Managen des SVM-Scoped NDMP-Modus für FlexVol Volumes

ONTAP 9

NetApp
April 24, 2024

Inhalt

Managen des SVM-Scoped NDMP-Modus für FlexVol Volumes

Überblick über das Managen des SVM-Scoped NDMP-Modus für FlexVol Volumes

Sie können NDMP auf Basis pro SVM mit den NDMP-Optionen und -Befehlen verwalten. Sie können die NDMP-Optionen mit dem ändern `vserver services ndmp modify` Befehl. Im SVM-Scoped NDMP-Modus ist die Benutzerauthentifizierung in den rollenbasierten Zugriffssteuerungsmechanismus integriert.

Sie können NDMP in die Liste der zugelassenen oder unzulässigen Protokolle hinzufügen, indem Sie das verwenden `vserver modify` Befehl. Standardmäßig befindet sich NDMP in der Liste der zugelassenen Protokolle. Wenn der Liste der nicht zulässigen Protokolle NDMP hinzugefügt wird, können NDMP-Sitzungen nicht erstellt werden.

Sie können den LIF-Typ steuern, auf dem eine NDMP-Datenverbindung mithilfe von hergestellt wird `-preferred-interface-role` Option. Während einer NDMP-Datenverbindung wählt NDMP eine IP-Adresse aus, die zum von dieser Option angegebenen LIF-Typ gehört. Wenn die IP-Adressen keiner dieser LIF-Typen angehören, kann die NDMP-Datenverbindung nicht hergestellt werden. Weitere Informationen zum `-preferred-interface-role` Weitere Informationen finden Sie auf den man-Pages.

Weitere Informationen zum `vserver services ndmp modify` Befehl, siehe die man-Pages.

Verwandte Informationen

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

Was ist Cluster-bewusste Backup-Erweiterung

"ONTAP-Konzepte"

Welcher SVM-Scoped NDMP-Modus ist

"Systemadministration"

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

Sie können das verwenden `vserver services ndmp` Befehle zum Managen von NDMP auf jeder Storage Virtual Machine (SVM, ehemals bekannt als Vserver)

Ihr Ziel ist	Befehl
Aktivieren des NDMP-Service	`vserver services ndmp on` Der NDMP-Service muss immer auf allen Nodes in einem Cluster aktiviert sein. Sie können den NDMP-Service auf einem Node mit aktivieren `system services ndmp on` Befehl. Standardmäßig ist der NDMP-Service immer auf einem Node aktiviert.
Deaktivieren des NDMP-Dienstes	`vserver services ndmp off`
Zeigt die NDMP-Konfiguration an	`vserver services ndmp show`
NDMP-Konfiguration ändern	`vserver services ndmp modify`
Zeigt die Standard-NDMP-Version an	`vserver services ndmp version`
Zeigt alle NDMP-Sitzungen an	`vserver services ndmp status`
Anzeigen detaillierter Informationen zu allen NDMP-Sitzungen	`vserver services ndmp probe`
Beenden Sie eine angegebene NDMP-Sitzung	`vserver services ndmp kill`
Beenden Sie alle NDMP-Sitzungen	`vserver services ndmp kill-all`
Erstellen Sie das NDMP-Passwort	`vserver services ndmp generate-password`
Zeigt den NDMP-Erweiterungsstatus an	`vserver services ndmp extensions show` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.
Ändern Sie den NDMP-Verlängerungsstatus (aktivieren oder deaktivieren)	`vserver services ndmp extensions modify` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.
Starten Sie die Protokollierung für die angegebene NDMP-Sitzung	`vserver services ndmp log start` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

Ihr Ziel ist	Befehl
Beenden der Protokollierung für die angegebene NDMP-Sitzung	`vserver services ndmp log stop` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages für die `vserver services ndmp` Befehle.

Was ist Cluster-bewusste Backup-Erweiterung

CAB (Cluster Aware Backup) ist eine NDMP v4 Protokollerweiterung. Mit dieser Erweiterung kann der NDMP-Server eine Datenverbindung auf einem Knoten einrichten, der ein Volume besitzt. So kann die Backup-Applikation auch ermitteln, ob sich Volumes und Tape-Geräte auf demselben Node in einem Cluster befinden.

Damit der NDMP-Server den Knoten identifizieren kann, der ein Volume besitzt, und eine Datenverbindung zu einem solchen Knoten hergestellt werden kann, muss die Backup-Anwendung die CAB-Erweiterung unterstützen. CAB-Erweiterung erfordert, dass die Backup-Anwendung den NDMP-Server über das zu sichernde Volume informiert oder wiederhergestellt, bevor die Datenverbindung hergestellt wird. So kann der NDMP-Server den Node ermitteln, der das Volume hostet, und die Datenverbindung entsprechend herstellen.

