데이터 보호 및 재해 복구

ONTAP 9

NetApp
March 04, 2026

목차

데이터 보호 및 재해 복구

클러스터 및 **SVM** 피어링

ONTAP 클러스터 및 **SVM** 피어링에 대해 알아보십시오

소스 및 타겟 클러스터와 소스 및 타겟 스토리지 가상 머신(SVM) 간에 피어 관계를 생성할 수 있습니다. SnapMirror를 사용하여 스냅샷을 복제하려면 먼저 이러한 엔터티 간에 피어 관계를 생성해야 합니다.

ONTAP 9.3은 클러스터와 SVM 간의 피어 관계를 간편하게 구성할 수 있도록 향상된 기능을 제공합니다. 모든 ONTAP 9 버전에서 클러스터 및 SVM 피어링 절차를 사용할 수 있습니다. 해당 버전의 ONTAP에 적합한 절차를 사용해야 합니다.

System Manager나 자동화된 스크립팅 도구가 아니라 CLI(Command-Line Interface)를 사용하여 절차를 수행합니다.

클러스터 및 **SVM** 피어링을 준비합니다

ONTAP 피어링 기초

SnapMirror를 사용하여 스냅샷을 복제하려면 소스 및 대상 클러스터 간, 소스 및 대상 SVM 간에 _peer 관계_를 생성해야 합니다. 피어 관계는 클러스터와 SVM이 데이터를 안전하게 교환할 수 있도록 네트워크 연결을 정의합니다.

피어 관계의 클러스터와 SVM은 _인터클러스터 논리 인터페이스(LIF)를 사용하여 인터클러스터 네트워크를 통해 통신합니다. _ 인터클러스터 LIF는 일반적으로 "기본 인터클러스터 코어" 네트워크 인터페이스 서비스 정책을 사용하여 생성되는 LIF입니다. 피어링된 클러스터의 모든 노드에 대한 인터클러스터 LIF를 생성해야 합니다.

인터클러스터 LIF는 해당 LIF가 할당된 시스템 SVM에 속하는 경로를 사용합니다. ONTAP에서 IPspace 내에서 클러스터 레벨 통신을 위한 시스템 SVM을 자동으로 생성합니다.

팬아웃 및 캐스케이드 토폴로지가 모두 지원됩니다. 계단식 토폴로지에서는 1차 클러스터와 2차 클러스터 간에 그리고 2차 클러스터와 3차 클러스터 간에 인터클러스터 네트워크만 만들어야 합니다. 1차 클러스터와 3차 클러스터 간에 인터클러스터 네트워크를 생성할 필요가 없습니다.

> 관리자가 기본 인터클러스터 서비스 정책에서 인터클러스터 코어 서비스를 제거할 수 있지만 권장하지는 않습니다. 이 경우 "default-인터클러스터"를 사용하여 만든 LIF는 실제로 인터클러스터 LIF가 아닙니다. 기본 인터클러스터 서비스 정책에 인터클러스터 코어 서비스가 포함되어 있는지 확인하려면 다음 명령을 사용합니다.
>
> 네트워크 인터페이스 서비스 정책 표시 정책 기본값 - 인터클러스터
>
> 에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 피어링 사전 요구사항

클러스터 피어링을 설정하기 전에 연결, 포트, IP 주소, 서브넷, 방화벽, 클러스터 명명

요구사항이 충족됩니다.

> ONTAP 9.6부터 클러스터 피어링은 데이터 복제를 위한 TLS 1.2 AES-256 GCM 암호화 지원을 기본적으로 제공합니다. 암호화를 사용하지 않는 경우에도 클러스터 피어링이 작동하려면 기본 보안 암호("PSK-AES256-GCM-SHA384")가 필요합니다.
>
> ONTAP 9.11.1부터 DHE-PSK 보안 사이퍼를 기본적으로 사용할 수 있습니다.
>
> ONTAP 9.15.1부터 클러스터 피어링은 기본적으로 데이터 복제를 위한 TLS 1.3 암호화 지원을 제공합니다.

연결 요구 사항

로컬 클러스터의 모든 인터클러스터 LIF는 원격 클러스터의 모든 인터클러스터 LIF와 통신할 수 있어야 합니다.

반드시 필요한 것은 아니지만 일반적으로 동일한 서브넷에 있는 인터클러스터 LIF에 사용되는 IP 주소를 구성하는 것이 더 간단합니다. IP 주소는 데이터 LIF와 동일한 서브넷 또는 다른 서브넷에 상주할 수 있습니다. 각 클러스터에 사용되는 서브넷은 다음 요구사항을 충족해야 합니다.

- 서브넷은 인터클러스터 통신에 사용되는 포트를 포함하는 브로드캐스트 도메인에 속해야 합니다.
- 서브넷에는 노드당 하나의 인터클러스터 LIF에 할당할 수 있는 충분한 IP 주소가 있어야 합니다.

  예를 들어, 4노드 클러스터에서 인터클러스터 통신에 사용되는 서브넷에는 사용 가능한 IP 주소 4개가 있어야 합니다.

각 노드에는 인터클러스터 네트워크의 IP 주소를 사용하는 인터클러스터 LIF가 있어야 합니다.

인터클러스터 LIF는 IPv4 주소 또는 IPv6 주소를 가질 수 있습니다.

> ONTAP를 사용하면 필요에 따라 두 프로토콜을 인터클러스터 LIF에 동시에 표시할 수 있으므로 피어링 네트워크를 IPv4에서 IPv6로 마이그레이션할 수 있습니다. 이전 릴리즈에서는 전체 클러스터에 대한 모든 인터클러스터 관계가 IPv4 또는 IPv6였습니다. 이는 프로토콜 변경이 잠재적으로 운영 중단이 발생할 수 있음을 의미합니다.

포트 요구 사항

인터클러스터 통신에 전용 포트를 사용하거나 데이터 네트워크에서 사용하는 포트를 공유할 수 있습니다. 포트는 다음 요구 사항을 충족해야 합니다.

- 지정된 원격 클러스터와 통신하는 데 사용되는 모든 포트는 동일한 IPspace에 있어야 합니다.

  여러 클러스터를 사용하여 다른 IPspace를 사용할 수 있습니다. IPspace 내에서만 쌍방향 전체 메시 연결이 필요합니다.

- 인터클러스터 통신에 사용되는 브로드캐스트 도메인에는 한 포트에서 다른 포트로 인터클러스터 통신이 페일오버할 수 있도록 노드당 두 개 이상의 포트가 포함되어야 합니다.

  브로드캐스트 도메인에 추가된 포트는 물리적 네트워크 포트, VLAN 또는 인터페이스 그룹(ifgrp)일 수 있습니다.

- 모든 포트는 케이블로 연결되어야 합니다.

- 모든 포트가 정상 상태여야 합니다.
- 포트의 MTU 설정이 일치해야 합니다.

방화벽 요구 사항

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 참조하십시오 "LIF의 방화벽 정책을 구성합니다".

방화벽과 인터클러스터 방화벽 정책은 다음 프로토콜을 허용해야 합니다.

- 양방향 ICMP 트래픽
- 포트 11104 및 11105를 통해 모든 인터클러스터 LIF의 IP 주소로 양방향으로 시작된 TCP 트래픽입니다
- 인터클러스터 LIF 간 양방향 HTTPS

  CLI를 사용하여 클러스터 피어링을 설정할 때는 HTTPS가 필요하지 않지만 나중에 System Manager를 사용하여 데이터 보호를 구성하면 HTTPS가 필요합니다.

기본 '인터클러스터' 방화벽 정책은 HTTPS 프로토콜을 통해 모든 IP 주소(0.0.0.0/0)에서 액세스할 수 있도록 합니다. 필요한 경우 정책을 수정하거나 대체할 수 있습니다.

클러스터 요구사항

클러스터는 다음 요구사항을 충족해야 합니다.

- 클러스터는 255개 이상의 클러스터와 피어 관계에 있을 수 없습니다.

공유 또는 전용 **ONTAP** 포트를 사용합니다

인터클러스터 통신에 전용 포트를 사용하거나 데이터 네트워크에서 사용하는 포트를 공유할 수 있습니다. 포트 공유 여부를 결정할 때는 네트워크 대역폭, 복제 간격 및 포트 가용성을 고려해야 합니다.

다른 피어링된 클러스터 중 전용 포트를 사용하여 포트 하나를 공유할 수 있습니다.

네트워크 대역폭

10GbE 같은 고속 네트워크가 있는 경우 데이터 액세스에 사용되는 것과 동일한 10GbE 포트를 사용하여 복제를 수행할 수 있는 충분한 로컬 LAN 대역폭이 있을 수 있습니다.

또한 사용 가능한 WAN 대역폭을 LAN 대역폭과 비교해야 합니다. 사용 가능한 WAN 대역폭이 10GbE보다 훨씬 작은 경우 전용 포트를 사용해야 할 수 있습니다.

이 규칙의 한 가지 예외는 클러스터의 전체 또는 여러 노드에서 데이터를 복제하는 경우입니다. 이 경우 대역폭 사용률을 일반적으로 노드 전체에 분산합니다.

전용 포트를 사용하지 않는 경우 복제 네트워크의 MTU(Maximum Transmission Unit) 크기는 일반적으로 데이터 네트워크의 MTU 크기와 같아야 합니다.

복제 간격입니다

사용량이 적은 시간에 복제가 수행되면 10GbE LAN 연결이 없어도 복제에 데이터 포트를 사용할 수 있습니다.

정상 업무 시간 중에 복제가 수행되는 경우 복제할 데이터의 양과 데이터 프로토콜 경합을 유발할 수 있는 대역폭이 너무 많이 필요한지 여부를 고려해야 합니다. 데이터 프로토콜(SMB, NFS, iSCSI)의 네트워크 활용률이 50%를 넘는 경우, 노드 페일오버가 발생할 경우 성능이 저하되지 않도록 인터클러스터 통신에 전용 포트를 사용해야 합니다.

포트 가용성

복제 트래픽이 데이터 트래픽을 방해한다고 판단할 경우 인터클러스터 LIF를 동일한 노드의 다른 인터클러스터 지원 공유 포트로 마이그레이션할 수 있습니다.

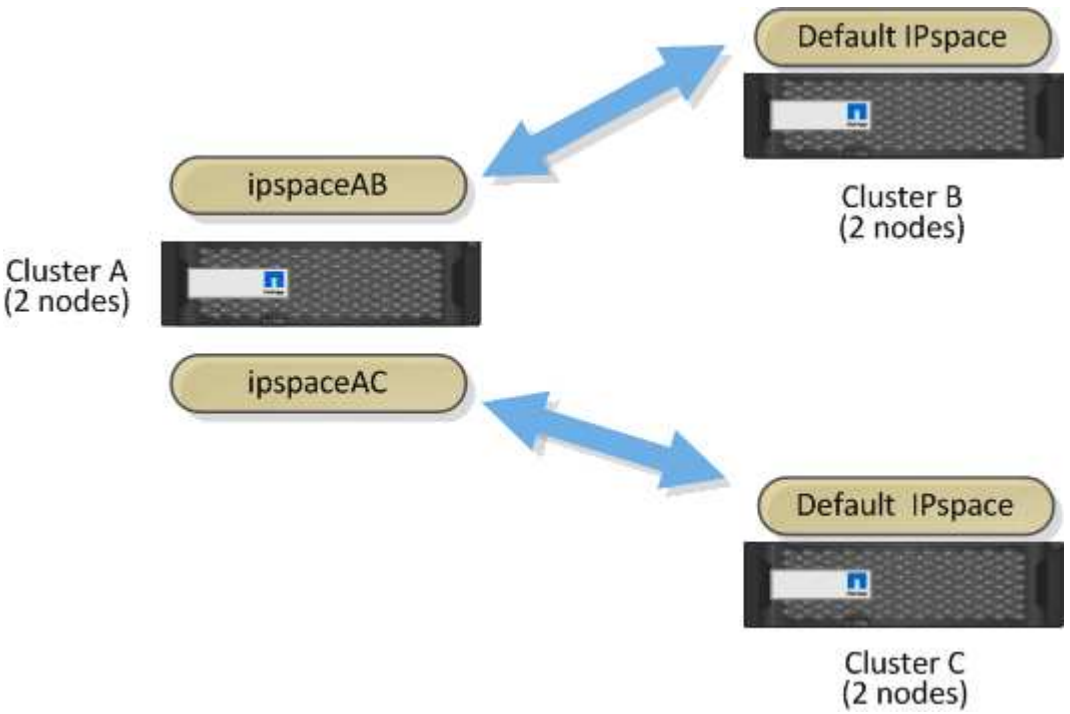
복제에 VLAN 포트를 전용으로 지정할 수도 있습니다. 포트의 대역폭은 모든 VLAN과 기본 포트 간에 공유됩니다.

사용자 지정 **ONTAP IPspace**를 사용하여 복제 트래픽을 격리합니다

맞춤형 IPspace를 사용하여 클러스터에서 다른 동료들과 상호 작용을 분리할 수 있습니다. _Designated 인터클러스터 연결 _ 이라고 하는 이 구성을 통해 서비스 공급자는 멀티 테넌트 환경에서 복제 트래픽을 격리할 수 있습니다.

예를 들어 클러스터 A와 클러스터 B 사이의 복제 트래픽을 클러스터 A와 클러스터 C 사이의 복제 트래픽과 분리하려고 한다고 가정합니다 이렇게 하려면 클러스터 A에서 2개의 IPspace를 생성할 수 있습니다

IPspace에는 클러스터 B와 통신하는 데 사용하는 인터클러스터 LIF가 포함되어 있습니다 다른 에는 다음 그림과 같이 클러스터 C와 통신하는 데 사용하는 인터클러스터 LIF가 포함되어 있습니다.



관련 정보

- "ONTAP IPspace 구성에 대해 자세히 알아보십시오"

인터클러스터 LIF를 구성합니다

공유 데이터 포트에 대한 ONTAP 인터클러스터 LIF를 구성합니다

데이터 네트워크와 공유하는 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 인터클러스터 네트워킹에 필요한 포트 수가 줄어듭니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. 관리자 SVM(기본 IPspace) 또는 시스템 SVM(사용자 지정 IPspace)에 대한 인터클러스터 LIF를 생성합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port port-address_port_ip_-netmask_mask_'
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-role l인터클러스터-home-node_node_ -home-port_port_-address_port_ip_ -netmask_mask_'

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface show – service-policy default-인터클러스터-failover'
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 e0c 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0d 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

전용 포트에 대한 **ONTAP** 인터클러스터 **LIF**를 구성합니다

전용 포트에 대한 인터클러스터 LIF를 구성할 수 있습니다. 이렇게 하면 일반적으로 복제 트래픽에 사용할 수 있는 대역폭이 증가합니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 인터클러스터 통신 전용으로 사용할 수 있는 포트를 확인합니다.

   네트워크 인터페이스 보기 필드 홈 포트, 통화 포트

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예제는 포트 e0e 및 e0f에 LIF가 할당되지 않음을 보여줍니다.

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. 전용 포트에 대한 페일오버 그룹을 생성합니다.

'network interface failover-groups create-vserver_system_SVM_-failover-group_failover_group_-targets_physical_or_logical_ports_'

다음 예에서는 시스템 SVM 'cluster01'의 페일오버 그룹 intercluster01에 포트 e0e와 e0f를 할당합니다.

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. 페일오버 그룹이 생성되었는지 확인합니다.

   네트워크 인터페이스 페일오버 그룹들이 보여줌

   에 대한 자세한 내용은 `network interface failover-groups show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. 시스템 SVM에 대한 인터클러스터 LIF를 생성한 다음 이를 페일오버 그룹에 할당합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	"네트워크 인터페이스 create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port_port_ -address_port_ip_-netmask_mask_-failover -group_group_"

옵션을 선택합니다	설명
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create -vserver_system_SVM_ -lif_LIF_name_-role 인터클러스터 -home -node_node_-home-port_port_-address_port_ip_ -netmask_mask_-failover -group_failover_group_'

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 페일오버 그룹 intercluster01에 인터클러스터 LIF 'cluster01_icl01'과 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

7. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM e0e 포트의 인터클러스터 LIF 'cluster01_icl01'과 cluster01_icl02가 e0f 포트로 페일오버된다는 것을 보여 줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

사용자 지정 IPspace에서 인터클러스터 LIF를 구성할 수 있습니다. 멀티 테넌트 환경에서 복제 트래픽을 분리할 수 있습니다.

사용자 지정 IPspace를 생성하는 경우 시스템은 시스템 SVM(스토리지 가상 머신)을 해당 IPspace의 시스템 개체에 대한 컨테이너 역할을 합니다. 새 SVM을 새 IPspace의 모든 인터클러스터 LIF의 컨테이너로 사용할 수 있습니다. 새 SVM은 사용자 지정 IPspace와 동일한 이름을 갖습니다.

단계

1. 클러스터의 포트 나열:

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 "cluster01"의 네트워크 포트를 보여줍니다.

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 클러스터에서 맞춤형 IPspace 생성:

   네트워크 IPspace 생성 - IPSpace_IPSpace_

   다음 예에서는 사용자 지정 IPspace "IPSpace-IC1"을 생성합니다.

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

에 대한 자세한 내용은 `network ipspace create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 인터클러스터 통신 전용으로 사용할 수 있는 포트를 확인합니다.

   네트워크 인터페이스 보기 필드 홈 포트, 통화 포트

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예제는 포트 e0e 및 e0f에 LIF가 할당되지 않음을 보여줍니다.

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. 기본 브로드캐스트 도메인에서 사용 가능한 포트를 제거합니다.

   네트워크 포트 브로드캐스트-도메인 제거-포트-브로드캐스트-도메인 기본 포트 포트

   포트는 한 번에 둘 이상의 브로드캐스트 도메인에 있을 수 없습니다. 에 대한 자세한 내용은 `network port broadcast-domain remove-ports` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 기본 브로드캐스트 도메인에서 포트 "e0e" 및 "e0f"를 제거합니다.

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. 포트가 기본 브로드캐스트 도메인에서 제거되었는지 확인합니다.

   네트워크 포트 쇼

   에 대한 자세한 내용은 `network port show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 기본 브로드캐스트 도메인에서 포트 "e0e"와 "e0f"가 제거되었음을 보여 줍니다.

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU     Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. 사용자 지정 IPspace에서 브로드캐스트 도메인 생성:

   'network port broadcast-domain create-IPSpace_IPSpace_-broadcast-domain_broadcast_domain_-mtu_mtu_-ports_ports_'

   다음 예에서는 IPspace 'IPSpace-IC1'에 브로드캐스트 도메인 'IPSpace-IC1-BD'를 생성합니다.

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. 브로드캐스트 도메인이 생성되었는지 확인합니다.

   네트워크 포트 브로드캐스트 도메인 쇼

   에 대한 자세한 내용은 `network port broadcast-domain show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  --------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a            complete
                            cluster01-01:e0b            complete
                            cluster01-02:e0a            complete
                            cluster01-02:e0b            complete
Default Default       1500
                            cluster01-01:e0c            complete
                            cluster01-01:e0d            complete
                            cluster01-01:e0f            complete
                            cluster01-01:e0g            complete
                            cluster01-02:e0c            complete
                            cluster01-02:e0d            complete
                            cluster01-02:e0f            complete
                            cluster01-02:e0g            complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e            complete
                            cluster01-01:e0f            complete
                            cluster01-02:e0e            complete
                            cluster01-02:e0f            complete
```

8. 시스템 SVM에 대한 인터클러스터 LIF를 생성한 후 이를 브로드캐스트 도메인에 할당합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-service-policy default-인터클러스터 -home-node_node_-home-port_port_ -address_port_ip_-netmask_mask_'
• ONTAP 9.5 및 이전 버전의 경우: *	'network interface create-vserver_system_SVM_-lif_LIF_name_-role l인터클러스터-home-node_node_ -home-port_port_-address_port_ip_ -netmask_mask_'

LIF는 홈 포트가 할당된 브로드캐스트 도메인에서 생성됩니다. 브로드캐스트 도메인에는 브로드캐스트 도메인과 동일한 이름의 기본 페일오버 그룹이 있습니다. 에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 브로드캐스트 도메인 IPSpace-IC1-BD에 인터클러스터 LIF 'cluster01_icl01' 및 'cluster01_icl02'를 생성합니다.

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. 인터클러스터 LIF가 생성되었는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터(network interface show-role 인터클러스터)

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

10. 인터클러스터 LIF가 중복되는지 확인합니다.

옵션을 선택합니다	설명
• ONTAP 9.6 이상: *	네트워크 인터페이스 show-service-policy default-인터클러스터-failover를 선택합니다
• ONTAP 9.5 및 이전 버전의 경우: *	네트워크 인터페이스 show-role 인터클러스터-failover를 참조하십시오

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM e0e 포트의 인터클러스터 LIF 'cluster01_icl01' 및 'cluster01_icl02'가 e0f 포트로 페일오버된 것을 보여줍니다.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

피어 관계를 구성합니다

ONTAP 클러스터 피어 관계를 생성합니다

데이터 백업 및 재해 복구를 위해 데이터를 원격 클러스터에 복제하여 데이터를 보호하려면 로컬 및 원격 클러스터 간에 클러스터 피어 관계를 생성해야 합니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 복제를 설정하려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

몇 가지 기본 보호 정책을 사용할 수 있습니다. 사용자 지정 정책을 사용하려면 보호 정책을 만들어야 합니다.

시작하기 전에

ONTAP CLI를 사용하는 경우 다음 방법 중 하나를 사용하여 피어링할 클러스터의 모든 노드에 인터클러스터 LIF를 생성해야 합니다.

- "공유 데이터 포트에 대한 인터클러스터 LIF를 구성합니다"
- "전용 데이터 포트에 대한 인터클러스터 LIF를 구성합니다"
- "사용자 지정 IPspace에서 인터클러스터 LIF를 구성합니다"

단계

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행합니다.

시스템 관리자

1. 로컬 클러스터에서 * 클러스터 > 설정 * 을 클릭합니다.
2. Intercluster Settings * 섹션에서 * Add Network Interfaces * 를 클릭하고 IP 주소와 서브넷 마스크를 입력하여 클러스터에 대한 클러스터 간 네트워크 인터페이스를 추가합니다.

   원격 클러스터에서 이 단계를 반복합니다.
3. 원격 클러스터에서 * 클러스터 > 설정 * 을 클릭합니다.
4. Cluster Peers * 섹션을 클릭하고 * Generate Passphrase * 를 선택합니다.
5. 원격 ONTAP 클러스터 버전을 선택합니다.
6. 생성된 암호를 복사합니다.
7. 로컬 클러스터의 * 클러스터 피어 * 에서 * 피어 클러스터 * 를 클릭하고 * 피어 클러스터 * 를 선택합니다.
8. 피어 클러스터 * 창에서 암호를 붙여 넣고 * 클러스터 피어링 초기화 * 를 클릭합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 소스 클러스터와의 피어 관계를 생성합니다.

```
cluster peer create -generate-passphrase -offer-expiration
<MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
<ipspace>
```

   '-generate-passphrase와 '-peer-addrs'를 모두 지정하면 '-peer-addrs'에 지정된 인터클러스터 LIF가 있는 클러스터만 생성된 암호를 사용할 수 있습니다.

   사용자 지정 IPspace를 사용하지 않는 경우에는 이 옵션을 무시할 `-ipspace` 수 있습니다. 에 대한 자세한 내용은 `cluster peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

   ONTAP 9.6 이상에서 피어링 관계를 생성하고 클러스터 간 피어링 통신을 암호화하지 않으려면, 암호화를 비활성화하려면 '-encryption-protocol-proposed none' 옵션을 사용해야 합니다.

   다음 예에서는 지정되지 않은 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터에서 SVM "VS1" 및 "VS2"와 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

다음 예에서는 인터클러스터 LIF IP 주소 192.140.112.103 및 192.140.112.104에서 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터의 SVM과의 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

다음 예에서는 지정되지 않은 원격 클러스터와 클러스터 피어 관계를 생성하고 로컬 클러스터에서 SVM `vs1' 및 VS2"와 피어 관계를 사전 승인합니다.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. 소스 클러스터에서 소스 클러스터를 대상 클러스터에 인증합니다.

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

에 대한 자세한 내용은 `cluster peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 인터클러스터 LIF IP 주소 192.140.112.101 및 192.140.112.102에서 원격 클러스터에 대한 로컬 클러스터를 인증합니다.

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

메시지가 나타나면 피어 관계에 대한 암호를 입력합니다.

3. 클러스터 피어 관계가 생성되었는지 확인합니다.

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                              Remote Cluster Name: cluster2
                              Active IP Addresses: 192.140.112.101,
192.140.112.102
                            Cluster Serial Number: 1-80-123456
                   Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. 피어 관계에서 노드의 접속 상태와 상태를 확인합니다.

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 준비 개요"

ONTAP 인터클러스터 **SVM** 피어 관계를 생성합니다

'vserver peer create' 명령을 사용하여 로컬 및 원격 클러스터의 SVM 간에 피어 관계를 생성할 수 있습니다.

시작하기 전에

- 소스 및 타겟 클러스터를 내다봐야 합니다.
- 원격 클러스터의 SVM에 대해 "사전 승인된" 피어 관계가 있어야 합니다.

  자세한 내용은 을 참조하십시오 "클러스터 피어 관계 생성".

이 작업에 대해

여러 SVM에 대한 피어 관계를 "사전 승인"하려면 SVM을 나열하세요. `-initial-allowed-vserver` 클러스터 피어 관계를 생성할 때의 옵션입니다. 자세한 내용은 을 "클러스터 피어 관계 생성"참조하십시오.

단계

1. 데이터 보호 대상 클러스터에서 피어링을 위해 사전 승인된 SVM을 표시합니다.

   'vserver peer permission show'

```
cluster02::> vserver peer permission show
Peer Cluster         Vserver               Applications
-------------------  --------------------  --------------------
cluster02            vs1,vs2               snapmirror
```

2. 데이터 보호 소스 클러스터에서 데이터 보호 대상 클러스터의 사전 승인된 SVM과 피어 관계를 생성합니다.

   'vserver peer create-vserver_local_SVM_-peer-vserver_remote_SVM_'

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 로컬 SVM 'pvs1'과 사전 승인된 원격 SVM 'VS1' 간에 피어 관계를 생성합니다.

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. SVM 피어 관계 확인:

   'vserver peer show'

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

ONTAP 인터클러스터 **SVM** 피어 관계를 추가합니다

클러스터 피어 관계를 구성한 후 SVM을 생성할 경우 SVM에 대한 피어 관계를 수동으로 추가해야 합니다. 'vserver peer create' 명령을 사용하여 SVM 간에 피어 관계를 생성할 수 있습니다. 피어 관계가 생성된 후 원격 클러스터에서 'vserver peer accept'를 실행하여 피어 관계를 승인할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터를 내다봐야 합니다.

이 작업에 대해

로컬 데이터 백업을 위해 동일한 클러스터에서 SVM 간에 피어 관계를 생성할 수 있습니다. 에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

관리자가 명령을 사용하여 제안된 SVM 피어 관계를 거부하는 경우가 `vserver peer reject` 있습니다. SVM 간 관계가 상태인 경우 `rejected` 관계를 삭제해야 새 관계를 생성할 수 있습니다. 에 대한 자세한 내용은 `vserver peer reject` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 데이터 보호 소스 클러스터에서 데이터 보호 타겟 클러스터의 SVM과 피어 관계를 생성합니다.

   'vserver peer create -vserver_local_SVM_-peer-vserver_remote_SVM_-applications SnapMirror|file-copy|lun-copy -peer -cluster_remote_cluster_'

   다음 예에서는 로컬 SVM `pvs1''과 원격 SVM` vs1" 간에 피어 관계를 생성합니다

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   로컬 및 원격 SVM의 이름이 동일한 경우 _ local name _ 을(를) 사용하여 SVM 피어 관계를 생성해야 합니다.

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. 데이터 보호 소스 클러스터에서 피어 관계가 시작되었는지 확인합니다.

   'vserver peer show-all'

   에 대한 자세한 내용은 `vserver peer show-all` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 SVM `pvs1''과 SVM` vs1" 간의 피어 관계가 시작된 것을 보여 줍니다.

   ```
   cluster01::> vserver peer show-all
               Peer        Peer                        Peering
   Vserver     Vserver     State      Peer Cluster     Applications
   --------    --------    ---------  -------------    ------------
   pvs1        vs1         initiated   Cluster02         snapmirror
   ```

3. 데이터 보호 대상 클러스터에서 보류 중인 SVM 피어 관계를 표시합니다.

   'vserver peer show'

   에 대한 자세한 내용은 `vserver peer show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 'cluster02'에 대해 보류 중인 피어 관계를 나열합니다.

```
cluster02::> vserver peer show

                    Peer                Peer
Vserver             Vserver             State
-----------         -----------         ------------
vs1                 pvs1                pending
```

4. 데이터 보호 대상 클러스터에서 보류 중인 피어 관계를 승인합니다.

   'vserver peer accept -vserver_local_SVM_-peer-vserver_remote_SVM_'

   에 대한 자세한 내용은 `vserver peer accept` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 로컬 SVM 'VS1'과 원격 SVM 'pvs1' 간의 피어 관계를 승인합니다.

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. SVM 피어 관계 확인:

   'vserver peer show'

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

피어 관계에서 **ONTAP** 클러스터 피어링 암호화를 활성화합니다

ONTAP 9.6부터 클러스터 피어링 암호화는 새로 생성한 모든 클러스터 피어링 관계에서 기본적으로 활성화됩니다. 클러스터 피어링 암호화는 미리 공유된 키(PSK) 및 전송 보안 계층(TLS)을 사용하여 클러스터 간 피어링 통신을 보호합니다. 그러면 피어링된 클러스터 사이에 보안 계층이 추가됩니다.

이 작업에 대해

피어링된 클러스터를 ONTAP 9.6 이상으로 업그레이드하고 ONTAP 9.5 이전 버전에서 피어링 관계가 생성된 경우, 업그레이드 후 클러스터 피어링 암호화를 수동으로 활성화해야 합니다. 클러스터 피어링 암호화를 활성화하려면 피어링 관계의 두 클러스터가 ONTAP 9.6 이상을 실행해야 합니다.

단계

1. 대상 클러스터에서 소스 클러스터와의 통신에 대해 암호화를 설정합니다.

   'cluster peer modify_source_cluster_-auth-status-admin use-authentication-encryption-protocol-proposed TLS-PSK

2. 메시지가 나타나면 암호를 입력합니다.
3. 데이터 보호 소스 클러스터에서 데이터 보호 대상 클러스터와의 통신을 위해 암호화를 설정합니다.

   'cluster peer modify_data_protection_destination_cluster_-auth-status-admin use-authentication-encryption-protocol-proposed TLS-PSK

4. 메시지가 표시되면 대상 클러스터에 입력한 것과 동일한 암호를 입력합니다.

에 대한 자세한 내용은 `cluster peer modify` "ONTAP 명령 참조입니다"을 참조하십시오.

피어 관계에서 **ONTAP** 클러스터 피어링 암호화를 제거합니다

기본적으로 클러스터 피어링 암호화는 ONTAP 9.6 이상에서 생성된 모든 피어 관계에서 활성화됩니다. 클러스터 간 피어링 통신에 암호화를 사용하지 않으려면 비활성화할 수 있습니다.

단계

1. 타겟 클러스터에서 소스 클러스터와의 통신을 수정하여 클러스터 피어링 암호화 사용을 중지합니다.
   - 암호화를 제거하고 인증을 유지하려면 다음을 입력합니다.

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - 암호화 및 인증 제거하기:
     i. 인증되지 않은 액세스를 허용하도록 클러스터 피어링 정책을 수정합니다.

     ```
     cluster peer policy modify -is-unauthenticated-access-permitted
     true
     ```

     ii. 암호화 및 인증 액세스 수정:

     ```
     cluster peer modify <source_cluster> -auth-status no-
     authentication
     ```

2. 메시지가 표시되면 암호를 입력합니다.
3. 암호를 다시 입력하여 확인합니다.
4. 소스 클러스터에서 대상 클러스터와의 통신에 대한 암호화를 해제합니다.
   - 암호화를 제거하고 인증을 유지하려면 다음을 입력합니다.

```
cluster peer modify <destination_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

◦ 암호화 및 인증 제거하기:

i. 인증되지 않은 액세스를 허용하도록 클러스터 피어링 정책을 수정합니다.

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

ii. 암호화 및 인증 액세스 수정:

```
cluster peer modify <destination_cluster> -auth-status no-
authentication
```

5. 메시지가 표시되면 대상 클러스터에서 사용한 것과 동일한 암호 구문을 입력하고 다시 입력합니다.

로컬 스냅샷을 관리합니다

로컬 **ONTAP** 스냅샷 관리에 대해 자세히 알아보십시오

스냅샷 _ 은(는) 볼륨의 읽기 전용 시점 이미지입니다. 이미지는 마지막 스냅샷 이후 파일의 변경 사항만 기록하기 때문에 최소한의 저장 공간을 사용하고 성능 오버헤드를 거의 일으키지 않습니다.

스냅샷을 사용하여 볼륨의 전체 내용을 복원하거나 개별 파일 또는 LUN을 복구할 수 있습니다. 스냅샷은 볼륨의 디렉토리에 저장됩니다. `.snapshot`

ONTAP 9.4 이상에서는 FlexVol volume 최대 1023개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 이하 버전에서는 볼륨에 최대 255개의 스냅샷을 포함할 수 있습니다.

ONTAP 9.8부터 FlexGroup 볼륨에는 1023개의 스냅샷이 포함될 수 있습니다. 자세한 내용은 을 "스냅샷을 사용하여 FlexGroup 볼륨을 보호합니다"참조하십시오.

ONTAP 장기 보존 스냅샷에 대해 알아보세요

정책 유형이 "vault" 또는 "mirror-vault"인 SnapMirror 관계를 사용하면 SnapMirror 관계의 보조 볼륨에 직접 스냅샷을 생성할 수 있습니다. 이러한 스냅샷은 대상 위치에 백업으로 보관됩니다. 이러한 스냅샷은 장기간 보존을 위해 생성되는 경우가 많으며, 장기 보존 스냅샷이라고 합니다.

SnapMirror 정책 규칙에서 스냅샷 생성 일정, 스냅샷 이름 접두사, SnapMirror 레이블 및 보존 횟수를 지정하여 장기 보존 스냅샷을 만듭니다. 이 스냅샷은 소스의 보존 규칙에 관계없이 SnapMirror 대상 볼륨에 보존됩니다.

장기 보존 스냅샷은 FlexVol SnapMirror 구성에서만 사용할 수 있습니다. FlexGroup SnapMirror 구성에 대해서는

장기 보존 스냅샷을 생성할 수 없습니다.

SnapMirror 캐스케이드 관계에서는 장기 보존 스냅샷을 캐스케이드의 마지막 볼륨에만 만들 수 있습니다.

관련 정보

- "캐스케이드 배포가 작동하는 방식에 대해 알아보세요"
- "ONTAP SnapMirror 스케줄을 정의하여 대상에 로컬 복제본을 생성합니다"

사용자 지정 스냅샷 정책을 구성합니다

사용자 지정 **ONTAP** 스냅샷 정책을 구성하는 방법에 대해 자세히 알아보십시오

스냅샷 정책 _ 은(는) 시스템에서 스냅샷을 생성하는 방법을 정의합니다. 정책은 스냅샷을 생성할 시기, 보존할 복제본 수 및 스냅샷 이름을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하며 복제본 이름을 "`daily""로 지정할 수 있습니다.*timestamp*.

볼륨에 대한 기본 정책은 다음 일정에 따라 스냅샷을 자동으로 생성하며 가장 오래된 스냅샷은 삭제되어 새 복제본을 위한 공간을 확보합니다.

- 시간당 최대 6개의 스냅샷이 해당 시간 이후 5분 동안 촬영되었습니다.
- 월요일부터 토요일까지 자정 이후 10분에 최대 2개의 일일 스냅샷을 촬영합니다.
- 매주 일요일 자정 이후 15분에 최대 2개의 주간 스냅샷이 촬영됩니다.

볼륨을 생성할 때 스냅샷 정책을 지정하지 않으면 해당 볼륨이 포함된 SVM(스토리지 가상 머신)과 연결된 스냅샷 정책을 상속합니다.

사용자 지정 **ONTAP** 스냅샷 정책을 구성하는 경우

기본 스냅샷 정책이 볼륨에 적합하지 않은 경우 스냅샷의 빈도, 보존 및 이름을 수정하는 사용자 지정 정책을 구성할 수 있습니다. 스케줄은 주로 활성 파일 시스템의 변경 속도에 따라 결정됩니다.

자주 사용하지 않는 파일을 하루에 한 번 백업하면서 자주 사용하는 파일 시스템을 데이터베이스와 같이 백업할 수 있습니다. 데이터베이스의 경우에도 일반적으로 전체 백업을 하루에 한 번 또는 두 번 실행하는 동시에 트랜잭션 로그를 매시간 백업합니다.

그 밖의 요인은 귀사에 파일이 중요한 이유, SLA(서비스 수준 계약), RPO(복구 시점 목표) 및 RTO(복구 시간 목표)입니다. 일반적으로 필요한 만큼의 스냅샷만 보존해야 합니다.

ONTAP 스냅샷 작업 일정을 생성합니다

스냅샷 정책에는 스냅샷 작업 스케줄이 하나 이상 필요합니다. System Manager 또는 명령을 사용하여 작업 일정을 생성할 수 있습니다 `job schedule cron create`. 에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 작업 일정을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

기본적으로 ONTAP는 작업 일정 이름에 타임스탬프를 추가하여 스냅샷의 이름을 구성합니다.

해당 월의 요일 및 요일에 대한 값을 모두 지정하면 값은 독립적으로 간주됩니다. 예를 들어, 일 사양 금요일과 월 사양 13일이 포함된 cron 일정은 금요일이 아니라 매달 13일에 각각 금요일과 13일에 실행됩니다.

예 **1.** 단계

시스템 관리자

1. Protection > Overview * 로 이동하고 * Local policy settings * 를 확장합니다.
2. Schedules * 창에서 를 →클릭합니다.
3. Schedules * 창에서 를 + Add 클릭합니다.
4. 일정 추가 * 창에서 일정 이름을 입력하고 컨텍스트 및 일정 유형을 선택합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 작업 일정 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

ONTAP 9.10.1.1부터는 작업 일정에 SVM을 포함할 수 있습니다.

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

다음 예에서는 토요일 오전 3시에 실행되는 'myweekly'라는 작업 일정을 생성합니다.

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

다음 예제에서는 여러 일, 시간 및 분을 지정하는 mywelymulti라는 일정을 만듭니다.

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

ONTAP 스냅샷 정책을 생성합니다

스냅샷 정책은 스냅샷을 생성할 시기, 보존할 복제본 수 및 스냅샷 이름을 지정하는 방법을 지정합니다. 예를 들어 시스템은 매일 오전 12시 10분에 스냅샷 하나를 생성하고 가장 최근의 복제본 두 개를 보존하고 이름을 ""매일""로 지정할 수.*timestamp* 있습니다. 스냅샷 정책에는 최대 5개의 작업 일정을 포함할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 스냅샷 정책을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

기본적으로 ONTAP는 작업 일정 이름에 타임스탬프를 추가하여 스냅샷의 이름을 구성합니다.

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

원하는 경우 작업 스케줄 이름의 접두사를 대체할 수 있습니다.

'스냅샷 레이블' 옵션은 SnapMirror 복제용 옵션입니다. 자세한 내용은 을 참조하십시오 "정책 규칙 정의".

단계

System Manager 또는 ONTAP CLI를 사용하여 스냅샷 정책을 생성할 수 있습니다. 이 절차에서는 로컬 클러스터에만 스냅샷 정책을 생성합니다.

