



Die Erweiterung abschließen

System Manager Classic

NetApp
June 22, 2024

Inhalt

- Die Erweiterung abschließen 1
 - Konfigurieren Sie die Details zum Node in System Manager 1
 - Konfigurieren Sie AutoSupport auf den neuen Nodes 1
 - Konfigurieren Sie das Service Processor Netzwerk 2
 - Überprüfen Sie die Konfiguration des erweiterten Clusters 4
 - Generieren Sie eine AutoSupport-Meldung über den Abschluss der Erweiterung 5
 - Aktualisieren Sie die LUN-Pfade für die neuen Nodes 6

Die Erweiterung abschließen

Nachdem beide Nodes dem Cluster hinzugefügt wurden, müssen Sie die Konfiguration der neu hinzugefügten Nodes beenden, indem Sie AutoSupport konfigurieren und das SP-Netzwerk abschließen. Anschließend validieren Sie das erweiterte Cluster und generieren eine AutoSupport-Meldung, um die Erweiterung abzuschließen. Wenn das Cluster SAN verwendet, sollten Sie die LUN-Pfade aktualisieren.

Konfigurieren Sie die Details zum Node in System Manager

Mit System Manager können Sie die LIF- und Service-Prozessor-Einstellungen für das Node-Management für die neu hinzugefügten Nodes konfigurieren.

Bevor Sie beginnen

- Im Standard-IPspace muss für die LIF-Erstellung eine ausreichende Anzahl von Ports vorhanden sein.
- Alle Ports müssen betriebsbereit sein und ausgeführt werden.

Schritte

1. Konfiguration des Node-Managements:
 - a. Geben Sie die IP-Adresse in das Feld * IP-Adresse* ein.
 - b. Wählen Sie den Port für die Knotenverwaltung im Feld **Port** aus.
 - c. Geben Sie die Netzmaske und Gateway-Details ein.
2. Konfigurieren Sie die Service Processor-Einstellungen:
 - a. Aktivieren Sie das Kontrollkästchen **Standard-einstellungen überschreiben**, um die Standardwerte zu überschreiben.
 - b. Geben Sie IP-Adresse, Netmask und Gateway-Details ein.
3. Klicken Sie auf **Senden und Fortfahren**, um die Netzwerkkonfiguration der Knoten abzuschließen.
4. Überprüfen Sie die Details der Knoten auf der Seite **Zusammenfassung**.

Nächste Schritte

- Wenn Ihr Cluster geschützt ist, sollten Sie die erforderliche Anzahl von Intercluster LIFs in den neu hinzugefügten Nodes erstellen, um TeilPeering und einen ungesunden Schutz zu vermeiden.
- Wenn SAN-Datenprotokolle in Ihrem Cluster aktiviert sind, sollten Sie die erforderliche Anzahl an SAN-Daten-LIFs für die Datenbereitstellung erstellen.

Konfigurieren Sie AutoSupport auf den neuen Nodes

Nachdem Sie einem Cluster Nodes hinzugefügt haben, müssen Sie AutoSupport auf den Nodes konfigurieren.

Bevor Sie beginnen

AutoSupport muss auf den vorhandenen Nodes des Clusters eingerichtet werden.

Über diese Aufgabe

Sie müssen dieses Verfahren auf beiden Knoten durchführen.

Schritte

1. Zeigen Sie die AutoSupport-Konfiguration mit dem `an system node autosupport show` Befehl mit dem `-node` Parameter gesetzt auf einen der Nodes im ursprünglichen Cluster.

```
cluster1::> system node autosupport show -node cluster1-1
                Node: cluster1-1
                State: enable
                SMTP Mail Hosts: smtp.example.com
...

```

2. Konfigurieren Sie AutoSupport auf einem der neu hinzugefügten Nodes so, dass sie mithilfe von auf den vorhandenen Nodes konfiguriert wird `system node autosupport modify` Befehl.

```
cluster1::> system node autosupport modify -node cluster1-3 -state
enable -mail-hosts smtp.example.com -from alerts@node3.example.com -to
support@example.com -support enable -transport https -noteto
pda@example.com -retry-interval 23m

```

3. Wiederholen Sie den vorherigen Schritt für den anderen neu hinzugefügten Node.

Konfigurieren Sie das Service Processor Netzwerk

Nachdem Sie ein Cluster erweitert haben, müssen Sie auf den neuen Nodes das SP-Netzwerk (Service Processor) konfigurieren. Wenn der SP die manuelle Netzwerkkonfiguration verwendet, müssen Sie die IP-Adressen für den SP auf den neuen Nodes konfigurieren. Wenn der SP eine automatische Netzwerkkonfiguration verwendet, müssen Sie die ausgewählten IP-Adressen angeben.

Schritte

1. Wenn der Cluster-SP eine manuelle Netzwerkkonfiguration verwendet, konfigurieren Sie auf beiden Nodes für das SP-Netzwerk mithilfe der IP-Adressen `system service-processor network modify` Befehl.

