



Einrichtung von Unified Manager für Hochverfügbarkeit

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

Inhalt

- Einrichtung von Unified Manager für Hochverfügbarkeit 1
 - Anforderungen an Unified Manager in VCS 1
 - Installieren von Unified Manager auf VCS 2
 - Konfiguration von Unified Manager mit VCS mithilfe von Konfigurationsskripten 2
 - Unified Manager Service-Ressourcen für VCS Konfiguration 4
 - Aktualisierung einer vorhandenen Unified Manager-Einrichtung für hohe Verfügbarkeit 4

Einrichtung von Unified Manager für Hochverfügbarkeit

Mithilfe des Veritas Cluster Server (VCS) können Sie eine Konfiguration mit hoher Verfügbarkeit erstellen. Das Hochverfügbarkeits-Setup bietet Failover-Funktionen und hilft bei Disaster Recovery.

In einer Hochverfügbarkeitseinrichtung bleibt jeweils nur ein Node aktiv. Wenn ein Node ausfällt, erkennt der VCS-Service dieses Ereignis und überträgt sofort die Kontrolle auf den anderen Node. Der zweite Node im Setup wird aktiv und beginnt mit der Bereitstellung von Services. Der Failover-Prozess erfolgt automatisch.

Ein VCS Cluster, der mit dem Unified Manager Server konfiguriert ist, besteht aus zwei Knoten, wobei jeder Knoten dieselbe Version des Unified Manager ausführt. Alle Unified Manager-Serverdaten müssen für den Zugriff von einer gemeinsam genutzten Datenfestplatte konfiguriert werden.

Nach der Installation von Unified Manager in VCS müssen Sie Unified Manager konfigurieren, um in der VCS-Umgebung arbeiten zu können. Über Konfigurationsskripte kann Unified Manager für die Arbeit in VCS Umgebungen eingerichtet werden.

Anforderungen an Unified Manager in VCS

Vor der Installation von Unified Manager in einer Veritas Cluster Server (VCS) Umgebung müssen Sie sicherstellen, dass die Clusterknoten ordnungsgemäß konfiguriert sind, um Unified Manager zu unterstützen.

Sie müssen sicherstellen, dass die VCS-Konfiguration die folgenden Anforderungen erfüllt:

- Auf beiden Cluster-Nodes muss eine unterstützte Betriebssystemversion ausgeführt werden.
- Die gleiche Version von Unified Manager muss auf beiden Cluster-Nodes mithilfe des gleichen Pfads installiert werden.
- Der MySQL-Benutzer auf beiden Knoten muss die gleiche Benutzer-ID und Gruppen-ID haben.
- Es müssen native ext3-, ext4-Dateisysteme und LVM (Logical Volume Manager) verwendet werden.
- Unified Manager muss über Fibre Channel (FC) oder iSCSI mit dem Storage-System verbunden sein.

Sie müssen außerdem sicherstellen, dass die FC-Verbindung aktiv ist und dass die auf den Storage-Systemen erstellten LUNs beiden Cluster-Nodes zugänglich sind.

- Die gemeinsam genutzte Datenfestplatte muss über ausreichend Speicherplatz (mindestens 80 GB) für die Unified Manager-Datenbank, Berichte, Zertifikate und Skript-Plug-in-Ordner verfügen.
- Auf jedem System müssen mindestens zwei Netzwerkschnittstellen eingerichtet sein: Eine für die Node-zu-Node-Kommunikation und die andere für die Node-to-Client-Kommunikation.

Der Name der für die Kommunikation zwischen Nodes und Clients verwendeten Netzwerkschnittstelle muss auf beiden Systemen identisch sein.

- Zwischen den Cluster-Nodes muss eine separate Heartbeat-Verbindung hergestellt werden. Andernfalls wird die Netzwerkschnittstelle für die Kommunikation zwischen den Cluster-Nodes verwendet.
- Optional: SnapDrive für UNIX sollte verwendet werden, um einen freigegebenen Speicherort zu erstellen, der beiden Knoten in einem hochverfügbaren Setup zugänglich ist.

Informationen zum Installieren und Erstellen eines gemeinsam genutzten Speicherorts finden Sie im Handbuch *SnapDrive for UNIX Installation and Administration*. Sie können auch LUNs über SnapDrive oder die Befehlszeilenschnittstelle des Storage-Systems verwalten. Weitere Informationen finden Sie in der Kompatibilitätsmatrix für SnapDrive für UNIX.