시스템 관리자

1. Protection > Overview * 로 이동하고 * Local policy settings * 를 확장합니다.
2. Snapshot policies * 창에서 를 →클릭합니다.
3. Snapshot policies * 탭에서 를 + Add 클릭합니다.
4. Add snapshot policy * 창에서 정책 이름을 입력하고 범위를 선택합니다.
5. 을 클릭합니다 + Add .
6. 일정을 선택하려면 현재 표시된 일정 이름을 클릭하고 를 ⌄클릭한 다음 다른 일정을 선택합니다.
7. 보존할 최대 스냅샷을 입력하고 필요한 경우 SnapMirror 레이블 및 SnapLock 보존 기간을 입력합니다.
8. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 정책 생성:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

다음 예에서는 일정에 따라 실행되는 `daily` 라는 스냅샷 정책을 `snap_policy_daily` 생성합니다. 정책에는 최대 5개의 스냅샷이 있으며 각 스냅샷에는 `daily.timestamp` 이름과 SnapMirror 레이블이 `daily`있습니다.

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

스냅샷을 수동으로 관리합니다

스냅샷을 수동으로 생성하고 삭제합니다

예약된 스냅샷이 생성될 때까지 기다릴 수 없는 경우 스냅샷을 수동으로 생성할 수 있으며 더 이상 필요하지 않은 경우 스냅샷을 삭제할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 주문형 스냅샷을 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

스냅샷을 수동으로 생성합니다

System Manager 또는 ONTAP CLI를 사용하여 스냅샷을 수동으로 생성할 수 있습니다.

시스템 관리자

단계

1. 저장소 **>** 볼륨*으로 이동하여 *스냅샷 탭을 선택합니다.
2. 을 클릭합니다 + Add .
3. Add a snapshot * 창에서 기본 스냅샷 이름을 그대로 사용하거나 원하는 경우 편집합니다.
4. * 선택 사항 *: SnapMirror 레이블 추가
5. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 생성:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

스냅샷을 수동으로 삭제합니다

System Manager 또는 ONTAP CLI를 사용하여 스냅샷을 수동으로 삭제할 수 있습니다.

시스템 관리자

단계

1. 스토리지 > 볼륨 * 으로 이동하고 * Snapshot 복사본 * 탭을 선택합니다.
2. 삭제하려는 스냅샷을 찾아 를 클릭하고 * Delete * 를 선택합니다.
3. 스냅샷 삭제 * 창에서 * 스냅샷 삭제 * 를 선택합니다.
4. 삭제 * 를 클릭합니다.

CLI를 참조하십시오

1. 명령을 사용하여 `volume snapshot show` 삭제할 스냅샷을 확인합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

이 예에서 명령은 SVM vs3의 볼륨 vol3에 대한 스냅샷을 표시합니다.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. 스냅샷 삭제:

원하는 작업	이 명령을 입력하십시오...
단일 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

원하는 작업	이 명령을 입력하십시오...
여러 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
모든 스냅샷을 삭제합니다	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

스냅샷을 삭제하기 전에 재확보 가능한 공간을 계산합니다

ONTAP 9.10.1부터 System Manager를 사용하여 삭제할 스냅샷을 선택하고 삭제하기 전에 재확보 가능한 공간을 계산할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 스냅샷을 삭제할 볼륨을 선택합니다.
3. *스냅샷*을 클릭하세요.
4. 스냅샷을 하나 이상 선택합니다.
5. 회수 가능 공간 계산 * 을 클릭합니다.

스냅숏 예비 공간을 관리합니다

ONTAP 스냅숏 예비 공간 관리에 대해 자세히 알아봅니다

snapshot reserve_는 스냅샷을 위한 디스크 공간의 비율을 기본값으로 5%로 설정합니다. 스냅숏 예비 공간이 소진된 경우 스냅숏은 활성 파일 시스템의 공간을 사용하므로 필요에 따라 스냅숏 예비 공간을 늘릴 수 있습니다. 또는 예약이 꽉 차면 스냅샷을 자동으로 삭제할 수 있습니다.

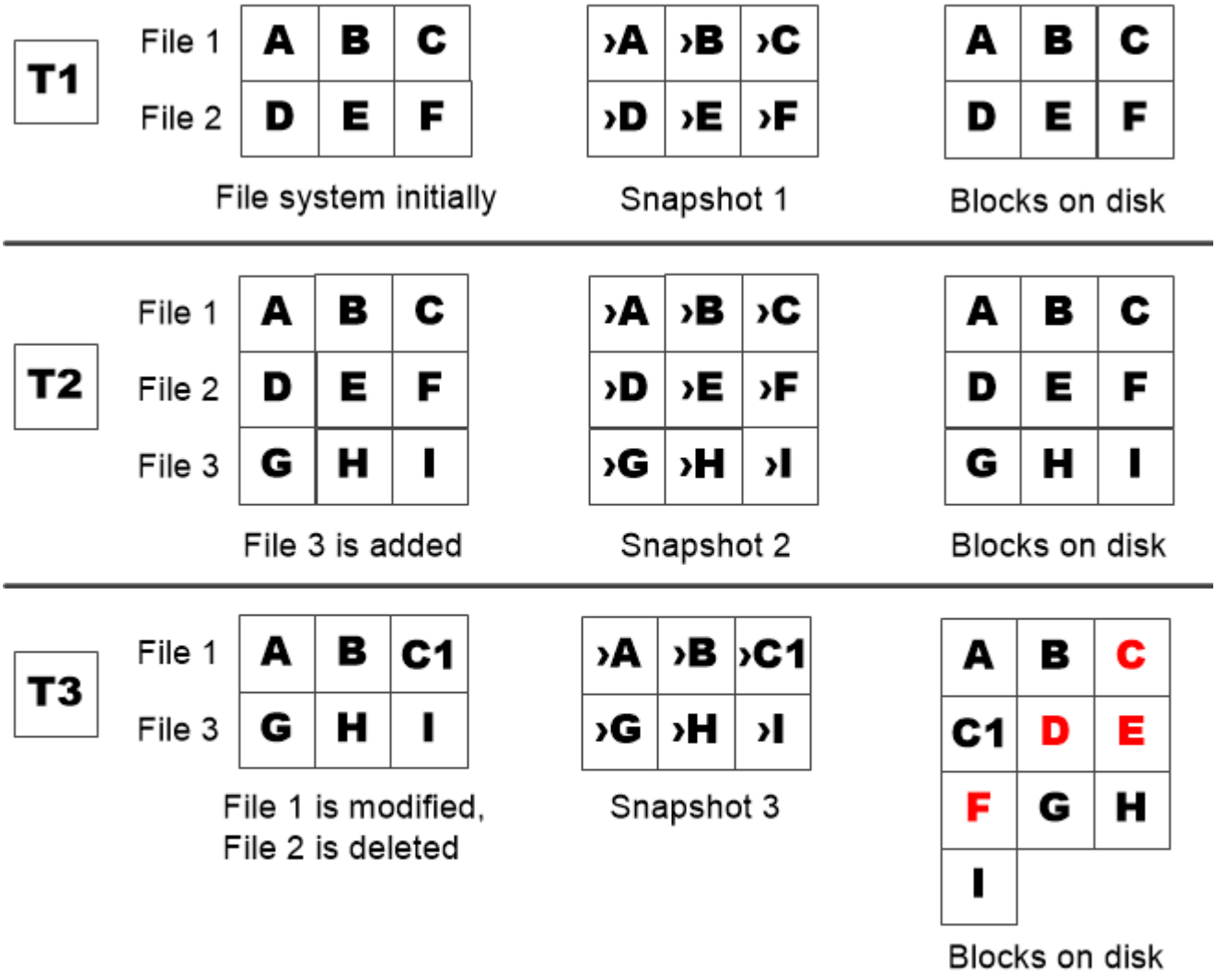
스냅숏 예비 공간을 늘릴 시기

스냅숏 예비 공간을 증가할지 여부를 결정할 때 스냅숏은 마지막 스냅숏이 만들어진 이후 파일의 변경 내용만 기록한다는 점을 기억해야 합니다. 활성 파일 시스템의 블록이 수정되거나 삭제될 때만 디스크 공간을 사용합니다.

즉, 파일 시스템의 변경률이 스냅샷에서 사용되는 디스크 공간의 양을 결정하는 데 중요한 요소가 됩니다. 생성한 스냅샷 수에 관계없이 활성 파일 시스템이 변경되지 않은 경우 디스크 공간을 소비하지 않습니다.

예를 들어 데이터베이스 트랜잭션 로그를 포함하는 FlexVol volume의 경우 변경 속도를 높이기 위해 20%의 스냅숏 예비 공간이 있을 수 있습니다. 더 자주 업데이트되는 데이터베이스를 캡처하기 위해 더 많은 스냅샷을 생성할 수 있을 뿐만 아니라 스냅샷이 사용하는 추가 디스크 공간을 처리할 수 있도록 더 큰 스냅숏 예비 공간이 필요합니다.

스냅샷은 블록 복제본이 아닌 블록에 대한 포인터로 구성됩니다. 포인터는 블록의 "클레임"이라고 생각할 수 있습니다. ONTAP는 스냅샷이 삭제될 때까지 블록을 "보류"합니다.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

보호된 파일을 삭제하면 예상보다 파일 공간이 줄어들 수 있습니다

스냅샷은 해당 블록을 사용한 파일을 삭제한 후에도 해당 블록을 가리킵니다. 따라서 스냅숏 예비 공간이 소진되면 전체 파일 시스템을 삭제하면 사용 중인 파일 시스템보다 사용 가능한 공간이 줄어드는 직관적인 결과가 발생할 수 있습니다.

다음 예제를 고려해 보십시오. 파일을 삭제하기 전에 'df' 명령 출력은 다음과 같습니다.

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

전체 파일 시스템을 삭제하고 볼륨의 스냅샷을 생성한 후 `df` 명령은 다음 출력을 생성합니다.

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

출력에서 알 수 있듯이, 이전에 활성 파일 시스템에서 사용했던 3GB의 전체 용량이 삭제되기 전에 사용된 0.5GB와 함께 스냅샷에 사용되고 있습니다.

스냅샷이 사용하는 디스크 공간이 스냅샷 예비 공간을 초과하기 때문에 활성 파일용으로 예약된 공간에 2.5GB의 "스필" 오버플로우가 발생하여 3GB가 예상될 수 있는 파일용으로 0.5GB의 여유 공간이 남습니다.

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP 스냅샷 디스크 사용량 모니터링

명령을 사용하여 스냅샷 디스크 사용량을 모니터링할 수 `df` 있습니다. 이 명령은 활성 파일 시스템의 사용 가능한 공간과 스냅숏 예비 공간을 표시합니다.

단계

1. 스냅샷 디스크 사용량 표시: `df`

   다음 예에서는 스냅샷 디스크 사용량을 보여 줍니다.

   ```
   cluster1::> df
   Filesystem           kbytes  used    avail  capacity
   /vol/vol0/           3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

볼륨에서 사용 가능한 **ONTAP** 스냅숏 예비 공간을 확인합니다

매개 변수를 명령과 함께 `volume show` 사용하여 볼륨에서 사용 가능한 스냅숏 예비 공간의 양을 확인할 수 `snapshot-reserve-available` 있습니다. 에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 볼륨에서 사용 가능한 스냅숏 예비 공간을 확인합니다.

'vol show -vserver_SVM_-volume_volume_-fields snapshot-reserve-available'

다음 예는 에 대해 사용 가능한 스냅숏 예비 공간을 `vol1` 표시합니다.

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

ONTAP 스냅숏 예비 공간을 수정합니다

스냅샷이 활성 파일 시스템에 예약된 공간을 사용하지 않도록 더 큰 스냅숏 예비 공간을 구성할 수 있습니다. 스냅샷을 위한 공간이 더 이상 필요하지 않으면 스냅숏 예비 공간을 줄일 수 있습니다.

단계

1. 스냅숏 예비 공간을 수정합니다.

   'volume modify -vserver_SVM_-volume_volume_- percent-snapshot-space_snap_reserve_'

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 에 대한 스냅숏 예비 공간을 `vol1` 10%로 설정합니다.

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

자동 삭제 ONTAP 스냅샷

명령을 사용하여 스냅숏 예비 공간이 초과되었을 때 스냅숏의 자동 삭제를 트리거할 수 `volume snapshot autodelete modify` 있습니다. 기본적으로 가장 오래된 스냅샷이 먼저 삭제됩니다. 에 대한 자세한 내용은 `volume snapshot autodelete modify` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

LUN 및 파일 클론은 삭제할 스냅샷이 더 이상 없으면 삭제됩니다.

단계

1. 자동 삭제 스냅샷:

   '볼륨 스냅샷 자동 삭제 수정 - vserver_SVM_-volume_volume_-enabled true|false-trigger volume|snap_reserve'

다음 예에서는 스냅숏 예비 공간이 소진된 경우 스냅샷을 자동으로 `vol1` 삭제합니다.

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

스냅샷에서 파일을 복원합니다

NFS 또는 **SMB** 클라이언트의 **ONTAP** 스냅샷에서 파일을 복구합니다

NFS 또는 SMB 클라이언트의 사용자는 스토리지 시스템 관리자의 개입 없이 스냅샷에서 직접 파일을 복구할 수 있습니다.

파일 시스템의 모든 디렉토리에는 NFS 및 SMB 사용자가 액세스할 수 있는 하위 디렉토리가 포함되어 `.snapshot` 있습니다. `.snapshot`하위 디렉토리에는 볼륨의 스냅샷에 해당하는 하위 디렉토리가 포함되어 있습니다.

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

각 하위 디렉토리에는 스냅샷이 참조하는 파일이 포함됩니다. 사용자가 실수로 파일을 삭제하거나 덮어쓸 경우 파일을 스냅샷 하위 디렉토리에서 읽기-쓰기 디렉토리로 복사하여 상위 읽기-쓰기 디렉토리로 복원할 수 있습니다.

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

ONTAP 스냅샷 디렉토리에 대한 **NFS** 및 **SMB** 클라이언트 액세스를 설정 및 해제합니다

명령의 ONTAP CLI 옵션을 `volume modify` 사용하여 스냅샷 디렉토리에 대한 액세스를 사용하거나 사용하지 않도록 설정할 수 `-snapdir-access` 있으며, ONTAP 9.10.1부터 System Manager를 사용하여 클라이언트 시스템이 볼륨의 스냅샷 디렉토리에 액세스하도록 설정하거나 해제할 수 있습니다. 액세스를 활성화하면 스냅샷 디렉토리가 클라이언트에 표시되고 Windows 클라이언트가 스냅샷 디렉토리에 드라이브를 매핑하여 해당 컨텐츠를 보고 액세스할 수 있습니다. 그러면 NFS 및 SMB 클라이언트가 스냅샷에서 파일 또는 LUN을 복구할 수

있습니다.

볼륨 설정을 편집하거나 볼륨의 공유 설정을 편집하여 볼륨의 스냅샷 디렉터리에 대한 액세스를 활성화하거나 비활성화할 수 있습니다.

볼륨을 편집하여 스냅샷 디렉토리에 대한 클라이언트 액세스를 설정 또는 해제합니다

단계

ONTAP System Manager 또는 ONTAP CLI를 사용하여 클라이언트 스냅샷 디렉토리 액세스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 볼륨의 스냅샷 디렉토리는 기본적으로 클라이언트가 액세스할 수 있습니다.

시스템 관리자

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 표시하거나 숨길 스냅샷 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
4. 스냅샷(로컬) 설정 섹션에서 *클라이언트에 스냅샷 디렉터리 표시*를 선택하거나 선택 해제합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 스냅샷 디렉토리 액세스 상태를 확인합니다.

```
volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
access
```

예:

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
access
vserver volume snapdir-access
------- ------ --------------
vs0     vol1   false
```

에 대한 자세한 내용은 `volume show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 스냅샷 디렉토리 액세스를 설정하거나 해제합니다.

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
<true|false>
```

다음 예에서는 vol1에서 스냅샷 디렉토리 액세스를 설정합니다.

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
true
Volume modify successful on volume vol1 of Vserver vs0.
```

에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

공유를 편집하여 스냅샷 디렉토리에 대한 클라이언트 액세스를 설정하거나 해제합니다

볼륨의 스냅샷 디렉토리는 기본적으로 클라이언트가 액세스할 수 있습니다.

단계

1. 스토리지 > 공유 * 를 클릭합니다.
2. 표시하거나 숨길 스냅샷 디렉토리가 포함된 볼륨을 선택합니다.
3. 을 ⋮ 클릭하고 * 편집 * 을 선택합니다.
4. Share Properties * 섹션에서 * Allow clients to access snapshots directory * 를 선택하거나 선택 취소합니다.
5. 저장 * 을 클릭합니다.

ONTAP 스냅샷에서 단일 파일을 복구합니다

명령을 사용하여 스냅샷에서 단일 파일 또는 LUN을 복원할 수 `volume snapshot restore-file` 있습니다. 기존 파일을 바꾸지 않으려는 경우 상위 읽기-쓰기 볼륨의 다른 위치로 파일을 복원할 수 있습니다.

이 작업에 대해

기존 LUN을 복구하는 경우 LUN 클론이 생성되고 스냅샷 형태로 백업됩니다. 복원 작업 중에 LUN에서 읽거나 LUN에 쓸 수 있습니다.

스트림이 있는 파일은 기본적으로 복원됩니다.

단계

1. 볼륨의 스냅샷을 나열합니다.

   'volume snapshot show -vserver_SVM_-volume_volume_'

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅샷에서 파일 복구:

   '볼륨 스냅샷 복원 - 파일 - vserver_SVM_-volume_volume_-snapshot_snapshot_-path_file_path_-restore-path_destination_path_'

에 대한 자세한 내용은 `volume snapshot restore-file` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 myfile.txt 파일을 복구합니다.

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

ONTAP 스냅샷에서 파일의 일부를 복원합니다

데이터의 시작 바이트 오프셋과 바이트 수를 알고 있다고 가정하면 명령을 사용하여 스냅샷에서 LUN으로 데이터 범위를 복원할 수 있습니다 `volume snapshot partial-restore-file`. 이 명령을 사용하여 여러 데이터베이스를 동일한 LUN에 저장하는 호스트에서 데이터베이스 중 하나를 복원할 수 있습니다.

ONTAP 9.12.1부터 를 사용하는 볼륨에 대해 부분 복원을 사용할 수 SnapMirror 활성 동기화있습니다.

단계

1. 볼륨의 스냅샷을 나열합니다.

   'volume snapshot show -vserver_SVM_-volume_volume_'

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅샷에서 파일의 일부를 복원합니다.

   '볼륨 스냅샷 부분 복구 파일 - vserver_SVM_-volume_volume_-snapshot_snapshot_-path_file_path_-start-byte_starting_byte_-byte-count_byte_count_'

   시작 바이트 오프셋 및 바이트 수는 4,096의 배수여야 합니다.

다음 예에서는 myfile.txt 파일의 첫 4,096바이트를 복원합니다.

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

ONTAP 스냅숏에서 볼륨의 내용을 복원합니다

스냅숏에서 복원하면 볼륨을 이전 시점으로 복구할 수 있습니다. System Manager 또는 명령을 사용하여 스냅샷에서 볼륨의 내용을 복원할 수 `volume snapshot restore` 있습니다. 에 대한 자세한 내용은 `volume snapshot restore` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

볼륨에 SnapMirror 관계가 있는 경우 스냅샷에서 복구한 직후 볼륨의 모든 미러 복사본을 수동으로 복제합니다. 그렇지 않으면 미러 복사본을 사용할 수 없게 되므로 복사본을 삭제하고 다시 생성해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 이전 스냅샷에서 복원할 수 있습니다.

시스템 관리자

1. Storage * 를 클릭하고 볼륨을 선택합니다.
2. Snapshot 복사본 * 에서 복원할 스냅샷 옆의 를 클릭하고 * 복원 * 을 선택합니다.

CLI를 참조하십시오

1. 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 의 스냅샷을 `vol1` 보여 줍니다.

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 스냅숏에서 볼륨의 내용 복원:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

다음 예에서는 vol1의 내용을 복원합니다.

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

SnapMirror 볼륨 복제

SnapMirror 볼륨 복제에 대해 알아보십시오

ONTAP SnapMirror 비동기식 재해 복구에 대해 알아보십시오

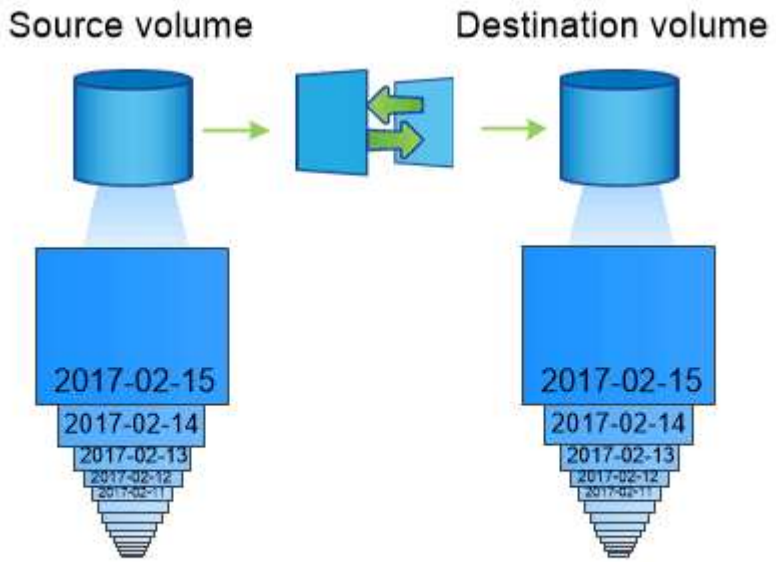
_SnapMirror_는 지리적으로 원격 사이트의 운영 스토리지에서 보조 스토리지로 페일오버하도록 설계된 재해 복구 기술입니다. 그 이름이 시사하듯이 SnapMirror는 운영 사이트에서 재해가 발생한 경우에도 데이터를 계속 제공할 수 있는 보조 스토리지에 작업 데이터의 복제본 또는 _MIRROR_를 생성합니다.

운영 사이트에서 데이터를 계속 제공할 수 있는 경우 필요한 데이터를 다시 전송하여 미러에서 클라이언트를 전혀 제공하지 않고 그대로 제공할 수 있습니다. 페일오버 사용 사례에서 알 수 있듯이, 2차 시스템의 컨트롤러는 미러링된 스토리지의 데이터를 효율적으로 지원하기 위해 운영 시스템의 컨트롤러와 동등하거나 거의 동등해야 합니다.

데이터 보호 관계

데이터가 볼륨 레벨에서 미러링됩니다. 운영 스토리지의 소스 볼륨과 2차 스토리지의 타겟 볼륨 간의 관계를 _ 데이터 보호 관계라고 합니다. _ 볼륨이 상주하는 클러스터와 볼륨의 데이터를 제공하는 SVM이 되어야 합니다."자세히 들여다보았습니다" 피어 관계를 통해 클러스터와 SVM이 데이터를 안전하게 교환할 수 있습니다.

다음 그림에서는 SnapMirror 데이터 보호 관계를 보여 줍니다.



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

데이터 보호 관계의 범위

볼륨 간 또는 볼륨을 소유한 SVM 간에 직접 데이터 보호 관계를 생성할 수 있습니다. SVM 데이터 보호 관계에서는 NFS 엑스포트 및 SMB 공유에서 RBAC에 이르는 SVM 구성의 전체 또는 일부를 복제할 뿐만 아니라 SVM이 소유한 볼륨의 데이터도 복제됩니다.

또한 다음과 같은 특수 데이터 보호 애플리케이션용 SnapMirror를 사용할 수도 있습니다.

- SVM 루트 볼륨의 _load 공유 mirror_copy를 사용하면 노드 운영 중단 또는 페일오버 발생 시에도 데이터에 액세스할 수 있습니다.

- SnapLock 볼륨 _ 간의 데이터 보호 관계를 통해 WORM 파일을 보조 스토리지로 복제할 수 있습니다.

  "SnapLock 기술을 사용한 아카이브 및 규정 준수"

- ONTAP 9.13.1부터 SnapMirror 비동기식을 사용하여 보호할 수 정합성 보장 그룹있습니다. ONTAP 9.14.1부터 SnapMirror 비동기식을 사용하여 일관성 그룹 관계를 사용하여 볼륨 세분화 스냅샷을 타겟 클러스터에 복제할 수 있습니다. 자세한 내용은 을 SnapMirror 비동기식 보호를 구성합니다참조하십시오.

SnapMirror 데이터 보호 관계가 초기화된 방식

SnapMirror를 처음 호출하면 소스 볼륨에서 대상 볼륨으로 _baseline transfer_를 수행합니다. 관계에 대한 _SnapMirror 정책_은 기준 및 모든 업데이트의 내용을 정의합니다.

기본 SnapMirror 정책 'MirorAllSnapshots'에 따른 기본 전송에는 다음 단계가 포함됩니다.

- 소스 볼륨의 스냅샷을 생성합니다.
- 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록을 대상 볼륨으로 전송합니다.
- ""활성"" 미러가 손상된 경우 사용할 수 있도록 소스 볼륨의 나머지 덜 최근의 스냅샷을 대상 볼륨으로 전송합니다.

SnapMirror 데이터 보호 관계가 업데이트되는 방법

업데이트는 구성한 일정에 따라 비동기식입니다. 보존은 소스의 스냅샷 정책을 미러링합니다.

정책에 따라 업데이트될 때마다 `MirrorAllSnapshots` SnapMirror는 소스 볼륨의 스냅샷을 생성하고 해당 스냅샷과 마지막 업데이트 이후에 생성된 모든 스냅샷을 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `MirrorAllSnapshots` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성함을 나타내는 ""true"" `MirrorAllSnapshots`입니다.
- `MirrorAllSnapshots` 에는 SnapMirror가 관계를 업데이트할 때 SnapMirror에서 생성한 스냅샷과 마지막 업데이트 이후에 생성된 모든 스냅샷이 모두 전송됨을 나타내는 "'sm_created'" 및 "'all_source_snapshots'" 규칙이 있습니다.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

대칭 복사 정책

사전 구성된 `MirrorLatest` 정책은 SnapMirror에서 생성된 스냅샷만 초기화 및 업데이트 시 전송된다는 점을 제외하고 와 동일하게 `MirrorAllSnapshots` 작동합니다.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

관련 정보

- "스냅미러 정책 보기"

ONTAP SnapMirror 동기식 재해 복구 에 대해 알아보십시오

ONTAP 9.5부터, SnapMirror 동기(SM-S) 기술은 최소 16GB의 메모리가 있는 모든 FAS 및

AFF 플랫폼 및 모든 ONTAP Select 플랫폼에서 지원됩니다. SnapMirror 동기식 기술은 볼륨 레벨에서 동기식 데이터 복제를 제공하는 라이센스된 노드별 기능입니다.

이 기능은 데이터 손실이 전혀 필요하지 않는 금융, 의료 및 기타 규제 대상 산업에서 동기식 복제에 대한 규제 및 국가 차원의 요구를 해결합니다.

SnapMirror 동기식 작업이 허용됩니다

HA 쌍당 SnapMirror 동기식 복제 작업 수의 제한은 컨트롤러 모델에 따라 다릅니다.

다음 표에는 플랫폼 유형 및 ONTAP 릴리즈에 따라 HA 쌍당 허용되는 SnapMirror 동기식 작업의 수가 나와 있습니다.

플랫폼	ONTAP 9.14.1부터 ONTAP 9.11.1까지	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.9.1 이전 릴리즈
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

지원되는 기능

다음 표에는 SnapMirror Synchronous 및 지원이 제공되는 ONTAP 릴리스에서 지원되는 기능이 나와 있습니다.

피처	첫 번째 릴리스가 지원됩니다	추가 정보
SnapMirror 동기식 관계의 운영 볼륨에 대한 바이러스 백신	ONTAP 9.6	
애플리케이션이 생성한 스냅샷 복제입니다	ONTAP 9.7	스냅샷이 해당 시점에 적절한 레이블로 태그된 경우 `snapshot create` SnapMirror CLI나 ONTAP API를 사용하여 애플리케이션을 정지시킨 후 사용자가 생성한 스냅샷이나 외부 스크립트로 생성한 스냅샷을 동기식으로 복제합니다. 스냅샷 정책을 사용하여 생성된 예약된 스냅샷은 복제되지 않습니다. 애플리케이션에서 생성된 스냅샷 복제에 대한 자세한 내용은 다음을 참조하세요 ."NetApp 지식 기반: SnapMirror 동기를 사용하여 애플리케이션에서 생성된 스냅샷을 복제하는 방법" .
클론 자동 삭제	ONTAP 9.6	
없음, 스냅샷 또는 자동의 계층화 정책이 있는 FabricPool 애그리게이트는 SnapMirror 동기식 소스 및 대상에서 지원됩니다.	ONTAP 9.5	FabricPool 애그리게이트의 타겟 볼륨을 모든 계층화 정책으로 설정할 수 없습니다.
FC	ONTAP 9.5	지연 시간이 10ms를 초과하지 않는 모든 네트워크
FC-NVMe를 참조하십시오	ONTAP 9.7	

파일 클론	ONTAP 9.7	
SnapMirror 동기식 관계의 운영 볼륨에 대한 FPolicy	ONTAP 9.6	
SnapMirror 동기식 관계의 운영 볼륨에 대한 하드 및 소프트 할당량	ONTAP 9.6	할당량 규칙은 대상에 복제되지 않으므로 할당량 데이터베이스가 대상에 복제되지 않습니다.
클러스터 내 동기식 관계	ONTAP 9.14.1	소스 볼륨과 타겟 볼륨이 서로 다른 HA 쌍에 배치된 경우 고가용성이 제공됩니다. 전체 클러스터가 다운되면 클러스터가 복구될 때까지 볼륨에 액세스할 수 없습니다. 클러스터 내 SnapMirror 동기식 관계는 동시 작업의 전체 제한에 기여합니다.HA 쌍당 관계
iSCSI	ONTAP 9.5	
LUN 클론 및 NVMe 네임스페이스 클론	ONTAP 9.7	
애플리케이션 생성 스냅샷을 통해 백업되는 LUN 클론입니다	ONTAP 9.7	
혼합 프로토콜 액세스(NFS v3 및 SMB)	ONTAP 9.6	
NDMP/NDMP 복구	ONTAP 9.13.1	SnapMirror Synchronous에 NDMP를 사용하려면 소스 클러스터와 대상 클러스터 모두 ONTAP 9.13.1 이상을 실행해야 합니다. 자세한 내용은 을 참조하십시오 NDMP 복제본을 사용하여 데이터를 전송합니다.
AFF/ASA 플랫폼에서만 무중단 SnapMirror 동기식 운영(NDO)이 가능합니다.	ONTAP 9.12.1	무중단 운영을 지원하므로 업무 중단 시간을 예약하지 않고 일반적인 여러 유지보수 작업을 수행할 수 있습니다. 지원되는 운영에는 2개의 클러스터 각각에서 단일 노드가 정상 작동하는 경우 테이크오버 및 반환, 볼륨 이동이 포함됩니다.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
높은 메타데이터 작업 빈도 제한을 제거합니다	ONTAP 9.6	
TLS 1.2 암호화를 사용하여 전송 중인 중요한 데이터에 대한 보안	ONTAP 9.6	
단일 파일 및 부분 파일 복구	ONTAP 9.13.1	
SMB 2.0 이상	ONTAP 9.6	
SnapMirror 동기식 미러 계단식 배열	ONTAP 9.6	SnapMirror 동기식 관계의 타겟 볼륨으로부터의 관계는 SnapMirror 비동기식 관계여야 합니다.

SVM 재해 복구	ONTAP 9.6	* SnapMirror 동기식 소스는 SVM 재해 복구 소스로도 될 수 있습니다. 예를 들어, 한 구간으로는 SnapMirror 동기식, 다른 구간으로는 SVM 재해 복구를 사용하는 팬아웃 구성이 될 수 있습니다. * SnapMirror 동기식 소스는 SnapMirror 동기식 소스는 데이터 보호 소스를 연속적으로 지원하지 않으므로 SVM 재해 복구 대상이 될 수 없습니다. 타겟 클러스터에서 SVM 재해 복구 플립 재동기화를 수행하기 전에 동기식 관계를 해제해야 합니다. * SnapMirror 동기식 대상은 SVM 재해 복구에서 DP 볼륨의 복제를 지원하지 않으므로 SVM 재해 복구 소스가 될 수 없습니다. 동기식 소스를 플립 재동기화하면 타겟 클러스터의 DP 볼륨을 제외하고 SVM 재해 복구가 수행됩니다.
소스 볼륨에 테이프 기반 복구	ONTAP 9.13.1	
NAS에 대한 소스 볼륨과 대상 볼륨 간의 타임 스탬프 패리티입니다	ONTAP 9.6	ONTAP 9.5에서 ONTAP 9.6으로 업그레이드한 경우 소스 볼륨의 새 파일 및 수정된 파일에 대해서만 타임스탬프가 복제됩니다. 소스 볼륨의 기존 파일 타임스탬프가 동기화되지 않습니다.

지원되지 않는 기능입니다

다음 기능은 SnapMirror 동기식 관계에서 지원되지 않습니다.

- 자율 랜섬웨어 보호
- 정합성 보장 그룹
- DP_Optimized(DPO) 시스템
- FlexGroup 볼륨
- FlexCache 볼륨
- 글로벌 제한
- 팬아웃 구성에서는 하나의 관계만 SnapMirror 동기식 관계가 될 수 있고 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다.
- LUN 이동
- MetroCluster 구성
- 혼합 SAN 및 NVMe 액세스 LUN과 NVMe 네임스페이스는 동일한 볼륨 또는 SVM에서 지원되지 않습니다.
- SnapCenter
- SnapLock 볼륨
- 변조 방지 스냅샷
- 대상 볼륨에서 dump 및 SMTape를 사용하여 테이프 백업 또는 복구를 수행합니다
- 소스 볼륨의 처리량(QoS Min
- Volume SnapRestore를 참조하십시오
- VVOL

작동 모드

SnapMirror Synchronous에는 사용되는 SnapMirror 정책 유형에 따라 두 가지 작동 모드가 있습니다.

- * 동기화 모드 * 동기화 모드에서는 애플리케이션 I/O 작업이 운영 및 보조 스토리지 시스템과 병렬로 전송됩니다. 어떤 이유로든 보조 스토리지에 대한 쓰기가 완료되지 않으면 애플리케이션이 운영 스토리지에 계속 쓸 수 있습니다. 오류 상태가 수정되면 SnapMirror 동기식 기술은 자동으로 보조 스토리지와 재동기화되고 동기식 모드에서 운영 스토리지에서 보조 스토리지로 복제를 재개합니다. 동기화 모드에서 RPO=0과 RTO는 2차 복제 장애가 발생할 때까지 매우 낮지만 RPO 및 RTO가 결정되지 않습니다. 그러나 2차 복제가 실패하고 재동기화가 완료된 문제를 복구하는 데 걸리는 시간과 동일합니다.
- * StrictSync 모드 * SnapMirror Synchronous는 선택적으로 StrictSync 모드로 작동할 수 있습니다. 어떤 이유로든 보조 스토리지에 대한 쓰기가 완료되지 않으면 애플리케이션 입출력이 실패하여 운영 스토리지와 보조 스토리지가 동일한지 확인합니다. SnapMirror 관계가 `InSync` 상태로 돌아간 후에만 운영 시스템에 대한 애플리케이션 입출력이 재개됩니다. 운영 스토리지에 장애가 발생할 경우 페일오버 후 데이터 손실 없이 보조 스토리지에서 애플리케이션 입출력을 재개할 수 있습니다. StrictSync 모드에서는 RPO가 항상 0이고 RTO는 매우 낮습니다.

관계 상태

SnapMirror 동기식 관계의 상태는 `InSync` 정상 작동 중에 항상 상태입니다. 어떤 이유로든 SnapMirror 전송이 실패하면 대상이 소스와 동기화되지 않으므로 `OutofSync` 상태로 이동할 수 있습니다.

SnapMirror 동기식 관계의 경우 시스템이 `InSync` `OutofSync`고정된 간격으로 관계 상태 또는)를 자동으로 확인합니다. 관계 상태가 인 `OutofSync` 경우 ONTAP는 자동으로 자동 재동기화 프로세스를 트리거하여 관계를 `InSync` 상태로 되돌립니다. 소스 또는 대상에서 계획되지 않은 스토리지 페일오버 또는 네트워크 중단과 같은 작업으로 인해 전송이 실패한 경우에만 자동 재동기화가 트리거됩니다. `snapmirror quiesce`및 과 같은 사용자 시작 작업은 `snapmirror break` 자동 재동기화를 트리거하지 않습니다.

관계 상태가 `OutofSync` StrictSync 모드에서 SnapMirror 동기 관계에 대한 상태가 되면 운영 볼륨에 대한 모든 I/O 작업이 중지됩니다. `OutofSync`동기화 모드에서 SnapMirror 동기식 관계의 상태는 운영 볼륨에 영향을 주지 않으며 운영 볼륨에 입출력 작업이 허용됩니다.

관련 정보

- "NetApp 기술 보고서 4733: SnapMirror 동기식 구성 및 모범 사례"
- "SnapMirror가 깨졌습니다"
- "SnapMirror 중지"

기본 **ONTAP** 데이터 보호 정책

ONTAP에는 데이터 보호 관계에 사용할 수 있는 몇 가지 기본 보호 정책이 포함되어 있습니다. 사용하는 정책은 보호 관계 유형에 따라 다릅니다.

기본 정책이 데이터 보호 관계 요구 사항을 충족하지 못하는 경우 다음을 수행할 수 "사용자 지정 정책을 만듭니다 "있습니다.

기본 보호 정책 및 설명 목록입니다

기본 보호 정책 및 관련 정책 유형은 아래에 설명되어 있습니다.

이름	설명	정책 유형입니다
비동기식	최신 활성 파일 시스템과 일별 및 주별 스냅샷을 시간별 전송 일정으로 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책	비동기식
자동화된 장애 조치	복제 실패 시 클라이언트 입출력이 중단되지 않는 제로 RTO 보장의 SnapMirror 동기식 정책입니다.	동기식이다
자동화된 장애 이중 모드	제로 RTO 보장 및 양방향 동기화 복제를 제공하는 SnapMirror Synchronous 정책입니다.	동기식이다
CloudBackupDefault를 선택합니다	일일 규칙을 포함한 볼트 정책.	비동기식
연속	S3 버킷 미러링 정책	연속
DailyBackup을 선택합니다	일일 규칙 및 일일 전송 일정이 포함된 볼트 정책	비동기식
DPDefault(기본값)	모든 스냅샷과 최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAllSnapshots을 선택합니다	모든 스냅샷과 최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAllSnapshotsDiscardNetwork 를 참조하십시오	네트워크 구성을 제외한 모든 스냅샷과 최신 활성 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책	비동기식
MirrorAndVault를 선택합니다	최신 활성 파일 시스템과 일별 및 주별 스냅샷을 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책입니다.	비동기식
MirrorAndVaultDiscardNetwork 를 참조하십시오	네트워크 구성을 제외한 최신 활성 파일 시스템과 일별 및 주별 스냅샷을 미러링하기 위한 통합된 SnapMirror 비동기식 및 볼트 정책.	비동기식
대칭 복사	최신 액티브 파일 시스템을 미러링하기 위한 SnapMirror 비동기식 정책입니다.	비동기식
SnapCenterSync 를 참조하십시오	SnapCenter with Application 생성 스냅샷 구성에 대한 SnapMirror Synchronous for Application에 대한 정책	동기식이다
StrictSync를 선택합니다	복제 실패 시 클라이언트 액세스가 중단되는 SnapMirror Synchronous에 대한 정책입니다.	동기식이다
동기식이다	복제 실패 시 클라이언트 액세스가 중단되지 않는 SnapMirror Synchronous에 대한 정책입니다.	동기식이다
Unified7년	7년 보존이 있는 Unified SnapMirror 정책	비동기식
XDPDefault	일별 및 주별 규칙을 포함한 볼트 정책.	비동기식

ONTAP StrictSync 및 동기화 정책에서 지원하는 워크로드에 대해 알아보십시오

StrictSync 및 동기화 정책은 FC, iSCSI 및 FC-NVMe 프로토콜을 사용하는 모든 LUN 기반 애플리케이션뿐만 아니라 데이터베이스, VMware, 할당량, SMB 등과 같은 엔터프라이즈 애플리케이션용 NFSv3 및 NFSv4 프로토콜을 지원합니다. ONTAP 9.6부터 SnapMirror 동기식 은 EDA(전자 설계 자동화), 홈 디렉토리, 소프트웨어 구축 워크로드와 같은 엔터프라이즈 파일 서비스에 사용할 수 있습니다.