Mit den folgenden Befehlen wird das SP-Netzwerk in den Cluster1-3- und cluster1-4-Knoten konfiguriert:

```
cluster1::> system service-processor network modify -node cluster1-3
-address-family IPv4 -enable true -ip-address 192.168.123.98-netmask
255.255.255.0 -gateway 192.168.123.1
cluster1::> system service-processor network modify -node cluster1-4
-address-family IPv4 -enable true -ip-address 192.168.123.99 -netmask
255.255.255.0 -gateway 192.168.123.1

```

2. Überprüfen Sie mithilfe von, ob das SP-Netzwerk bei beiden neuen Nodes ordnungsgemäß konfiguriert ist
`system service-processor network show` Befehl für jeden Node.

Der Status sollte sein `succeeded`. In allen Situationen ist eine Überprüfung erforderlich. Selbst wenn das SP-Netzwerk automatisch konfiguriert wurde, sollten Sie überprüfen, ob es erfolgreich konfiguriert wurde, und Sie müssen ermitteln, welche IP-Adressen zugewiesen wurden.

Die folgende Ausgabe gibt an, dass sowohl für die Cluster-1-3- als auch für die cluster1-4-Nodes ein erfolgreiches Setup des SP-Netzwerks durchgeführt wird:

```
cluster1::> system service-processor network show -node cluster1-3
                                     Address
Node      Status      Family  Link State  IP Address
-----
cluster1-3  online      IPv4    up          192.168.123.98

                                     DHCP: none
                                     MAC Address: 00:a0:98:43:a1:1e
                                     Network Gateway: 10.60.172.1
Network Mask (IPv4 only): 255.255.255.0
Prefix Length (IPv6 only): -
IPv6 RA Enabled: -
Subnet Name: -
SP Network Setup Status: succeeded
...

cluster1::> system service-processor network show -node cluster1-4
                                     Address
Node      Status      Family  Link State  IP Address
-----
cluster1-4  online      IPv4    up          192.168.123.99

                                     DHCP: none
                                     MAC Address: 00:a0:98:43:a1:1e
                                     Network Gateway: 10.60.172.1
Network Mask (IPv4 only): 255.255.255.0
Prefix Length (IPv6 only): -
IPv6 RA Enabled: -
Subnet Name: -
SP Network Setup Status: succeeded
...
```

3. Wenn an Ihrem Standort normalerweise DNS-Einträge für das SP-Netzwerk vorhanden sind, vergewissern Sie sich, dass die DNS-Einträge für die neuen Knoten erstellt werden.

Überprüfen Sie die Konfiguration des erweiterten Clusters

Nach dem erweitern des Clusters müssen Sie die Konfiguration validieren, indem Sie Config Advisor ausführen und einige Befehle verwenden, die den Cluster-Zustand und die Cluster-Replizierungsringe überprüfen.

Schritte

1. Überprüfen Sie den Zustand der Konfiguration, indem Sie Config Advisor ausführen:

- a. Starten Sie Config Advisor, und klicken Sie dann auf **Daten sammeln**.

Config Advisor zeigt alle gefundenen Probleme an.

- b. Wenn Probleme gefunden werden, beheben Sie sie, und führen Sie das Tool erneut aus.

2. Stellen Sie sicher, dass sich alle Nodes im Cluster mithilfe von in einem ordnungsgemäßen Zustand befinden `cluster show` Befehl.

```
cluster-1::> cluster show
Node                Health  Eligibility
-----
cluster1-1          true   true
cluster1-2          true   true
cluster1-3          true   true
cluster1-4          true   true
4 entries were displayed.
```

3. Stellen Sie sicher, dass die Cluster-Replikationsringe die gleiche Epoche, den gleichen Datenbankzeitraum und die gleichen Datenbanktransaktionsnummern auf allen Knoten im Cluster haben:

Am einfachsten können Sie die Transaktionsnummern vergleichen, wenn Sie sie jeweils für einen Einheitennamen anzeigen.

- a. Stellen Sie die Berechtigungsebene mithilfe der auf Erweiterungssatz ein `set -privilege advanced` Befehl.
- b. Zeigen Sie Cluster-Ringinformationen über den Namen der ersten Einheit mithilfe von an `cluster ring show` Befehl mit dem `-unitname mgmt` Parameter und stellen Sie sicher, dass alle Knoten die gleiche Nummer in den Spalten `Epoch`, `DB Epoch` und `DB Trnxs` haben.

```

cluster-1::*> cluster ring show -unitname mgmt
Node          UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
cluster1-1
      mgmt      2          2          959      cluster1-1
                                           master
cluster1-2
      mgmt      2          2          959      cluster1-2
                                           secondary
cluster1-3
      mgmt      2          2          959      cluster1-3
                                           master
cluster1-4
      mgmt      2          2          959      cluster1-3
                                           secondary

4 entries were displayed.