Mit der von der Backup-Applikation unterstützten CAB-Erweiterung bietet der NDMP-Server Affinitätsdaten zu Volumes und Bandgeräten. Mithilfe dieser Affinitätsdaten kann die Backup-Applikation ein lokales Backup durchführen, statt eines Dreiwege-Backups durchzuführen, wenn sich ein Volume- und ein Tape-Gerät auf demselben Node eines Clusters befinden.

Verfügbarkeit von Volumes und Tape-Geräten für Backup und Restore bei unterschiedlichen LIF-Typen

Sie können eine Backup-Applikation konfigurieren, um eine NDMP-Steuerverbindung auf einem der LIF-Typen in einem Cluster herzustellen. Im NDMP-Modus mit Storage Virtual Machine (SVM) können Sie die Verfügbarkeit von Volumes und Tape-Geräten für Backup- und Restore-Vorgänge bestimmen, abhängig von diesen LIF-Typen und dem Status der CAB-Erweiterung.

In der folgenden Tabelle sind die Verfügbarkeit von Volumes und Bandgeräten für NDMP Control Connection LIF-Typen und der Status der CAB-Erweiterung aufgeführt:

Verfügbarkeit von Volumes und Bandgeräten, wenn CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	Volumes verfügbar für Backup und Restore	Bandgeräte für Backup oder Restore verfügbar
Node-Management-LIF	Alle Volumes werden von einem Node gehostet	Mit dem Node, der die Node-Management-LIF hostet, verbundene Tape-Geräte
Daten-LIF	Nur Volumes, die zu der SVM gehören, die von einem Node gehostet wird, der die Daten-LIF hostet	Keine
Cluster-Management-LIF	Alle Volumes werden von einem Node gehostet, der die LIF zum Cluster-Management hostet	Keine
Intercluster-LIF	Alle Volumes werden von einem Node gehostet, der die Intercluster LIF hostet	Mit dem Node, der die Intercluster-LIF hostet, verbundene Bandgeräte

Verfügbarkeit von Volumes und Bandgeräten, wenn die CAB-Erweiterung von der Backup-Anwendung unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	Volumes verfügbar für Backup und Restore	Bandgeräte für Backup oder Restore verfügbar
Node-Management-LIF	Alle Volumes werden von einem Node gehostet	Mit dem Node, der die Node-Management-LIF hostet, verbundene Tape-Geräte
Daten-LIF	Alle Volumes, die zu der SVM gehören, die die Daten-LIF hostet	Keine
Cluster-Management-LIF	Alle Volumes im Cluster	Alle Bandgeräte im Cluster
Intercluster-LIF	Alle Volumes im Cluster	Alle Bandgeräte im Cluster

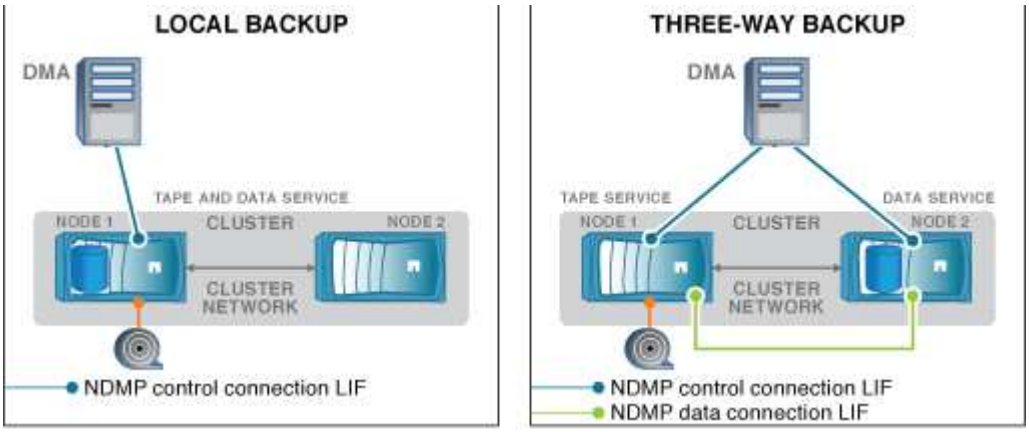
Was ist Affinität Information

Da die Backup-Applikation CAB-orientiert ist, bietet der NDMP-Server einzigartige Speicherinformationen über Volumes und Tape-Geräte. Mithilfe dieser Affinitätsdaten kann die Backup-Applikation ein lokales Backup durchführen, statt eines Backups der drei Wege, wenn sich ein Volume und ein Tape-Gerät dieselbe Affinität teilen.