ONTAP 9.5에서 동기화 정책의 경우 NFSv3 또는 NFSv4 워크로드를 선택하는 동안 몇 가지 중요한 측면을 고려해야 합니다. 동기화 정책은 높은 읽기 또는 쓰기 입출력 워크로드를 처리할 수 있으므로 워크로드별로 데이터 읽기 또는 쓰기 작업의 양은 고려하지 않습니다. ONTAP 9.5에서는 과도한 파일 생성, 디렉토리 생성, 파일 권한 변경 또는 디렉토리 권한 변경이 있는 워크로드가 적합하지 않을 수 있습니다(이러한 작업을 메타데이터 워크로드가 높은 워크로드라고 함). 메타데이터가 많은 워크로드의 전형적인 예로는 여러 개의 테스트 파일을 만들고, 자동화를 실행하고, 파일을 삭제하는 DevOps 워크로드가 있습니다. 또 다른 예로는 컴파일 중에 여러 임시 파일을 생성하는 병렬 빌드 워크로드가 있습니다. 쓰기 메타데이터 작업이 높으면 미러 간의 동기화가 일시적으로 중단되어 클라이언트의 읽기 및 쓰기 입출력이 중단될 수 있습니다.

ONTAP 9.6부터는 이러한 제한이 제거되며 SnapMirror Synchronous는 홈 디렉토리 및 소프트웨어 빌드 워크로드 등과 같은 다중 사용자 환경이 포함된 엔터프라이즈 파일 서비스 워크로드에 사용할 수 있습니다.

관련 정보

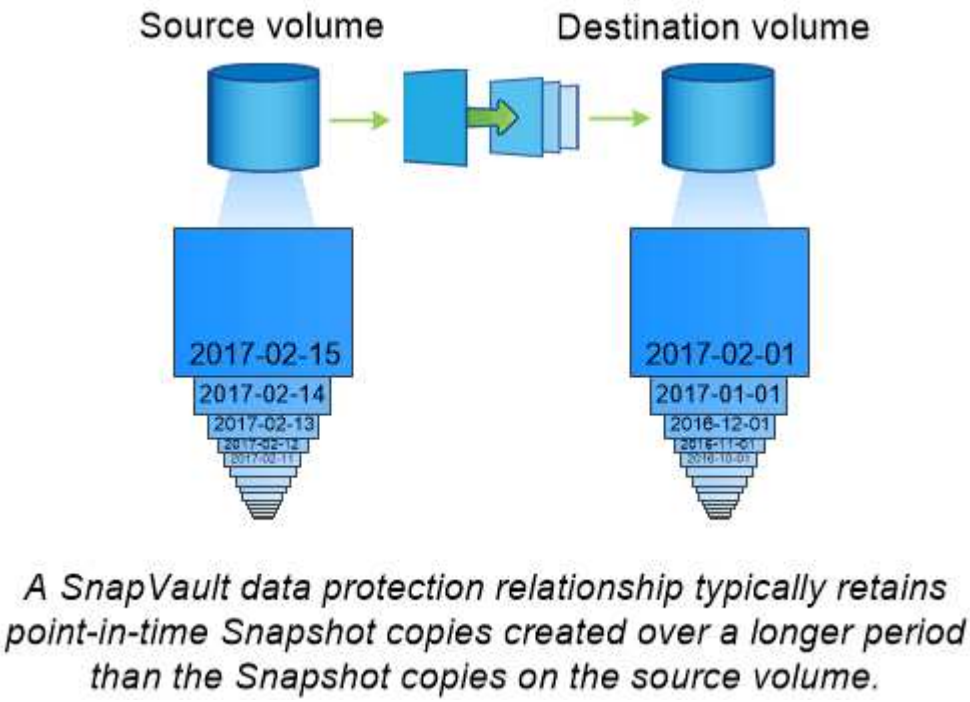
"SnapMirror 동기식 구성 및 모범 사례"

ONTAP SnapMirror 기술을 사용한 볼트 보관에 대해 알아봅니다

SnapMirror 볼트 정책은 ONTAP 9.3 이상에서 SnapVault 기술을 대체합니다. 표준 준수 및 기타 거버넌스 관련 목적을 위해 D2D 스냅샷 복제에는 SnapMirror 소산 정책을 사용합니다. 일반적으로 대상에 현재 소스 볼륨에 있는 스냅샷만 포함되는 SnapMirror 관계와는 달리, 볼트 대상은 훨씬 더 긴 기간 동안 생성된 시점 스냅샷을 보존합니다.

예를 들어, 비즈니스의 정부 회계 규정을 준수하기 위해 데이터의 월별 스냅샷을 20년 동안 보관할 수 있습니다. 볼트 스토리지에서 데이터를 제공할 필요가 없으므로 대상 시스템에서 느리고 저렴한 디스크를 사용할 수 있습니다.

아래 그림은 SnapMirror 볼트 데이터 보호 관계를 보여줍니다.



볼트 데이터 보호 관계가 초기화되는 방법

관계에 대한 SnapMirror 정책에서는 기본 내용과 모든 업데이트를 정의합니다.

기본 볼트 정책에 따른 기본 전송은 `XDPDefault` 소스 볼륨의 스냅샷을 만든 다음 해당 복사본과 해당 복사본이 참조하는 데이터 블록을 대상 볼륨에 전송합니다. SnapMirror 관계와 달리 볼트 백업에는 기준선에 이전 스냅샷이 포함되지 않습니다.

볼트 데이터 보호 관계를 업데이트하는 방법

업데이트는 구성한 일정에 따라 비동기식입니다. 관계 정책에 정의된 규칙은 업데이트에 포함할 새 스냅샷과 보존할 복제본 수를 식별합니다. 정책에 정의된 레이블(예: ""월")은 소스의 스냅샷 정책에 정의된 하나 이상의 레이블과 일치해야 합니다. 그렇지 않으면 복제가 실패합니다.

정책에 따라 업데이트될 때마다 `XDPDefault` SnapMirror는 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 경우 마지막 업데이트 이후 생성된 스냅샷을 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `XDPDefault` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성하지 않음을 나타내는 "'false"' `XDPDefault`입니다.
- `XDPDefault` 에는 ""daily"" 및 ""weekly"" 규칙이 있습니다. 이는 SnapMirror에서 관계를 업데이트할 때 소스에 레이블이 일치하는 모든 스냅샷이 전송됨을 나타냅니다.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                    Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

관련 정보

- "스냅미러 정책 보기"

ONTAP SnapMirror 통합 복제에 대해 알아보십시오

SnapMirror_Unified replication_을 사용하면 동일한 대상 볼륨에 재해 복구 및 아카이빙을 구성할 수 있습니다. 통합 복제가 적절한 경우 필요한 보조 스토리지의 양을 줄이고 기본 전송 수를 제한하며 네트워크 트래픽을 줄일 수 있습니다.

통합 데이터 보호 관계의 초기화 방법

SnapMirror와 마찬가지로 통합 데이터 보호는 처음 호출할 때 기본 전송을 수행합니다. 관계에 대한 SnapMirror 정책에서는 기본 내용과 모든 업데이트를 정의합니다.

기본 통합 데이터 보호 정책에 따른 기본 전송은 `MirrorAndVault` 소스 볼륨의 스냅샷을 생성한 다음 해당 복사본과 이 복사본이 타겟 볼륨에 참조하는 데이터 블록을 전송합니다. 볼트 보관과 마찬가지로, 통합 데이터 보호에는 기준선에 이전 스냅샷이 포함되지 않습니다.

통합 데이터 보호 관계를 업데이트하는 방법

정책에 따라 업데이트될 때마다 `MirrorAndVault` SnapMirror는 소스 볼륨의 스냅샷을 생성하고 해당 스냅샷과 마지막 업데이트 이후 생성된 모든 스냅샷을 스냅샷 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 경우 전송합니다. 정책의 다음 출력에서 다음 `snapmirror policy show` 사항에 `MirrorAndVault` 유의하십시오.

- `Create Snapshot` 는 SnapMirror에서 관계를 업데이트할 때 스냅샷을 생성함을 나타내는 ""true"" `MirrorAndVault`입니다.
- `MirrorAndVault` 에는 SnapMirror가 관계를 업데이트할 때 SnapMirror에 의해 생성된 스냅샷과 소스에 일치하는 레이블이 있는 스냅샷이 모두 전송됨을 나타내는 "'sm_created'", "'daily'" 및 "'weekly" 규칙이 있습니다.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7년 정책입니다

사전 구성된 `Unified7year` 정책은 과 정확히 동일하게 `MirrorAndVault` 작동합니다. 단, 네 번째 규칙은 월별 스냅샷을 전송하고 7년 동안 보존한다는 점이 다릅니다.

```
                           Rules: SnapMirror Label     Keep   Preserve Warn
Schedule Prefix
                                  ----------------     ----   -------- ----
--------- ------
                                  sm_created              1   false       0 -
-
                                  daily                   7   false       0 -
-
                                  weekly                 52   false       0 -
-
                                  monthly                84   false       0 -
-
```

데이터 손상을 방지합니다

통합 복제는 초기화할 때 SnapMirror에서 생성한 스냅샷으로 기본 전송 내용을 제한합니다. 업데이트할 때마다 SnapMirror는 소스의 다른 스냅샷을 생성하고 스냅샷 정책 규칙에 정의된 레이블과 일치하는 레이블이 있는 새 스냅샷과 해당 스냅샷을 전송합니다.

대상에 마지막으로 전송된 스냅샷의 복사본을 생성하여 업데이트된 스냅샷이 손상되는 것을 방지할 수 있습니다. 이 ""로컬 복사본""은 소스의 보존 규칙에 관계없이 보존되므로 SnapMirror에 의해 원래 전송된 스냅샷을 소스에서 더 이상 사용할 수 없는 경우에도 대상에서 해당 복제본을 사용할 수 있습니다.

통합 데이터 복제를 사용하는 경우

전체 미러 유지 관리의 이점을 통합 복제가 2차 스토리지의 양을 줄이고 기본 전송 수를 제한하며 네트워크 트래픽을 감소시켜 주는 이점과 비교하여 평가해야 합니다.

통합 복제의 적절성을 결정하는 주요 요인은 활성 파일 시스템의 변경률입니다. 예를 들어, 기존 미러는 데이터베이스 트랜잭션 로그의 시간별 스냅샷을 저장하는 볼륨에 더 적합합니다.

관련 정보

- "스냅미러 정책 보기"

ONTAP 데이터 보호 대상 볼륨이 자동으로 증가하는 경우

볼륨에 포함된 가용 공간이 애그리게이트에 있는 경우 데이터 보호 미러 전송 중에 소스 볼륨이 증가하면 타겟 볼륨의 크기가 자동으로 커집니다.

이 동작은 대상의 자동 증가 설정에 관계없이 발생합니다. 볼륨의 증가를 제한하거나 ONTAP가 볼륨을 증가하도록 할 수는 없습니다.

기본적으로 데이터 보호 볼륨은 'grow_shrink' 자동 크기 조정 모드로 설정되어 있으며, 이 모드에서는 사용된 공간의 양에 따라 볼륨이 커지거나 축소됩니다. 데이터 보호 볼륨의 최대 자동 크기 조정 크기는 최대 FlexVol 크기와 동일하며 플랫폼에 따라 다릅니다. 예를 들면 다음과 같습니다.

- FAS8200, 기본 DP 볼륨 최대 크기 조정 = 100TB

자세한 내용은 을 참조하십시오 "NetApp Hardware Universe를 참조하십시오".

fan-out_deployment 를 사용하여 데이터 보호를 여러 보조 시스템으로 확장할 수 있습니다. cascade_deployment를 사용하여 데이터 보호를 3차 시스템으로 확장할 수 있습니다.

팬아웃 및 계단식 구축 모두 SnapMirror DR, SnapVault 또는 통합 복제의 모든 조합을 지원합니다. ONTAP 9.5부터 SnapMirror 동기식 관계는 하나 이상의 SnapMirror 비동기식 관계를 통해 팬아웃 구축을 지원합니다. 팬아웃 구성에서는 하나의 관계만 SnapMirror 동기식 관계가 될 수 있으며 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다. SnapMirror 동기식 관계는 ONTAP 9.6부터 계단식 배포를 지원하지만 SnapMirror 동기식 관계의 타겟 볼륨과의 관계는 SnapMirror 비동기식 관계여야 합니다. SnapMirror 활성 동기화 (ONTAP 9.13.1부터 지원됨) 팬아웃 구성도 지원합니다.

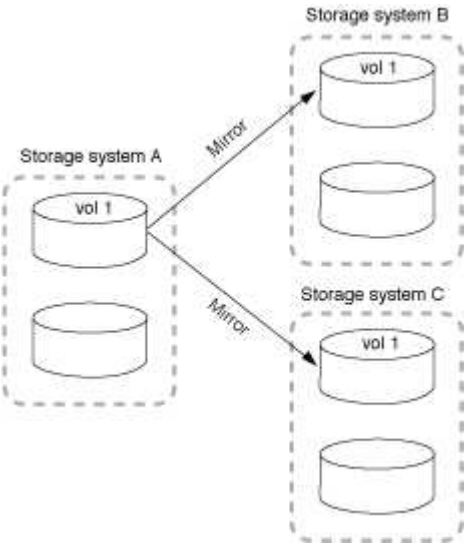
fan-in_deployment를 사용하여 여러 운영 시스템과 단일 보조 시스템 간에 데이터 보호 관계를 생성할 수 있습니다. 각 관계는 2차 시스템에서 다른 볼륨을 사용해야 합니다.

팬아웃 또는 캐스케이드 구성의 일부인 볼륨은 재동기화에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

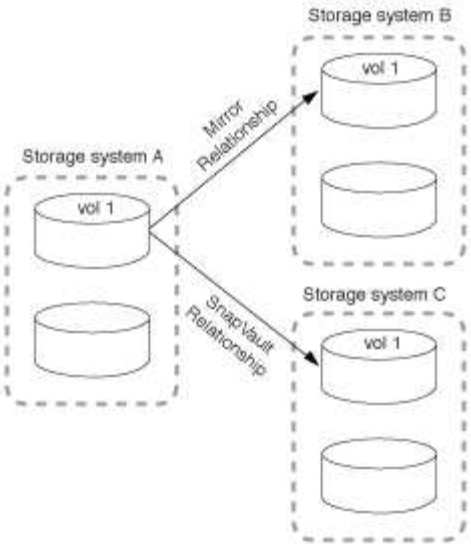
팬아웃**(fan-out)** 배포의 작동 방식

SnapMirror는 _multiple-mirror_and_mirror-vault_fan-out 배포를 지원합니다.

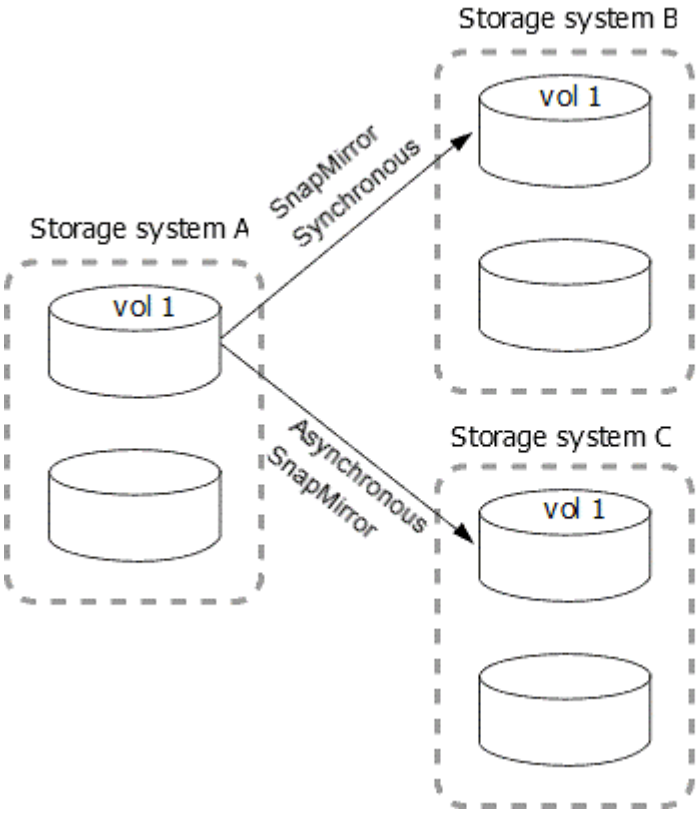
다중 미러 팬아웃 구축은 여러 보조 볼륨에 대한 미러 관계가 있는 소스 볼륨으로 구성됩니다.



미러 볼트(mirror-vault) 팬아웃 구축은 2차 볼륨에 대한 미러 관계와 다른 2차 볼륨에 대한 SnapVault 관계를 가진 소스 볼륨으로 구성됩니다.



ONTAP 9.5부터는 SnapMirror 동기식 관계를 통해 팬아웃 환경을 구축할 수 있지만, 팬아웃 구성에서 하나의 관계만 SnapMirror 동기식 관계가 될 수 있으며 소스 볼륨의 다른 모든 관계는 SnapMirror 비동기식 관계여야 합니다.



다중 구간 배포의 작동 방식

SnapMirror는 *mirror-mirror_mirror-vault*,_vault-mirror_and_vault-vault_cascade 배포를 지원합니다.

미러 계단식 배열 구축은 소스 볼륨이 2차 볼륨으로 미러링되고 2차 볼륨이 3차 볼륨으로 미러링되는 관계 체인으로 구성됩니다. 2차 볼륨을 사용할 수 없게 되면 새로운 기준 전송을 수행하지 않고도 1차 볼륨과 3차 볼륨 간의 관계를 동기화할 수 있습니다.

계층형 볼륨 관계에서 장기 보존 스냅샷은 모든 ONTAP 9 버전에서 계층 구조의 최종 SnapMirror 대상 볼륨에서만 지원됩니다. 캐스케이드 구조의 중간 볼륨에서 장기 보존 스냅샷을 활성화하면 백업 및 스냅샷이 누락될 수 있습니다.

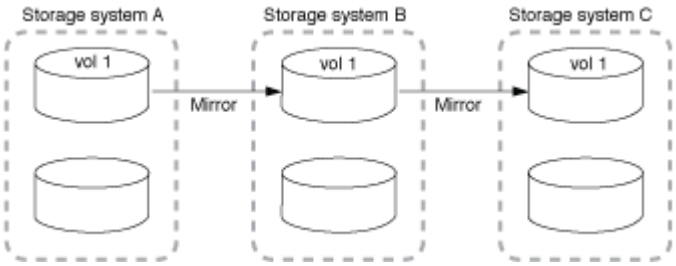
캐스케이드 구성에서 중간 볼륨 중 하나라도 장기 보존 스냅샷이 활성화된 지원되지 않는 구성인 경우 기술 지원팀에 문의하여 다음 내용을 참조하십시오. "NetApp 기술 자료: 장기 보존(LTR) 스냅샷이 활성화된 볼륨을 계단식으로 배열하는 것은 지원되지 않습니다." 도움이 필요합니다.

다음 ONTAP 버전에서는 최종 SnapMirror 대상 볼륨을 제외한 캐스케이드의 모든 볼륨에서 장기 보존 스냅샷을 활성화할 수 없습니다.

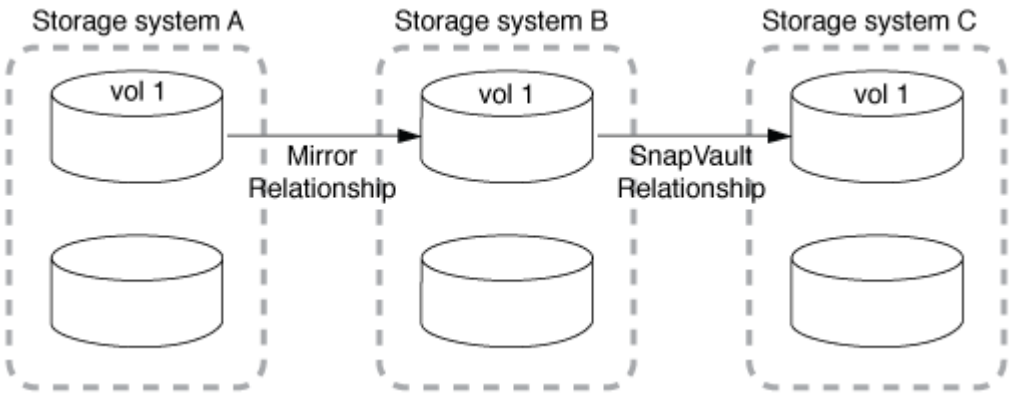
- 9.15.1 이상
- 9.14.1P2 및 P4부터 P14까지
- 9.13.1P9부터 P17까지
- 9.12.1 P12부터 P19까지
- 9.11.1P15부터 P20까지
- 9.10.1P18부터 P20까지
- 9.9.1P20

자세히 알아보세요"장기 보존 스냅샷" .

ONTAP 9.6부터 미러 계단식 구축 환경에서 SnapMirror 동기식 관계가 지원됩니다. 운영 볼륨 및 2차 볼륨만 SnapMirror 동기식 관계에 있을 수 있습니다. 2차 볼륨과 3차 볼륨 간의 관계는 비동기식이어야 합니다.



미러 소산 다중 구간 구축은 소스 볼륨이 보조 볼륨으로 미러링되고 2차 볼륨이 3차 볼륨으로 저장되는 관계 체인으로 구성됩니다.



Vault-mirror 및 Vault-Vault Cascade 배포도 지원됩니다.

- 볼트 미러 계단식 배열 구축은 소스 볼륨을 보조 볼륨으로 보관하고 2차 볼륨을 3차 볼륨으로 미러링하는 관계 체인으로 구성됩니다.
- 볼트-볼트 캐스케이드 배포는 소스 볼륨이 보조 볼륨으로 볼트되고 보조 볼륨이 3차 볼륨으로 볼트되는 관계 체인으로 구성됩니다.

관련 정보

- SnapMirror 활성 동기화를 사용하여 팬아웃 구성에서 보호를 다시 시작합니다

ONTAP SnapMirror 라이센스에 대해 알아보십시오

ONTAP 9.3부터 ONTAP 인스턴스 간 복제를 위한 라이센스가 간소화되었습니다. ONTAP 9 릴리즈에서는 SnapMirror 라이센스가 볼트와 미러 관계를 모두 지원합니다. SnapMirror 라이센스를 사용하여 백업 및 재해 복구 사용 사례 모두에 대해 ONTAP 복제를 지원할 수 있습니다.

ONTAP 9.3 릴리즈 이전에는 ONTAP ONTAP 인스턴스 간의 _vault_관계를 구성하기 위해 별도의 SnapVault 라이센스가 필요했습니다. DP 인스턴스는 보존 시간이 더 긴 백업 사용 사례를 지원하기 위해 더 많은 스냅샷을 보존할 수 있고, ONTAP 인스턴스 간의 _mirror_관계를 구성하기 위해 SnapMirror 라이센스가 필요했습니다. SnapMirror 및 SnapVault 라이센스는 모두 ONTAP 8.x 및 9.x 릴리즈에 대해 계속 사용 및 지원됩니다.

SnapVault 사용권은 계속 작동하고 ONTAP 8.x 및 9.x 릴리즈 모두에서 지원되지만, SnapVault 사용권 대신 SnapMirror 사용권을 사용할 수 있으며 미러 및 볼트 구성에 모두 사용할 수 있습니다.

ONTAP 비동기식 복제의 경우 ONTAP 9.3부터 단일 통합 복제 엔진을 사용하여 확장된 데이터 보호 모드(XDP) 정책을 구성합니다. 이때 미러 정책, 볼트(Vault) 정책 또는 미러 볼트(Mirror-Vault) 정책에 대해 SnapMirror 라이센스를 구성할 수 있습니다. 소스 및 타겟 클러스터 모두에 SnapMirror 라이센스가 필요합니다. SnapMirror 라이센스가 이미 설치되어 있는 경우에는 SnapVault 라이센스가 필요하지 않습니다. SnapMirror 비동기 영구 라이센스는 새로운 AFF 및 FAS 시스템에 설치된 ONTAP One 소프트웨어 제품군에 포함됩니다.

데이터 보호 구성 제한은 ONTAP 버전, 하드웨어 플랫폼 및 설치된 라이센스를 비롯한 여러 요소를 사용하여 결정됩니다. 자세한 내용은 을 참조하십시오 "Hardware Universe".

SnapMirror 동기식 라이센스

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. SnapMirror 동기식 관계를 생성하려면 다음 라이센스가 필요합니다.

- 소스 클러스터와 대상 클러스터 모두에 SnapMirror 동기식 라이센스가 필요합니다.

  SnapMirror 동기식 라이센스는 의 "ONTAP One 라이센스 제품군"일부입니다.

  2019년 6월 이전에 프리미엄 또는 플래시 번들과 함께 시스템을 구매하신 경우, NetApp 마스터 키를 다운로드하여 NetApp 지원 사이트 에서 필요한 SnapMirror 동기식 라이센스를 얻을 수 있습니다 "마스터 라이센스 키".

- 소스 클러스터와 대상 클러스터 모두에 SnapMirror 라이센스가 필요합니다.

SnapMirror 클라우드 라이센스

ONTAP 9.8부터 SnapMirror 클라우드 라이센스는 ONTAP 인스턴스에서 오브젝트 스토리지 엔드포인트로 스냅샷의 비동기 복제를 제공합니다. 복제 대상은 사내 오브젝트 저장소뿐만 아니라 S3 및 S3 호환 퍼블릭 클라우드 오브젝트 스토리지 서비스를 사용하여 구성할 수 있습니다. SnapMirror 클라우드 관계는 ONTAP 시스템에서 사전 검증된 오브젝트 스토리지 대상까지 지원됩니다.

SnapMirror 클라우드는 독립 실행형 라이센스로 사용할 수 없습니다. ONTAP 클러스터당 하나의 라이센스만 필요합니다. SnapMirror 클라우드 라이센스 외에 SnapMirror 비동기식 라이센스도 필요합니다.

SnapMirror 클라우드 관계를 생성하려면 다음 라이센스가 필요합니다.

- 오브젝트 저장소 엔드포인트로 직접 복제하기 위한 SnapMirror 라이센스와 SnapMirror 클라우드 라이센스 모두
- 다중 정책 복제 워크플로우(예: 디스크-디스크-클라우드)를 구성할 경우 모든 ONTAP 인스턴스에 SnapMirror 라이센스가 필요하며, SnapMirror 클라우드 라이센스는 오브젝트 스토리지 엔드포인트로 직접 복제되는 소스 클러스터에 대해서만 필요합니다.

ONTAP 9.9.1부터 "SnapMirror 클라우드 복제에 System Manager를 사용하십시오"가능합니다.

공인 SnapMirror 클라우드 타사 애플리케이션 목록이 NetApp 웹 사이트에 게시됩니다.

데이터 보호 최적화 라이센스

DPO(Data Protection Optimized) 라이센스는 더 이상 판매되지 않으며 DPO는 현재 플랫폼에서 지원되지 않습니다. 그러나 지원되는 플랫폼에 DPO 라이센스가 설치되어 있는 경우 NetApp은 해당 플랫폼의 가용성이 끝날 때까지 계속해서 지원을 제공합니다.

DPO는 ONTAP One 라이센스 번들에 포함되지 않으며, DPO 라이센스가 시스템에 설치되어 있는 경우 ONTAP One 라이센스 번들로 업그레이드할 수 없습니다.

지원되는 플랫폼에 대한 자세한 내용은 을 참조하십시오 "Hardware Universe".

ONTAP DPO 시스템은 향상된 기능을 제공합니다

ONTAP 9.6부터는 DP_Optimized(DPO) 라이센스가 설치될 때 지원되는 최대 FlexVol 볼륨 수가 증가합니다. ONTAP 9.4부터 DPO 라이센스가 있는 시스템은 SnapMirror 백오프, 볼륨 간 백그라운드 중복제거, 스냅샷 블록을 도너로 사용 및 컴팩션을 지원합니다.

ONTAP 9.6부터 보조 또는 데이터 보호 시스템에서 지원되는 최대 FlexVol 볼륨 수가 증가하여 노드당 최대 2,500개의 FlexVol 볼륨 또는 페일오버 모드에서 최대 5,000개까지 확장할 수 있습니다. 에서 FlexVol 볼륨 증가를 활성화할 수 "DP_Optimized(DPO) 라이센스"있습니다. 소스 노드와 대상 노드 모두에서 A가 "SnapMirror 라이센스"필요합니다.

ONTAP 9.4부터는 DPO 시스템에 다음과 같은 기능이 향상되었습니다.

- SnapMirror 백 오프: DPO 시스템에서 복제 트래픽은 클라이언트 워크로드가 제공하는 것과 동일한 우선순위를 갖습니다.

  DPO 시스템에서는 SnapMirror 백오프가 기본적으로 사용되지 않습니다.

- 볼륨 백그라운드 중복제거 및 볼륨 간 백그라운드 중복제거: DPO 시스템에서 볼륨 백그라운드 중복제거 및 볼륨 간 백그라운드 중복제거가 활성화됩니다.

  'Storage aggregate Efficiency cross-volume-dedupe start-aggregate_aggregate_name_-scan-old-data true' 명령을 실행하여 기존 데이터를 중복 제거할 수 있습니다. 가장 좋은 방법은 사용량이 적은 시간에 명령을 실행하여 성능에 미치는 영향을 줄이는 것입니다.

  에 대한 자세한 내용은 `storage aggregate efficiency cross-volume-dedupe start` "ONTAP 명령 참조입니다"을 참조하십시오.

- 스냅샷 블록을 기부자로 사용하여 공간 절감 증가: 액티브 파일 시스템에서 사용할 수 없지만 스냅샷에 트래핑된 데이터 블록은 볼륨 중복제거의 기부자로 사용됩니다.

  또한 새 데이터는 스냅샷에 트래핑된 데이터로 중복 제거할 수 있어 스냅샷 블록을 효과적으로 공유할 수 있습니다. 도너 공간이 늘어나면 특히 볼륨에 많은 수의 스냅샷이 있을 때 더 많은 절감 효과를 얻을 수 있습니다.

- 컴팩션: DPO 볼륨에서는 데이터 컴팩션이 기본적으로 사용됩니다.

ONTAP SnapMirror 명령의 경로 이름 패턴 일치에 대해 알아봅니다

패턴 일치를 사용하여 '스냅샷 미러' 명령에서 소스 및 대상 경로를 지정할 수 있습니다.

'스냅미러' 명령은 'vserver:volume' 형식으로 정규화된 경로 이름을 사용합니다. SVM 이름을 입력하지 않고 경로 이름을 약어로 입력할 수 있습니다. 이 경우 '스냅샷 미러' 명령은 사용자의 로컬 SVM 컨텍스트를 가정합니다.

SVM이 "vserver1"이라고 하고 볼륨이 "vol1"이라고 가정하면 정규화된 경로 이름은 vserver1:vol1입니다.

경로에서 별표(*)를 와일드카드로 사용하여 일치하는 정규화된 경로 이름을 선택할 수 있습니다. 다음 표에서는 와일드카드를 사용하여 볼륨 범위를 선택하는 예를 보여 줍니다.

'*'	모든 경로를 일치시킵니다.
' vs * '	모든 SVM과 볼륨을 "V"로 시작하는 SVM 이름으로 일치시킵니다.
'*: * src * '	모든 SVM을 'rc' 텍스트가 포함된 볼륨 이름과 일치시킵니다.
' *:vol *'	모든 SVM을 볼륨 이름부터 찾습니다.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 관계 작업의 확장 쿼리에 대해 알아봅니다

_extended query_를 사용하여 여러 SnapMirror 관계에 대해 한 번에 SnapMirror 작업을 수행할 수 있습니다. 예를 들어, 하나의 명령을 사용하여 초기화하려는 초기화되지 않은 SnapMirror 관계가 여러 개 있을 수 있습니다.

이 작업에 대해

다음 SnapMirror 작업에 확장 쿼리를 적용할 수 있습니다.

- 초기화되지 않은 관계를 초기화하는 중입니다
- 중단된 관계를 재개하는 중입니다
- 끊어진 관계를 재동기화합니다
- 유휴 관계를 업데이트하는 중입니다
- 관계 데이터 전송을 중단합니다

단계

1. 다양한 관계에서 SnapMirror 작업 수행:

   '*SnapMirror* 명령{-state 상태} *'

   다음 명령을 실행하면 '초기화되지 않음' 상태인 SnapMirror 관계가 초기화됩니다.

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 관계에 대한 호환 **ONTAP** 버전

소스 및 타겟 볼륨에서 SnapMirror 데이터 보호 관계를 생성하기 전에 호환되는 ONTAP 버전을 실행해야 합니다. ONTAP를 업그레이드하기 전에 현재 ONTAP 버전이 SnapMirror 관계에 대한 대상 ONTAP 버전과 호환되는지 확인해야 합니다.

통합 복제 관계

사내 또는 Cloud Volumes ONTAP 릴리즈를 사용하여 "XDP" 유형의 SnapMirror 관계 구축:

ONTAP 9.9.0부터:

- ONTAP 9.x.0 릴리즈는 클라우드 전용 릴리즈이며 Cloud Volumes ONTAP 시스템을 지원합니다. 릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

  ⓘ ONTAP 9.16.0은 클라우드 전용 규칙에 대한 예외입니다."ASA r2 시스템" . 릴리스 버전 뒤에 있는 더하기 기호(+)는 ASA r2와 클라우드 지원 릴리스를 모두 나타냅니다. ASA r2 시스템은 다른 ASA r2 시스템에 대해서만 SnapMirror 관계를 지원합니다.

- ONTAP 9.x.1 릴리스는 일반 릴리스이며 온-프레미스 및 Cloud Volumes ONTAP 시스템을 모두 지원합니다.

ⓘ 경우 "고급 용량 밸런싱"ONTAP 9.16.1 이상을 실행하는 클러스터의 볼륨에서 이 설정된SnapMirror 전송이 ONTAP ONTAP 9.16.1 이전 버전을 실행하는 클러스터에 지원되지 않습니다.

ⓘ 상호 운용성은 양방향입니다.

• ONTAP 버전 9.4 이상에 대한 상호 운용성*

ONTAP 버전…	이러한 이전 ONTAP 버전과의 상호 작용…																				
	9.18.1	9.17.1	9.16.1	9.16.0 이상	9.15.1	9.15.0 *	9.14.1	9.14.0 *	9.13.1	9.13.0 *	9.12.1	9.12.0 *	9.11.1	9.11.0 *	9.10.1	9.10.0 *	9.9.1	9.9.0 *	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.0 이상	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.15.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.14.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요	아니요	아니요
9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.0 *	아니요	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	아니요	아니요
9.12.1	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요

9.12.0*	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	아니요	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.11.0*	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.10.0*	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.9.0 *	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.8	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.7	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *

SnapMirror 동기식 관계

SnapMirror 동기식은 ONTAP 클라우드 인스턴스에 지원되지 않습니다.

ONTAP 버전 …	이러한 이전 ONTAP 버전과의 상호 작용…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.17.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.16.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요	아니요

9.15.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요	아니요
9.14.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.13.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.12.1	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.11.1	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요	아니요
9.10.1	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요	아니요
9.9.1	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요	아니요
9.8	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *	아니요
9.7	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *	* 예 *
9.6	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *	* 예 *
9.5	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	* 예 *	* 예 *	* 예 *

SnapMirror SVM 재해 복구 관계

- 이 매트릭스는 ONTAP 9.10.1부터 시작되는 SVM 데이터 이동성 마이그레이션 기능에 적용됩니다.
- SVM DR을 사용하면 표시된 제한 사항을 충족하지 않는 SVM을 마이그레이션할 수 있습니다. "SVM 마이그레이션(SVM 데이터 이동성)".
- 두 경우 모두 최대 2개의 주요 최신 ONTAP 버전으로 소스 클러스터와 대상 클러스터를 분리할 수 있으며, 대상 버전은 소스 ONTAP 버전과 동일하거나 더 최신 버전이어야 합니다.

SVM 재해 복구 데이터 및 **SVM** 보호**:**

SVM 재해 복구는 동일한 버전의 ONTAP를 실행하는 클러스터 간에만 지원됩니다. * SVM 복제에 대해 버전 독립성이 지원되지 않습니다 *.

SVM 마이그레이션을 위한 **SVM** 재해 복구**:**

- 복제는 소스의 이전 ONTAP 버전에서 대상에 있는 동일한 버전 또는 이후 버전의 ONTAP로 단일 방향으로 지원됩니다.
- 타겟 클러스터의 ONTAP 버전은 아래 표와 같이 최신 주요 온프레미스 버전 2개 또는 최신 주요 클라우드 버전 2개(ONTAP 9.9.0부터 시작)를 초과할 수 없습니다.
  - 장기 데이터 보호 사용 사례에는 복제가 지원되지 않습니다.

릴리스 버전 뒤의 별표(*)는 클라우드 전용 릴리스를 나타냅니다.

지원을 확인하려면 왼쪽 표 열에서 소스 버전을 찾은 다음 맨 위 행에서 대상 버전을 찾습니다(같은 버전에 대한 DR/마이그레이션 및 최신 버전에 대한 마이그레이션만).

ONTAP 9.10.1 이상을 사용하는 경우 다음을 사용할 수 있습니다. "SVM 데이터 이동성" SVM DR 대신 SVM을 한 클러스터에서 다른 클러스터로 마이그레이션하는 기능을 제공합니다.

출처	목적지

	9.5	9.6	9.7	9.8	9.9.0 *	9.9.1	9.10.0 *	9.10.1	9.11.0 *	9.11.1	9.12.0 *	9.12.1	9.13.0 *	9.13.1	9.14.0 *	9.14.1	9.15.0 *	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1
9.5	DR/마이그레이션	마이그레이션	마이그레이션																			
9.6		DR/마이그레이션	마이그레이션	마이그레이션																		
9.7			DR/마이그레이션	마이그레이션	마이그레이션																	
9.8				DR/마이그레이션	마이그레이션	마이그레이션		마이그레이션														
9.9.0 *					DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션												
9.9.1						DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션												
9.10.0 *							DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션										

9.10.1								DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션								
9.11.0*									DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.11.1										DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션						
9.12.0*											DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션				
9.12.1												DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션				
9.13.0*													DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션		
9.13.1														DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션		

9.14.0*															DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.14.1																DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.0*																	DR/마이그레이션	마이그레이션	마이그레이션	마이그레이션	
9.15.1																		DR/마이그레이션	마이그레이션	마이그레이션	
9.16.0																			DR/마이그레이션	마이그레이션	마이그레이션
9.16.1																				DR/마이그레이션	마이그레이션
9.17.1																					DR/마이그레이션

9.1 8.1																					DR /마 이 그 레 이 션

SnapMirror 재해 복구 관계

"DP" 유형의 SnapMirror 관계 및 정책 유형 ""비동기 미러""의 경우:

DP 유형 미러는 ONTAP 9.11.1부터 초기화할 수 없으며 ONTAP 9.12.1에서 완전히 사용되지 않습니다. 자세한 내용은 을 참조하십시오 "데이터 보호 SnapMirror 관계의 사용 중단".

다음 표에서 왼쪽에 있는 열은 소스 볼륨의 ONTAP 버전을 나타내고, 맨 위 행은 대상 볼륨에 있을 수 있는 ONTAP 버전을 나타냅니다.