- Für die SnapDrive- und VCS-Anwendungen muss zusätzlicher RAM verfügbar sein.

Installieren von Unified Manager auf VCS

Zur Konfiguration der Hochverfügbarkeit müssen Sie Unified Manager auf beiden Cluster-Knoten von VCS installieren.

Bevor Sie beginnen

- VCS muss auf beiden Knoten des Clusters installiert und konfiguriert sein.

Weitere Informationen zur Installation von VCS finden Sie in der Anleitung zum *Veritas Cluster Server 6.2.1 Installation Guide*.

- Sie müssen über klare Root-Berechtigungen verfügen, um sich bei der Unified Manager-Serverkonsole anzumelden.

Über diese Aufgabe

Sie müssen beide Instanzen von Unified Manager konfigurieren, um dieselbe Datenbank zu verwenden und denselben Satz Nodes zu überwachen.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.
2. Installation von Unified Manager auf dem ersten Node

[Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS](#)

3. Wiederholen Sie die Schritte 1 und 2 auf dem zweiten Node des Clusters.
4. Melden Sie sich bei der zweiten Instanz von Unified Manager als Root-Benutzer beim Red hat Enterprise Linux oder CentOS Server an und geben Sie das gleiche umadmin Passwort ein, das Sie in der ersten Instanz von Unified Manager festgelegt haben.`passwd umadmin`

Konfiguration von Unified Manager mit VCS mithilfe von Konfigurationsskripten

Sie können Unified Manager mit Veritas Cluster Server (VCS) mit Konfigurationsskripten konfigurieren.

Bevor Sie beginnen

- Unified Manager muss auf beiden Knoten in der VCS Setup installiert sein.
- Das XML: LibXML-Modul muss mit Perl gebündelt werden, damit VCS-Skripte funktionieren können.

- Sie müssen eine gemeinsame LUN mit ausreichender Größe erstellt haben, um den Quell-Unified Manager-Daten gerecht zu werden.
- Sie müssen den absoluten Mount-Pfad angegeben haben, damit das Skript funktioniert.

Das Skript funktioniert nicht, wenn Sie einen Ordner im Mount-Pfad erstellen.

- Sie müssen das heruntergeladen haben `ha_setup.pl` Skript an `/opt/netapp/ocum/scripts`.

Über diese Aufgabe

Im VCS-Setup ist der Knoten, für den die virtuelle IP-Schnittstelle und der Mount Point aktiv sind, der erste Knoten. Der andere Node ist der zweite Node.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.

Im Hochverfügbarkeitseinstellungen müssen Sie alle Unified Manager-Services auf dem zweiten Node angehalten haben.

2. Fügen Sie das VCS-Installationsverzeichnis hinzu `/opt/VRTSvcs/bin` Zum PFAD Umgebungsvariable.
3. Wenn Sie eine vorhandene Unified Manager Einrichtung konfigurieren, erstellen Sie ein Unified Manager Backup und erstellen Sie das Support Bundle.

4. Führen Sie die aus `ha_setup.pl` Skript: `perl ha_setup.pl --first -t vcs -g group_name -e eth_name -i cluster_ip -m net_mask -n fully_qualified_cluster_name -f mount_path -v volume_group -d disk_group -l install_dir -u user_name -p password`

```
perl \ha_setup.pl --first -t vcs -g umgroup -e eth0 -i 10.11.12.13 -m
255.255.255.0 -n cluster.eng.company.com -f /mnt/ocumdb -v ocumdb_SdHv -d
ocumdb_SdDg -l /opt/netapp/ -u admin -p wx17yz
```

5. Überprüfen Sie mithilfe der Veritas Operations Manager Webkonsole oder VCS Cluster Manager, ob eine Failover-Gruppe erstellt wird und ob die Unified Manager Serverdienste, Bereitstellungspunkt, virtuelle IP, Netzwerkschnittstellenkarte (NIC) und Volume-Gruppe der Cluster-Gruppe hinzugefügt werden.
6. Verschieben Sie die Unified Manager Service-Gruppe manuell zum sekundären Node und überprüfen Sie, ob ein Cluster-Failover funktioniert.
7. Überprüfen Sie, ob VCS auf den zweiten Knoten des Clusters umgeschaltet wurde.

Vergewissern Sie sich, dass der Datenmounten, die virtuelle IP, die Volume-Gruppe und die NIC auf dem zweiten Node des Clusters online sind.