Wenn die NDMP-Steuerverbindung auf einer Node-Management-LIF aufgebaut ist, Clustermanagement-LIF, Oder eine Intercluster-LIF: Die Backup-Applikation kann die Affinitätsdaten nutzen, um festzustellen, ob sich ein Volume und ein Tape-Gerät auf demselben Node befinden, und kann anschließend ein lokales oder dreistuges Backup oder eine Wiederherstellung durchführen. Wenn die NDMP-Steuerverbindung auf einer

Daten-LIF aufgebaut ist, führt die Backup-Applikation immer ein drei-Wege-Backup durch.

Lokales NDMP-Backup und drei-Wege-NDMP-Backup



Unter Verwendung der Affinitätsdaten zu Volumes und Bandgeräten führt der DMA (Backup-Applikation) eine lokale NDMP-Sicherung auf dem Volume und dem Bandgerät durch, das sich auf Node 1 im Cluster befindet. Wenn das Volume von Node 1 zu Node 2 verschoben wird, ändert sich die Affinität über das Volume und das Tape-Gerät. Daher führt der DMA für ein nachfolgender Backup einen dreistufenden NDMP-Backup-Vorgang durch. Dadurch wird unabhängig vom Node, auf den das Volume verschoben wird, Continuity der Backup-Richtlinie für das Volume sichergestellt.

Verwandte Informationen

Was ist Cluster-bewusste Backup-Erweiterung

Der NDMP-Server unterstützt sichere Kontrollverbindungen im SVM-Scoped-Modus

Eine sichere Steuerungsverbindung zwischen der Data Management Application (DMA) und dem NDMP-Server kann über Secure Sockets (SSL/TLS) als Kommunikationsmechanismus hergestellt werden. Diese SSL-Kommunikation basiert auf den Serverzertifikaten. Der NDMP-Server wartet auf Port 30000 (von der IANA zugewiesen für den „`ndmps`“-Service).

Nach dem Herstellen der Verbindung vom Client auf diesem Port erfolgt der Standard-SSL-Handshake, in dem der Server das Zertifikat dem Client vorstellt. Wenn der Client das Zertifikat akzeptiert, ist der SSL-Handshake abgeschlossen. Nach Abschluss dieses Prozesses wird die gesamte Kommunikation zwischen Client und Server verschlüsselt. Der NDMP-Protokoll-Workflow bleibt exakt wie zuvor. Für die sichere NDMP-Verbindung ist nur eine serverseitige Zertifikatauthentifizierung erforderlich. Ein DMA kann eine Verbindung herstellen, indem er eine Verbindung zum sicheren NDMP-Dienst oder dem Standard-NDMP-Dienst herstellt.

Standardmäßig ist der sichere NDMP-Service für eine Storage Virtual Machine (SVM) deaktiviert. Sie können den sicheren NDMP-Service für eine bestimmte SVM über die aktivieren oder deaktivieren `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` Befehl.

NDMP-Datenverbindungsarten

Im NDMP-Modus (Storage Virtual Machine) mit Scoped (SVM) hängen die unterstützten NDMP-Datenverbindungstypen vom LIF-Steuerverbindung-Typ und dem Status der CAB-Erweiterung ab. Dieser NDMP-Datenverbindungstyp gibt an, ob Sie ein lokales oder dreistuges NDMP-Backup oder eine Wiederherstellung durchführen können.

Sie können eine dreiseitige NDMP-Sicherung oder Wiederherstellung über ein TCP- oder TCP/IPv6-Netzwerk durchführen. In den folgenden Tabellen werden die NDMP-Datenverbindungsarten auf Basis des LIF-Typs NDMP-Steuerverbindung und des Status der CAB-Erweiterung angezeigt.