출처	목적지								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.10.1	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
9.9.1	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
9.8	아니요	예	예	예	아니요	아니요	아니요	아니요	아니요
9.7	아니요	아니요	예	예	예	아니요	아니요	아니요	아니요
9.6	아니요	아니요	아니요	예	예	예	아니요	아니요	아니요
9.5	아니요	아니요	아니요	아니요	예	예	예	아니요	아니요
9.4	아니요	아니요	아니요	아니요	아니요	예	예	예	아니요
9.3	아니요	아니요	아니요	아니요	아니요	아니요	예	예	예

상호 운용성은 양방향성이 아닙니다.

ONTAP SnapMirror 제한 사항에 대해 알아보십시오

데이터 보호 관계를 생성하기 전에 기본적인 SnapMirror 제한을 숙지해야 합니다.

- 타겟 볼륨에는 소스 볼륨이 하나만 있을 수 있습니다.

  소스 볼륨에는 여러 개의 대상 볼륨이 있을 수 있습니다. 타겟 볼륨은 모든 유형의 SnapMirror 복제 관계의 소스 볼륨이 될 수 있습니다.

- 스토리지 모델에 따라 단일 소스 볼륨에서 최대 8개 또는 16개의 대상 볼륨을 팬아웃할 수 있습니다. 를 참조하십시오 "Hardware Universe" 를 참조하십시오.
- SnapMirror DR 관계의 대상에 파일을 복원할 수 없습니다.

- 소스 또는 대상 SnapVault 볼륨은 32비트일 수 없습니다.
- SnapVault 관계의 소스 볼륨은 FlexClone 볼륨이 아니어야 합니다.

> 관계는 작동하지만 FlexClone 볼륨에서 제공하는 효율성은 유지되지 않습니다.

SnapMirror 볼륨 복제를 구성합니다

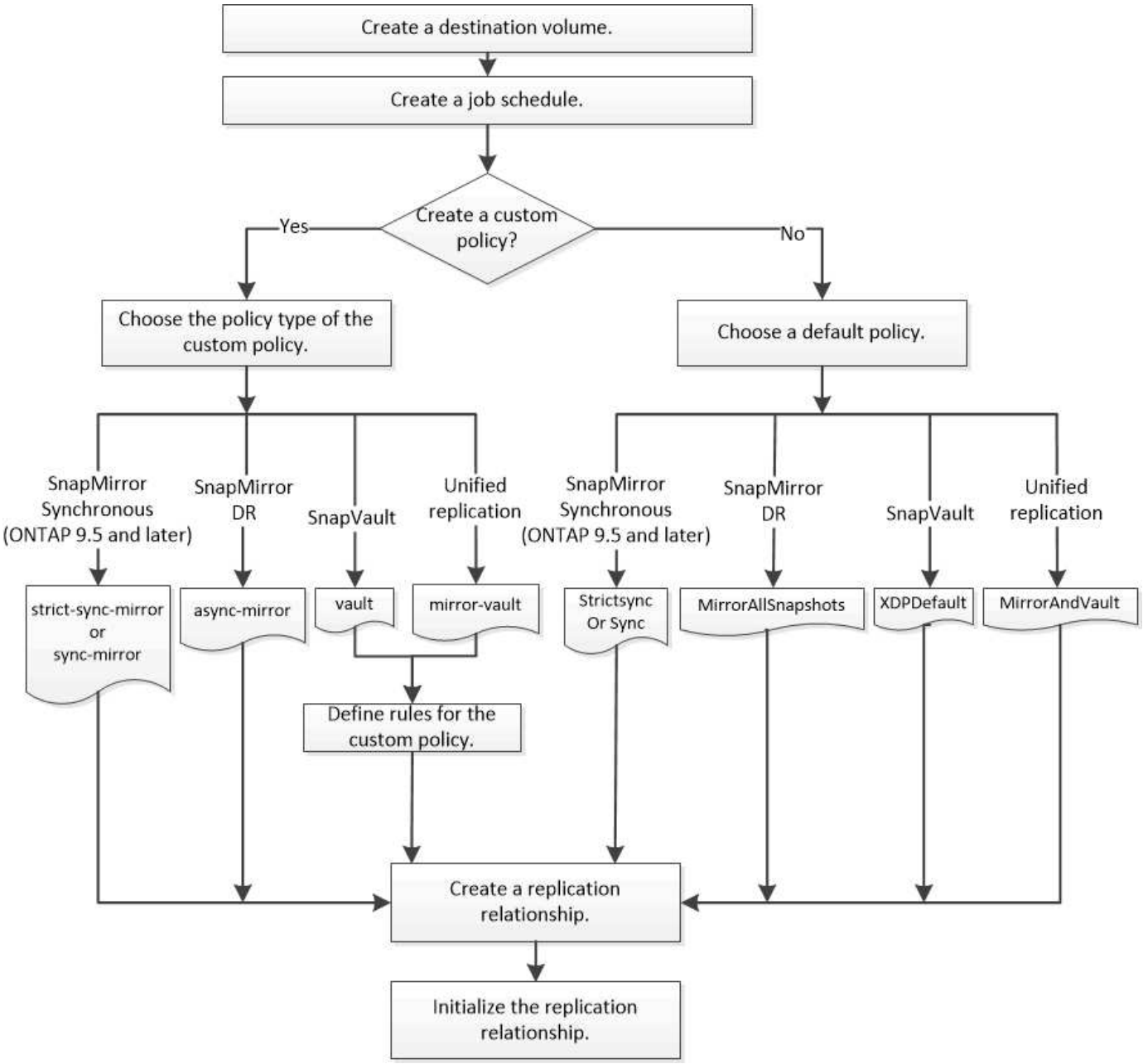
ONTAP SnapMirror 복제 워크플로우

SnapMirror는 SnapMirror DR, 아카이브(이전의 SnapVault) 및 통합 복제라는 세 가지 유형의 데이터 보호 관계를 제공합니다. 동일한 기본 워크플로를 따라 각 관계 유형을 구성할 수 있습니다.

ONTAP 9.9.1부터는 GA될 수 있습니다. "SnapMirror 활성 동기화" 제로 RTO(Zero Recovery Time Objective) 또는 TAF(Transparent Application Failover)를 제공하여 SAN 환경에서 업무상 중요한 애플리케이션의 자동 페일오버를 지원합니다.

SnapMirror 데이터 보호 관계의 각 유형에 대해 워크플로는 동일합니다. 대상 볼륨 생성, 작업 일정 생성, 정책 지정, 관계 생성 및 초기화

ONTAP 9.3부터는 '스냅샷 보호' 명령을 사용하여 한 번에 데이터 보호 관계를 구성할 수 있습니다. 스냅샷 보호 기능을 사용하더라도 워크플로우의 각 단계를 이해해야 합니다.



관련 정보

- "SnapMirror 보호"

한 번에 **ONTAP SnapMirror** 복제 관계를 구성합니다

ONTAP 9.3부터 다음을 사용할 수 있습니다. `snapmirror protect` 단일 단계로 데이터 보호 관계를 구성하는 명령입니다. 복제할 볼륨 목록, 대상 클러스터의 SVM, 작업 일정 및 SnapMirror 정책을 지정합니다. `snapmirror protect` 나머지는 다 해줍니다.

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 대상 볼륨의 언어는 소스 볼륨의 언어와 동일해야 합니다.

이 작업에 대해

'스냅샷 보호' 명령은 지정된 SVM과 연결된 애그리게이트를 선택합니다. SVM과 연결된 애그리게이트가 없으면 클러스터의 모든 애그리게이트 중에서 선택합니다. Aggregate는 여유 공간의 양과 애그리게이트의 볼륨 수를 기준으로 합니다.

그런 다음 'napmirror protect' 명령은 다음 단계를 수행합니다.

- 복제할 볼륨 목록에서 각 볼륨에 대해 적절한 유형과 예약된 공간을 사용하여 대상 볼륨을 생성합니다.
- 지정한 정책에 적합한 복제 관계를 구성합니다.
- 관계를 초기화합니다.

대상 볼륨의 이름은 '*source_volume_name_dst*' 형식입니다. 기존 이름과 충돌하는 경우 명령이 볼륨 이름에 번호를 추가합니다. 명령 옵션에서 접두사 및/또는 접미사를 지정할 수 있습니다. 접미사는 시스템 제공 st 접미사를 대체합니다.

ONTAP 9.4 이상에서는 대상 볼륨에 최대 1019개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 및 이전 버전에서는 대상 볼륨에 최대 251개의 스냅샷을 포함할 수 있습니다.

> ⓘ 초기화에는 시간이 오래 걸릴 수 있습니다. 스냅미러 보호 기능은 작업이 완료되기 전에 초기화가 완료될 때까지 기다리지 않습니다. 따라서 초기화가 완료되는 시점을 결정하려면 job show 명령 대신 sapmirror show 명령을 사용해야 합니다.

ONTAP 9.5부터 `snapmirror protect` 명령을 사용하여 SnapMirror 동기식 관계를 만들 수 있습니다.

자세히 알아보세요 `snapmirror protect` 에서 "ONTAP 명령 참조입니다" .

단계

1. 한 단계로 복제 관계를 생성하고 초기화합니다.

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > ⓘ 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. '-auto-initialize' 옵션은 기본적으로 ""true""로 설정됩니다.

   다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성하고 초기화합니다.

   ```
   cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
   -destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
   replication_daily
   ```

원하는 경우 사용자 지정 정책을 사용할 수 있습니다. 자세한 내용은 을 참조하십시오 "사용자 지정 복제 정책 생성".

다음 예에서는 기본 "XDPDefault" 정책을 사용하여 SnapVault 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

다음 예제에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

다음 예에서는 기본 `Sync` 정책을 사용하여 SnapMirror 동기식 관계를 만들고 초기화합니다.

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

SnapVault 및 통합 복제 정책의 경우 대상에서 마지막으로 전송된 스냅샷의 복제본을 생성하기 위한 일정을 정의하는 것이 유용할 수 있습니다. 자세한 내용은 을 "대상에 로컬 복제본을 생성하기 위한 스케줄 정의"참조하십시오.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "작업 표시"

한 번에 한 단계씩 복제 관계를 구성합니다

ONTAP SnapMirror 대상 볼륨을 생성합니다

타겟에서 명령을 사용하여 대상 볼륨을 생성할 수 `volume create` 있습니다. 대상 볼륨의 크기는 소스 볼륨보다 크거나 같아야 합니다. 에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 대상 볼륨 생성:

   'volume create-vserver_SVM_-volume volume-aggregate_aggregate_-type DP-size_size_'

다음 예에서는 이름이 "VolA_DST"인 2GB 대상 볼륨을 생성합니다.

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
-aggregate node01_aggr -type DP -size 2GB
```

ONTAP SnapMirror 복제 작업 일정을 생성합니다

작업 일정은 SnapMirror에서 일정이 할당된 데이터 보호 관계를 자동으로 업데이트할지 여부를 결정합니다. System Manager 또는 명령을 사용하여 복제 작업 일정을 생성할 수 `job schedule cron create` 있습니다. 에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

이 작업에 대해

데이터 보호 관계를 생성할 때 작업 일정을 할당합니다. 작업 일정을 할당하지 않으면 관계를 수동으로 업데이트해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 복제 작업 일정을 생성할 수 있습니다.

시스템 관리자

1. Protection > Overview * 로 이동한 후 * Local policy settings * 를 확장합니다.
2. Schedules * 창에서 를 →클릭합니다.
3. Schedules * 창에서 를 + Add 클릭합니다.
4. 일정 추가 * 창에서 일정 이름을 입력하고 컨텍스트 및 일정 유형을 선택합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 작업 일정 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

ONTAP 9.10.1.1부터는 작업 일정에 SVM을 포함할 수 있습니다.

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

볼륨 SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 5분입니다. 볼륨 SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

SnapMirror 복제 정책을 사용자 지정합니다

사용자 지정 **ONTAP SnapMirror** 복제 정책을 생성합니다

관계의 기본 정책이 적합하지 않은 경우 사용자 지정 복제 정책을 생성할 수 있습니다. 예를 들어 네트워크 전송에서 데이터를 압축하거나 SnapMirror에서 스냅샷을 전송하는 시도 횟수를 수정할 수 있습니다.

복제 관계를 생성할 때 기본 또는 사용자 지정 정책을 사용할 수 있습니다. 사용자 지정 아카이브(이전 SnapVault) 또는 통합 복제 정책의 경우 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 _rules_를 하나 이상 정의해야 합니다. 대상에 로컬 스냅샷을 생성하기 위한 스케줄을 정의할 수도 있습니다.

복제 정책의 _policy type_은 이 정책이 지원하는 관계 유형을 결정합니다. 아래 표에는 사용 가능한 정책 유형이 나와 있습니다.

정책 유형입니다	관계 유형
비동기식 - 미러	SnapMirror DR
볼트	SnapVault
대칭 복사 - 볼트	통합 복제
엄격한 동기식 미러링	StrictSync 모드의 SnapMirror 동기(ONTAP 9.5부터 지원됨)
동기식-미러	동기화 모드의 SnapMirror 동기(ONTAP 9.5부터 지원됨)

사용자 지정 복제 정책을 생성할 때는 기본 정책 다음에 정책을 모델링하는 것이 좋습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 맞춤형 데이터 보호 정책을 생성할 수 있습니다. ONTAP 9.11.1부터 System Manager를 사용하여 사용자 정의 미러 및 볼트 정책을 생성하고 레거시 정책을 표시 및 선택할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.

소스 클러스터와 대상 클러스터 모두에 사용자 지정 보호 정책을 생성합니다.

시스템 관리자

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭합니다.
2. 보호 정책 * 에서 을 →클릭합니다.
3. 보호 정책 * 창에서 을 + Add 클릭합니다.
4. 새 정책 이름을 입력하고 정책 범위를 선택합니다.
5. 정책 유형을 선택합니다. 볼트 전용 또는 미러 전용 정책을 추가하려면 * Asynchronous * 를 선택하고 * 기존 정책 유형 사용 * 을 클릭합니다.
6. 필수 필드에 내용을 입력합니다.
7. 저장 * 을 클릭합니다.
8. 다른 클러스터에서 이 단계를 반복합니다.

CLI를 참조하십시오

1. 사용자 지정 복제 정책 생성:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

ONTAP 9.5부터 매개 변수를 사용하여 SnapMirror 동기식 관계에 대한 일반 스냅샷 스케줄을 생성하기 위한 스케줄을 지정할 수 `-common-snapshot-schedule` 있습니다. 기본적으로 SnapMirror 동기식 관계에 대한 일반적인 스냅샷 일정은 1시간입니다. SnapMirror 동기식 관계의 스냅샷 스케줄에 대해 30분에서 2시간 사이의 값을 지정할 수 있습니다.

다음 예에서는 데이터 전송에 대해 네트워크 압축을 활성화하는 SnapMirror DR에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

다음 예에서는 SnapVault에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

다음 예에서는 통합 복제에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

다음 예에서는 StrictSync 모드에서 SnapMirror 동기식 관계에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

에 대한 자세한 내용은 `snapmirror policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

"'볼트' 및 "미러 볼트" 정책 유형의 경우 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 규칙을 정의해야 합니다.

사용하세요 `snapmirror policy show` SnapMirror 정책이 생성되었는지 확인하는 명령입니다.

자세히 알아보세요 `snapmirror policy show` 에서 "ONTAP 명령 참조입니다" .

ONTAP SnapMirror 정책에 대한 규칙을 정의합니다

또는 `mirror-vault` 정책 유형을 사용하는 사용자 지정 정책의 경우 `vault` 초기화 및 업데이트 중에 전송되는 스냅샷을 결정하는 규칙을 하나 이상 정의해야 합니다. 또는 `mirror-vault` 정책 유형을 사용하여 기본 정책에 대한 규칙을 정의할 수도 `vault` 있습니다.

이 작업에 대해

또는 `mirror-vault` 정책 유형을 사용하는 모든 정책에는 `vault` 복제할 스냅샷을 지정하는 규칙이 있어야 합니다. 예를 들어 이 규칙은 `bi-monthly` SnapMirror 레이블이 할당된 스냅샷만 복제해야 함을 `bi-monthly` 나타냅니다. 소스에서 스냅샷 정책을 구성할 때 SnapMirror 레이블을 지정합니다.

각 정책 유형은 하나 이상의 시스템 정의 규칙과 연결됩니다. 이러한 규칙은 정책 유형을 지정할 때 정책에 자동으로 할당됩니다. 아래 표에는 시스템 정의 규칙이 나와 있습니다.

시스템 정의 규칙	정책 유형에 사용됩니다	결과
SM_생성됨	비동기 미러, 미러 볼트, 동기화, StrictSync	SnapMirror에 의해 생성된 스냅샷은 초기화 및 업데이트 시 전송됩니다.
ALL_SOURCE_SNAPSHOTS 를 선택합니다	비동기식 - 미러	초기화 및 업데이트 시 소스의 새 스냅샷이 전송됩니다.
매일	볼트, 미러 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `daily` 전송됩니다.
매주	볼트, 미러 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `weekly` 전송됩니다.

매월	대칭 복사 - 볼트	초기화 및 업데이트 시 SnapMirror 레이블이 있는 소스의 새 스냅샷이 `monthly` 전송됩니다.
app_consistent	동기화, StrictSync	소스에 SnapMirror 레이블이 있는 스냅샷은 `app_consistent` 동기식으로 대상에 복제됩니다. ONTAP 9.7부터 지원됩니다.

""비동기 미러" 정책 유형을 제외하고 필요에 따라 기본 또는 사용자 지정 정책에 대한 추가 규칙을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- 기본 정책의 경우 `MirrorAndVault` 소스의 스냅샷을 SnapMirror 레이블과 일치시키기 위해 `bi-monthly` 이라는 규칙을 생성할 수 `bi-monthly` 있습니다.
- 정책 유형이 지정된 사용자 지정 정책의 경우 `mirror-vault` 소스의 스냅숏을 SnapMirror 레이블과 일치시키기 위해 `bi-weekly` 이라는 규칙을 만들 수 `bi-weekly` 있습니다.

단계

1. 정책의 규칙 정의:

   '스냅샷 정책 추가 규칙 -vserver_SVM_-policy_policy_for_rule_-snapmirror-label_snapmirror-label_ -keep_retention_count_'

   다음 예제에서는 기본 MirorAndVault 정책에 SnapMirror 레이블 '격월'이 있는 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   다음 예에서는 사용자 지정 my_SnapVault 정책에 SnapMirror 레이블 "격주"가 포함된 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   다음 예에서는 사용자 지정 'Sync' 정책에 SnapMirror 레이블 'app_consistent'가 포함된 규칙을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

   그런 다음 이 SnapMirror 레이블과 일치하는 소스 클러스터에서 스냅샷을 복제할 수 있습니다.

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

ONTAP SnapMirror 스케줄을 정의하여 대상에 로컬 복제본을 생성합니다

SnapVault 및 통합 복제 관계의 경우 마지막으로 전송된 스냅샷의 복사본을 대상에 생성하여 업데이트된 스냅샷이 손상되는 것을 방지할 수 있습니다. 이 "로컬 복사본"은 소스의 보존 규칙에 관계없이 보존되므로 SnapMirror에서 원래 전송한 스냅샷을 소스에서 더 이상 사용할 수 없는 경우에도 대상에서 해당 복제본을 사용할 수 있습니다.

이 작업에 대해

로컬 복사본을 만드는 일정을 지정합니다. `-schedule` 옵션 `snapmirror policy add-rule` 명령.

단계

1. 대상에 로컬 복제본을 생성하기 위한 스케줄을 정의합니다.

   '스냅샷 정책 추가-규칙-vserver_SVM_-policy_policy_for_rule_-snapmirror-label_snapmirror-label_ -schedule_schedule_'

   작업 일정을 작성하는 방법에 대한 예는 을 참조하십시오"복제 작업 스케줄 생성".

   다음 예제에서는 기본 MirorAndVault 정책에 로컬 복사본을 만들기 위한 일정을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   다음 예에서는 사용자 지정 my_unified" 정책에 로컬 복사본을 만들기 위한 일정을 추가합니다.

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 복제 관계를 생성합니다

운영 스토리지의 소스 볼륨과 보조 스토리지의 대상 볼륨 간의 관계를 _ 데이터 보호 관계라고 합니다. _ 명령을 사용하여 SnapMirror DR, SnapVault 또는 통합 복제 데이터 보호 관계를 생성할 수 있습니다. `snapmirror create`

> ⓘ 이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 복제 관계를 생성합니다. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 미리 작성된 사용자 정의 미러 및 볼트 정책을 선택하고, 레거시 정책을 표시 및 선택하고, 볼륨 및 스토리지 VM을 보호할 때 보호 정책에 정의된 전송 일정을 재정의할 수 있습니다. 이 기능은 ONTAP 9.8P12 이상의 ONTAP 9.8 패치에서도 사용할 수 있습니다.

ONTAP 9.8P12 이상 ONTAP 9.8 패치 릴리즈를 사용하고 시스템 관리자를 사용하여 SnapMirror를 구성한 경우, ONTAP 9.9.1 또는 ONTAP 9.10.1 릴리즈로 업그레이드할 계획이면 ONTAP 9.9.1.1P13 이상 및 ONTAP 9.10.1P10 이상 패치 릴리즈를 사용해야 합니다.

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 대상 볼륨의 언어는 소스 볼륨의 언어와 동일해야 합니다.

이 작업에 대해

ONTAP 9.3까지 SnapMirror는 DP 모드에서 호출되고 SnapMirror는 XDP 모드에서 호출될 때까지 서로 다른 복제 엔진을 사용했으며, 버전 의존성에 대한 접근법도 다릅니다.

- DP 모드에서 호출된 SnapMirror는 ONTAP 버전이 운영 스토리지와 2차 스토리지에서 동일해야 하는 _version-dependent_replication 엔진을 사용합니다.

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- XDP 모드에서 호출된 SnapMirror는 운영 스토리지와 보조 스토리지에서 서로 다른 ONTAP 버전을 지원하는 _version-flexible_replication 엔진을 사용했습니다.

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

성능이 향상됨에 따라 버전에 상관없이 유연한 SnapMirror의 주요 이점이 버전에 따라 달라지는 복제 처리량의 약간 이점보다 훨씬 큽니다. 이러한 이유로 ONTAP 9.3부터 XDP 모드가 새로운 기본값이 되었으며 명령줄이나 신규 또는 기존 스크립트에서 DP 모드를 호출하는 경우 XDP 모드가 자동으로 XDP 모드로 변환됩니다.

기존 관계는 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. 아래 표에는 예상되는 동작이 나와 있습니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAllSnapshots(SnapMirror DR)
XDP	XDP	XDPDefault(SnapVault)

아래 절차의 예를 참조하십시오.

변환 예외 사항은 다음과 같습니다.

- SVM 데이터 보호 관계는 DP 모드로 계속 기본이 됩니다.

  XDP를 명시적으로 지정하여 기본 MirorAllSnapshots 정책으로 XDP 모드를 가져옵니다.

- 로드 공유 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- SnapLock 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- DP의 명시적 호출은 다음 클러스터 전체 옵션을 설정한 경우 계속해서 DP 모드로 설정됩니다.

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DP를 명시적으로 호출하지 않으면 이 옵션은 무시됩니다.

ONTAP 9.14.1부터, `-backoff-level` 및 명령에 옵션이 추가되어 `snapmirror create` `snapmirror modify` `snapmirror restore` 관계별 백오프 레벨을 지정할 수 있습니다. 이 옵션은 FlexVol SnapMirror 관계에서만 지원됩니다. 선택적 명령은 클라이언트 작업에 따른 SnapMirror 백 오프 레벨을 지정합니다. Backoff 값은 high, medium 또는 none일 수 있습니다. 기본값은 high 입니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다.

ONTAP 9.4 이상에서는 대상 볼륨에 최대 1019개의 스냅샷을 포함할 수 있습니다. ONTAP 9.3 및 이전 버전에서는 대상 볼륨에 최대 251개의 스냅샷을 포함할 수 있습니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 복제 관계를 생성할 수 있습니다.

시스템 관리자

1. 보호할 볼륨 또는 LUN을 선택합니다. * 스토리지 > 볼륨 * 또는 * 스토리지 > LUN * 을 클릭한 다음 원하는 볼륨 또는 LUN 이름을 클릭합니다.
2. 을 Protect 클릭합니다.
3. 대상 클러스터와 스토리지 VM을 선택합니다.
4. 비동기식 정책이 기본적으로 선택됩니다. 동기식 정책을 선택하려면 * 추가 옵션 * 을 클릭합니다.
5. 보호 * 를 클릭합니다.
6. 선택한 볼륨 또는 LUN의 * SnapMirror(로컬 또는 원격) * 탭을 클릭하여 보호가 올바르게 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 복제 관계를 생성합니다.

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   `schedule`매개 변수는 SnapMirror 동기식 관계를 생성할 때 적용할 수 없습니다.

   다음 예에서는 기본 'MirorLatest' 정책을 사용하여 SnapMirror DR 관계를 생성합니다.

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   다음 예에서는 기본 "XDPDefault" 정책을 사용하여 SnapVault 관계를 생성합니다.

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   다음 예에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 생성합니다.

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

   다음 예에서는 사용자 지정 my_unified" 정책을 사용하여 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

다음 예에서는 기본 `Sync` 정책을 사용하여 SnapMirror 동기식 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

다음 예에서는 기본 `StrictSync` 정책을 사용하여 SnapMirror 동기식 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. DP 유형이 자동으로 XDP로 변환되고 정책이 지정되지 않은 경우 정책은 기본적으로 'MirorAllSnapshots' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. 유형이나 정책이 지정되지 않은 경우 정책은 기본적으로 'MirorAllSnapshots' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

다음 예에서는 SnapMirror DR 관계를 생성합니다. 정책이 지정되지 않은 경우 정책은 기본적으로 'XDPDefault' 정책으로 설정됩니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

다음 예에서는 사전 정의된 정책과 SnapMirror 동기식 관계를 `SnapCenterSync` 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

미리 정의된 정책의 `SnapCenterSync` 유형이 `Sync`입니다. 이 정책은 "`app_consistent`"로 생성된 모든 스냅샷을 `snapmirror-label` 복제합니다.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "SnapMirror 페일오버 테스트 볼륨을 생성하고 삭제합니다"..

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SnapVault를 사용한 볼륨 백업 개요"

관련 정보

- "SnapMirror 생성"

ONTAP SnapMirror 복제 관계를 초기화합니다

모든 관계 유형에 대해 초기화는 a_baseline transfer_:를 수행합니다. 즉, 소스 볼륨의 스냅샷을 생성한 다음 해당 복사본과 해당 복제본이 참조하는 모든 데이터 블록을 대상 볼륨에 전송합니다. 그렇지 않으면 전송 내용이 정책에 따라 달라집니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

"클러스터 및 SVM 피어링"

이 작업에 대해

초기화에는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 기준 전송을 실행할 수 있습니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다.

노드 재부팅, 인수/반환 또는 패닉 등의 이유로 파일 시스템이 재부팅되는 경우 초기화가 자동으로 재개되지 않으므로 수동으로 다시 시작해야 합니다.

단계

1. 복제 관계 초기화:

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 미러 볼트 배포에서 공통 스냅샷을 보장합니다

당신은 사용할 수 있습니다 `snapmirror snapshot-owner create` 미러-볼트 배포 환경에서 보조 노드에 레이블이 지정된 스냅샷을 보존하는 명령입니다. 이렇게 하면 볼트 관계 업데이트를 위한 공통 스냅샷이 생성됩니다.

이 작업에 대해

미러 볼트 팬 아웃 또는 캐스케이드 배포를 함께 사용하는 경우 소스 및 대상 볼륨에 공통 스냅샷이 없으면 업데이트가 실패한다는 점에 유의해야 합니다.

SnapMirror는 업데이트를 수행하기 전에 항상 소스 볼륨의 스냅샷을 생성하므로 미러 볼트 팬아웃 또는 캐스케이드 배포에서는 미러 관계에 문제가 되지 않습니다.

그러나 SnapMirror는 볼트 관계를 업데이트할 때 원본 볼륨의 스냅샷을 생성하지 않기 때문에 볼트 관계의 문제일 수 있습니다. 볼트 관계의 원본과 대상 모두에 공통 스냅샷이 하나 이상 있는지 확인하려면 을 사용해야 `snapmirror snapshot-owner create` 합니다. "데이터 보호 팬아웃 및 캐스케이드 구축에 대해 자세히 알아보십시오"..

단계

1. 소스 볼륨에서 보존하려는 레이블이 지정된 스냅샷에 소유자를 할당합니다.

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   다음 예에서는 `ApplicationA` 스냅샷의 소유자로 `snap1` 할당합니다.

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   자세히 알아보세요 `snapmirror snapshot-owner create` 에서 "ONTAP 명령 참조입니다" .

2. 에 설명된 대로 미러 관계를 업데이트합니다 "복제 관계를 수동으로 업데이트합니다".

   또는 미러 관계의 예약된 업데이트를 기다릴 수 있습니다.

3. 레이블이 지정된 스냅샷을 볼트 대상으로 전송:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

다음 예에서는 **snap1** 스냅샷을 전송합니다

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

볼트 관계가 업데이트될 때 레이블이 지정된 스냅샷이 보존됩니다.

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 소스 볼륨에서 레이블이 지정된 스냅샷에서 소유자를 제거합니다.

'스냅샷-소유자 삭제 - vserver_SVM_-volume_volume_-snapshot_snapshot_-owner_owner_'

다음 예에서는 스냅샷 소유자로서 `snap1` 를 제거합니다 `ApplicationA`.

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

에 대한 자세한 내용은 `snapmirror snapshot-owner delete` "ONTAP 명령 참조입니다"을 참조하십시오.

예: **ONTAP SnapMirror** 볼트-볼트 캐스케이드를 구성합니다

한 번에 한 단계씩 복제 관계를 구성하는 방법을 구체적으로 보여 주는 예가 나와 있습니다. 이 예제에서 구성한 볼트-볼트 캐스케이드 배포를 사용하여 라벨이 붙은 251개 이상의 스냅샷을 보존할 수 `my-weekly` 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

이 작업에 대해

이 예제에서는 다음을 가정합니다.

- 소스 클러스터에 SnapMirror 레이블, `my-weekly` 및 `my-monthly` 을 사용하여 스냅샷을 구성했습니다. `my-daily`
- 2차 및 3차 대상 클러스터에 이라는 대상 볼륨을 구성했습니다. `volA`
- 2차 및 3차 대상 클러스터에서 이름이 지정된 복제 작업 일정을 구성했습니다. `my_snapvault`

이 예에서는 두 개의 사용자 지정 정책을 기반으로 복제 관계를 생성하는 방법을 보여 줍니다.

- 이 `snapvault_secondary` 정책은 2차 대상 클러스터에 매일 7개, 주별 52개 및 월별 180개의 스냅샷을 보존합니다.
- 는 `snapvault_tertiary policy` 3차 대상 클러스터에 매주 250개의 스냅샷을 보존합니다.

단계

1. 보조 대상 클러스터에서 정책을 생성합니다 `snapvault_secondary`.

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-daily`.

   'cluster_secondary::> snapmirror policy add-rule-policy snapvault_secondary-snapmirror-label my-daily-keep 7-vserver svm_secondary'

3. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-weekly`.

   'cluster_secondary::> snapmirror policy add-rule-policy snapvault_secondary-snapmirror-label my-weekly-keep 52-vserver svm_secondary'

4. 보조 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-monthly`.

   'cluster_secondary::> SnapMirror 정책 add-rule-policy snapvault_secondary-snapmirror-label my-monthly-keep 180-vserver svm_secondary'

5. 보조 대상 클러스터에서 정책을 확인합니다.

   'cluster_secondary:::> snapmirror policy show snapvault_secondary-instance'

```
                     Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily               7  false       0 -
-
                              my-weekly             52  false       0 -
-
                              my-monthly           180  false       0 -
-
```

6. 보조 대상 클러스터에서 소스 클러스터와의 관계를 생성합니다.

   'cluster_secondary::> snapmirror create-source-path svm_primary: VolA-destination-path svm_secondary: VolA-type XDP - schedule my_SnapVault-policy SnapVault_secondary'

7. 보조 대상 클러스터에서 소스 클러스터와의 관계를 초기화합니다.

   'cluster_secondary::> snapmirror initialize-source-path svm_primary: VolA-destination-path svm_secondary: VolA'

8. 3차 대상 클러스터에서 `snapvault_tertiary` 정책을 생성합니다.

   ```
   cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type vault -comment "Policy on tertiary for vault to vault cascade" -vserver svm_tertiary
   ```

9. 3차 대상 클러스터에서 정책에 대한 규칙을 정의합니다 `my-weekly`.

   'cluster_tertiary::> SnapMirror 정책 add-rule-policy snapvault_tertiary-snapmirror-label my-weekly-keep 250-vserver svm_tertiary'

10. 3차 대상 클러스터에서 정책을 확인합니다.

    'cluster_tertiary:::> snapmirror policy show snapvault_tertiary-instance'

    ```
                        Vserver: svm_tertiary
          SnapMirror Policy Name: snapvault_tertiary
          SnapMirror Policy Type: vault
                    Policy Owner: cluster-admin
                     Tries Limit: 8
                Transfer Priority: normal
       Ignore accesstime Enabled: false
         Transfer Restartability: always
     Network Compression Enabled: false
                 Create Snapshot: false
                         Comment: Policy on tertiary for vault to vault
    cascade
           Total Number of Rules: 1
                      Total Keep: 250
                           Rules: SnapMirror Label     Keep  Preserve Warn
    Schedule Prefix
                                  ----------------     ----  -------- ----
    -------- ------
                                  my-weekly             250  false       0 -
    -
    ```

11. 3차 대상 클러스터에서 2차 클러스터와의 관계를 생성합니다.

    'cluster_tertiary::> snapmirror create-source-path svm_secondary: VolA-destination-path svm_tertiary:

VolA-type XDP - schedule my_SnapVault-policy SnapVault_tertiary'

12. 3차 대상 클러스터에서 2차 클러스터와의 관계를 초기화합니다.

    'cluster_tertiary::> snapmirror initialize-source-path svm_secondary: VolA-destination-path svm_tertertiary: VolA'

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 추가 규칙"
- "스냅미러 정책 생성"
- "스냅미러 정책 보기"

SnapMirror 볼륨 복제를 관리합니다

기존 ONTAP SnapMirror DP 유형 관계를 XDP로 변환합니다

ONTAP 9.12.1 이상으로 업그레이드하는 경우 업그레이드하기 전에 DP 유형 관계를 XDP로 변환해야 합니다. ONTAP 9.12.1 이상은 DP 유형 관계를 지원하지 않습니다. 기존 DP 유형 관계를 XDP로 쉽게 변환하여 버전에 상관없이 유연한 SnapMirror를 활용할 수 있습니다.

ONTAP 9.12.1로 업그레이드하기 전에 기존 DP 유형 관계를 XDP로 변환해야 ONTAP 9.12.1 이상 릴리즈로 업그레이드할 수 있습니다.

이 작업에 대해

- SnapMirror는 기존 DP 유형 관계를 XDP로 자동 변환하지 않습니다. 관계를 변환하려면 기존 관계를 분리 및 삭제하고 새로운 XDP 관계를 생성한 다음 관계를 다시 동기화해야 합니다.
- 전환을 계획할 때는 XDP SnapMirror 관계의 백그라운드 준비 및 데이터 웨어하우징 단계에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

> SnapMirror 관계 유형을 DP에서 XDP로 변환한 후에는 자동 크기 조정 및 공간 보장과 같은 공간 관련 설정이 더 이상 대상에 복제되지 않습니다.

단계

1. 대상 클러스터에서 SnapMirror 관계가 DP 유형이고, 미러 상태가 SnapMired 상태이고, 관계 상태가 Idle 상태이고, 관계가 정상 상태인지 확인합니다.

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   다음 예제는 'napmirror show' 명령의 출력을 보여줍니다.

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

명령 출력의 복사본을 유지하여 기존 관계 설정을 추적하는 것이 유용할 수 있습니다 `snapmirror show`. 에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 소스 볼륨과 대상 볼륨에서 두 볼륨에 모두 공통 스냅샷이 있는지 확인합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예에서는 를 보여 줍니다 `volume snapshot show` 소스 및 대상 볼륨의 출력:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 변환 중에 예약된 업데이트가 실행되지 않도록 하려면 기존 DP 유형 관계를 중지합니다.

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 설정합니다.

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 기존 DP 유형 관계 끊기:

```
snapmirror break -destination-path <SVM:volume>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 볼륨에 스냅샷 자동 삭제가 설정되어 있는 경우 비활성화합니다.

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

다음 예에서는 대상 볼륨에서 스냅샷 자동 삭제를 `volA_dst` 비활성화합니다.

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 기존 DP 유형 관계 삭제:

```
snapmirror delete -destination-path <SVM:volume>
```

에 대한 자세한 내용은 `snapmirror-delete` "ONTAP 명령 참조입니다"을 참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 삭제합니다.

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. 소스에서 원본 SVM 재해 복구 관계 해제:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

다음 예에서는 SVM 재해 복구 관계를 해제합니다.

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 'napmirror show' 명령에서 보존한 출력을 사용하여 새로운 XDP 유형 관계를 생성할 수 있습니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

새 관계는 동일한 소스 볼륨과 타겟 볼륨을 사용해야 합니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 소스 볼륨 간에 SnapMirror 재해 복구 관계를 생성합니다 `volA` 켜짐 `svm1` 및 타겟 볼륨입니다 `volA_dst` 켜짐 `svm_backup` 기본값 사용 `MirrorAllSnapshots` 정책:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. 소스 및 대상 볼륨 재동기화:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

재동기화 시간을 개선하려면 다음을 사용할 수 있습니다. `-quick-resync` 옵션은 있지만 저장 효율성으로 인한 절감 효과가 사라질 수 있다는 점을 알아야 합니다.

> ⓘ 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 재동기화한다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

자세히 알아보세요 `snapmirror resync` 에서 "ONTAP 명령 참조입니다" .

10. 스냅샷의 자동 삭제를 해제한 경우 다시 설정합니다.

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

작업을 마친 후

1. 를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

   에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. SnapMirror XDP 대상 볼륨이 SnapMirror 정책에 정의된 대로 스냅샷 업데이트를 시작하면 소스 클러스터의 명령 출력을 사용하여 `snapmirror list-destinations` 새 SnapMirror XDP 관계를 표시합니다.

DP 유형 관계에 대한 추가 정보

ONTAP 9.3부터 XDP 모드가 기본값이며 명령줄이나 새 스크립트 또는 기존 스크립트에서 DP 모드를 호출하면 자동으로 XDP 모드로 변환됩니다.

기존 관계는 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. ONTAP 9.5부터 MirrorAndVault는 데이터 보호 모드가 지정되지 않았거나 XDP 모드가 관계 유형으로 지정된 경우 기본 정책입니다. 아래 표는 예상되는 동작을 보여줍니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAndVault(통합 복제)
XDP	XDP	MirrorAndVault(통합 복제)

표에서 볼 수 있듯이 다른 상황에서 XDP에 할당된 기본 정책은 변환이 이전 유형과 동일한 기능을 유지하도록 합니다. 물론 필요에 따라 통합 복제에 대한 정책을 비롯한 다양한 정책을 사용할 수 있습니다.

지정하는 경우…	정책은…	그 결과…
DP	MirrorAllSnapshots을 선택합니다	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault를 선택합니다
통합 복제	XDP	MirrorAllSnapshots을 선택합니다
SnapMirror DR	XDPDefault	SnapVault

변환 예외 사항은 다음과 같습니다.

- SVM 데이터 보호 관계는 ONTAP 9.3 및 이전 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.4부터 SVM 데이터 보호 관계는 기본적으로 XDP 모드로 설정됩니다.

- 루트 볼륨 로드 공유 데이터 보호 관계는 기본적으로 DP 모드로 유지됩니다.
- SnapLock 데이터 보호 관계는 ONTAP 9.4 이하 버전에서 DP 모드로 계속 기본값입니다.