8. Beenden Sie Unified Manager mit Veritas Operations Manager.
9. Führen Sie die aus `perl ha_setup.pl --join -t vcs -f`mount_path` Befehl im zweiten Node des Clusters, sodass der Unified Manager Server auf die LUN verweist.
10. Überprüfen Sie, ob die Unified Manager Server Services auf dem zweiten Knoten des Clusters ordnungsgemäß gestartet werden.
11. Generieren Sie das Unified Manager-Zertifikat erneut, nachdem Sie die Konfigurationsskripte ausgeführt haben, um die globale IP-Adresse abzurufen.

- a. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im Menü **Setup** auf **HTTPS-Zertifikat**.
- b. Klicken Sie auf **HTTPS-Zertifikat erneut erstellen**.

Das neu erstellte Zertifikat enthält nur die Cluster-IP-Adresse, nicht den vollqualifizierten Domännennamen (FQDN). Zur Einrichtung von Unified Manager für Hochverfügbarkeit müssen Sie die globale IP-Adresse verwenden.

12. Greifen Sie über folgende Ressourcen auf die Unified Manager-UI zu: `https://<FQDN of Global IP>`

Nachdem Sie fertig sind

Nach der Konfiguration der Hochverfügbarkeit müssen Sie einen freigegebenen Backup-Speicherort erstellen. Der freigegebene Speicherort ist erforderlich, um die Backups zu enthalten, die Sie vor und nach dem Failover erstellen. Die beiden Nodes in der Hochverfügbarkeitseinrichtung müssen auf den gemeinsamen Speicherort zugreifen können.

Unified Manager Service-Ressourcen für VCS Konfiguration

Sie müssen die Cluster Service Ressourcen von Unified Manager zu Veritas Cluster Server (VCS) hinzufügen. Diese Cluster-Service-Ressourcen werden für verschiedene Zwecke eingesetzt, beispielsweise für das Monitoring von Storage-Systemen, die Planung von Jobs, Verarbeitungsereignisse und das Monitoring aller anderen Unified Manager Services.

Die folgende Tabelle enthält die Kategorie aller Unified Manager Services:

Kategorie	Services
Speicherressource	<ul style="list-style-type: none"> • vol • mount
Datenbankressource	<ul style="list-style-type: none"> • mysqld
Netzwerkressource	<ul style="list-style-type: none"> • nic • vip
Unified Manager Ressource	<ul style="list-style-type: none"> • ocie • ocieau

Aktualisierung einer vorhandenen Unified Manager-Einrichtung für hohe Verfügbarkeit

Sie können Ihre vorhandene Unified Manager Installation aktualisieren und Ihre Setup-Umgebung auf hohe Verfügbarkeit konfigurieren.

Bevor Sie beginnen

- Sie müssen ein Backup- und Support-Bundle Ihrer vorhandenen Daten erstellt haben.
- Sie müssen über die Rolle „OnCommand Administrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen dem Cluster einen zweiten Knoten hinzugefügt und Veritas Cluster Server (VCS) auf dem zweiten Knoten installiert haben.

Siehe *Veritas Cluster Server 6.2.1 Installation Guide*.

- Der neu hinzugefügte Node muss konfiguriert werden, um auf denselben freigegebenen Speicherort wie den des bestehenden Nodes im Hochverfügbarkeitsaufbau zuzugreifen.

Schritte

1. Melden Sie sich bei dem neuen Node des Clusters an.
2. Installation von Unified Manager auf dem Knoten

[Installation von Unified Manager unter Red hat Enterprise Linux oder CentOS](#)

3. Konfigurieren Sie den Unified Manager-Server mithilfe von Konfigurationsskripten auf dem bestehenden Node mit Daten.
4. Initiieren Sie ein manuelles Failover auf den zweiten Node.
5. Führen Sie die aus `perl ha_setup.pl --join -t vcs -f ``mount_path` Befehl auf dem zweiten Node des Clusters, sodass der Unified Manager Server Daten auf die Shared LUN verweist.
6. Wenn OnCommand Workflow Automation (WFA) für Unified Manager konfiguriert ist, deaktivieren Sie die WFA Verbindung und konfigurieren Sie sie dann neu.
7. Wenn SnapProtect mit Unified Manager konfiguriert ist, konfigurieren Sie SnapProtect mit einer neuen Cluster-IP-Adresse und den vorhandenen Storage-Richtlinien neu.
8. Generieren Sie die benutzerdefinierten Berichte erneut, und fügen Sie diese Berichte mit der neuen Cluster-IP-Adresse zu Unified Manager hinzu.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.