```

- c. Wiederholen Sie den Befehl mit dem `-unitname vldb` Parameter.
- d. Wiederholen Sie den Befehl mit dem `-unitname vifmgr` Parameter.
- e. Wiederholen Sie den Befehl mit dem `-unitname bcomd` Parameter.
- f. Wiederholen Sie den Befehl mit dem `-unitname crs` Parameter.
- g. Stellen Sie die Berechtigungsebene mit zurück `set -privilege admin` Befehl.

Generieren Sie eine AutoSupport-Meldung über den Abschluss der Erweiterung

Nachdem Sie ein Cluster erweitert haben, sollten Sie eine AutoSupport Meldung senden, um anzugeben, dass die Erweiterung abgeschlossen ist. Diese Nachricht teilt internen und externen Support-Mitarbeitern mit, dass die Erweiterung abgeschlossen ist und als Zeitstempel für jegliche spätere Fehlerbehebung fungiert.

Bevor Sie beginnen

AutoSupport muss eingerichtet sein.

Schritte

1. Senden Sie für jeden Node im Cluster eine AutoSupport Meldung mithilfe von `system node autosupport invoke` Befehl.

Sie müssen einmal die Meldung für jeden Node im Cluster ausgeben, einschließlich der neu hinzugefügten Nodes.

Wenn Sie einem 2-Node-Cluster zwei Nodes hinzugefügt haben, müssen Sie die Meldung viermal senden.

```
cluster1::> system node autosupport invoke -node * -message "cluster
expansion complete" -type all
The AutoSupport was successfully invoked on node "cluster1-1". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-2". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-3". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-4". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
4 entries were acted on.
```

Aktualisieren Sie die LUN-Pfade für die neuen Nodes

Wenn Ihr Cluster für SAN konfiguriert ist, müssen Sie SAN-LIFs auf den neu hinzugefügten Nodes erstellen und anschließend Pfade aktualisieren.

Über diese Aufgabe

Diese Vorgehensweise ist nur erforderlich, wenn das Cluster LUNs enthält. Wenn das Cluster nur Dateien enthält, können Sie diesen Vorgang überspringen.

Schritte

1. Erstellen Sie für jede Storage Virtual Machine (SVM) im Cluster neue LIFs für die neu hinzugefügten Nodes:
 - a. Identifizieren Sie die SVMs, die FC- oder iSCSI-Protokolle mithilfe von verwenden `vserver show` Befehl mit dem `-fields allowed-protocols` Parameter und Überprüfung der Ausgabe.


```
cluster1::> vserver show -fields allowed-protocols
vserver allowed-protocols
-----
vs1      cifs,ndmp
vs2      fcp
vs3      iscsi
...
```

- b. Erstellen Sie für jede SVM, die FC oder iSCSI verwendet, mithilfe der mindestens zwei Daten-LIFs auf jedem der neu hinzugefügten Nodes `network interface create` Befehl mit dem `-role data` Parameter.

```
cluster1::> network interface create -vserver vs1 -lif lif5 -role
data
-data-protocol iscsi -home-node cluster1-3 -home-port e0b
-address 192.168.2.72 -netmask 255.255.255.0
```

- c. Vergewissern Sie sich bei jeder SVM, dass mithilfe der LIFs für alle Nodes im Cluster vorhanden sind `network interface show` Befehl mit dem `-vserver` Parameter.

2. Portsätze aktualisieren:

- Bestimmen Sie mithilfe des, ob Portsätze vorhanden sind `lun portset show` Befehl.
- Wenn Sie die neuen LIFs für vorhandene Hosts sichtbar machen möchten, fügen Sie mithilfe der jede neue LIF zu den Portsätzen hinzu `lun portset add` Einmal-Befehl für jede LIF.

3. Wenn Sie FC oder FCoE verwenden, aktualisieren Sie Zoning:

- Überprüfen Sie, ob das Zoning ordnungsgemäß eingerichtet ist, um die vorhandenen Initiator-Ports auf dem Host zu aktivieren, um eine Verbindung zu den neuen Ziel-Ports auf den neuen Nodes herzustellen.
- Aktualisieren Sie das Switch-Zoning, um die neuen Nodes mit vorhandenen Initiatoren zu verbinden.

Das Zoning-Setup variiert abhängig von dem Switch, den Sie verwenden.

- Wenn Sie LUNs zu den neuen Nodes verschieben möchten, zeigen Sie die neuen Pfade zu den Hosts mithilfe von `an lun mapping add-reporting-nodes` Befehl.

- Suchen Sie auf allen Host-Betriebssystemen nach, um die neu hinzugefügten Pfade zu ermitteln.
- Entfernen Sie je nach den Host-Betriebssystemen alle veralteten Pfade.
- Fügen Sie Pfade zu Ihrer MPIO-Konfiguration hinzu oder entfernen Sie diese.

Verwandte Informationen

["San-Konfiguration"](#)

["SAN-Administration"](#)

Copyright-Informationen

Copyright © 2024 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.