  ONTAP 9.5부터 SnapLock 데이터 보호 관계는 XDP 모드로 기본 설정됩니다.

- DP의 명시적 호출은 다음 클러스터 전체 옵션을 설정한 경우 계속해서 DP 모드로 설정됩니다.

  ```
  options replication.create_data_protection_rels.enable on
  ```

  DP를 명시적으로 호출하지 않으면 이 옵션은 무시됩니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 관계의 유형을 변환합니다

ONTAP 9.5부터 SnapMirror Synchronous가 지원됩니다. 기본 전송을 수행하지 않고도 SnapMirror 비동기식 관계를 SnapMirror 동기식 관계로 변환하거나 그 반대로 전환할 수 있습니다.

이 작업에 대해

SnapMirror 정책을 변경하여 SnapMirror 비동기식 관계를 SnapMirror 동기식 관계로 변환하거나 그 반대로 변환할 수 없습니다.

단계

- * SnapMirror 비동기 관계를 SnapMirror 동기 관계로 변환 *

  a. 대상 클러스터에서 SnapMirror 비동기식 관계를 삭제합니다.

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM>:<destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  c. 대상 클러스터에서 SnapMirror 동기식 관계를 생성합니다.

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM>:<destination_volume> -policy sync-mirror
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  d. SnapMirror 동기식 관계 재동기화:

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * SnapMirror 동기식 관계를 SnapMirror 비동기식 관계로 변환 *

  a. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 중지합니다.

  ```
  snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
  ```

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. 대상 클러스터에서 SnapMirror 비동기식 관계를 삭제합니다.

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. 대상 클러스터에서 SnapMirror 비동기식 관계를 생성합니다.

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. SnapMirror 동기식 관계 재동기화:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 동기식 관계의 모드를 변환합니다

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. SnapMirror 동기식 관계의 모드를 StrictSync에서 Sync로 또는 그 반대로 변환할 수 있습니다.

이 작업에 대해

SnapMirror 동기식 관계의 정책을 수정하여 모드를 변환할 수는 없습니다.

단계

1. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 중지합니다.

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. 대상 클러스터에서 기존 SnapMirror 동기식 관계를 삭제합니다.

```
snapmirror delete -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. 소스 클러스터에서 일반 스냅샷을 삭제하지 않고 SnapMirror 관계를 해제합니다.

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. 대상 클러스터에서 SnapMirror 동기식 관계를 변환할 모드를 지정하여 SnapMirror 동기식 관계를 생성합니다.

```
snapmirror create -source-path vs1:vol1 -destination-path
<destination_SVM>:<destination_volume> -policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. 대상 클러스터에서 SnapMirror 관계를 다시 동기화합니다.

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 페일오버 테스트 볼륨을 생성하고 삭제합니다

ONTAP 9.14.1부터 System Manager를 사용하여 활성 SnapMirror 관계를 중단하지 않고 SnapMirror 페일오버 및 재해 복구를 테스트하는 볼륨 클론을 생성할 수 있습니다. 테스트를 마치면 연결된 데이터를 정리하고 테스트 볼륨을 삭제할 수 있습니다.

SnapMirror 페일오버 테스트 볼륨을 생성합니다

이 작업에 대해

- 동기식 및 SnapMirror 비동기식 관계에 대해 페일오버 테스트를 수행할 수 있습니다.
- 재해 복구 테스트를 수행하기 위한 볼륨 클론이 생성됩니다.
- 클론 볼륨은 SnapMirror 대상과 동일한 스토리지 VM에 생성됩니다.
- FlexVol 및 FlexGroup SnapMirror 관계를 사용할 수 있습니다.
- 선택한 관계에 대한 테스트 클론이 이미 있으면 해당 관계에 대해 다른 클론을 생성할 수 없습니다.
- SnapLock 볼트 관계는 지원되지 않습니다.

시작하기 전에

- 클러스터 관리자여야 합니다.
- SnapMirror 라이센스를 소스 및 대상 클러스터에 설치해야 합니다.

단계

1. 대상 클러스터에서 * 보호 > 관계 * 를 선택합니다.
2. 관계 소스 옆에 있는 을 ⋮ 선택하고 * Test Failover * 를 선택합니다.
3. Test Failover * 창에서 * Test Failover * 를 선택합니다.
4. 스토리지 > 볼륨 * 을 선택하고 테스트 페일오버 볼륨이 표시되는지 확인합니다.
5. 스토리지 > 공유 * 를 선택합니다.
6. 을 + Add 선택하고 * 공유 * 를 선택합니다.
7. 공유 추가 * 창의 * 공유 이름 * 필드에 공유 이름을 입력합니다.
8. 폴더 * 필드에서 * 찾아보기 * 를 선택하고 테스트 클론 볼륨을 선택한 다음 * 저장 * 을 선택합니다.
9. 공유 추가 * 창 아래쪽에서 * 저장 * 을 선택합니다.
10. 스토리지 > 공유 * 창에서 생성한 공유를 찾은 후 를 선택하여 ⌄ 공유 정보를 봅니다.
11. SMB/CIFS 액세스 * 에서 공유에 대한 액세스 경로를 복사하거나 기록해 둡니다(예 `\\123.456.7.890\failover_test`:).
12. SMB 액세스 경로를 사용하여 클라이언트에서 공유를 열고 테스트 볼륨에 읽기 및 쓰기 기능이 있는지 확인합니다.

장애 조치 데이터를 정리하고 테스트 볼륨을 삭제합니다

장애 조치 테스트를 완료한 후 테스트 볼륨과 연결된 모든 데이터를 정리하고 삭제할 수 있습니다.

단계

1. 대상 클러스터에서 * 보호 > 관계 * 를 선택합니다.

2. 관계 소스 옆에 있는 을 ⋮ 선택하고 * Clean Up Test Failover * 를 선택합니다.
3. Clean Up Test Failover * 창에서 * Clean Up * 을 선택합니다.
4. 스토리지 > 볼륨 * 을 선택하고 테스트 볼륨이 삭제되었는지 확인합니다.

SnapMirror DR 대상 볼륨의 데이터를 제공합니다

ONTAP SnapMirror 대상 볼륨을 쓰기 가능하게 만듭니다

볼륨에서 클라이언트로 데이터를 제공하려면 먼저 대상 볼륨을 쓰기 가능하게 만들어야 합니다. 소스를 사용할 수 없게 될 때 미러 대상에서 데이터를 제공하려면 대상에 대한 예약된 전송을 중지한 다음 SnapMirror 관계를 끊어 대상을 쓰기 가능으로 만듭니다.

이 작업에 대해

이 작업은 대상 SVM 또는 타겟 클러스터에서 수행해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 대상 볼륨을 쓰기 가능하게 만들 수 있습니다.

시스템 관리자

1. 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭한 후 원하는 볼륨 이름을 클릭합니다.
2. 을 클릭합니다.
3. 예약된 전송 중지: * 일시 중지 * 를 클릭합니다.
4. 대상을 쓰기 가능 상태로 만듭니다. * Break * (중단 *)를 클릭합니다.
5. 기본 * 관계 * 페이지로 이동하여 관계 상태가 "연결 해제"로 표시되는지 확인합니다.

다음 단계

대상 볼륨을 쓰기 가능한 볼륨으로 만든 후에 이 "복제 관계를 역방향으로 재동기화합니다" 작업을 수행해야 합니다.

비활성화된 소스 볼륨을 다시 사용할 수 있게 되면 관계를 다시 역동기화하여 현재 데이터를 원래 소스 볼륨에 복제해야 합니다.

CLI를 참조하십시오

1. 목적지로의 예약된 전송 중지:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 예약된 전송을 중지합니다.

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 목적지로의 진행 중인 전송을 중지합니다.

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

SnapMirror 동기식 관계에는 이 단계가 필요하지 않습니다(ONTAP 9.5부터 지원됨).

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 지속적인 전송을 중지합니다.

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror abort` "ONTAP 명령 참조입니다"을 참조하십시오.

3. SnapMirror DR 관계 끊기:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

대상 볼륨을 쓰기 가능한 볼륨으로 만든 후에 이 "복제 관계를 다시 동기화합니다" 작업을 수행해야 합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"볼륨 재해 복구 개요"

데이터 액세스를 위한 **ONTAP SnapMirror** 대상 볼륨을 구성합니다

대상 볼륨을 쓰기 가능한 상태로 만든 후 데이터 액세스를 위해 볼륨을 구성해야 합니다. 소스 볼륨이 다시 활성화될 때까지 NAS 클라이언트, NVMe 하위 시스템 및 SAN 호스트가 대상 볼륨의 데이터에 액세스할 수 있습니다.

NAS 환경:

1. 소스 볼륨이 소스 SVM에 마운트된 것과 동일한 접합 경로를 사용하여 NAS 볼륨을 네임스페이스에 마운트합니다.
2. 대상 볼륨의 SMB 공유에 적절한 ACL을 적용합니다.
3. 대상 볼륨에 NFS 내보내기 정책을 할당합니다.
4. 대상 볼륨에 할당량 규칙을 적용합니다.
5. 대상 볼륨으로 클라이언트를 리디렉션합니다.
6. 클라이언트에서 NFS 및 SMB 공유를 다시 마운트합니다.

SAN 환경:

1. 볼륨의 LUN을 적절한 이니시에이터 그룹에 매핑합니다.
2. iSCSI의 경우 SAN 호스트 이니시에이터에서 SAN LIF로 iSCSI 세션을 생성합니다.
3. SAN 클라이언트에서 스토리지 재검색을 수행하여 연결된 LUN을 검색합니다.

NVMe 환경에 대한 자세한 내용은 을 참조하십시오 "SAN 관리".

원래 **ONTAP SnapMirror** 소스 볼륨을 다시 활성화합니다

대상에서 데이터를 더 이상 제공할 필요가 없을 때 소스 볼륨과 타겟 볼륨 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다.

이 작업에 대해

- 아래 절차에서는 원본 소스 볼륨의 기준선이 온전한 것으로 가정합니다. 기준선이 변경되지 않은 경우 절차를 수행하기 전에 데이터를 제공하는 볼륨과 원본 소스 볼륨 간의 관계를 생성하고 초기화해야 합니다.
- XDP SnapMirror 관계의 백그라운드 준비 및 데이터 웨어하우징 단계는 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.

단계

1. 원래 데이터 보호 관계를 반대로 전환합니다.

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

   > ⓘ 이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다. 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 svm1의 원본 소스 볼륨 VolA와 SVM_BACKUP의 데이터 제공 볼륨 VolA_DST 사이의 관계를 반전시킵니다.

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. 원래 소스에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 볼륨에 대한 액세스를 중지하십시오. 한 가지 방법은 원래 대상 SVM을 중지하는 것입니다.

   'vserver stop-vserver_SVM_'

   > ⓘ 이 명령은 원래 대상 SVM 또는 원래 대상 클러스터에서 실행해야 합니다. 이 명령을 사용하면 사용자가 전체 원래 대상 SVM에 액세스할 수 없습니다. 다른 방법을 사용하여 원래 대상 볼륨에 대한 액세스를 중지할 수 있습니다.

   다음 예에서는 원래 대상 SVM을 중지합니다.

   ```
   cluster_dst::> vserver stop svm_backup
   ```

   에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 반대 관계 업데이트:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 데이터를 제공하고 있는 볼륨, VM_BACKUP의 VolA_DST, Svm1의 원본 소스 볼륨 VolA의 관계를 업데이트합니다.

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 원래 소스 SVM 또는 원래 소스 클러스터에서 역방향 관계에 대한 예약된 전송을 중지합니다.

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 원래 대상 볼륨 간의 예약된 전송을 중지합니다. `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 분리합니다.

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   이 명령은 원래 소스 SVM 또는 소스 클러스터에서 실행해야 합니다.

   다음 예에서는 원래 대상 볼륨 간의 관계를 끊는 경우를 보여 줍니다. `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

   ```
   cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 원래 소스 SVM 또는 원래 소스 클러스터에서 역방향 데이터 보호 관계를 삭제합니다.

`snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

다음 예에서는 svm1의 원래 소스 볼륨 VolA와 SVM_BACKUP의 VolA_DST에서 데이터를 제공하고 있는 볼륨 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

7. 원래 대상 SVM 또는 원래 대상 클러스터에서 역방향 관계를 해제합니다.

`snapmirror release -source-path SVM:volume -destination-path SVM:volume`

이 명령은 원래 대상 SVM 또는 원래 대상 클러스터에서 실행해야 합니다.

다음 예에서는 원래 타겟 볼륨 간의 역방향 관계를 해제하며 `volA_dst` 켜짐 `svm_backup`및 원본 소스 볼륨, `volA` 켜짐 `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 대상에서 원래 데이터 보호 관계를 다시 설정합니다.

`snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

다음 예에서는 svm1의 원본 소스 볼륨 VolA와 sm_backup의 원래 대상 볼륨 VolA_dst 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

9. 필요한 경우 원래 대상 SVM을 시작합니다.

'vserver start-vserver_SVM_'

다음 예에서는 원래 대상 SVM을 시작합니다.

```
cluster_dst::> vserver start svm_backup
```

에 대한 자세한 내용은 `vserver start` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 대상 볼륨에서 파일을 복원합니다

ONTAP SnapMirror 대상에서 파일, LUN 또는 NVMe 네임스페이스를 복원합니다

단일 파일, LUN, 스냅샷에서 파일 또는 LUN 세트를 복원하거나 SnapMirror 대상 볼륨에서 NVMe 네임스페이스를 복원할 수 있습니다. ONTAP 9.7부터는 SnapMirror 동기식 대상에서 NVMe 네임스페이스를 복원할 수도 있습니다. 파일을 원래 소스 볼륨이나 다른 볼륨으로 복원할 수 있습니다.

시작하기 전에

SnapMirror 동기 대상(ONTAP 9.5부터 지원됨)에서 파일 또는 LUN을 복구하려면 먼저 관계를 삭제하고 해제해야 합니다.

이 작업에 대해

파일 또는 LUN(대상 볼륨)을 복원하는 볼륨은 읽기-쓰기 볼륨이어야 합니다.

- SnapMirror는 소스 및 대상 볼륨에 공통 스냅샷이 있는 경우 _ 증가분 복구 _ 를 수행합니다(일반적으로 원래 소스 볼륨으로 복구할 때와 마찬가지로).
- 그렇지 않으면 SnapMirror가 _baseline restore_를 수행하여 지정된 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록이 대상 볼륨으로 전송됩니다.

단계

1. 대상 볼륨의 스냅샷을 나열합니다.

   ```
   volume snapshot show -vserver <SVM> -volume volume
   ```

   에 대한 자세한 내용은 `volume snapshot show` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예는 대상의 스냅샷을 보여 `vserverB:secondary1` 줍니다.

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirror 대상 볼륨의 스냅샷에서 단일 파일 또는 LUN 또는 파일 또는 LUN 집합 복구:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 명령을 실행하면 `daily.2013-01-25_0010` 원래 대상 볼륨의 스냅샷과 `file2` 파일이 원래 소스 볼륨의 `secondary1` 활성 파일 시스템의 동일한 위치로 `primary1` 복원됩니다. `file1`

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

다음 명령을 실행하면 `daily.2013-01-25_0010` 원래 대상 볼륨의 `secondary1` 스냅샷과 `file2` 파일이 원래 소스 볼륨의 활성 파일 시스템의 다른 위치로 `primary1` 복원됩니다. `file1`

대상 파일 경로는 @ 기호와 원본 소스 볼륨의 루트에서 파일 경로로 시작합니다. 이 예에서는 file1 이 /dir1/file1로

복구되고 file2 가 기본 y1의 /dir2.new/file2 로 복원됩니다.

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

다음 명령을 실행하면 `file3` 원래 대상 볼륨의 `secondary1` 스냅샷과 `daily.2013-01-25_0010` 파일이 원래 소스 볼륨의 활성 파일 시스템의 다른 위치로 복원되고 `file1` 에서 `snap1` 의 활성 파일 시스템의 `primary1` 동일한 위치로 `primary1` 복원됩니다. `file2`

이 예에서는 파일 'file1'이 '/dir1/file1'로 복원되고 새 파일3이 '/dir3.new/file3'로 복원됩니다.

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

관련 정보

- "SnapMirror 복원"

ONTAP SnapMirror 대상에서 볼륨 내용을 복원합니다

SnapMirror 대상 볼륨의 스냅숏에서 전체 볼륨의 내용을 복원할 수 있습니다. 볼륨의 내용을 원래 소스 볼륨 또는 다른 볼륨으로 복원할 수 있습니다.

이 작업에 대해

이 절차는 FAS, AFF, ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 또는 ASA C30)이 있는 경우 다음을 따르세요. "수행할 수 있습니다" 데이터를 복구하려면. ASA R2 시스템은 SAN 전용 고객을 대상으로 단순화된 ONTAP 환경을 제공합니다.

복원 작업의 대상 볼륨은 다음 중 하나여야 합니다.

- 소스 및 대상 볼륨에 공통 스냅샷이 있는 경우(일반적으로 원래 소스 볼륨으로 복구할 때와 마찬가지로) 읽기-쓰기 볼륨인 경우 SnapMirror가 _증분 복구_를 수행합니다.

  공통 스냅샷이 없는 경우 명령이 실패합니다. 볼륨의 내용을 빈 읽기-쓰기 볼륨으로 복원할 수 없습니다.

- 빈 데이터 보호 볼륨으로서, 이 경우 SnapMirror가 _baseline restore_를 수행하고, 지정된 스냅샷과 해당

스냅샷이 참조하는 모든 데이터 블록이 소스 볼륨으로 전송됩니다.

볼륨의 내용을 복원하는 것은 운영 중단이 발생합니다. 복원 작업이 실행 중일 때는 SnapVault 운영 볼륨에서 SMB 트래픽이 실행되고 있지 않아야 합니다.

복원 작업의 타겟 볼륨에 압축이 활성화되어 있고 소스 볼륨에 압축이 활성화되어 있지 않은 경우 타겟 볼륨에서 압축을 비활성화합니다. 복원 작업이 완료된 후 압축을 다시 활성화해야 합니다.

대상 볼륨에 대해 정의된 할당량 규칙은 복구를 수행하기 전에 비활성화됩니다. 복원 작업이 완료된 후 "volume quota modify" 명령을 사용하여 할당량 규칙을 다시 활성화할 수 있습니다.

볼륨의 데이터가 손실되거나 손상된 경우 이전 스냅샷에서 복원하여 데이터를 롤백할 수 있습니다.

이 절차는 소스 볼륨의 현재 데이터를 이전 스냅샷 버전의 데이터로 대체합니다. 대상 클러스터에서 이 작업을 수행해야 합니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 볼륨의 콘텐츠를 복원할 수 있습니다.

시스템 관리자

1. 보호 > 관계 * 를 클릭한 다음 소스 볼륨 이름을 클릭합니다.
2. 을 ⋮ 클릭한 다음 * 복원 * 을 선택합니다.
3. 소스 * 에서 소스 볼륨은 기본적으로 선택됩니다. 소스 이외의 볼륨을 선택하려면 * 기타 볼륨 * 을 클릭합니다.
4. 대상 * 에서 복원할 스냅샷을 선택합니다.
5. 소스와 대상이 서로 다른 클러스터에 있는 경우 원격 클러스터에서 * 보호 > 관계 * 를 클릭하여 복구 진행률을 모니터링합니다.

CLI를 참조하십시오

1. 대상 볼륨의 스냅샷을 나열합니다.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

다음 예는 대상의 스냅샷을 보여 `vserverB:secondary1` 줍니다.

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. SnapMirror 대상 볼륨에 있는 스냅샷에서 볼륨의 내용 복원:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
```

```
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

이 명령은 원래 소스 SVM 또는 원래 소스 클러스터에서 실행해야 합니다.

다음 명령을 실행하면 원래 대상 볼륨에 있는 `secondary1` 스냅샷에서 `daily.2013-01-25_0010` 원본 소스 볼륨의 콘텐츠가 복원됩니다. `primary1`

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. 복원된 볼륨을 다시 마운트하고 볼륨을 사용하는 모든 애플리케이션을 다시 시작합니다.

ONTAP에서 이 작업을 수행하는 다른 방법

에서 이러한 작업을 수행하려면...	이 콘텐츠 보기...
System Manager Classic(ONTAP 9.7 이하에서 사용 가능)	"SnapVault를 사용한 볼륨 복원 개요"

관련 정보

- "SnapMirror 복원"
- "볼륨 스냅샷 표시"

ONTAP SnapMirror 복제 관계를 수동으로 업데이트합니다

소스 볼륨이 이동되었기 때문에 업데이트에 실패하면 복제 관계를 수동으로 업데이트해야 할 수 있습니다.

이 작업에 대해

SnapMirror는 복제 관계를 수동으로 업데이트할 때까지 이동된 소스 볼륨에서 전송을 중단합니다.

ONTAP 9.5부터 SnapMirror 동기식 관계가 지원됩니다. 소스 볼륨과 타겟 볼륨이 항상 이 관계에서 동기화되지만, 보조 클러스터의 뷰는 매시간 기준으로 운영 클러스터와 동기화됩니다. 대상에서 시점 데이터를 보려면 `snapmirror update` 명령을 실행하여 수동 업데이트를 수행해야 합니다.

단계

1. 복제 관계를 수동으로 업데이트합니다.

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 복제 관계를 다시 동기화합니다

대상 볼륨을 쓰기 가능하게 만든 후, 소스 및 대상 볼륨에 공통 스냅샷이 없기 때문에 업데이트가 실패한 후 또는 관계에 대한 복제 정책을 변경하려는 경우 복제 관계를 다시 동기화해야 합니다.

ONTAP 9.8부터 System Manager를 사용하여 역방향 재동기화 작업을 수행하여 기존 보호 관계를 삭제하고 소스 볼륨과 대상 볼륨의 기능을 반대로 되돌릴 수 있습니다. 그런 다음, 소스를 복구 또는 교체하고 소스를 업데이트하고 시스템의 원래 구성을 다시 설정하는 동안 대상 볼륨을 사용하여 데이터를 제공합니다.

> System Manager는 클러스터 내 관계와의 역방향 재동기화를 지원하지 않습니다. ONTAP CLI를 사용하여 클러스터 내 관계와 역방향 재동기화 작업을 수행할 수 있습니다.

이 작업에 대해

- 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.
- 팬아웃 또는 캐스케이드 구성의 일부인 볼륨은 재동기화에 시간이 오래 걸릴 수 있습니다. SnapMirror 관계가 오랫동안 "준비 중" 상태를 보고하는 것을 보면 흔히 볼 수 있습니다.
- ONTAP 9.13.1부터 ONTAP 기본적으로 빠른 재동기화를 사용하여 재동기화 시간을 줄이려고 합니다. 기본적으로 빠른 재동기화를 사용하려면 다음 조건이 충족되어야 합니다.
  - FlexVol 볼륨에는 볼륨에 복제본이 없습니다.
  - MirrorAllSnapshots 정책을 사용하는 경우

> 사용 중 `-quick-resync` 전송된 데이터 블록의 저장 효율성이 제거되어 재동기화 대상 볼륨에서 추가 공간을 소모할 수 있습니다. 이러한 추가 공간 소비는 재동기화 대상에서 인라인 또는 복제 후 스토리지 효율성 적용의 일부로 복구됩니다.

그만큼 `-quick-resync` 매개변수는 선택 사항입니다. 다음을 사용하여 빠른 재동기화를 활성화하거나 비활성화할 수 있습니다. `-quick-resync true|false` 매개변수와 함께 `snapmirror resync` 명령.

더 많은 정보를 원하시면 `-quick-resync`, 참조 "ONTAP 명령 참조입니다".

단계

System Manager 또는 ONTAP CLI를 사용하여 이 작업을 수행할 수 있습니다. ONTAP CLI를 사용하는 경우 대상 볼륨을 쓰기 가능하게 만들지, 복제 관계를 업데이트하는지에 관계없이 절차는 동일합니다.

System Manager 역방향 재동기화

"관계를 끊습니다"대상을 쓰기 가능하게 만들려면 관계를 역순으로 다시 동기화합니다.

1. 대상 클러스터에서 * 보호 > 관계 * 를 클릭합니다.
2. 되돌릴 분리된 관계 위로 마우스를 가져가 를 클릭하고 * Reverse Resync * 를 선택합니다.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.
4. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 역방향 재동기화 진행률을 모니터링합니다.

다음 단계

원래 원본을 다시 사용할 수 있게 되면 역방향 관계를 해제하고 다른 역방향 재동기화 작업을 수행하여 원래 관계를 다시 설정할 수 있습니다. 역방향 재동기화 프로세스는 데이터를 제공하는 사이트의 모든 변경 사항을 원래 소스로 복사하고 원래 소스를 다시 읽기-쓰기 가능하게 만듭니다.

System Manager가 다시 동기화됩니다

1. 보호 > 관계 * 를 클릭합니다.
2. 재동기화할 관계 위로 마우스를 가져간 후 를 클릭하고 * Break * 를 선택합니다.
3. 관계 상태가 "해제"로 표시되면 를 클릭한 다음 * 재동기화 * 를 선택합니다.
4. 관계 * 에서 관계 상태를 확인하여 재동기화 진행률을 모니터링합니다. 재동기화가 완료되면 상태가 "미러링 "으로 변경됩니다.

CLI를 참조하십시오

1. 소스 및 대상 볼륨 재동기화:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 의 소스 볼륨과 의 대상 볼륨 간의 관계를 다시 `volA svm1 volA_dst` `svm_backup`동기화합니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- "ONTAP SnapMirror 대상 SVM에서 데이터를 다시 동기화합니다"

ONTAP SnapMirror 볼륨 복제 관계를 삭제합니다

및 `snapmirror release` 명령을 사용하여 볼륨 복제 관계를 삭제할 수 `snapmirror delete` 있습니다. 그런 다음 불필요한 대상 볼륨을 수동으로 삭제할 수 있습니다.

이 작업에 대해

이 `snapmirror release` 명령은 SnapMirror에서 생성된 스냅샷을 소스에서 삭제합니다. 옵션을 사용하여 스냅샷을 보존할 수 `-relationship-info-only` 있습니다.

단계

1. 복제 관계를 중지합니다.

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. (선택 사항) 대상 볼륨이 읽기/쓰기 볼륨이어야 하는 경우 복제 관계를 끊으십시오. 대상 볼륨을 삭제할 계획이거나 읽기/쓰기가 필요한 볼륨이 없는 경우 이 단계를 건너뛸 수 있습니다.

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 관계를 삭제합니다.

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ⓘ 대상 클러스터 또는 대상 SVM에서 이 명령을 실행해야 합니다.

   다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 소스 SVM에서 복제 관계 정보 해제:

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

소스 클러스터 또는 소스 SVM에서 이 명령을 실행해야 합니다.

다음 예에서는 소스 SVM의 vm1에서 지정된 복제 관계에 대한 정보를 해제합니다.

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 볼륨에서 스토리지 효율성 관리

SnapMirror는 타겟 볼륨에 사후 처리 데이터 압축이 활성화되어 있는 경우를 제외하고 소스 및 타겟 볼륨에서 스토리지 효율성을 유지합니다. 이 경우 타겟 볼륨에서 스토리지 효율성이 모두 손실됩니다. 이 문제를 해결하려면 타겟 볼륨에서 사후 처리 압축을 비활성화하고 관계를 수동으로 업데이트하며 스토리지 효율성을 다시 활성화해야 합니다.

이 작업에 대해

명령을 사용하여 볼륨에 효율성이 활성화되어 있는지 여부를 확인할 수 `volume efficiency show` 있습니다. 에 대한 자세한 내용은 `volume efficiency show` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 감사 로그를 보고 전송 설명을 찾아 SnapMirror에서 스토리지 효율성이 유지되는지 확인할 수 있습니다. 전송 설명이 `transfer_desc=Logical Transfer with Storage Efficiency`표시되면 SnapMirror는 스토리지 효율성을 유지하는 것입니다. 전송 설명이 `transfer_desc=Logical Transfer`표시되면 SnapMirror는 스토리지 효율성을 유지하는 것이 아닙니다. 예를 들면 다음과 같습니다.

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

시작하기 전에

- 소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

  "클러스터 및 SVM 피어링"

- 타겟 볼륨에서 사후 처리 압축을 비활성화해야 합니다.
- 스토리지를 사용한 논리적 전송: ONTAP 9.3부터 스토리지 효율성을 다시 활성화하기 위해 더 이상 수동 업데이트가 필요하지 않습니다. SnapMirror에서 사후 처리 압축이 비활성화되었다고 감지하면 다음 예약 업데이트에서 스토리지 효율성을 자동으로 다시 활성화합니다. 소스와 대상 모두 ONTAP 9.3을 실행해야 합니다.
- ONTAP 9.3부터 AFF 시스템은 타겟 볼륨을 쓰기 가능한 상태로 만든 후 FAS 시스템과 다른 방식으로 스토리지

효율성 설정을 관리합니다.

- 다음을 사용하여 대상 볼륨을 쓰기 가능하게 만든 후 `snapmirror break` 명령을 실행하면 볼륨의 캐싱 정책이 자동으로 설정됩니다. `auto` (기본값).

  이 동작은 FlexVol 볼륨에만 적용되며 FlexGroup 볼륨에는 적용되지 않습니다.

  에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

- 재동기화 시 캐싱 정책이 자동으로 설정됩니다. `none` 원래 설정과 관계없이 중복 제거 및 인라인 압축은 자동으로 비활성화됩니다. 필요에 따라 설정을 수동으로 수정해야 합니다.

스토리지 효율성을 활성화한 수동 업데이트는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 작업을 실행할 수 있습니다.

단계

1. 복제 관계를 업데이트하고 스토리지 효율성을 다시 설정합니다.

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다. 소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다. 에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA_dst 간의 관계를 업데이트하고 스토리지 효율성을 다시 활성화합니다.

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror 전역 제한을 사용합니다

글로벌 네트워크 스로틀링은 모든 SnapMirror 및 SnapVault 전송에 대해 노드 단위로 사용할 수 있습니다.

이 작업에 대해

SnapMirror 글로벌 제한 때문에 들어오고/또는 나가는 SnapMirror 및 SnapVault 전송에 사용되는 대역폭이 제한됩니다. 이 제한은 클러스터의 모든 노드에서 클러스터 전체에 적용됩니다.

예를 들어, 발신 스로틀이 100Mbps로 설정된 경우 클러스터의 각 노드는 발신 대역폭을 100Mbps로 설정합니다. 글로벌 임계치 조절이 비활성화된 경우 모든 노드에서 비활성화됩니다.

데이터 전송 속도는 대개 초당 비트 수(bps)로 표현되지만 스로틀 값은 초당 킬로바이트(kbps)로 입력해야 합니다.

ONTAP 9.9.1 이하 릴리스에서는 스로틀이 전송 또는 로드 공유 미러 전송에 영향을 미치지 `volume move` 않습니다. ONTAP 9.10.0부터 볼륨 이동 작업을 제한하는 옵션을 지정할 수 있습니다. 자세한 내용은 을 참조하십시오 "ONTAP 9.10 이상에서 볼륨 이동을 제한하는 방법".

글로벌 제한은 SnapMirror 및 SnapVault 전송을 위한 관계별 스로틀 기능과 함께 작동합니다. 관계별 전송의 결합된 대역폭이 글로벌 스로틀의 값을 초과할 때까지, 즉 글로벌 스로틀이 적용될 때까지 관계별 스로틀이 적용됩니다. 스로틀 값 0은 글로벌 스로틀링이 비활성화됨을 의미합니다.

SnapMirror 글로벌 제한은 동기화 상태에서의 SnapMirror 동기식 관계에는 영향을 미치지 않습니다. 그러나 초기화 작업과 같은 비동기 전송 단계를 수행하거나 동기화 중단 이벤트 후에 스로틀이 SnapMirror 동기식 관계에 영향을 줍니다. 따라서 SnapMirror 동기식 관계에서 글로벌 제한을 설정하지 않는 것이 좋습니다.

단계

1. 글로벌 제한 활성화:

   'options-option-name replication.throttle.enable on|off'

   다음 예에서는 "cluster_dst"에서 SnapMirror 글로벌 제한을 활성화하는 방법을 보여 줍니다.

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. 대상 클러스터에서 들어오는 전송에 사용되는 최대 총 대역폭을 지정합니다.

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   권장되는 최소 스로틀 대역폭은 4kbps(초당 킬로바이트)이며 최대 초당 최대 2TB입니다(Tbps). 이 옵션의 기본값은 입니다 `unlimited`. 즉, 사용된 총 대역폭에 대한 제한이 없습니다.

   다음 예는 들어오는 전송에 사용되는 최대 총 대역폭을 100Mbps(초당 메가비트)로 설정하는 방법을 보여줍니다.

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   초당 100메가비트(Mbps) = 12500KB/초(kbps)

3. 소스 클러스터에서 보내는 전송에 사용되는 최대 총 대역폭을 지정합니다.

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

   권장되는 최소 스로틀 대역폭은 4kbps이고 최대 스로틀 대역폭은 2Tbps입니다. 이 옵션의 기본값은 입니다 `unlimited`. 즉, 사용된 총 대역폭에 대한 제한이 없습니다. 매개 변수 값은 초당 킬로바이트(kbps)입니다.

   다음 예에서는 송신 전송에 사용되는 최대 총 대역폭을 100Mbps로 설정하는 방법을 보여 줍니다.

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

SnapMirror SVM 복제 관리

ONTAP SnapMirror SVM 복제에 대해 알아보십시오

SnapMirror를 사용하여 SVM 간에 데이터 보호 관계를 생성할 수 있습니다. 이러한 유형의 데이터 보호 관계에서 NFS 엑스포트, SMB 공유에서 RBAC에 이르는 SVM 구성의 전체 또는 일부를 복제할 뿐만 아니라 SVM이 소유한 볼륨의 데이터도 복제됩니다.

지원되는 관계 유형

데이터를 지원하는 SVM만 복제할 수 있습니다. 지원되는 데이터 보호 관계 유형은 다음과 같습니다.

- _SnapMirror DR, _ 이 경우 일반적으로 대상에 현재 소스에 있는 스냅샷만 포함됩니다.

  ONTAP 9.9.1부터 이 동작은 미러 볼트 정책을 사용할 때 변경됩니다. ONTAP 9.9.1부터 소스와 대상에 다른 스냅샷 정책을 생성할 수 있으며, 소스의 스냅샷이 대상의 스냅샷을 덮어쓰지 않습니다.

  - 정상적인 예약 작업, 업데이트 및 재동기화 중에 소스에서 타겟으로 덮어써지지 않습니다
  - 분리 작업 중에는 삭제되지 않습니다.
  - 플립 재동기화 작업 중에는 삭제되지 않습니다.
    ONTAP 9.9.1 이상을 사용하여 미러 소산 정책을 사용하여 SVM 재해 관계를 구성하면 정책은 다음과 같이 작동합니다.
  - 소스의 사용자 정의 스냅샷 정책은 대상에 복제되지 않습니다.
  - 시스템 정의 스냅샷 정책은 대상에 복제되지 않습니다.
  - 사용자 및 시스템 정의 스냅샷 정책과의 볼륨 연결은 대상에 복제되지 않습니다. SVM.
- _SnapMirror 통합 복제_는 대상이 DR과 장기 보존을 위해 구성됩니다.

SnapMirror 통합 복제에 대한 자세한 내용은 을 참조하십시오 "SnapMirror 통합 복제 기본 사항".

복제 정책의 _policy type_은 이 정책이 지원하는 관계 유형을 결정합니다. 다음 표에는 사용 가능한 정책 유형이 나와 있습니다.

정책 유형입니다	관계 유형
비동기식 - 미러	SnapMirror DR
대칭 복사 - 볼트	통합 복제

XDP는 ONTAP 9.4에서 SVM 복제 기본값으로 DP를 대체합니다

ONTAP 9.4부터 SVM 데이터 보호 관계는 기본적으로 XDP 모드로 설정됩니다. SVM 데이터 보호 관계는 ONTAP 9.3 및 이전 버전에서 DP 모드로 계속 기본값입니다.

기존 관계는 XDP 기본값의 영향을 받지 않습니다. 관계가 이미 DP 유형인 경우 DP 유형이 됩니다. 다음 표에서는 예상할 수 있는 동작을 보여 줍니다.

지정하는 경우…	유형은…	기본 정책(정책을 지정하지 않은 경우)은…
DP	XDP	MirrorAllSnapshots(SnapMirror DR)
아무것도 없습니다	XDP	MirrorAllSnapshots(SnapMirror DR)
XDP	XDP	MirrorAndVault(통합 복제)

DP 관계를 XDP 관계로 변환하는 방법과 기타 세부 정보는 다음에서 확인할 수 있습니다"기존 ONTAP DP 유형 관계를 XDP로 변환합니다".

> SVM 복제에서는 버전에 상관없이 지원되지 않습니다. SVM 재해 복구 구성에서 페일오버 및 페일백 작업을 지원하려면 타겟 SVM이 소스 SVM 클러스터와 동일한 ONTAP 버전을 실행 중인 클러스터에 있어야 합니다.

"SnapMirror 관계에 대한 호환 ONTAP 버전"

SVM 구성을 복제하는 방법

SVM 복제 관계의 내용은 다음 필드의 상호 작용에 의해 결정됩니다.

- 'napMirror create' 명령의 '-identity-preserve true' 옵션은 전체 SVM 구성을 복제합니다.

  를 클릭합니다 `-identity-preserve false` 옵션은 SVM의 볼륨, 인증 및 권한 부여 구성과 에 나와 있는 프로토콜 및 이름 서비스 설정만 복제합니다 "SVM 재해 복구 관계에 복제된 구성".

- 'napMirror policy create' 명령의 '-discard-configs network' 옵션은 소스 및 대상 SVM이 서로 다른 서브넷에 있는 경우에 사용하기 위해 SVM 복제에서 LIF 및 관련 네트워크 설정을 제외합니다.
- 볼륨 수정 명령의 '-vserver-dr-protection protected' 옵션은 SVM 복제에서 지정된 볼륨을 제외합니다.

그렇지 않으면 SVM 복제가 볼륨 복제와 거의 동일합니다. 볼륨 복제에 사용하는 것과 동일한 워크플로우를 SVM 복제에 사용할 수 있습니다.

지원 세부 정보

다음 표에서는 SnapMirror SVM 복제에 대한 지원 정보를 보여 줍니다.

리소스 또는 기능	지원 세부 정보

배포 유형	• 단일 소스에서 단일 대상으로 • ONTAP 9.4, 팬아웃. 두 개의 대상으로만 팬아웃할 수 있습니다. 기본적으로 소스 SVM당 하나의 ID만 보존되며 진정한 관계는 유지됩니다.
관계 유형	• SnapMirror 재해 복구 • SnapMirror 통합 복제
복제 범위	인터클러스터 전용 동일한 클러스터에서 SVM을 복제할 수 없습니다.
자율 랜섬웨어 보호	• ONTAP 9.12.1부터 지원됩니다. 자세한 내용은 을 "자율 랜섬웨어 보호"참조하십시오.
정합성 보장 그룹 비동기식 지원	ONTAP 9.14.1부터 일관성 그룹이 있을 경우 최대 32개의 SVM 재해 복구 관계가 지원됩니다. 을 참조하십시오 "일관성 그룹 보호" 및 "정합성 보장 그룹 제한" 를 참조하십시오.
FabricPool	ONTAP 9.6부터 FabricPool에서 SnapMirror SVM 복제가 지원됩니다. SVM DR 관계인 경우 소스 및 타겟 볼륨에서 FabricPool 애그리게이트를 사용할 필요가 없지만 동일한 계층화 정책을 사용해야 합니다. ONTAP 9.12.1부터 SnapMirror SVM 복제는 FabricPool 및 FlexGroup 볼륨이 함께 작동하는 경우에 지원됩니다. 9.12.1 이전에는 이러한 기능 중 두 가지가 함께 작동했지만 세 가지 기능이 모두 함께 작동되지는 않았습니다.

MetroCluster	ONTAP 9.11.1부터 MetroCluster 구성 내 SVM 재해 복구 관계의 양측이 추가 SVM 재해 복구 구성의 소스 역할을 할 수 있습니다. ONTAP 9.5부터 MetroCluster 구성에서 SnapMirror SVM 복제가 지원됩니다. • ONTAP 9.10.X 이전 릴리즈에서는 MetroCluster 구성이 SVM 재해 복구 관계의 대상이 될 수 없습니다. • ONTAP 9.10.1 이상 릴리즈에서 MetroCluster 구성은 마이그레이션 목적으로만 SVM 재해 복구 관계의 대상이 될 수 있으며 에 설명된 모든 필수 요구사항을 충족해야 합니다 "TR-4966: SVM을 MetroCluster 솔루션으로 마이그레이션". • MetroCluster 구성 내의 활성 SVM만 SVM 재해 복구 관계의 소스가 될 수 있습니다. 전환 전 동기화 소스 SVM이나 전환 후 동기화 대상 SVM이 소스가 될 수 있습니다. • MetroCluster 구성이 안정적인 상태인 경우 볼륨이 온라인 상태가 아니기 때문에 MetroCluster 동기화 대상 SVM이 SVM 재해 복구 관계의 소스가 될 수 없습니다. • 동기식 소스 SVM이 SVM 재해 복구 관계의 소스인 경우 소스 SVM 재해 복구 관계 정보가 MetroCluster 파트너에게 복제됩니다. • 스위치오버 및 스위치백 프로세스 중에 SVM 재해 복구 대상으로의 복제가 실패할 수 있습니다. 그러나 스위치오버 또는 스위치백 프로세스가 완료된 후에는 다음 SVM 재해 복구 예정된 업데이트가 성공적으로 수행됩니다.
일관성 그룹	ONTAP 9.14.1부터 지원됩니다. 자세한 내용은 을 참조하십시오 일관성 그룹 보호.
ONTAP S3	SVM 재해 복구는 지원되지 않습니다.
SnapMirror Synchronous	SVM 재해 복구는 지원되지 않습니다.
버전 독립적	지원되지 않습니다.

볼륨 암호화	• 소스의 암호화된 볼륨은 대상에서 암호화됩니다. • 온보드 키 관리자 또는 KMIP 서버를 타겟에 구성해야 합니다. • 대상에서 새 암호화 키가 생성됩니다. • 대상에 volume.encryption을 지원하는 노드가 없으면 복제가 성공하지만 대상 볼륨은 암호화되지 않습니다.

SVM 재해 복구 관계에 복제된 구성

다음 표에서는 의 상호 작용을 보여 줍니다 `snapmirror create -identity-preserve` 옵션과 `snapmirror policy create -discard-configs network` 옵션:

구성이 복제되었습니다		'-**identity**-**preserve true**'		'-**identity**-**preserve false**'
		'-discard-configs 네트워크'가 설정되지 않은 정책 *	* '-discard-configs 네트워크'가 설정된 정책 *	
네트워크	NAS LIF	예	아니요	아니요
LIF Kerberos 구성	예	아니요	아니요	SAN LIF
아니요	아니요	아니요	방화벽 정책	예
예	아니요	서비스 정책	예	예
아니요	루트	예	아니요	아니요
브로드캐스트 도메인	아니요	아니요	아니요	서브넷
아니요	아니요	아니요	IPspace	아니요
아니요	아니요	중소기업	SMB 서버	예
예	아니요	로컬 그룹 및 로컬 사용자	예	예
예	권한	예	예	예
섀도 복사본	예	예	예	BranchCache입니다
예	예	예	서버 옵션	예

예	예	서버 보안	예	예
아니요	더 높여 줍니다	예	예	예
symlink	예	예	예	FPolicy 정책, Fsecurity 정책 및 Fsecurity NTFS입니다
예	예	예	이름 매핑 및 그룹 매핑	예
예	예	감사 정보	예	예
예	NFS 를 참조하십시오	엑스포트 정책	예	예
아니요	엑스포트 정책 규칙	예	예	아니요
NFS 서버	예	예	아니요	RBAC
보안 인증서	예	예	아니요	로그인 사용자, 공개 키, 역할 및 역할 구성
예	예	예	SSL	예
예	아니요	네임 서비스	DNS 및 DNS 호스트	예
예	아니요	Unix 사용자 및 UNIX 그룹	예	예
예	Kerberos 영역 및 Kerberos 키 블록	예	예	아니요
LDAP 및 LDAP 클라이언트	예	예	아니요	넷그룹
예	예	아니요	NIS를 선택합니다	예
예	아니요	웹 및 웹 액세스	예	예
아니요	볼륨	오브젝트	예	예
예	스냅샷 및 스냅샷 정책	예	예	예

자동 삭제 정책	아니요	아니요	아니요	효율성 정책
예	예	예	할당량 정책 및 할당량 정책 규칙입니다	예
예	예	복구 대기열	예	예
예	루트 볼륨	네임스페이스	예	예
예	사용자 데이터	아니요	아니요	아니요
Qtree	아니요	아니요	아니요	할당량
아니요	아니요	아니요	파일 레벨 QoS	아니요
아니요	아니요	속성: 루트 볼륨 상태, 공간 보장, 크기, 크기 조정 및 총 파일 수입니다	아니요	아니요
아니요	스토리지 QoS	QoS 정책 그룹	예	예
예	파이버 채널(FC)	아니요	아니요	아니요
iSCSI	아니요	아니요	아니요	LUN을 클릭합니다
오브젝트	예	예	예	Igroup
아니요	아니요	아니요	포트 세트	아니요
아니요	아니요	일련 번호	아니요	아니요
아니요	SNMP를 선택합니다	V3 사용자	예	예

SVM 재해 복구 스토리지 제한

다음 표는 스토리지 오브젝트당 지원되는 최대 볼륨 수 및 SVM 재해 복구 관계의 권장 최대 수를 보여줍니다. 제한 사항은 플랫폼에 따라 다를 수 있습니다. 을 참조하십시오 "Hardware Universe" 특정 구성에 대한 제한 사항을 알아봅니다.

스토리지 객체	제한
SVM	300개의 유연한 볼륨

HA 쌍	1,000개의 유연한 볼륨
클러스터	128개의 SVM 재해 관계

관련 정보

- "SnapMirror 생성"
- "스냅미러 정책 생성"

SVM 구성 복제

ONTAP SnapMirror SVM 복제 워크플로우

SnapMirror SVM 복제에는 대상 SVM 생성, 복제 작업 일정 생성, SnapMirror 관계 생성 및 초기화가 포함됩니다.

요구 사항에 가장 적합한 복제 워크플로우를 결정해야 합니다.

- "전체 SVM 구성을 복제합니다"
- "SVM 복제에서 LIF 및 관련 네트워크 설정을 제외합니다"
- "SVM 구성의 Exlude 네트워크, 네임 서비스 및 기타 설정"

볼륨을 **ONTAP SnapMirror** 대상 **SVM**에 배치하는 기준입니다

소스 SVM에서 타겟 SVM으로 볼륨을 복제할 때 애그리게이트 선택 기준을 파악하는 것이 중요합니다.

애그리게이트는 다음 기준에 따라 선택됩니다.

- 볼륨은 항상 비루트 애그리게이트에 배치되어 있습니다.
- 사용 가능한 여유 공간과 애그리게이트에 이미 호스팅되는 볼륨의 수를 기준으로 비 루트 애그리게이트를 선택합니다.

  여유 공간이 더 많은 애그리게이트를 사용하고 더 적은 볼륨을 우선 순위로 지정합니다. 가장 높은 우선순위를 가진 애그리게이트는 선택됩니다.

- FabricPool 애그리게이트에서 소스 볼륨은 동일한 계층화-정책을 사용하여 대상의 FabricPool 애그리게이트에 배치됩니다.
- 소스 SVM의 볼륨이 Flash Pool 애그리게이트에 있는 경우, 그러한 애그리게이트와 사용 가능한 공간이 충분할 경우, 타겟 SVM의 Flash Pool 애그리게이트에 볼륨을 배치하면 됩니다.
- 복제된 볼륨의 '-space-보증' 옵션이 'volume'으로 설정된 경우 사용 가능한 공간이 볼륨 크기보다 큰 애그리게이트만 고려됩니다.
- 소스 볼륨 크기에 따라 복제 중에 타겟 SVM에서 볼륨 크기가 자동으로 커집니다.

  대상 SVM에서 크기를 사전 예약하려면 볼륨 크기를 조정해야 합니다. 소스 SVM을 기반으로 하는 타겟 SVM에서 볼륨 크기가 자동으로 축소되지 않습니다.

한 Aggregate에서 다른 Aggregate로 볼륨을 이동할 경우, 대상 SVM에서 'volume move' 명령을 사용할 수 있습니다.

전체 **ONTAP SVM** 구성을 복제합니다

SVM DR(재해 복구) 관계를 생성하여 하나의 SVM 구성을 다른 SVM 구성으로 복제할 수 있습니다. 운영 사이트에 재해가 발생하면 대상 SVM을 빠르게 활성화할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다. 자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 작업에 대해

이 워크플로우에서는 이미 기본 정책 또는 사용자 지정 복제 정책을 사용하고 있다고 가정합니다.

ONTAP 9.9.1부터 미러 소산 정책을 사용할 때 소스 및 대상 SVM에 다른 스냅샷 정책을 생성할 수 있으며 대상의 스냅샷은 소스의 스냅샷으로 덮어쓰지 않습니다. 자세한 내용은 을 "SnapMirror SVM 복제 이해"참조하십시오.

대상에서 이 절차를 완료합니다. 예를 들어 소스 스토리지 VM에 SMB가 구성된 경우 새 보호 정책을 생성해야 하는 경우 정책을 생성하고 * Identity preserve * 옵션을 사용해야 합니다. 자세한 내용은 을 "사용자 지정 데이터 보호 정책을 생성합니다"참조하십시오.

단계

이 작업은 System Manager 또는 ONTAP CLI에서 수행할 수 있습니다.

시스템 관리자

1. 대상 클러스터에서 * 보호 > 관계 * 를 클릭합니다.
2. 관계 * 에서 * 보호 * 를 클릭하고 * 스토리지 VM(DR) * 를 선택합니다.
3. 보호 정책을 선택합니다. 맞춤형 보호 정책을 생성한 경우 해당 정책을 선택한 다음 복제할 소스 클러스터와 스토리지 VM을 선택합니다. 새 스토리지 VM 이름을 입력하여 새 대상 스토리지 VM을 생성할 수도 있습니다.
4. 필요한 경우 대상 설정을 변경하여 ID 보존을 재정의하고 네트워크 인터페이스 및 프로토콜을 포함하거나 제외합니다.
5. 저장 * 을 클릭합니다.

CLI를 참조하십시오

1. 대상 SVM 생성:

```
vserver create -vserver <SVM_name> -subtype dp-destination
```

SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-
destination
```

에 대한 자세한 내용은 `vserver create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 작업 스케줄 생성:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

> SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

에 대한 자세한 내용은 `job schedule cron create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 타겟 SVM 또는 타겟 클러스터에서 복제 관계를 생성합니다.

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다.

다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

다음 예에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 생성합니다.

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

정책 유형인 '비동기 미러'를 사용하여 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 SnapMirror DR 관계가 생성됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

정책 유형 'Mirror-vault'로 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 중지:

```
vserver stop -vserver <SVM_name>
```

다음 예에서는 svm_backup이라는 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop -vserver svm_backup
```

에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 대상 SVM 또는 대상 클러스터에서 SVM 복제 관계를 초기화합니다.

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다.

다음 예에서는 소스 SVM, svm1, 대상 SVM, svm_backup 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror SVM 복제에서 **LIF** 및 관련 네트워크 설정을 제외합니다

소스 및 타겟 SVM이 서로 다른 서브넷에 있는 경우 '스냅샷 정책 생성' 명령의 '-discard-configs network' 옵션을 사용하여 SVM 복제에서 LIF 및 관련 네트워크 설정을 제외할 수 있습니다.

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

이 작업에 대해

SVM 복제 관계를 생성할 때 'napmirror create' 명령의 '-identity-preserve' 옵션을 'true'로 설정해야 합니다.

단계

1. 대상 SVM 생성:

'vserver create-vserver_SVM_-subtype DP-destination'

SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

   자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 작업 일정 생성:

   "작업 일정 cron create-name_job_name_-month_month_-DayOfWeek_day_of_week_-day_day_of_month_-hour_hour_-minute_minute_"

   월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

   > SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

   다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. 사용자 지정 복제 정책 생성:

   '스냅샷 정책 생성 - vserver_SVM_-policy_policy_-type async-mirror|vault|mirror-vault-comment_comment_-transfer_rs-priority low|normal-is-network-compression-enabled true|false-discard-configs network'

   다음 예제에서는 LIF를 제외한 SnapMirror DR에 대한 사용자 지정 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

   다음 예에서는 LIF를 제외한 유니파이드 복제에 대한 맞춤형 복제 정책을 생성합니다.

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

   > 향후 페일오버 및 페일백 시나리오를 지원하기 위해 소스 클러스터에 동일한 맞춤형 SnapMirror 정책을 생성하는 것을 고려해 보십시오.

에 대한 자세한 내용은 `snapmirror policy create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 또는 대상 클러스터에서 다음 명령을 실행하여 복제 관계를 생성합니다.

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false -discard
-configs true|false
```

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예제에서는 LIF를 제외한 SnapMirror DR 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

다음 예제에서는 LIF를 제외한 SnapMirror 통합 복제 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 대상 SVM 중지:

'vserver stop'

'_SVM 이름 _'

다음 예에서는 svm_backup이라는 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. 대상 SVM 또는 대상 클러스터에서 복제 관계를 초기화합니다.

'스냅샷 초기화-소스-경로_SVM_:-대상-경로_SVM_:'

다음 예에서는 소스 'svm1'과 대상 'svm_backup' 간의 관계를 초기화합니다.

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

재해가 발생할 경우 데이터 액세스를 위해 대상 SVM에서 네트워크 및 프로토콜을 구성해야 합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 생성"

ONTAP를 통한 **SVM** 복제에서 네트워크, 네임 서비스 및 기타 설정을 제외합니다

타겟 SVM과의 충돌 또는 구성 차이를 방지하기 위해 SVM 복제 관계에서 네트워크, 네임 서비스 및 기타 설정을 제외할 수 있습니다.

스냅샷 생성 명령의 '-identity-preserve false' 옵션을 사용하여 SVM의 볼륨 및 보안 구성만 복제할 수 있습니다. 일부 프로토콜 및 이름 서비스 설정도 보존됩니다.

이 작업에 대해

보존된 프로토콜 및 이름 서비스 설정 목록은 를 참조하십시오 "SVM DR 관계에 복제된 구성".

시작하기 전에

소스 및 타겟 클러스터와 SVM을 피어링해야 합니다.

자세한 내용은 을 참조하십시오 "클러스터 피어 관계를 생성합니다" 및 "SVM 인터클러스터 피어 관계를 생성합니다".

단계

1. 대상 SVM 생성:

   'vserver create-vserver_SVM_-subtype DP-destination'

   SVM 이름은 소스 및 타겟 클러스터 전체에서 고유해야 합니다.

   다음 예에서는 sm_backup이라는 대상 SVM을 생성합니다.

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. 대상 클러스터에서 'vserver peer create' 명령을 사용하여 SVM 피어 관계를 생성합니다.

   자세한 내용은 을 참조하십시오 "SVM 인터클러스터 피어 관계를 생성합니다".

   에 대한 자세한 내용은 `vserver peer create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 복제 작업 스케줄 생성:

   "작업 일정 cron create-name_job_name_-month_month_-DayOfWeek_day_of_week_-day_day_of_month_-hour_hour_-minute_minute_"

   월-일-일-주-시-시간의 경우 월, 일, 시 순으로 모두 작업을 실행하도록 지정할 수 있습니다.

SVM SnapMirror 관계에서 FlexVol 볼륨의 최소 지원 일정(RPO)은 15분입니다. SVM SnapMirror 관계에서 FlexGroup 볼륨의 최소 지원 일정(RPO)은 30분입니다.

다음 예에서는 토요일 오전 3시에 실행되는 my_weekly라는 작업 일정을 생성합니다.

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. 네트워크, 이름 서비스 및 기타 구성 설정을 제외한 복제 관계를 생성합니다.

'sapmirror create-source-path_SVM_:-destination-path_SVM_:-type DP|XDP-schedule schedule -policy -identity -preserve false'

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오. 이 명령은 타겟 SVM 또는 타겟 클러스터에서 실행해야 합니다.

다음 예에서는 기본 'MirorAllSnapshots' 정책을 사용하여 SnapMirror DR 관계를 생성합니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

다음 예제에서는 기본 MirorAndVault 정책을 사용하여 통합 복제 관계를 만듭니다. 네트워크, 이름 서비스 및 기타 구성 설정은 관계가 제외됩니다.

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

정책 유형인 '비동기 미러'를 사용하여 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 SnapMirror DR 관계가 생성됩니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

정책 유형 'Mirror-vault'로 사용자 지정 정책을 생성했다고 가정하면 다음 예에서는 통합 복제 관계를 생성합니다. 네트워크, 네임 서비스 및 기타 구성 설정은 SVM 복제에서 제외됩니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 대상 SVM 중지:

   'vserver stop'

   '_SVM 이름 _'

   다음 예는 dv1이라는 대상 SVM을 중지합니다.

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. SMB를 사용하는 경우 SMB 서버도 구성해야 합니다.

   을 참조하십시오 "SMB 전용: SMB 서버 생성".

7. 대상 SVM 또는 대상 클러스터에서 SVM 복제 관계를 초기화합니다.

   '스냅샷 초기화-소스-경로_SVM_이름_:-대상-경로_SVM_이름_:'

   에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

작업을 마친 후

재해가 발생할 경우 데이터 액세스를 위해 대상 SVM에서 네트워크 및 프로토콜을 구성해야 합니다.

ONTAP SnapMirror SVM DR 관계에 사용할 로컬 계층 지정

재해 복구 SVM이 생성된 후 명령과 함께 옵션을 `vserver modify` 사용하여 SVM DR 타겟 볼륨을 호스팅하는 데 사용되는 로컬 계층을 제한할 수 `aggr-list` 있습니다.

단계

1. 대상 SVM 생성:

   'vserver create-vserver_SVM_-subtype DP-destination'

2. 재해 복구 SVM의 집계 목록을 수정하여 재해 복구 SVM 볼륨을 호스팅하는 데 사용되는 로컬 계층을 제한합니다.

   'cluster_dest::> vserver modify -vserver_SVM_-aggr-list <comma-separated-list>'

DR 관계에서 **ONTAP SnapMirror** 대상 **SVM**에 대한 **SMB** 서버를 생성합니다

소스 SVM에 SMB 구성이 있으며 을 로 `false` 설정하도록 선택한 경우 `identity-`

`preserve`, 대상 SVM에 대한 SMB 서버를 생성해야 합니다. SnapMirror 관계를 초기화할 때 공유와 같은 일부 SMB 구성에는 SMB 서버가 필요합니다.

단계

1. 명령을 사용하여 타겟 SVM을 `vserver start` 시작합니다.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

에 대한 자세한 내용은 `vserver start` "ONTAP 명령 참조입니다"을 참조하십시오.

2. vserver show 명령을 사용하여 대상 SVM이 "Running" 상태이고 하위 유형이 dp-destination인지 확인하십시오.

```
destination_cluster::> vserver show
                                    Admin      Operational Root
Vserver  Type    Subtype            State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

에 대한 자세한 내용은 `vserver show` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 네트워크 인터페이스 생성 명령을 사용하여 LIF를 생성합니다.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. network route create 명령을 사용하여 route를 생성한다.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"네트워크 관리"

에 대한 자세한 내용은 `network route create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 'vserver services dns create' 명령을 사용하여 DNS를 구성합니다.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

에 대한 자세한 내용은 `vserver services dns create` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 'vserver cifs domain preferred-dc add' 명령을 사용하여 기본 도메인 컨트롤러를 추가합니다.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

에 대한 자세한 내용은 `vserver cifs domain preferred-dc add` "ONTAP 명령 참조입니다"을 참조하십시오.

7. 'vserver cifs create' 명령을 사용하여 SMB 서버를 생성합니다.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

에 대한 자세한 내용은 `vserver cifs create` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 'vserver stop' 명령을 사용하여 대상 SVM을 중지합니다.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapMirror SVM DR 관계에서 볼륨을 제외합니다

기본적으로 소스 SVM의 모든 RW 데이터 볼륨이 복제됩니다. 소스 SVM의 모든 볼륨을 보호하지 않으려는 경우 '볼륨 수정' 명령의 '-vserver-dr-protection protected' 옵션을 사용하여 SVM 복제에서 볼륨을 제외할 수 있습니다.

단계

1. SVM 복제에서 볼륨 제외:

   'volume modify -vserver_SVM_-volume_volume_-vserver-dr-protection protected'

   에 대한 자세한 내용은 `volume modify` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 SVM 복제에서 볼륨 'VolA_src'를 제외합니다.

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

나중에 원래 제외된 SVM 복제에 볼륨을 포함하려면 다음 명령을 실행합니다.

'볼륨 수정 - vserver_SVM_-volume_volume_-vserver-dr-protection protected

다음 예에서는 SVM 복제의 볼륨 VolA_src를 포함합니다.

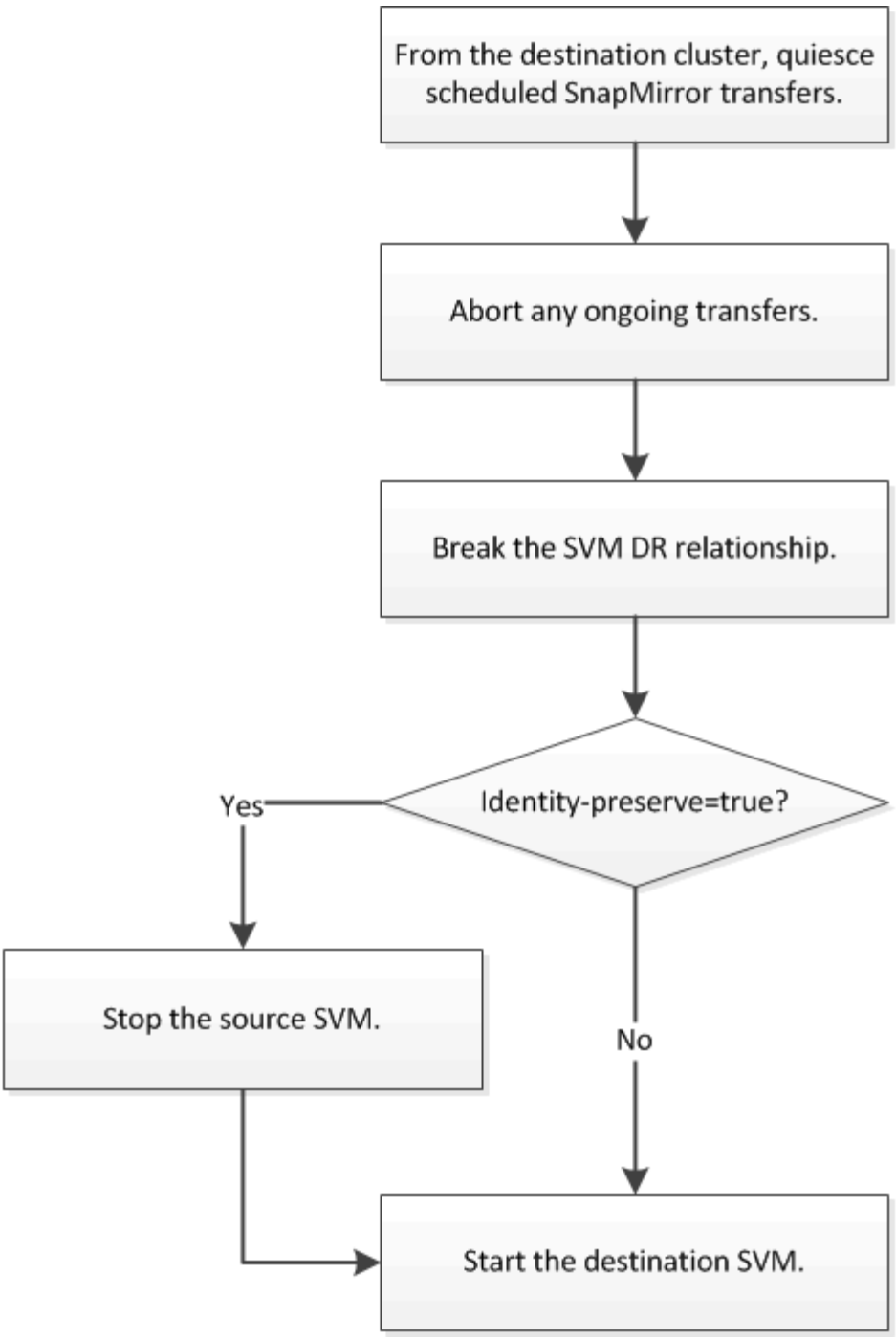
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. 에 설명된 대로 SVM 복제 관계를 생성하고 초기화합니다 "전체 SVM 구성 복제".

SnapMirror SVM DR 대상에서 데이터 제공

ONTAP SnapMirror SVM 재해 복구 워크플로우

재해를 복구하고 타겟 SVM에서 데이터를 제공하려면 타겟 SVM을 활성화해야 합니다. 타겟 SVM을 활성화하려면 예약된 SnapMirror 전송을 중지하고, 지속적인 SnapMirror 전송을 중단하고, 복제 관계를 중단하고, 소스 SVM을 중지하고, 타겟 SVM을 시작해야 합니다.



ONTAP SnapMirror SVM 대상 볼륨을 쓰기 가능으로 구성합니다

클라이언트에 데이터를 제공하려면 SVM 대상 볼륨을 쓰기 가능하게 해야 합니다.

이 절차는 볼륨 복제 절차와 크게 동일하지만 한 가지 예외가 있습니다. SVM 복제 관계를 생성할 때 를 설정한 `-identity-preserve true` 경우, 대상 SVM을 활성화하기 전에 소스 SVM을 중지해야 합니다.

이 작업에 대해

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

재해 복구 시나리오에서는 소스 SVM과 해당 데이터에 액세스할 수 없고 마지막 재동기화 이후의 업데이트가 불량하거나 손상되었을 수 있으므로 소스 SVM에서 재해 복구 대상 SVM으로 SnapMirror 업데이트를 수행할 수 없습니다.

ONTAP 9.8부터 System Manager를 사용하여 재해 발생 후 대상 스토리지 VM을 활성화할 수 있습니다. 대상 스토리지 VM을 활성화하면 SVM 대상 볼륨을 쓸 수 있고 데이터를 클라이언트에 제공할 수 있습니다.

단계

이 작업은 System Manager 또는 ONTAP CLI에서 수행할 수 있습니다.

시스템 관리자

1. 소스 클러스터에 액세스할 수 있는 경우 SVM이 중지되었는지 확인합니다. * 스토리지 > 스토리지 VM * 으로 이동하고 SVM을 위한 * 상태 * 열을 확인합니다.
2. 소스 SVM 상태가 "실행 중"인 경우 중지하십시오. 를 선택하고 ⋮ * 중지 * 를 선택하십시오.
3. 대상 클러스터에서 원하는 보호 관계를 찾습니다. * 보호 > 관계 * 로 이동합니다.
4. 원하는 소스 스토리지 VM 이름 위로 마우스를 가져가 를 클릭하고 ⋮* 대상 스토리지 VM 활성화 * 를 선택합니다.
5. 대상 스토리지 VM 활성화 * 창에서 * 대상 스토리지 VM 활성화 및 관계 해제 * 를 선택합니다.
6. Activate * 를 클릭합니다.

CLI를 참조하십시오

1. 대상 SVM 또는 대상 클러스터에서 SVM을 중지하여 대상으로 예약된 전송을 중지합니다.

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 예약된 전송을 중지합니다.

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 대상 SVM 또는 대상 클러스터에서 목적지로의 진행 중인 전송을 중지합니다.

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 지속적인 전송을 중지합니다.

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

에 대한 자세한 내용은 `snapmirror abort` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 타겟 SVM 또는 타겟 클러스터에서 복제 관계를 중단하십시오.

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 나눕니다.

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

4. SVM 복제 관계를 생성할 때 '-identity-preserve true'를 설정하면 소스 SVM을 중지합니다.

```
vserver stop -vserver <SVM>
```

다음 예에서는 소스 SVM의 vm1'를 중지합니다.

```
cluster_src::> vserver stop svm1
```

5. 대상 SVM 시작:

```
vserver start -vserver <SVM>
```

다음 예에서는 대상 SVM의 VM_BACKUP을 시작합니다.

```
cluster_dst::> vserver start svm_backup
```

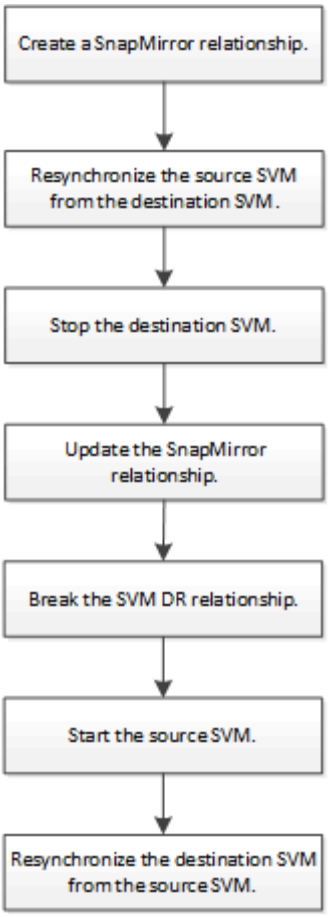
작업을 마친 후

에 설명된 대로 데이터 액세스를 위해 SVM 대상 볼륨을 구성합니다 "데이터 액세스를 위한 대상 볼륨을 구성합니다".

SnapMirror 소스 SVM을 재활성화합니다

ONTAP SnapMirror 소스 **SVM** 재활성화 워크플로우

재해 발생 후 소스 SVM이 있으면 SVM 재해 복구 관계를 재생성하여 재활성화하고 보호할 수 있습니다.



원래 **ONTAP SnapMirror** 소스 **SVM**을 다시 활성화합니다

대상에서 데이터를 더 이상 사용할 필요가 없을 경우 소스 및 타겟 SVM 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다. 이 절차는 볼륨 복제 절차와 크게 동일하지만 한 가지 예외가 있습니다. 소스 SVM을 다시 활성화하기 전에 타겟 SVM을 중지해야 합니다.

시작하기 전에

- 데이터를 제공하는 동안 대상 볼륨의 크기를 늘인 경우 소스 볼륨을 다시 활성화하기 전에 원본 소스 볼륨의 최대 크기 자동 크기 조정을 수동으로 늘려 충분히 성장할 수 있도록 해야 합니다.

"타겟 볼륨이 자동으로 증가하는 경우"

클러스터 관리자는 데이터 손실을 방지하기 위해 원래 소스 SVM을 다시 활성화하기 전에 클라이언트의 쓰기 작업을 일시 중지해야 합니다.

이 작업에 대해

ONTAP 9.11.1부터 `-quick-resync true` `snapmirror resync`SVM DR 관계의 역재동기화를 수행하는 동안 명령의 `CLI` 옵션을 사용하여 재해 복구 예행 연습 중에 재동기화 시간을 줄일 수 있습니다. 빠른 재동기화를 통해 데이터 웨어하우스 재구축 및 복원 작업을 바이패스하여 운영 상태로 돌아가는 데 걸리는 시간을 줄일 수 있습니다. 에 대한 자세한 내용은 `snapmirror resync` "ONTAP 명령 참조입니다"을 참조하십시오.

빠른 재동기화는 타겟 볼륨의 스토리지 효율성을 유지하지 않습니다. 빠른 재동기화를 설정하면 대상 볼륨에서 사용하는 볼륨 공간이 증가할 수 있습니다.

이 절차에서는 원본 소스 볼륨의 기준선이 온전한 것으로 가정합니다. 기준선이 변경되지 않은 경우 절차를 수행하기 전에 데이터를 제공하는 볼륨과 원본 소스 볼륨 간의 관계를 생성하고 초기화해야 합니다.

ONTAP 9.8부터 시스템 관리자를 사용하여 재해 발생 후 소스 스토리지 VM을 다시 활성화할 수 있습니다.

단계

이 작업은 시스템 관리자 또는 ONTAP CLI를 사용하여 수행할 수 있습니다.

시스템 관리자 **ONTAP 9.17.1** 이상

1. 대상 클러스터에서 원하는 보호 관계를 선택하려면 *보호 > 복제*를 클릭하십시오.
2. 소스 이름 위에 마우스 커서를 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.

   해당 관계는 복제 테이블에서 사라지고 이제 원래 소스 클러스터에서 관리됩니다.

4. 원본 소스 클러스터에서 *보호 > 복제*를 클릭하고 상태가 *미러링됨*으로 표시되는지 확인하여 역방향 재동기화가 완료되었는지 확인합니다.
5. 원래 대상 클러스터에서 *클러스터 > 스토리지 VM*으로 이동합니다.
6. 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올린 다음 클릭합니다. ⋮그리고 *정지*를 클릭하세요.
7. 저장소 **VM** 중지 창에서 *중지*를 클릭합니다.
8. 원본 클러스터에서 *보호 > 복제*로 이동하여 다시 활성화할 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올려놓은 다음 클릭합니다. ⋮그런 다음 *대상 스토리지 VM 활성화*를 클릭합니다.
9. 대상 스토리지 **VM** 활성화 창에서 *대상 스토리지 VM을 활성화하고 연결을 해제*를 선택한 다음 *활성화*를 클릭합니다.
10. 복제 페이지로 돌아가면 스토리지 VM 이름 위에 마우스 커서를 다시 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.

시스템 관리자 **ONTAP 9.16.1** 및 이전 버전

1. 대상 클러스터에서 원하는 보호 관계를 선택하려면 *보호 > 관계*를 클릭하십시오.
2. 소스 이름 위에 마우스 커서를 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.
3. Reverse resync relationship * 창에서 * Reverse resync * 를 클릭합니다.

   해당 관계는 이제 원래 소스 클러스터에서 관리되므로 관계 테이블에서 사라집니다.

4. 원본 소스 클러스터에서 *보호 > 관계*를 클릭하고 상태가 *미러링됨*으로 표시되는지 확인하여 역방향 재동기화가 완료되었는지 확인합니다.
5. 원래 대상 클러스터에서 *스토리지 > 스토리지 VM*으로 이동합니다.
6. 스토리지 VM을 찾고, 스토리지 VM 이름 위에 마우스 커서를 올린 다음 클릭합니다. ⋮그리고 *정지*를 클릭하세요.
7. 저장소 **VM** 중지 창에서 *중지*를 클릭합니다.
8. 원본 클러스터에서 스토리지 VM(이제 역관계의 원본 SVM)을 찾고, SVM 이름 위에 마우스 커서를 올려놓은 다음 클릭합니다. ⋮그런 다음 *대상 스토리지 VM 활성화*를 클릭합니다.
9. 대상 스토리지 **VM** 활성화 창에서 *대상 스토리지 VM 활성화 및 연결 해제*를 선택하고 *활성화*를 클릭합니다.
10. 관계 페이지로 돌아가서 스토리지 VM 이름 위에 마우스 커서를 다시 올려놓고 클릭하세요. ⋮그리고 *역방향 동기화*를 클릭하세요.

CLI를 참조하십시오

1. 원본 소스 SVM 또는 원본 소스 클러스터에서 동일한 구성, 정책 및 ID 보존 설정을 원본 SVM DR 관계로

사용하여 역방향 SVM DR 관계를 생성합니다.

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 SVM과 SVM_BACKUP, 그리고 원래 소스 SVM, Svm1 간의 관계를 생성합니다.

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 데이터 보호 관계를 반대로 전환합니다.

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다.

다음 예에서는 원래 소스 SVM, svm1, 데이터를 제공하는 SVM, svm_backup의 관계를 반전시킵니다.

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

사용 예 - 빠른 재동기화 옵션:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. 원래 소스 SVM에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 SVM을 중지하고 원래 타겟 SVM에 현재 연결된 모든 클라이언트의 연결을 끊습니다.

```
vserver stop -vserver <SVM>
```

다음 예에서는 현재 데이터를 제공하고 있는 원래 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

4. 'vserver show' 명령을 사용하여 원래 대상 SVM이 중지됨 상태인지 확인합니다.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계의 최종 업데이트를 수행하고 원래 대상 SVM에서 원래 소스 SVM으로 모든 변경 사항을 전송합니다.

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

6. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계에 대한 예약된 전송을 중지합니다.

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 SVM, 'sVM_backup'과 원래 SVM, svm1 간의 예약된 전송을 중지합니다.

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 나눕니다.

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하고 있는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 나눕니다.

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 소스 SVM이 이전에 중지된 경우 원래 소스 클러스터에서 원본 소스 SVM을 시작합니다.

```
vserver start -vserver <SVM>
```

다음 예에서는 원본 소스 SVM을 시작합니다.

```
cluster_src::> vserver start svm1
```

9. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 데이터 보호 관계를 다시 설정합니다.

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

'-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 데이터 보호 관계를 삭제합니다.

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 대상 SVM, sVM_backup과 원래 소스 SVM, svm1 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. 원래 대상 SVM 또는 원래 대상 클러스터에서 역방향 데이터 보호 관계를 해제합니다.

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간의 역방향 관계를 해제합니다

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

다음 단계

- 를 사용합니다 `snapmirror show` 명령을 사용하여 SnapMirror 관계가 생성되었는지 확인합니다.

  에 대한 자세한 내용은 `snapmirror show` "ONTAP 명령 참조입니다"을 참조하십시오.

- 클라이언트에서 원래 소스 SVM으로 쓰기 작업을 재개합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 중지"

- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

FlexGroup 볼륨에 대해 원래의 **ONTAP SnapMirror** 소스 **SVM**을 다시 활성화합니다

대상에서 데이터를 더 이상 사용할 필요가 없을 경우 소스 및 타겟 SVM 간에 원래 데이터 보호 관계를 다시 설정할 수 있습니다. FlexGroup 볼륨을 사용할 때 원본 소스 SVM을 다시 활성화하려면 원래 SVM DR 관계를 삭제하고 관계를 반대로 설정하기 전에 원래 관계를 해제하는 등 몇 가지 추가 단계를 수행해야 합니다. 또한 예약된 전송을 중지하기 전에 역방향 관계를 해제하고 원래 관계를 다시 생성해야 합니다.

단계

1. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 SVM DR 관계를 삭제합니다.

   '스냅샷 삭제 - 소스 경로 SVM: - 대상 경로 SVM:

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 원래 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. 원본 소스 SVM 또는 원본 소스 클러스터에서 스냅샷을 그대로 유지하면서 원본 관계를 해제합니다.

   '냅미러 해제-소스-경로 SVM:-대상-경로 SVM:-관계-정보-전용 true'

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 원래 관계를 해제합니다.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. 원본 소스 SVM 또는 원본 소스 클러스터에서 동일한 구성, 정책 및 ID 보존 설정을 원본 SVM DR 관계로 사용하여 역방향 SVM DR 관계를 생성합니다.

   "napMirror create-source-path SVM:-destination-path SVM:

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하는 SVM과 SVM_BACKUP, 그리고 원래 소스 SVM, Svm1 간의 관계를

생성합니다.

```
cluster_src::> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 데이터 보호 관계를 반대로 전환합니다.

   '스냅샷 미러 재동기화 - 소스 경로_SVM_: - 대상-경로_SVM_:'

   '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   소스와 대상에 공통 스냅샷이 없는 경우 명령이 실패합니다. `snapmirror initialize`관계를 다시 초기화하는 데 사용합니다.

