unified Manager nach dem Datum des Clusters liegt. Sie müssen sicherstellen, dass die Uhren mit NTP oder einem ähnlichen Dienst synchronisiert werden.
- Wenn der Cluster die maximale Anzahl von EMS-Benachrichtigungszielen erreicht hat, kann die Unified Manager-Adresse nicht hinzugefügt werden. Standardmäßig können nur 20 EMS-Benachrichtigungsziele auf dem Cluster definiert werden.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

"Installieren einer Zertifizierungsstelle, die signiert ist und ein HTTPS-Zertifikat zurückgegeben hat"

Cluster werden bearbeitet

Sie können die Einstellungen eines vorhandenen Clusters, z. B. Host-Name oder IP-Adresse, Benutzername, Passwort und Port, über das Dialogfeld Cluster bearbeiten ändern.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.

Ab Unified Manager 9.7 können Cluster nur mit HTTPS hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie auf der Seite **Cluster Setup** den Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Cluster bearbeiten** die Werte nach Bedarf. + Wenn Sie die Details für einen zu Unified Manager 9.12 hinzugefügten Cluster geändert haben, können Sie die Zertifikatsdetails für die gegenseitige TLS-Kommunikation auf Grundlage der ONTAP-Version anzeigen. Weitere Informationen zur ONTAP-Version finden Sie unter "Zertifikate für die gegenseitige TLS-Kommunikation". + Sie können die Zertifikatsdetails anzeigen, indem Sie auf **Zertifikatdetails** klicken. Wenn das Zertifikat abgelaufen ist, klicken Sie auf die Schaltfläche **regenerieren**, um das neue Zertifikat einzubauen.
4. Klicken Sie Auf **Absenden**.
5. Klicken Sie im Dialogfeld Host autorisieren auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie Auf **Ja**.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

Cluster werden entfernt

Sie können ein Cluster mithilfe der Seite Cluster-Setup aus Unified Manager entfernen. Beispielsweise können Sie ein Cluster entfernen, wenn die Cluster-Erkennung ausfällt oder wenn Sie ein Storage-System stilllegen möchten.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle oder die Speicheradministratorrolle verfügen.

Durch diese Aufgabe wird das ausgewählte Cluster aus Unified Manager entfernt. Nachdem ein Cluster entfernt wurde, wird er nicht mehr überwacht. Die beim entfernten Cluster registrierte Instanz des Unified Manager wird auch vom Cluster nicht registriert.

Durch das Entfernen eines Clusters werden auch alle seine Storage-Objekte, historischen Daten, Storage-Services und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden auf den Bestandsseiten und den Detailseiten nach dem nächsten Datenerfassungszyklus angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Wählen Sie auf der Seite Cluster Setup den Cluster aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Dialogfeld **Datenquelle entfernen** auf **Entfernen**, um die Anforderung zum Entfernen zu bestätigen.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Cluster-Liste und der Details"

Cluster-Erkennung neu ermitteln

Sie können ein Cluster manuell auf der Seite Cluster Setup neu finden, um die neuesten Informationen über den Systemzustand, den Monitoring-Status und den Performance-Status des Clusters abzurufen.

Sie können ein Cluster manuell wiederentdecken, wenn Sie den Cluster aktualisieren möchten - z. B. indem Sie die Größe eines Aggregats erhöhen, wenn der Speicherplatz nicht ausreicht - und Sie möchten, dass Unified Manager die Änderungen entdeckt, die Sie vornehmen.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) kombiniert wird, löst das Pairing die Neuerfassung der von WFA gecachten Daten aus.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Cluster-Setup**.
2. Klicken Sie auf der Seite **Cluster Setup** auf **Wiederentdecken**.

   Unified Manager erkennt das ausgewählte Cluster erneut und zeigt den neuesten Zustand und Performance-Status an.

Verwandte Informationen

"Anzeigen der Cluster-Liste und der Details"

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, 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.