NDMP-Datenverbindungstyp, wenn CAB-Erweiterung von der Backup-Applikation unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	NDMP-Datenverbindungsart
Node-Management-LIF	LOKAL, TCP, TCP/IPV6
Daten-LIF	TCP, TCP/IPv6
Cluster-Management-LIF	LOKAL, TCP, TCP/IPV6
Intercluster-LIF	LOKAL, TCP, TCP/IPV6

NDMP-Datenverbindungstyp, wenn CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	NDMP-Datenverbindungsart
Node-Management-LIF	LOKAL, TCP, TCP/IPV6
Daten-LIF	TCP, TCP/IPv6
Cluster-Management-LIF	TCP, TCP/IPv6
Intercluster-LIF	LOKAL, TCP, TCP/IPV6

Verwandte Informationen

Was ist Cluster-bewusste Backup-Erweiterung

"Netzwerkmanagement"

Benutzerauthentifizierung im NDMP-Modus mit SVM-Umfang

Die NDMP-Benutzerauthentifizierung ist im NDMP-Modus (Storage Virtual Machine) mit

Scoped integriert in die rollenbasierte Zugriffssteuerung. Im SVM-Kontext muss der NDMP-Benutzer entweder über die Rolle „`vsadmin`“ oder „`vsadmin-Backup`“ verfügen. In einem Cluster-Kontext muss der NDMP-Benutzer entweder über die Rolle „`admin`“ oder „`Backup`“ verfügen.

Neben diesen vordefinierten Rollen kann ein Benutzerkonto, das einer benutzerdefinierten Rolle zugeordnet ist, auch für die NDMP-Authentifizierung verwendet werden, vorausgesetzt, dass die benutzerdefinierte Rolle den Ordner „`vserver Services ndmp`“ in ihrem Befehlsverzeichnis hat und die Zugriffsebene des Ordners nicht „`none`“ ist. In diesem Modus müssen Sie ein NDMP-Passwort für ein bestimmtes Benutzerkonto generieren, das über die rollenbasierte Zugriffssteuerung erstellt wird. Cluster-Benutzer in einer Administrator- oder Backup-Rolle können auf eine Node-Management-LIF, eine Cluster-Management-LIF oder eine Intercluster-LIF zugreifen. Benutzer in einer vsadmin-Backup- oder vsadmin-Rolle können nur auf die Daten-LIF für diese SVM zugreifen. Daher kann die Verfügbarkeit von Volumes und Bandgeräten für Backup- und Wiederherstellungsvorgänge je nach Benutzerrolle unterschiedlich sein.

Dieser Modus unterstützt auch die Benutzerauthentifizierung für NIS- und LDAP-Benutzer. Daher können NIS- und LDAP-Benutzer mit einer gemeinsamen Benutzer-ID und einem gemeinsamen Passwort auf mehrere SVMs zugreifen. Allerdings unterstützt die NDMP-Authentifizierung Active Directory-Benutzer nicht.

In diesem Modus muss ein Benutzerkonto mit der SSH-Anwendung und der Authentifizierungsmethode „`User password`“ verknüpft sein.

Verwandte Informationen

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

"Systemadministration"

"ONTAP-Konzepte"

Erstellen Sie ein NDMP-spezifisches Passwort für NDMP-Benutzer

Im NDMP-Modus (Storage Virtual Machine) mit Scoped (SVM) müssen Sie ein Passwort für eine bestimmte Benutzer-ID generieren. Das generierte Passwort basiert auf dem tatsächlichen Login-Passwort für den NDMP-Benutzer. Wenn sich das tatsächliche Anmeldepasswort ändert, müssen Sie das NDMP-spezifische Passwort erneut generieren.

Schritte

1. Verwenden Sie die `vserver services ndmp generate-password` Befehl zum Generieren eines NDMP-spezifischen Passworts.

   Sie können dieses Passwort bei jedem aktuellen oder zukünftigen NDMP-Vorgang verwenden, der die Passworteingabe erfordert.

   > Im Kontext der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) können Sie NDMP-Passwörter für Benutzer generieren, die nur der SVM angehören.

   Das folgende Beispiel zeigt, wie ein NDMP-spezifisches Passwort für einen Benutzer-ID-Benutzer1 generiert wird:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Wenn Sie das Passwort auf Ihr reguläres Speichersystem-Konto ändern, wiederholen Sie dieses Verfahren, um Ihr neues NDMP-spezifisches Passwort zu erhalten.

Auswirkungen von Tape-Backup- und -Restore-Vorgängen bei Disaster Recovery in der MetroCluster Konfiguration

Sie können Tape-Backup und Restore-Vorgänge gleichzeitig während des Disaster Recovery in einer MetroCluster-Konfiguration durchführen. Die Auswirkungen dieser Vorgänge auf das Disaster Recovery müssen klar sein.

Wenn Backup- und Restore-Prozesse auf Tape auf einem Volume einer SVM in einer Disaster-Recovery-Beziehung durchgeführt werden, können Sie nach einem Switchover und einem Switchback weiterhin inkrementelle Tape-Backups durchführen und Vorgänge wiederherstellen.