   다음 예에서는 원래 소스 SVM, svm1, 데이터를 제공하는 SVM, svm_backup의 관계를 반전시킵니다.

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. 원래 소스 SVM에 대한 데이터 액세스를 다시 설정할 준비가 되면 원래 타겟 SVM을 중지하고 원래 타겟 SVM에 현재 연결된 모든 클라이언트의 연결을 끊습니다.

   'vserver stop-vserver_SVM_'

   다음 예에서는 현재 데이터를 제공하고 있는 원래 대상 SVM을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

6. 'vserver show' 명령을 사용하여 원래 대상 SVM이 중지됨 상태인지 확인합니다.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계의 최종 업데이트를 수행하고 원래

대상 SVM에서 원래 소스 SVM으로 모든 변경 사항을 전송합니다.

'스냅미러 업데이트 - source-path_SVM_: - destination-path_SVM_:'

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 데이터를 제공하는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 업데이트합니다.

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

8. 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계에 대한 예약된 전송을 중지합니다.

   'sapmirror quiesce-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하는 SVM, 'sVM_backup'과 원래 SVM, svm1 간의 예약된 전송을 중지합니다.

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
   -path svm1:
   ```

   에 대한 자세한 내용은 `snapmirror quiesce` "ONTAP 명령 참조입니다"을 참조하십시오.

9. 최종 업데이트가 완료되고 관계가 관계 상태에 "중지됨"으로 표시되면 원래 소스 SVM 또는 원래 소스 클러스터에서 다음 명령을 실행하여 역방향 관계를 나눕니다.

   '스냅미러 break-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 데이터를 제공하고 있는 원래 대상 SVM, 'sVM_backup' 및 원래 소스 SVM, 'svm1' 간의 관계를 나눕니다.

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

10. 원래 소스 SVM이 이전에 중지된 경우 원래 소스 클러스터에서 원본 소스 SVM을 시작합니다.

'vserver start-vserver_SVM_'

다음 예에서는 원본 소스 SVM을 시작합니다.

```
cluster_src::> vserver start svm1
```

11. 원래 소스 SVM 또는 원본 소스 클러스터에서 역방향 SVM DR 관계를 삭제합니다.

    '스냅샷 삭제 - 소스 경로 SVM: - 대상 경로 SVM:

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간의 역방향 관계를 삭제합니다.

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. 원래의 대상 SVM 또는 원래의 대상 클러스터에서 스냅샷을 그대로 유지하면서 반대 관계를 해제합니다.

    '냅미러 해제-소스-경로 SVM:-대상-경로 SVM:-관계-정보-전용 true'

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 대상 SVM, svm_backup 및 원래 소스 SVM, svm1 간에 반전된 관계를 해제합니다.

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 관계를 다시 생성합니다. 동일한 구성, 정책 및 ID 보존 설정을 원래 SVM DR 관계와 동일하게 사용:

    "napMirror create-source-path SVM:-destination-path SVM:

    '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

    다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간에 관계를 생성합니다.

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. 원래 대상 SVM 또는 원래 대상 클러스터에서 원래 데이터 보호 관계를 다시 설정합니다.

'스냅샷 미러 재동기화 - 소스 경로_SVM_: - 대상-경로_SVM_:'

> '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

다음 예에서는 원래 소스 SVM, svm1, 원래 대상 SVM, svm_backup 간의 관계를 다시 설정합니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror 대상 **SVM**에서 데이터를 다시 동기화합니다

ONTAP 9.11.1에는 재해 복구 연습을 수행할 때 전체 데이터 웨어하우스 재구축을 우회하는 옵션이 도입되어 생산 단계로 빠르게 돌아갈 수 있습니다.

ONTAP 9.8부터는 System Manager를 사용하여 소스 스토리지 VM의 데이터 및 구성 세부 정보를 손상된 보호 관계에 있는 대상 스토리지 VM으로 재동기화하고 관계를 다시 설정할 수 있습니다.

원래 관계의 대상에서만 재동기화 작업을 수행합니다. 재동기화를 수행하면 소스 스토리지 VM의 데이터보다 최신 대상 스토리지 VM의 데이터가 삭제됩니다.

단계

System Manager 또는 ONTAP CLI를 사용하여 이 작업을 수행할 수 있습니다.

시스템 관리자

1. 타겟에서 원하는 보호 관계를 선택합니다. * 보호 > 관계 * 를 클릭합니다.
2. 선택적으로 * 빠른 재동기화 수행 * 을 선택하여 재해 복구 리허설 중에 전체 데이터 웨어하우스 재구축을 우회합니다.
3. 을 클릭하고 ⋮ * 재동기화 * 를 클릭합니다.
4. 관계 * 에서 관계에 대한 * 전송 상태 * 를 확인하여 재동기화 진행률을 모니터링합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 관계를 다시 동기화합니다.

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

관련 정보

- "스냅미러 재동기화"

ONTAP SnapMirror 볼륨 DR 관계를 SVM DR 관계로 변환합니다

소스의 각 볼륨(루트 볼륨 제외)이 복제되고 있는 경우, 볼륨을 소유하는 SVM(스토리지 가상 머신) 간의 복제 관계를 SVM(스토리지 가상 머신) 간에 복제 관계로 전환할 수 있습니다. 소스(루트 볼륨 포함)의 각 볼륨의 이름은 대상의 볼륨과 동일합니다.

이 작업에 대해

`volume rename`필요한 경우 SnapMirror 관계가 유휴 상태일 때 명령을 사용하여 대상 볼륨의 이름을 바꿉니다. 에 대한 자세한 내용은 `volume rename` link:https://docs.netapp.com/us-en/ontap-cli/volume-rename.html["ONTAP 명령 참조입니다"^]을 참조하십시오.

단계

1. 타겟 SVM 또는 타겟 클러스터에서 소스 볼륨과 타겟 볼륨을 다시 동기화하려면 다음 명령을 실행합니다.

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   에 대한 자세한 내용은 snapmirror resync "ONTAP 명령 참조입니다"을 참조하십시오.

   재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   다음 예에서는 svm1의 소스 볼륨 VolA와 sm_backup의 대상 볼륨 VolA의 관계를 재동기화했습니다.

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

2. 에 설명된 대로 소스 및 타겟 SVM 간에 SVM 복제 관계를 생성합니다 "SVM 구성 복제".

   복제 관계를 생성할 때 'napmirror create' 명령의 '-identity-preserve true' 옵션을 사용해야 합니다.

   에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 대상 SVM 중지:

   'vserver stop-vserver_SVM_'

   에 대한 자세한 내용은 `vserver stop` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 대상 SVM의 VM_BACKUP을 중지합니다.

```
cluster_dst::> vserver stop svm_backup
```

4. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 소스 및 타겟 SVM을 다시 동기화하십시오.

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.
   >
   > 재동기화에는 기본 전송이 필요하지 않지만 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 재동기화를 실행할 수 있습니다.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 재동기화했습니다.

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

관련 정보

- "SnapMirror 생성"
- "스냅미러 재동기화"

ONTAP SnapMirror SVM 복제 관계를 삭제합니다

및 `snapmirror release` 명령을 사용하여 SVM 복제 관계를 삭제할 수 있습니다 `snapmirror delete`. 그런 다음 불필요한 대상 볼륨을 수동으로 삭제할 수 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

이 작업에 대해

이 `snapmirror release` 명령은 SnapMirror에서 생성된 스냅샷을 소스에서 삭제합니다. 옵션을 사용하여 스냅샷을 보존할 수 `-relationship-info-only` 있습니다.

단계

1. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 복제 관계를 중단하십시오.

   '스냅미러 break-source-path_SVM_:-destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 나눕니다.

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

   에 대한 자세한 내용은 `snapmirror break` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 타겟 SVM 또는 타겟 클러스터에서 다음 명령을 실행하여 복제 관계를 삭제합니다.

   '스냅샷 삭제-소스-경로_SVM_:-대상-경로_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1과 대상 SVM의 vm_backup 간의 관계를 삭제합니다.

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   에 대한 자세한 내용은 `snapmirror delete` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 소스 클러스터 또는 소스 SVM에서 다음 명령을 실행하여 소스 SVM에서 복제 관계 정보를 해제합니다.

   '스냅미러 해제 - source-path_SVM_: - destination-path_SVM_:'

   > '-source-path' 및 '-destination-path' 옵션에서 SVM 이름 뒤에 콜론(:)을 입력해야 합니다. 아래 예를 참조하십시오.

   다음 예에서는 소스 SVM의 vm1에서 지정된 복제 관계에 대한 정보를 해제합니다.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

에 대한 자세한 내용은 `snapmirror release` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapMirror 루트 볼륨 복제를 관리합니다

ONTAP SnapMirror 루트 볼륨 복제에 대해 알아보십시오

NAS 환경의 모든 SVM에는 고유한 네임스페이스가 있습니다. 운영 체제 및 관련 정보가 포함된 SVM_root 볼륨은 네임스페이스 계층 구조의 진입점입니다. 노드 운영 중단 또는 페일오버 발생 시 클라이언트가 데이터에 계속 액세스할 수 있도록 SVM 루트 볼륨의 로드 공유 미러 복사본을 생성해야 합니다.

SVM 루트 볼륨을 위한 로드 공유 미러의 주요 용도는 더 이상 로드 공유를 위한 것이 아니라, 재해 복구를 위한 것입니다.

- 루트 볼륨을 일시적으로 사용할 수 없는 경우 로드 공유 미러에서 루트 볼륨 데이터에 대한 읽기 전용 액세스를 자동으로 제공합니다.
- 루트 볼륨을 영구적으로 사용할 수 없는 경우 로드 공유 볼륨 중 하나를 승격하여 루트 볼륨 데이터에 대한 쓰기 액세스를 제공할 수 있습니다.

ONTAP 로드 공유 미러 관계를 생성하고 초기화합니다

클러스터에서 NAS 데이터를 처리하는 각 SVM 루트 볼륨에 대해 로드 공유 미러(LSM)를 생성해야 합니다. 두 개 이상의 HA 쌍으로 구성된 클러스터의 경우, HA 쌍의 두 노드 모두에 장애가 발생하더라도 클라이언트가 네임스페이스에 계속 액세스할 수 있도록 SVM 루트 볼륨의 로드 공유 미러를 고려해야 합니다. 로드 공유 미러는 단일 HA 쌍으로 구성된 클러스터에는 적합하지 않습니다.

시작하기 전에

ONTAP 9.16.1부터 로드 공유 미러 관계를 생성할 때 대상 SVM에서 저장소 제한을 활성화할 수 없습니다.

이 작업에 대해

동일한 노드에서 LSM을 생성하고 해당 노드를 사용할 수 없는 경우, 단일 장애 지점이 있으며, 클라이언트가 데이터에 계속 액세스할 수 있도록 하기 위한 두 번째 복제본이 없습니다. 그러나 루트 볼륨이 포함된 노드 이외의 노드 또는 다른 HA 쌍에서 LSM을 생성할 경우, 중단 시에도 데이터에 액세스할 수 있습니다.

예를 들어, 3개 노드에 루트 볼륨이 있는 4노드 클러스터의 경우:

- HA 1 노드 1의 루트 볼륨의 경우 HA 2 노드 1 또는 HA 2 노드 2에 LSM을 생성한다.
- HA 1 노드 2의 루트 볼륨의 경우 HA 2 노드 1 또는 HA 2 노드 2에 LSM을 생성한다.
- HA 2 노드 1의 루트 볼륨의 경우 HA 1 노드 1 또는 HA 1 노드 2에 LSM을 생성한다.

단계

1. LSM의 대상 볼륨을 생성한다.

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

대상 볼륨의 크기는 루트 볼륨보다 크거나 같아야 합니다.

루트 및 대상 볼륨에 접미사를 지정하는 것이 가장 좋습니다. 예를 들어, '_root' 및 '_m1' 등이 있습니다.

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 예에서는 "cluster_src"에 루트 볼륨 svm1_root에 대한 로드 공유 미러 볼륨을 생성합니다.

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "복제 작업 일정을 생성합니다".
3. SVM 루트 볼륨과 LSM의 대상 볼륨 간에 로드 공유 미러 관계를 생성합니다.

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

다음 예에서는 루트 볼륨 'vm1_root'와 로드 공유 미러 볼륨 'svm1_m1' 간에 로드 공유 미러 관계를 생성합니다.

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

부하 공유 미러의 유형 속성이 DP에서 LS로 변경됩니다.

에 대한 자세한 내용은 `snapmirror create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 로드 공유 미러 초기화:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

다음 예에서는 루트 볼륨 'svm1_root'에 대한 로드 공유 미러를 초기화합니다.

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

에 대한 자세한 내용은 `snapmirror initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 로드 공유 미러 관계를 업데이트합니다

SVM에 볼륨이 마운트 또는 마운트 해제된 이후, 그리고 옵션을 포함하는 운영 `junction-path` 중에 SVM 루트 볼륨에 대한 로드 공유 미러(LSM) 관계가 자동으로 업데이트됩니다 `volume create`. 다음 번 예약된 업데이트 전에 업데이트하려는 경우 LSM 관계를 수동으로 업데이트할 수 있습니다.

다음과 같은 경우 로드 공유 미러 관계가 자동으로 업데이트됩니다.

- 예약된 업데이트를 할 시간입니다
- SVM 루트 볼륨의 볼륨에 대해 마운트 또는 마운트 해제 작업이 수행됩니다
- 에이 `volume create` 다음을 포함하는 명령이 발행됩니다. `junction-path` 옵션

  에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 로드 공유 미러 관계를 수동으로 업데이트:

   이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   다음 예에서는 루트 볼륨 'svm1_root'에 대한 로드 공유 미러 관계를 업데이트합니다.

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   에 대한 자세한 내용은 `snapmirror update` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 로드 공유 미러를 상향 이동합니다

루트 볼륨을 영구적으로 사용할 수 없는 경우 LSM(Load-sharing mirror) 볼륨을 프로모션하여 루트 볼륨 데이터에 대한 쓰기 액세스를 제공할 수 있습니다.

시작하기 전에

이 작업에는 고급 권한 레벨 명령을 사용해야 합니다.

단계

1. 고급 권한 레벨로 변경:

   ```
   set -privilege advanced
   ```

2. LSM 볼륨 승격:

이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

```
snapmirror promote -destination-path <SVM:volume>
```

다음 예에서는 볼륨의 vm1_m2를 새 SVM 루트 볼륨으로 상향 이동합니다.

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

y를 입력합니다. ONTAP는 LSM 볼륨을 읽기/쓰기 볼륨으로 만들고, 액세스 가능한 경우 원래 루트 볼륨을 삭제한다.

> 마지막 업데이트가 최근에 수행되지 않은 경우 상향 이동된 루트 볼륨에 원래 루트 볼륨에 있던 데이터가 모두 없을 수 있습니다.

에 대한 자세한 내용은 `snapmirror promote` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 관리자 권한 레벨로 돌아가기:

```
set -privilege admin
```

4. 루트 볼륨에 사용한 명명 규칙에 따라 승격된 볼륨의 이름을 바꿉니다.

이 명령을 실행하기 전에 꺾쇠 괄호 안의 변수를 필수 값으로 바꾸어야 합니다.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

다음 예에서는 승격된 볼륨의 이름을 vm1_m2로 바꾸고 이름은 svm1_root로 바꿉니다.

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. 의 3단계에서 4단계에 설명된 대로 이름이 변경된 루트 볼륨을 보호합니다 "로드 공유 미러 관계 생성 및 초기화".

클라우드에 백업

ONTAP SnapMirror 클라우드 라이센스를 설치합니다

SnapMirror 클라우드 관계는 사전 검증된 타사 백업 애플리케이션을 사용하여 조정할 수 있습니다. ONTAP 9.9.1부터 System Manager를 사용하여 SnapMirror 클라우드 복제를 오케스트레이션할 수도 있습니다. System Manager를 사용하여 온프레미스 ONTAP를 오브젝트 스토리지 백업으로 조정하는 경우 SnapMirror 및 SnapMirror 클라우드 용량 라이센스가 모두 필요합니다. 또한 SnapMirror 클라우드 API 라이센스를 요청하여 설치해야 합니다.

이 작업에 대해

SnapMirror 클라우드 및 SnapMirror S3 라이센스는 노드 라이센스가 아니라 클러스터 라이센스이므로 ONTAP One 라이센스 번들과 함께 _ 제공되지 않습니다. 이러한 라이선스는 별도의 ONTAP One 호환성 번들에 포함되어 있습니다. SnapMirror 클라우드를 활성화하려면 이 번들을 요청해야 합니다.

또한 오브젝트 스토리지에 대한 SnapMirror 클라우드 백업을 System Manager에서 오케스트레이션하려면 SnapMirror Cloud API 키가 필요합니다. 이 API 라이센스는 단일 인스턴스 클러스터 전체 라이센스이므로 클러스터의 모든 노드에 설치할 필요가 없습니다.

단계

ONTAP One 호환성 번들과 SnapMirror Cloud API 라이센스를 요청하여 다운로드한 다음, System Manager를 사용하여 설치해야 합니다.

1. 라이센스할 클러스터의 클러스터 UUID를 찾아 기록합니다.

   클러스터에 맞는 ONTAP One 호환성 번들을 주문하기 위한 요청을 제출할 때 클러스터 UUID가 필요합니다.

2. NetApp 영업 팀에 문의하여 ONTAP One 호환성 번들을 요청하십시오.
3. NetApp 지원 사이트에 제공된 지침에 따라 SnapMirror 클라우드 API 라이센스를 요청합니다.

   "SnapMirror 클라우드 API 라이센스 키를 요청합니다"

4. 라이센스 파일을 받아 다운로드하면 시스템 관리자를 사용하여 ONTAP 클라우드 호환성 NLF 및 SnapMirror 클라우드 API NLF를 클러스터에 업로드합니다.
   a. 클러스터 > 설정 * 을 클릭합니다.
   b. 설정 * 창에서 * 라이센스 * 를 클릭합니다.
   c. 라이센스 * 창에서 를 + Add 클릭합니다.
   d. 라이센스 추가 * 대화 상자에서 * 찾아보기 * 를 클릭하여 다운로드한 NLF를 선택한 다음 * 추가 * 를 클릭하여 파일을 클러스터에 업로드합니다.

관련 정보

"SnapMirror를 사용하여 데이터를 클라우드에 백업합니다"

"NetApp 소프트웨어 라이센스 검색"

ONTAP SnapMirror를 사용하여 클라우드에 데이터를 백업합니다

ONTAP 9.9.1부터 System Manager를 사용하여 데이터를 클라우드로 백업하고 클라우드 스토리지에서 다른 볼륨으로 데이터를 복원할 수 있습니다. StorageGRID 또는 ONTAP S3를 클라우드 오브젝트 저장소로 사용할 수 있습니다.

ONTAP 9.18.1부터:

- SnapMirror 클라우드는 기존 "ONTAP REST API"을(를) 사용하여 MetroCluster 구성의 FlexGroup 볼륨에 대한 백업 및 복원 작업을 지원합니다. 이 기능을 통해 스위치오버 및 스위치백 후 파트너 사이트에서 유지 관리되는 MetroCluster 구성의 FlexGroup 볼륨에 대해 SnapMirror 클라우드 관계를 생성할 수 있습니다.

ONTAP 9.16.1부터:

- SnapMirror 클라우드 백업은 팬아웃 관계를 지원합니다. 즉, 서로 다른 두 오브젝트 저장소에서 SnapMirror 백업을 동시에 생성할 수 있습니다. SnapMirror 클라우드는 ONTAP 9.16.1을 통해 2가지 팬아웃 관계를 지원합니다. 팬아웃은 두 개의 오브젝트 저장소와 두 개의 서로 다른 오브젝트 저장소에 있는 하나 또는 두 개의 버킷으로 구성될 수 있습니다. 3개 이상의 팬아웃 관계를 생성하려는 시도는 실패합니다.
- SnapMirror 클라우드는 기존 볼륨을 사용하는 보다 효율적인 동기화 프로세스를 사용하여 클라우드로 마이그레이션된 볼륨을 백업할 수 있도록 "ONTAP REST API"지원합니다. 이 기능은 기준선 변경 작업을 수행할 필요 없이 클라우드의 마이그레이션된 볼륨에서 동일한 타겟 오브젝트 저장소 엔드포인트로 SnapMirror 클라우드 백업을 지원합니다. FlexVol 볼륨과 FlexGroup 볼륨이 모두 지원됩니다.

SnapMirror 클라우드 기능을 사용하기 전에 NetApp 지원 사이트에서 SnapMirror 클라우드 API 라이센스 키를 요청해야 합니다"SnapMirror 클라우드 API 라이센스 키를 요청합니다". 지침에 따라 비즈니스 기회에 대한 간단한 설명을 제공하고 제공된 이메일 주소로 이메일을 보내 API 키를 요청해야 합니다. API 키를 얻는 방법에 대한 추가 지침이 포함된 이메일 응답을 24시간 이내에 받아야 합니다.

클라우드 오브젝트 저장소를 추가합니다

SnapMirror 클라우드 백업을 구성하기 전에 StorageGRID 또는 ONTAP S3 클라우드 오브젝트 저장소를 추가해야 합니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.
2. 을 클릭합니다 + Add .

기본 정책을 사용하여 백업합니다

기본 클라우드 보호 정책인 DailyBackup을 사용하여 기존 볼륨에 대한 SnapMirror 클라우드 백업을 빠르게 구성할 수 있습니다.

단계

1. 보호 > 개요 * 를 클릭하고 * Cloud에 볼륨 백업 * 을 선택합니다.
2. 처음으로 클라우드로 백업하는 경우 표시된 대로 라이센스 필드에 SnapMirror 클라우드 API 라이센스 키를 입력합니다.
3. 인증 및 계속 * 을 클릭합니다.
4. 소스 볼륨을 선택합니다.

5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

사용자 지정 클라우드 백업 정책을 생성합니다

SnapMirror 클라우드 백업에 기본 DailyBackup 클라우드 정책을 사용하지 않으려면 자체 정책을 생성할 수 있습니다.

단계

1. 보호 > 개요 > 로컬 정책 설정 * 을 클릭하고 * 보호 정책 * 을 선택합니다.
2. 추가 * 를 클릭하고 새 정책 세부 정보를 입력합니다.
3. Policy Type * 섹션에서 * Back to Cloud * 를 선택하여 클라우드 정책을 생성하고 있음을 나타냅니다.
4. 저장 * 을 클릭합니다.

볼륨 * 페이지에서 백업을 생성합니다

한 번에 여러 볼륨에 대한 클라우드 백업을 선택하여 생성하거나 사용자 지정 보호 정책을 사용하려는 경우 System Manager * Volumes * 페이지를 사용할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭합니다.
2. 클라우드에 백업할 볼륨을 선택하고 * 보호 * 를 클릭합니다.
3. 볼륨 보호 * 창에서 * 추가 옵션 * 을 클릭합니다.
4. 정책을 선택합니다.

   기본 정책, DailyBackup 또는 직접 생성한 사용자 지정 클라우드 정책을 선택할 수 있습니다.

5. 클라우드 오브젝트 저장소를 선택합니다.
6. 저장 * 을 클릭합니다.

클라우드에서 복원

System Manager를 사용하여 클라우드 스토리지에서 소스 클러스터의 다른 볼륨으로 백업된 데이터를 복원할 수 있습니다.

> ONTAP 9.16.1 이상을 사용 중이고 SnapMirror 클라우드 단일 파일 복원을 FlexGroup 볼륨으로 수행하는 경우 FlexGroup 볼륨의 새 디렉토리로만 파일을 복원해야 하며 세부 데이터는 타겟 FlexGroup 볼륨에서 로 설정해야 합니다. `advanced` 옵션 설정에 대한 자세한 `-granular-data advanced` 내용은 을 "파일 데이터를 재배포하여 ONTAP FlexGroup 볼륨의 균형을 조정합니다 "참조하십시오.

단계

1. SnapMirror-to-Cloud 관계의 소스 클러스터에서 * 스토리지 > 볼륨 * 을 클릭합니다.
2. 복원할 볼륨을 선택합니다.
3. Back Up to Cloud * 탭을 선택합니다.
4. 복원할 소스 볼륨 옆에 있는 을 ⋮ 클릭하여 메뉴를 표시하고 * Restore * 를 선택합니다.

5. 소스 * 에서 스토리지 VM을 선택한 다음 데이터를 복원할 볼륨의 이름을 입력합니다.
6. 대상 * 에서 복원할 스냅샷을 선택합니다.
7. 저장 * 을 클릭합니다.

SnapMirror 클라우드 관계를 삭제합니다

System Manager를 사용하여 클라우드 관계를 삭제할 수 있습니다.

단계

1. 스토리지 > 볼륨 * 을 클릭하고 삭제할 볼륨을 선택합니다.
2. 소스 볼륨 옆에 있는 을 ⋮ 클릭하고 * Delete * 를 선택합니다.
3. 클라우드 오브젝트 저장소 끝점을 삭제하려면 * 클라우드 오브젝트 저장소 끝점 삭제(선택 사항) * 를 선택합니다.
4. 삭제 * 를 클릭합니다.

클라우드 오브젝트 저장소를 제거합니다

클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부가 아닌 경우 System Manager를 사용하여 클라우드 오브젝트 저장소를 제거할 수 있습니다. 클라우드 오브젝트 저장소가 클라우드 백업 관계의 일부인 경우 삭제할 수 없습니다.

단계

1. 보호 > 개요 > 클라우드 오브젝트 저장소 * 를 클릭합니다.
2. 삭제하려는 개체 저장소를 선택하고 를 ⋮ 클릭한 다음 * 삭제 * 를 선택합니다.

NetApp Backup and Recovery를 사용하여 데이터 백업

ONTAP 9.9.1부터 NetApp 백업 및 복구 서비스를 사용하여 System Manager에서 클라우드의 데이터를 백업할 수 있습니다.

백업 및 복구는 FlexVol 읽기-쓰기 볼륨과 데이터 보호(DP) 볼륨을 지원합니다. ONTAP 9.12.1부터 백업 및 복구는 FlexGroup 볼륨과 SnapLock 볼륨을 지원합니다.

자세히 알아보세요 "NetApp 백업 및 복구" .

시작하기 전에

NetApp 콘솔에서 계정을 설정하려면 다음 절차를 수행해야 합니다. 서비스 계정의 경우 "계정 관리자" 역할을 만들어야 합니다. (다른 서비스 계정 역할에는 시스템 관리자에서 연결을 설정하는 데 필요한 권한이 없습니다.)

1. "NetApp 콘솔에서 계정 만들기" .
2. "NetApp 콘솔에서 콘솔 에이전트 만들기"다음 클라우드 공급자 중 하나와 함께:
   - Microsoft Azure를 참조하십시오
   - AWS(Amazon Web Services)
   - Google Cloud Platform(GCP)
   - StorageGRID(ONTAP 9.10.1)

ONTAP 9.10.1부터 NetApp 콘솔이 온프레미스에 배포된 경우에만 StorageGRID 클라우드 백업 공급자로 선택할 수 있습니다. 콘솔 에이전트는 온프레미스에 설치해야 하며 NetApp 콘솔 SaaS(Software-as-a-Service) 애플리케이션을 통해 사용할 수 있어야 합니다.

3. "NetApp 콘솔에서 NetApp 백업 및 복구 구독"(적절한 라이센스가 필요합니다).
4. "NetApp 콘솔을 사용하여 액세스 키와 비밀 키 생성" .

NetApp 콘솔에 클러스터 등록

콘솔이나 시스템 관리자를 사용하여 NetApp 콘솔에 클러스터를 등록할 수 있습니다.

단계

1. System Manager에서 * 보호 개요 * 로 이동합니다.
2. * NetApp 백업 및 복구*에서 다음 세부 정보를 제공합니다.
   - 클라이언트 ID입니다
   - 클라이언트 암호 키입니다
3. Register and Continue * 를 선택합니다.

NetApp 백업 및 복구 활성화

클러스터가 NetApp 콘솔에 등록된 후 NetApp 백업 및 복구를 활성화하고 클라우드에 대한 첫 번째 백업을 시작해야 합니다.

단계

1. System Manager에서 * 보호 > 개요 * 를 선택한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 클라이언트 ID * 및 * 클라이언트 암호 * 를 입력합니다.

ONTAP 9.10.1부터 * 클라우드 사용 비용에 대해 자세히 알아보기 * 를 선택하여 클라우드 사용 비용에 대해 알아볼 수 있습니다.

3. 연결 및 Cloud Backup Service 활성화 * 를 선택합니다.
4. * NetApp 백업 및 복구 활성화* 페이지에서 선택한 공급자에 따라 다음 세부 정보를 제공합니다.

이 클라우드 공급자의 경우…	다음 데이터를 입력하십시오…
Azure를 지원합니다	• Azure 구독 ID입니다 • 지역 • 리소스 그룹 이름(기존 또는 신규)
설치하고	• AWS 계정 ID입니다 • 액세스 키 • 비밀 키 • 지역

Google Cloud Project(GCP)	• Google Cloud 프로젝트 이름 • Google Cloud Access 키 • Google Cloud 비밀 키 • 지역
StorageGRID (ONTAP 9.10.1 이상, NetApp 콘솔의 온프레미스 배포에만 해당)	• 서버 • SG 액세스 키 • SG 비밀 키

5. 보호 정책 * 선택:
   - * 기존 정책 *: 기존 정책을 선택합니다.
   - * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.

     ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.

     Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

     Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

     - 볼륨이 아카이빙된 후 경과한 일 수입니다.
     - 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정하십시오.
     - AWS의 경우 아카이브 스토리지 클래스를 선택합니다.
6. 백업할 볼륨을 선택합니다.
7. 저장 * 을 선택합니다.

NetApp 백업 및 복구에 사용되는 보호 정책 편집

NetApp Backup and Recovery에서 사용되는 보호 정책을 변경할 수 있습니다.

단계

1. System Manager에서 * 보호 > 개요 * 를 선택한 다음 * Cloud Backup Service * 섹션으로 스크롤합니다.
2. 을 선택한 다음 * 편집 * 을 선택합니다.
3. 보호 정책 * 선택:
   - * 기존 정책 *: 기존 정책을 선택합니다.
   - * 새 정책 *: 이름을 지정하고 전송 일정을 설정합니다.

     ONTAP 9.10.1부터 Azure 또는 AWS로 아카이빙할 것인지 여부를 지정할 수 있습니다.

     Azure 또는 AWS로 볼륨에 대한 아카이브를 활성화하면 아카이브를 비활성화할 수 없습니다.

Azure 또는 AWS에 대해 아카이브를 설정하는 경우 다음을 지정합니다.

- 볼륨이 아카이빙된 후 경과한 일 수입니다.
- 아카이브에 보존할 백업 수입니다. 최신 백업까지 보관하려면 "0"(영)을 지정하십시오.
- AWS의 경우 아카이브 스토리지 클래스를 선택합니다.

4. 저장 * 을 선택합니다.

클라우드에서 새 볼륨 또는 **LUN** 보호

새 볼륨 또는 LUN을 생성할 때 볼륨 또는 LUN에 대해 클라우드에 백업할 수 있도록 SnapMirror 보호 관계를 설정할 수 있습니다.

시작하기 전에

- SnapMirror 라이센스가 있어야 합니다.
- 인터클러스터 LIF를 구성해야 합니다.
- NTP를 구성해야 합니다.
- 클러스터에서 ONTAP 9.9.1 이상을 실행해야 함

이 작업에 대해

다음과 같은 클러스터 구성에서는 클라우드에서 새 볼륨 또는 LUN을 보호할 수 없습니다.

- 클러스터가 MetroCluster 환경에 있을 수 없습니다.
- SVM-DR은 지원되지 않습니다.
- FlexGroup 볼륨은 NetApp Backup and Recovery를 사용하여 백업할 수 없습니다.

단계

1. 볼륨 또는 LUN을 프로비저닝할 때 System Manager의 * 보호 * 페이지에서 * SnapMirror 사용(로컬 또는 원격) * 확인란을 선택합니다.
2. 백업 및 복구 정책 유형을 선택합니다.
3. 백업 및 복구가 활성화되어 있지 않으면 * NetApp 백업 및 복구를 사용하여 백업 활성화*를 선택합니다.

클라우드의 기존 볼륨 또는 **LUN** 보호

기존 볼륨 및 LUN에 대해 SnapMirror 보호 관계를 설정할 수 있습니다.

단계

1. 기존 볼륨 또는 LUN을 선택하고 * Protect * 를 선택합니다.
2. 볼륨 보호 페이지에서 보호 정책에 대해 * NetApp Backup and Recovery를 사용하여 백업*을 지정합니다.
3. protect * 를 선택합니다.
4. 보호 * 페이지에서 * SnapMirror 활성화(로컬 또는 원격) * 확인란을 선택합니다.
5. * NetApp 백업 및 복구 연결 및 활성화*를 선택합니다.

백업 파일에서 데이터를 복원합니다

데이터 복원, 관계 업데이트, 관계 삭제 등의 백업 관리 작업은 NetApp 콘솔을 사용하는 경우에만 수행할 수 있습니다. . "백업 파일에서 데이터를 복원합니다" 자세한 내용은.

SnapLock 기술을 사용한 아카이브 및 규정 준수

ONTAP SnapLock 에 대해 알아보세요

SnapLock는 WORM 스토리지를 사용하여 규정 및 거버넌스 목적으로 수정되지 않은 형태로 파일을 유지하는 조직을 위한 고성능 규정 준수 솔루션입니다.

SnapLock는 SEC 17a-4(f), HIPAA, FINRA, CFTC, GDPR과 같은 규정을 충족하도록 데이터의 삭제, 변경 또는 이름을 바꾸는 것을 방지합니다. SnapLock를 사용하면 파일을 저장한 후 지정된 보존 기간 또는 무기한으로 삭제할 수 없고 쓸 수 없는 상태로 커밋하는 특수한 용도의 볼륨을 생성할 수 있습니다. SnapLock에서는 CIFS 및 NFS와 같은 표준 개방형 파일 프로토콜을 통해 파일 레벨에서 이 보존을 수행할 수 있습니다. SnapLock에서 지원되는 개방형 파일 프로토콜은 NFS(버전 2, 3 및 4) 및 CIFS(SMB 1.0, 2.0 및 3.0)입니다.

SnapLock를 사용하여 파일 및 스냅샷을 WORM 스토리지에 커밋하고 WORM 보호 데이터의 보존 기간을 설정할 수 있습니다. SnapLock WORM 스토리지는 NetApp 스냅샷 기술을 사용하며 SnapMirror 복제 및 SnapVault 백업을 데이터에 대한 백업 복구 보호를 제공하기 위한 기본 기술로 활용할 수 있습니다. WORM 스토리지에 대해 자세히 "NetApp SnapLock-TR-4526을 사용하여 WORM 스토리지를 준수합니다"알아보십시오.

애플리케이션을 사용하여 NFS 또는 CIFS를 통해 WORM에 파일을 커밋하거나 SnapLock 자동 커밋 기능을 사용하여 파일을 WORM에 자동으로 커밋할 수 있습니다. _WORM 추가 가능 파일_을 사용하여 로그 정보와 같이 점증적으로 기록된 데이터를 보존할 수 있습니다. 자세한 내용은 을 참조하십시오 "볼륨 추가 모드를 사용하여 WORM 추가 가능 파일을 생성합니다".

SnapLock는 대부분의 규정 준수 요구사항을 충족하는 데이터 보호 방법을 지원합니다.

- SnapVault용 SnapLock를 사용하여 보조 스토리지에서 WORM으로 스냅샷을 보호할 수 있습니다. 을 "WORM에 스냅샷 커밋"참조하십시오.
- SnapMirror를 사용하여 재해 복구를 위해 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 을 참조하십시오 "WORM 파일 미러링".

SnapLock 은 ONTAP 의 라이선스 기반 기능입니다. 단일 라이선스를 통해 엄격한 규정 준수 모드에서 SnapLock 사용하여 SEC 규칙 17a-4(f)와 같은 외부 의무를 충족하고, 느슨한 엔터프라이즈 모드에서 디지털 자산 보호를 위한 내부적으로 의무화된 규정을 충족할 수 있습니다. SnapLock 라이센스는 다음의 일부입니다. "ONTAP 1 을 참조하십시오" 소프트웨어 제품군.

SnapLock는 모든 AFF 및 FAS 시스템과 ONTAP Select에서 지원됩니다. SnapLock는 소프트웨어 전용 솔루션이 아니라 통합 하드웨어 및 소프트웨어 솔루션입니다. 이러한 차이는 통합 하드웨어 및 소프트웨어 솔루션이 필요한 SEC 17a-4(f)와 같은 엄격한 WORM 규정에서 중요합니다. 자세한 내용은 을 "전자 저장 매체 사용에 대한 중개 딜러에 대한 SEC 지침"참조하십시오.

SnapLock로 할 수 있는 일

SnapLock를 구성한 후 다음 작업을 수행할 수 있습니다.

- "WORM에 파일을 커밋합니다"

- "보조 스토리지를 위해 WORM에 스냅샷을 커밋합니다"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "법적 증거 자료 보관 을 사용하여 소송 중에 WORM 파일을 보관하십시오"
- "권한 있는 삭제 기능을 사용하여 WORM 파일을 삭제합니다"
- "파일 보존 기간을 설정합니다"
- "SnapLock 볼륨을 이동합니다"
- "랜섬웨어 공격으로부터 보호하기 위해 스냅샷을 잠급니다"
- "감사 로그와 함께 SnapLock 사용을 검토합니다"
- "SnapLock API 사용"

SnapLock 규정 준수 및 엔터프라이즈 모드

SnapLock 규정 준수 및 엔터프라이즈 모드는 각 모드에서 WORM 파일을 보호하는 수준에 따라 크게 다릅니다.

SnapLock 모드	보호 수준	WORM 파일 보존 중 삭제
준수 모드	디스크 레벨에서 복구	삭제할 수 없습니다
엔터프라이즈 모드	파일 레벨에서	감사된 "특권 삭제" 절차를 사용하여 규정 준수 관리자가 삭제할 수 있습니다.

보존 기간이 경과하면 더 이상 필요하지 않은 파일을 삭제할 책임이 있습니다. 파일이 규정 준수 모드이든 엔터프라이즈 모드이든 WORM에 커밋되면 보존 기간이 만료된 후에도 수정할 수 없습니다.

보존 기간 중 또는 이후에 WORM 파일을 이동할 수 없습니다. WORM 파일을 복사할 수 있지만 WORM 특성이 유지되지 않습니다.

다음 표에는 SnapLock 규정 준수 및 엔터프라이즈 모드에서 지원하는 기능의 차이가 나와 있습니다.

제공합니다	SnapLock 규정 준수	SnapLock 엔터프라이즈
권한 있는 삭제를 사용하여 파일을 활성화 및 삭제합니다	아니요	예
디스크를 다시 초기화합니다	아니요	예
보존 기간 동안 SnapLock 애그리게이트 및 볼륨을 제거합니다	아니요	예. SnapLock 감사 로그 볼륨을 제외하고 가능합니다
Aggregate 또는 볼륨의 이름을 바꿉니다	아니요	예
비NetApp 디스크를 사용합니다	아니요	아니요

감사 로깅을 위해 SnapLock 볼륨을 사용합니다	예	예, ONTAP 9.5부터 시작합니다

SnapLock에서 지원 및 지원되지 않는 기능

다음 표에는 SnapLock 규정 준수 모드, SnapLock 엔터프라이즈 모드 또는 둘 다에서 지원되는 기능이 나와 있습니다.

피처	SnapLock 규정 준수 지원	SnapLock Enterprise에서 지원됩니다
일관성 그룹	아니요	아니요
암호화된 볼륨	네, 자세히 알아보세요 암호화 및 SnapLock .	네, 자세히 알아보세요 암호화 및 SnapLock .
SnapLock 애그리게이트에서 Fabric으로 구성	아니요	예, ONTAP 9.8부터 시작합니다. 에 대해 자세히 알아보십시오 FabricPool on SnapLock 엔터프라이즈 애그리게이트.
Flash Pool 애그리게이트로 전환 가능	예.	예.
플랙스클론	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.	SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.
FlexGroup 볼륨	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].	예, ONTAP 9.11.1부터 시작합니다. 에 대해 자세히 알아보십시오 [flexgroup].
LUN을 클릭합니다	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.	아니요 에 대해 자세히 알아보십시오 LUN 지원 SnapLock와 함께.
MetroCluster 구성	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.	예, ONTAP 9.3부터 시작합니다. 에 대해 자세히 알아보십시오 MetroCluster 지원.
MAV(Multi-admin verification)	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.	예, ONTAP 9.13.1. 에 대해 자세히 알아보십시오 MAV 지원.
산	아니요	아니요
단일 파일 SnapRestore	아니요	예
SnapMirror 활성 동기화	아니요	아니요

SnapRestore	아니요	예
SMTape	아니요	아니요
SnapMirror Synchronous	아니요	아니요
SSD를 지원합니다	예.	예.
스토리지 효율성 기능	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.	예, ONTAP 9.9.1부터 시작합니다. 에 대해 자세히 알아보십시오 스토리지 효율성 지원.

FabricPool on SnapLock 엔터프라이즈 애그리게이트

FabricPool은 ONTAP 9.8부터 SnapLock 엔터프라이즈 애그리게이트에서 지원됩니다. 그러나 클라우드 관리자가 해당 데이터를 삭제할 수 있으므로 FabricPool 데이터를 퍼블릭 또는 프라이빗 클라우드로 계층화하면 SnapLock에서 더 이상 보호되지 않는다는 사실을 NetApp 어카운트 팀이 설명하는 제품 분산 요청을 개설해야 합니다.

FabricPool에서 퍼블릭 또는 프라이빗 클라우드로 계층화하는 데이터는 클라우드 관리자가 삭제할 수 있으므로 SnapLock에서 더 이상 보호되지 않습니다.

FlexGroup 볼륨

SnapLock는 ONTAP 9.11.1부터 FlexGroup 볼륨을 지원하지만 다음 기능은 지원되지 않습니다.

- 법적 증거 자료 보관
- 이벤트 기반 보존
- SnapLock for SnapVault(ONTAP 9.12.1부터 지원됨)

또한 다음과 같은 행동을 인지해야 합니다.

- FlexGroup 볼륨의 VCC(Volume Compliance Clock)는 루트 구성 요소 VCC에 의해 결정됩니다. 모든 비루트 구성 요소들은 VCC를 루트 VCC와 긴밀히 동기화하게 됩니다.
- SnapLock 구성 속성은 FlexGroup 전체에 대해서만 설정됩니다. 개별 구성 요소마다 기본 보존 시간 및 자동 커밋 기간과 같은 서로 다른 구성 속성을 사용할 수 없습니다.

LUN 지원

LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

MetroCluster 지원

MetroCluster 구성에서 SnapLock 지원은 SnapLock 규정 준수 모드와 SnapLock 엔터프라이즈 모드 간에 다릅니다.

SnapLock 규정 준수

- ONTAP 9.3부터 SnapLock 규정 준수는 미러링되지 않은 MetroCluster 애그리게이트에서 지원됩니다.
- ONTAP 9.3부터 SnapLock 규정 준수는 미러링된 애그리게이트에서 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 지원됩니다.
- MetroCluster를 사용하여 SVM별 SnapLock 구성을 운영 사이트 및 2차 사이트에 복제할 수 있습니다.

SnapLock 엔터프라이즈

- SnapLock Enterprise 집계가 지원됩니다.
- ONTAP 9.3부터는 권한이 있는 삭제 기능이 있는 SnapLock 엔터프라이즈 애그리게이트가 지원됩니다.
- MetroCluster를 사용하여 SVM별 SnapLock 구성을 두 사이트 모두에 복제할 수 있습니다.

MetroCluster 구성 및 규정 준수 클럭

MetroCluster 구성에는 VCC(Volume Compliance Clock)와 SCC(System Compliance Clock)라는 두 가지 준수 클록 메커니즘이 사용됩니다. VCC 및 SCC는 모든 SnapLock 구성에 사용할 수 있습니다. 노드에 새 볼륨을 생성할 때 해당 노드에 있는 SCC의 현재 값으로 VCC가 초기화됩니다. 볼륨이 생성된 후에는 항상 VCC를 통해 볼륨 및 파일 보존 시간을 추적합니다.

볼륨이 다른 사이트에 복제되면 해당 VCC도 복제됩니다. 예를 들어, 사이트 A에서 사이트 B로 볼륨 전환이 발생하면 사이트 A의 SCC가 사이트 A가 오프라인이 되면 사이트 B에서 VCC가 계속 업데이트됩니다.

사이트 A가 다시 온라인 상태가 되고 볼륨 스위치백을 수행하면 볼륨의 VCC가 계속 업데이트되는 동안 사이트 A SCC 클록이 다시 시작됩니다. 스위치오버 및 스위치백 작업과 관계없이 VCC가 지속적으로 업데이트되기 때문에 파일 보존 시간은 SCC 클럭에 의존하지 않고 늘어나지 않습니다.

MAV(Multi-admin verification) 지원

ONTAP 9.13.1 부터는 클러스터 관리자가 일부 SnapLock 작업을 실행하기 전에 쿼럼을 승인해야 하는 클러스터에서 다중 관리 검증을 명시적으로 활성화할 수 있습니다. MAV가 활성화되면 기본 보존 시간, 최소 보존 시간, 최대 보존 시간, 볼륨 추가 모드, 자동 커밋 기간 및 권한 삭제 등의 SnapLock 볼륨 속성에 쿼럼이 승인되어야 합니다. 에 대해 자세히 알아보십시오 "5일".

스토리지 효율성

ONTAP 9.9.1부터 SnapLock은 데이터 컴팩션, 볼륨 간 중복제거, SnapLock 볼륨 및 애그리게이트를 위한 적응형 압축과 같은 스토리지 효율성 기능을 지원합니다. 스토리지 효율성에 대한 자세한 내용은 를 참조하십시오 "ONTAP 스토리지 효율성 개요".

암호화

ONTAP는 스토리지 미디어의 용도 변경, 반환, 잘못된 위치 변경 또는 도난 시 유휴 데이터를 읽을 수 없도록 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공합니다.

- 법적 고지 사항: * NetApp은 자체 암호화 드라이브 또는 볼륨의 SnapLock 보호 WORM 파일이 인증 키가 손실되거나 실패한 인증 시도 횟수가 지정된 제한을 초과하여 드라이브가 영구적으로 잠기는 경우 이를 복구할 수 있다고 보장할 수 없습니다. 인증 실패에 대한 책임은 사용자에게 있습니다.

암호화된 볼륨은 SnapLock 집계에서 지원됩니다.

7-Mode 전환

7-Mode 전환 도구의 CBT(Copy-Based Transition) 기능을 사용하여 SnapLock 볼륨을 7-Mode에서 ONTAP로 마이그레이션할 수 있습니다. 대상 볼륨의 SnapLock 모드인 Compliance 또는 Enterprise는 소스 볼륨의 SnapLock 모드와 일치해야 합니다. CFT(Copy-Free Transition)를 사용하여 SnapLock 볼륨을 마이그레이션할 수는 없습니다.

SnapLock를 구성합니다

ONTAP SnapLock 구성에 대해 알아보세요

SnapLock를 사용하기 전에 "SnapLock 라이센스를 설치합니다"SnapLock 볼륨으로 애그리게이트를 호스팅하는 각 노드에 대해 등의 다양한 작업을 완료하여 SnapLock를 구성하고"규정 준수 시계", 를 초기화하며, ONTAP 9.10.1 이전의 ONTAP 릴리즈를 실행하는 클러스터에 대해 SnapLock 애그리게이트를 생성할 "SnapLock 볼륨을 생성하고 마운트합니다"수 있어야 합니다.

ONTAP 규정 준수 시계 초기화

SnapLock는 _ volume Compliance Clock _ 을(를) 사용하여 WORM 파일의 보존 기간을 변경할 수 있는 변조를 방지합니다. 먼저 SnapLock 애그리게이트를 호스팅하는 각 노드에서 _SYSTEM ComplianceClock_을 초기화해야 합니다.

ONTAP 9.14.1부터 SnapLock 볼륨이 없거나 스냅샷 잠금이 설정된 볼륨이 없는 경우 시스템 규정 준수 클록을 초기화하거나 다시 초기화할 수 있습니다. 시스템 관리자는 재초기화 기능을 사용하여 시스템 규정 준수 클록이 잘못 초기화되었을 수 있는 경우에 시스템 규정 준수 클록을 재설정하거나 시스템의 클럭 편차를 수정할 수 있습니다. ONTAP 9.13.1 이하 릴리즈에서는 노드에서 규정 준수 클록을 초기화한 후 다시 초기화할 수 없습니다.

시작하기 전에

규정 준수 클록을 다시 초기화하려면 다음을 수행합니다.

- 클러스터의 모든 노드가 정상 상태여야 합니다.
- 모든 볼륨이 온라인 상태여야 합니다.
- 복구 큐를 표시할 볼륨이 없습니다.
- SnapLock 볼륨이 없을 수 있습니다.
- 스냅샷 잠금이 활성화된 볼륨이 없을 수 있습니다.

규정 준수 시계 초기화를 위한 일반 요구 사항:

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다"..

이 작업에 대해

시스템 Compliance Clock의 시간은 _ VOLUME Compliance Clock _ 에 의해 상속되며, 이 시간 중 후자는 볼륨에 있는 WORM 파일의 보존 기간을 제어합니다. 볼륨 준수 시계는 새 SnapLock 볼륨을 생성할 때 자동으로 초기화됩니다.

시스템 규정 준수 클럭의 초기 설정은 현재 하드웨어 시스템 클록을 기반으로 합니다. 따라서 각 노드에서 시스템 규정 준수 클록을 초기화하기 전에 시스템 시간과 시간대가 올바른지 확인해야 합니다. 노드에서 시스템 규정 준수 클록을 초기화하고 나면 SnapLock 볼륨 또는 잠금이 설정된 볼륨이 존재할 때 이를 다시 초기화할 수 없습니다.

단계

ONTAP CLI를 사용하여 규정 준수 클록을 초기화하거나 ONTAP 9.12.1부터 System Manager를 사용하여 규정 준수 클록을 초기화할 수 있습니다.

시스템 관리자

1. 클러스터 > 개요 * 로 이동합니다.
2. 노드 * 섹션에서 * SnapLock 준수 클럭 초기화 * 를 클릭합니다.
3. 규정 준수 시계 * 열을 표시하고 규정 준수 시계가 초기화되었는지 확인하려면 * 클러스터 > 개요 > 노드 * 섹션에서 * 표시/숨기기 * 를 클릭하고 * SnapLock 규정 준수 시계 * 를 선택합니다.

CLI를 참조하십시오

1. 시스템 규정 준수 클록을 초기화합니다.

   `snaplock compliance-clock initialize -node node_name`

   다음 명령을 실행하면 시스템 Compliance Clock On이 초기화됩니다 `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock initialize` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 메시지가 표시되면 시스템 클록이 올바른지, 규정 준수 클록을 초기화할지 확인합니다.

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. SnapLock 애그리게이트를 호스팅하는 각 노드에 대해 이 절차를 반복합니다.

NTP 구성 시스템에 대해 규정 준수 클럭 재동기화를 설정합니다

NTP 서버가 구성되면 SnapLock Compliance 시계 동기화 기능을 활성화할 수 있습니다.

시작하기 전에

- 이 기능은 고급 권한 수준에서만 사용할 수 있습니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- "노드에 SnapLock 라이센스가 설치되어 있어야 합니다"..
- 이 기능은 Cloud Volumes ONTAP, ONTAP Select 및 VIM 플랫폼에서만 사용할 수 있습니다.

이 작업에 대해

SnapLock 보안 클럭 데몬이 임계값을 초과하는 편중을 감지하면 ONTAP는 시스템 시간을 사용하여 시스템 및 볼륨 규정 준수 클럭을 모두 재설정합니다. 24시간이 기울기 임계값으로 설정됩니다. 즉, 편중이 하루 이상 지난 경우에만 시스템 규정 준수 클록이 시스템 클록과 동기화됩니다.

SnapLock 보안 클록 데몬은 편중을 감지하고 규정 준수 클럭을 시스템 시간으로 변경합니다. 시스템 시간이 NTP 시간과 동기화되는 경우에만 규정 준수 클록이 시스템 시간과 동기화되기 때문에 규정 준수 클록이 시스템 시간과 동기화되도록 시스템 시간을 수정하려는 시도가 실패합니다.

단계

1. NTP 서버가 구성된 경우 SnapLock Compliance 시계 동기화 기능을 활성화합니다.

   `snaplock compliance-clock ntp`

   다음 명령은 시스템 규정 준수 시계 동기화 기능을 활성화합니다.

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock ntp modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 메시지가 표시되면 구성된 NTP 서버가 신뢰할 수 있고 통신 채널이 보안 상태인지 확인합니다.
3. 기능이 활성화되어 있는지 확인합니다.

   `snaplock compliance-clock ntp show`

   다음 명령은 시스템 규정 준수 시계 동기화 기능이 활성화되어 있는지 확인합니다.

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   에 대한 자세한 내용은 `snaplock compliance-clock ntp show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapLock 집계 생성

볼륨 '-snaplock-type' 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전 릴리스의 경우 별도의 SnapLock 애그리게이트를 만들어야 합니다. ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을 사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 노드의 SnapLock"라이센스를 설치해야 합니다"입니다. 이 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오 "있습니다.
- "노드의 규정 준수 클록을 초기화해야 합니다"..
- 디스크를 "루트", "루트", "다토1" 및 "다토2"로 분할한 경우 스페어 디스크를 사용할 수 있는지 확인해야 합니다.

업그레이드 고려 사항

ONTAP 9.10.1로 업그레이드할 때 기존 SnapLock 및 비 SnapLock 애그리게이트는 SnapLock 볼륨과 비 SnapLock 볼륨 모두를 지원하도록 업그레이드되지만 기존 SnapLock 볼륨 특성은 자동으로 업데이트되지 않습니다. 예를 들어, 데이터 컴팩션, 볼륨 간 중복제거, 볼륨 간 백그라운드 중복제거 필드는 변경되지 않습니다. 기존 애그리게이트에 생성된 새로운 SnapLock 볼륨의 기본값이 비 SnapLock 볼륨과 같고, 새 볼륨 및 애그리게이트의 기본 값은 플랫폼에 따라 다릅니다.

되돌리기 고려 사항

9.10.1 이전의 ONTAP 버전으로 복구해야 하는 경우 모든 SnapLock 규정 준수, SnapLock 엔터프라이즈 및 SnapLock 볼륨을 고유한 SnapLock 애그리게이트로 이동해야 합니다.

이 작업에 대해

- SyncMirror 옵션을 사용하여 준수 애그리게이트를 생성할 수 없습니다.
- MetroCluster 구성에서 미러링된 Compliance Aggregate는 SnapLock 감사 로그 볼륨을 호스팅하는 데 사용되는 경우에만 생성할 수 있습니다.

> MetroCluster 구성에서는 SnapLock Enterprise가 미러링된 Aggregate 및 미러링되지 않은 Aggregate에서 지원됩니다. SnapLock 규정 준수는 미러링되지 않은 애그리게이트에서만 지원됩니다.

단계

1. SnapLock 애그리게이트 생성:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

다음 명령을 실행하면 node1에 3개의 디스크가 있는 "aggr1"이라는 SnapLock "Compliance" Aggregate가 생성됩니다.

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

에 대한 자세한 내용은 `storage aggregate create` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SnapLock 볼륨 생성 및 마운트

WORM 상태로 커밋하려는 파일 또는 스냅샷에 대한 SnapLock 볼륨을 생성해야 합니다. ONTAP 9.10.1.1부터 애그리게이트 유형에 관계없이 생성한 모든 볼륨은 기본적으로 비 SnapLock 볼륨으로 생성됩니다. SnapLock 유형으로 Compliance 또는 Enterprise를 지정하여 SnapLock 볼륨을 명시적으로 생성하려면 옵션을 사용해야 `-snaplock-type` 합니다. 기본적으로 SnapLock 유형은 로 `non-snaplock`설정됩니다.

시작하기 전에

- SnapLock 애그리게이트는 온라인 상태여야 합니다.
- 해야 "SnapLock 라이센스가 설치되어 있는지 확인합니다"합니다. 노드에 SnapLock 라이센스가 설치되어 있지 않으면 반드시 설치해야 "설치합니다"합니다. 이 라이센스는 에 "ONTAP 1 을 참조하십시오"포함되어 있습니다. ONTAP One 이전에는 SnapLock 라이센스가 보안 및 규정 준수 번들에 포함되어 있었습니다. 보안 및 규정 준수 번들은 더 이상 제공되지 않지만 여전히 유효합니다. 현재는 필요하지 않지만 기존 고객은 선택할 수 "ONTAP One으로 업그레이드하십시오"있습니다.
- "노드의 규정 준수 클록을 초기화해야 합니다"..

이 작업에 대해

적절한 SnapLock 권한을 사용하여 언제든지 엔터프라이즈 볼륨을 삭제하거나 이름을 바꿀 수 있습니다. 보존 기간이 경과하기 전에는 Compliance 볼륨을 폐기할 수 없습니다. Compliance 볼륨의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다. 클론 볼륨은 상위 볼륨과 동일한 SnapLock 유형이 됩니다.

> LUN은 SnapLock 볼륨에서 지원되지 않습니다. LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 이 작업을 수행합니다.

시스템 관리자

ONTAP 9.12.1부터 시스템 관리자를 사용하여 SnapLock 볼륨을 생성할 수 있습니다.

단계

1. Storage > Volumes * 로 이동한 다음 * Add * 를 클릭합니다.
2. 볼륨 추가 * 창에서 * 추가 옵션 * 을 클릭합니다.
3. 볼륨의 이름과 크기를 포함하여 새 볼륨 정보를 입력합니다.
4. SnapLock 사용 * 을 선택하고 SnapLock 유형(준수 또는 엔터프라이즈)을 선택합니다.
5. 자동 커밋 파일 * 섹션에서 * 수정 * 을 선택하고 파일이 자동으로 커밋되기 전에 변경되지 않은 상태로 유지되는 시간을 입력합니다. 최소값은 5분이고 최대값은 10년입니다.
6. Data Retention * 섹션에서 최소 및 최대 보존 기간을 선택합니다.
7. 기본 보존 기간을 선택합니다.
8. 저장 * 을 클릭합니다.
9. 볼륨 * 페이지에서 새 볼륨을 선택하여 SnapLock 설정을 확인합니다.

CLI를 참조하십시오

1. SnapLock 볼륨 생성:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

에 대한 자세한 내용은 `volume create` "ONTAP 명령 참조입니다"을 참조하십시오. SnapLock 볼륨에는 , `-atime-update`, , `-is-autobalance-eligible` `-space-mgmt-try-first` 및 `vmalign` 옵션을 사용할 수 없습니다 `-nvfail`.

다음 명령을 실행하면 vs1에 vol1이라는 SnapLock "Compliance" 볼륨이 생성됩니다.

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

SnapLock 볼륨을 마운트합니다

NAS 클라이언트 액세스를 위해 SVM 네임스페이스의 접합 경로에 SnapLock 볼륨을 마운트할 수 있습니다.

시작하기 전에

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

- SnapLock 볼륨은 SVM의 루트 아래에서만 마운트할 수 있습니다.
- SnapLock 볼륨 아래에 일반 볼륨을 마운트할 수 없습니다.

단계

1. SnapLock 볼륨 마운트:

   '* 볼륨 마운트 - vserver_SVM_name_-volume_volume_name_-junction-path_path_*'

   에 대한 자세한 내용은 `volume mount` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 이름이 vol1인 SnapLock 볼륨이 VS1 네임스페이스에서 junction path/sales에 마운트됩니다.

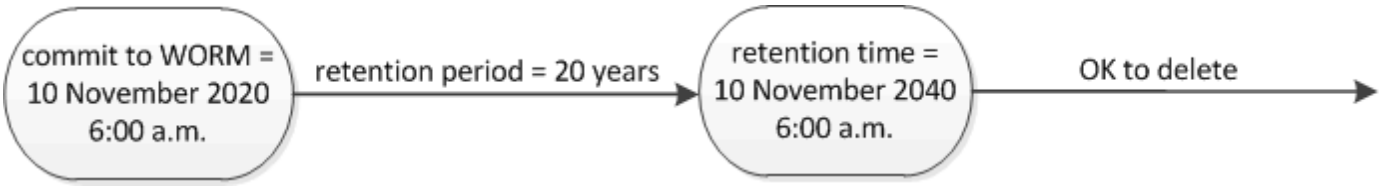
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

ONTAP SnapLock 보존 시간 설정

파일의 보존 시간을 명시적으로 설정하거나 볼륨에 대한 기본 보존 기간을 사용하여 보존 시간을 파생시킬 수 있습니다. 보존 시간을 명시적으로 설정하지 않으면 SnapLock에서는 기본 보존 기간을 사용하여 보존 시간을 계산합니다. 이벤트 후에 파일 보존을 설정할 수도 있습니다.

보존 기간 및 보존 시간에 대해 설명합니다

WORM 파일의 _retention period_는 파일이 WORM 상태로 커밋된 후 보존되어야 하는 시간을 지정합니다. WORM 파일의 _retention time_은 파일을 더 이상 보존할 필요가 없는 시간입니다. 예를 들어, 2020년 11월 10일 오전 6시부터 WORM 상태로 커밋된 파일의 보존 기간은 20년이며, 보존 기간은 2010년 11월 10일 오전 6시입니다



ONTAP 9.10.1부터 최대 10월 26일, 3058까지의 보존 기간 및 최대 100년의 보존 기간을 설정할 수 있습니다. 보존 날짜를 확장하면 이전 정책이 자동으로 변환됩니다. ONTAP 9.9.1 및 이전 릴리즈에서는 기본 보존 기간을 무한으로 설정하지 않으면 지원되는 최대 보존 시간은 1월 19 2071(GMT)입니다.

중요한 복제 고려 사항

1월 19일 2071(GMT) 이후의 보존 날짜를 사용하여 SnapLock 소스 볼륨과 SnapMirror 관계를 설정할 때 타겟 클러스터에서 ONTAP 9.10.1 이상이 실행 중이어야 하며, 그렇지 않으면 SnapMirror 전송이 실패합니다.

중요한 되돌리기 고려 사항

ONTAP 보존 기간이 "2071년 1월 19일 오전 8시 44분 7초" 이후인 파일이 있는 경우 클러스터를 ONTAP 9.10.1에서 이전 ONTAP 버전으로 되돌리는 것을 방지합니다.

보존 기간 이해

SnapLock 규정 준수 또는 엔터프라이즈 볼륨의 보존 기간은 4가지입니다.

- 최소 보존 기간(min), 기본값 0
- 최대 보존 기간(최대)(기본값: 30년

- ONTAP 9.10.1부터 준수 모드 및 엔터프라이즈 모드 모두에 대해 기본 보존 기간(기본값: "in")입니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 기본 보존 기간이 모드에 따라 다릅니다.
  - 준수 모드의 경우 기본값은 'Max'입니다.
  - 엔터프라이즈 모드의 경우 기본값은 'in'입니다.
- 지정되지 않은 보존 기간.

> ⓘ ONTAP 9.10.1 이전 릴리스에서는 규정 준수 모드 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 해당 파일은 30년 동안 보존됩니다. 이 변경 사항은 실행 취소할 수 없습니다. 마찬가지로 ONTAP 9.10.1 이상에서는 엔터프라이즈 모드 파일을 WORM 상태로 커밋하기 전에 보존 시간을 명시적으로 설정하지 않고 기본값을 수정하지 않으면 해당 파일은 0년 동안 보존되거나 사실상 전혀 보존되지 않습니다.

ONTAP 9.8부터 볼륨에 있는 파일의 보존 기간을 '지정 안 됨'으로 설정하여 절대 보존 시간을 설정할 때까지 파일을 보존할 수 있습니다. 새 절대 보존 시간이 이전에 설정한 절대 시간보다 이후인 경우 절대 보존 시간을 지정하지 않은 보존으로 설정하고 다시 절대 보존으로 설정할 수 있습니다.

ONTAP 9.12.1부터 보존 기간이 설정된 WORM 파일 `unspecified` SnapLock 볼륨에 대해 구성된 최소 보존 기간으로 보존 기간을 설정해야 합니다. 에서 파일 보존 기간을 변경하는 경우 `unspecified` 지정된 새 보존 시간은 파일에 이미 설정된 최소 보존 시간보다 커야 합니다.

기본 보존 기간을 설정합니다

'volume SnapLock modify' 명령을 사용하여 SnapLock 볼륨의 파일에 대한 기본 보존 기간을 설정할 수 있습니다.

시작하기 전에

SnapLock 볼륨이 온라인 상태여야 합니다.

이 작업에 대해

다음 표에는 기본 보존 기간 옵션에 사용할 수 있는 값이 나와 있습니다.

> ⓘ 기본 보존 기간은 최소 보존 기간보다 크거나 같고 최대 보존 기간보다 작거나 같아야 합니다(<=).

값	단위	참고
0-65535	초	
0-24	시간	
0-365일	일	
0-12로 설정합니다	개월	
0-100입니다	년	ONTAP 9.10.1부터. 이전 ONTAP 릴리스의 경우 값은 0-70입니다.
최대	-	최대 보존 기간을 사용합니다.

값	단위	참고
최소	-	최소 보존 기간을 사용합니다.
무한대	-	파일을 영구적으로 보존합니다.
지정되지 않음	-	절대 보존 기간이 설정될 때까지 파일을 보존합니다.

최대 및 최소 보존 기간의 값과 범위는 해당되지 않는 최대 및 최소 보존 기간을 제외하고 동일합니다. 이 작업에 대한 자세한 내용은 을 참조하십시오 "보존 시간 개요를 설정합니다".

명령을 사용하여 볼륨의 보존 기간 설정을 볼 수 `volume snaplock show` 있습니다. 에 대한 자세한 내용은 `volume snaplock show` "ONTAP 명령 참조입니다"을 참조하십시오.

파일이 WORM 상태로 커밋된 후에는 보존 기간을 늘릴 수 있지만 줄일 수는 없습니다.

단계

1. SnapLock 볼륨에 있는 파일의 기본 보존 기간을 설정합니다.

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-default-retention -period_default_retention_period_-minimum-retention-period_min_retention_period_-maximum-retention -period_max_retention_period_ *'

   에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 예에서는 최소 및 최대 보존 기간이 이전에 수정되지 않은 것으로 가정합니다.

   다음 명령을 실행하면 Compliance 또는 Enterprise 볼륨의 기본 보존 기간이 20일로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 70년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   -retention-period 70years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10년으로 설정됩니다.

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period max -maximum-retention-period 10years
   ```

   다음 명령을 실행하면 엔터프라이즈 볼륨의 기본 보존 기간이 10일로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

다음 명령을 실행하면 Compliance 볼륨의 기본 보존 기간이 무한으로 설정됩니다.

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

파일의 보존 시간을 명시적으로 설정합니다

파일의 마지막 액세스 시간을 수정하여 파일의 보존 시간을 명시적으로 설정할 수 있습니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 마지막 액세스 시간을 수정할 수 있습니다.

이 작업에 대해

파일이 WORM에 커밋된 후에는 보존 시간을 늘릴 수 있지만 줄일 수는 없습니다. 보존 시간은 파일의 atime 필드에 저장됩니다.

> ⓘ 파일의 보존 시간을 명시적으로 '무한'으로 설정할 수는 없습니다. 이 값은 기본 보존 기간을 사용하여 보존 시간을 계산하는 경우에만 사용할 수 있습니다.

단계

1. 적절한 명령 또는 프로그램을 사용하여 보존 시간을 설정할 파일의 마지막 액세스 시간을 수정합니다.

   UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 "document.txt" 파일에서 다음을 수행합니다.

   ```
   touch -a -t 202011210600 document.txt
   ```

   > ⓘ 적합한 명령 또는 프로그램을 사용하여 Windows의 마지막 액세스 시간을 수정할 수 있습니다.

이벤트 후 파일 보존 기간을 설정합니다

ONTAP 9.3부터 EBR(SnapLock_Event Based Retention)_Feature를 사용하여 이벤트 발생 후 파일이 유지되는 기간을 정의할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.

  "SnapLock 관리자 계정을 만듭니다"

- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

이벤트 보존 정책 _ 은(는) 이벤트가 발생한 후 파일의 보존 기간을 정의합니다. 정책은 단일 파일 또는 디렉토리의 모든 파일에 적용할 수 있습니다.

- 파일이 WORM 파일이 아닌 경우 정책에 정의된 보존 기간 동안 WORM 상태로 커밋됩니다.
- 파일이 WORM 파일 또는 WORM 추가 가능 파일인 경우 보존 기간은 정책에 정의된 보존 기간만큼 연장됩니다.

Compliance-mode 또는 Enterprise-mode 볼륨을 사용할 수 있습니다.

EBR 정책은 법적 증거 자료 보관 아래의 파일에 적용할 수 없습니다.

고급 사용법은 를 "NetApp SnapLock를 사용하여 WORM 스토리지 규정 준수"참조하십시오.

* _ EBR을 사용하여 이미 존재하는 WORM 파일의 보존 기간을 연장합니다. _ *
EBR은 기존 WORM 파일의 보존 기간을 연장하려는 경우에 편리합니다. 예를 들어, 직원이 원천징수를 변경한 후 3년 동안 직원 W-4 기록을 수정되지 않은 형태로 유지하는 것이 회사의 정책일 수 있습니다. 다른 회사 정책에서는 직원이 종료된 후 5년 동안 W-4 기록을 보관해야 할 수 있습니다. 이 경우 5년의 보존 기간을 사용하여 EBR 정책을 생성할 수 있습니다. 직원이 종료된 후("이벤트") 직원의 W-4 기록에 EBR 정책을 적용하여 보존 기간이 연장될 수 있습니다. 이는 일반적으로 보존 기간을 수동으로 연장하는 것보다 쉽습니다. 특히 많은 수의 파일이 관련된 경우 더욱 그렇습니다.

단계

1. EBR 정책 생성:

   ```
   snaplock event-retention policy create -vserver SVM_name -name policy_name
   -retention-period retention_period
   ```

   다음 명령은 VS1, 보존 기간 10년을 포함한 EBR 정책 'EMPLOYEE_EXIT'를 생성한다.

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. EBR 정책 적용:

   ```
   snaplock event-retention apply -vserver SVM_name -name policy_name -volume
   volume_name -path path_name
   ```

   다음 명령을 실행하면 VS1 디렉토리에 있는 모든 파일에 VS1 의 EBR 정책 'EMPLOYEE_EXIT'가 적용됩니다.

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

관련 정보

- "SnapLock 이벤트 보존 정책 생성"

- "SnapLock 이벤트 보존 적용"

ONTAP SnapLock 으로 보호되는 감사 로그 생성

ONTAP 9.9.1 이하 버전을 사용하는 경우, 권한 있는 삭제 또는 SnapLock 볼륨 이동을 수행하기 전에 먼저 SnapLock 애그리게이트를 생성한 다음 SnapLock 보호 감사 로그를 생성해야 합니다. 감사 로그는 SnapLock 관리자 계정의 생성 및 삭제, 로그 볼륨 수정, 권한 있는 삭제 활성화 여부, 권한 있는 삭제 작업 및 SnapLock 볼륨 이동 작업을 기록합니다.

ONTAP 9.10.1부터는 SnapLock 애그리게이트를 생성할 수 없습니다. "SnapLock 볼륨을 명시적으로 생성합니다 "SnapLock 형식으로 Compliance 또는 Enterprise를 지정하려면 -SnapLock-type 옵션을 사용해야 합니다.

시작하기 전에

ONTAP 9.9.1 이하 버전을 사용하는 경우 SnapLock 애그리게이트를 생성하려면 클러스터 관리자여야 합니다.

이 작업에 대해

로그 파일 보존 기간이 경과할 때까지 감사 로그를 삭제할 수 없습니다. 보존 기간이 경과한 후에도 감사 로그를 수정할 수 없습니다. 이는 SnapLock 규정 준수 모드와 엔터프라이즈 모드 모두에서 마찬가지입니다.

ONTAP 9.4 이하 버전에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨을 사용할 수 없습니다. SnapLock 준수 볼륨을 사용해야 합니다. ONTAP 9.5 이상에서는 감사 로깅을 위해 SnapLock 엔터프라이즈 볼륨 또는 SnapLock 규정 준수 볼륨을 사용할 수 있습니다. 모든 경우에 감사 로그 볼륨은 교차점 경로 '/snaplock_audit_log'에 마운트되어야 합니다. 다른 볼륨은 이 접합 경로를 사용할 수 없습니다.

SnapLock Audit 로그는 감사 로그 볼륨의 루트 아래의 '/sSnapLock_log' 디렉토리에서 privdel_log'(권한 삭제 작업) 및 'system_log'(기타 모든 것)라는 하위 디렉토리에 있습니다. 감사 로그 파일 이름에는 첫 번째 기록 작업의 타임스탬프가 포함되어 있어 작업이 실행된 대략적인 시간만큼 레코드를 쉽게 검색할 수 있습니다.

- 'SnapLock log file show' 명령을 사용하여 감사 로그 볼륨에서 로그 파일을 볼 수 있습니다.
- 'SnapLock log file archive' 명령을 사용하여 현재 로그 파일을 보관하고 새 로그 파일을 만들 수 있습니다. 이 명령은 별도의 파일에 감사 로그 정보를 기록해야 하는 경우에 유용합니다.

및 `snaplock log file archive` 에 대한 자세한 `snaplock log file show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

데이터 보호 볼륨은 SnapLock 감사 로그 볼륨으로 사용할 수 없습니다.

단계

1. SnapLock Aggregate를 생성합니다.

   SnapLock Aggregate를 생성합니다

2. 감사 로깅을 위해 구성하려는 SVM에서 SnapLock 볼륨을 생성합니다.

   SnapLock 볼륨을 생성합니다

3. 감사 로깅을 위해 SVM 구성:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```

> 감사 로그 파일의 최소 기본 보존 기간은 6개월입니다. 영향을 받는 파일의 보존 기간이 감사 로그의 보존 기간보다 긴 경우 로그의 보존 기간이 파일의 보존 기간을 상속합니다. 따라서 권한이 있는 삭제를 사용하여 삭제된 파일의 보존 기간이 10개월이고 감사 로그의 보존 기간이 8개월인 경우 로그 보존 기간은 10개월로 연장됩니다. 보존 시간 및 기본 보존 기간에 대한 자세한 내용은 을 참조하십시오"보존 시간을 설정합니다".

다음 명령어는 SnapLock volume logVol을 이용하여 Audit logging을 위한 'VM1'을 설정한다. 감사 로그의 최대 크기는 20GB이며 8개월 동안 유지됩니다.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

에 대한 자세한 내용은 `snaplock log create` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 감사 로깅을 위해 구성한 SVM에서 SnapLock 볼륨을 연결 경로 '/sSnapLock_audit_log'에 마운트합니다.

   SnapLock 볼륨을 마운트합니다

ONTAP SnapLock 설정 확인

'volume file fingerprint start' 및 'volume file fingerprint dump' 명령을 사용하여 파일 유형(Regular, WORM 또는 WORM appendable), 볼륨 만료 날짜 등 파일 및 볼륨에 대한 주요 정보를 볼 수 있습니다.

단계

1. 파일 지문 생성:

   ```
   volume file fingerprint start -vserver <SVM_name> -file <file_path>
   ```

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   이 명령어는 'volume file fingerprint dump' 명령어에 대한 입력으로 사용할 수 있는 세션 ID를 생성한다.

   > 세션 ID와 함께 볼륨 파일 fingerprint show 명령을 사용하여 지문 작업의 진행률을 모니터링할 수 있습니다. 지문 표시를 시도하기 전에 작업이 완료되었는지 확인하십시오.

2. 파일의 지문을 표시합니다.

   ```
   volume file fingerprint dump -session-id <session_ID>
   ```

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
```

```
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

WORM 파일 관리

ONTAP SnapLock 사용하여 WORM 파일 관리

WORM 파일은 다음과 같은 방법으로 관리할 수 있습니다.

- "WORM에 파일을 커밋합니다"
- "볼트 대상에서 WORM에 스냅샷을 커밋합니다"
- "재해 복구를 위해 WORM 파일을 미러링합니다"
- "소송 중에 WORM 파일 보존"
- "WORM 파일을 삭제합니다"

ONTAP SnapLock 사용하여 WORM에 파일 커밋

파일을 수동으로 커밋하거나 자동으로 커밋하여 WORM(Write Once, Read Many)에 커밋할 수 있습니다. WORM 추가 가능 파일을 생성할 수도 있습니다.

WORM에 파일을 수동으로 커밋합니다

파일을 읽기 전용으로 만들어 WORM에 파일을 수동으로 커밋합니다. NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경할 수 있습니다. 응용 프로그램이 파일에 대한 쓰기를 완료했는지 확인하여 파일이 너무 일찍 커밋되지 않았는지 또는 많은 볼륨 때문에 자동 커밋 스캐너에 대한 배율 조정 문제가 있는지 확인하려면 파일을 수동으로 커밋하도록 선택할 수 있습니다.

시작하기 전에

- 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- 파일에 쓸 수 있어야 합니다.

이 작업에 대해

볼륨 ComplianceClock 시간은 명령이나 프로그램이 실행될 때 파일의 ctime 필드에 기록됩니다. ComplianceClock 시간은 파일의 보존 시간에 도달한 시점을 결정합니다.

단계

1. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

   UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod -w document.txt
```

Windows 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
attrib +r document.txt
```

파일을 **WORM**에 자동으로 커밋합니다

SnapLock 자동 커밋 기능을 사용하면 파일을 WORM에 자동으로 커밋할 수 있습니다. 자동 커밋 기능은 자동 커밋 기간 동안 파일이 변경되지 않은 경우 SnapLock 볼륨에서 파일을 WORM 상태로 커밋합니다. 자동 커밋 기능은 기본적으로 비활성화되어 있습니다.

시작하기 전에

- 자동 커밋하려는 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨이 온라인 상태여야 합니다.
- SnapLock 볼륨은 읽기-쓰기 볼륨이어야 합니다.

> SnapLock 자동 커밋 기능은 볼륨에 있는 모든 파일을 검사하여 자동 커밋 요구 사항을 충족하는 경우 파일을 커밋합니다. 파일이 자동 커밋될 준비가 된 시점과 SnapLock 자동 커밋 스캐너에서 실제로 커밋된 시점 사이에 시간 간격이 있을 수 있습니다. 그러나 파일이 자동 커밋될 수 있는 즉시 파일 시스템에 의해 수정 및 삭제로부터 보호됩니다.

이 작업에 대해

autocommit period _ 는 파일이 자동 커밋되기 전에 변경되지 않은 상태로 유지해야 하는 시간을 지정합니다. 자동 커밋 기간이 경과하기 전에 파일을 변경하면 파일의 자동 커밋 기간이 다시 시작됩니다.

다음 표에는 자동 커밋 기간에 대해 가능한 값이 나와 있습니다.

값	단위	참고
없음	-	기본값입니다.
5-5256000	분	-
1-87600)을 참조하십시오	시간	-
1-3650	일	-
1-120으로 설정합니다	개월	-
1-10	년	-

> 최소값은 5분이고 최대값은 10년입니다.

단계

1. SnapLock 볼륨의 파일을 WORM에 자동 커밋:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-autos커밋 -period_autosit_period_ *'

   에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령은 파일이 5시간 동안 변경되지 않는 한 SVM VS1 볼륨 'vol1'에 있는 파일을 자동으로 커밋합니다.

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

WORM 추가 가능 파일을 생성합니다

WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성하거나 SnapLock_VOLUME append mode_feature를 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다.

명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성합니다

NFS 또는 CIFS를 통해 적합한 명령 또는 프로그램을 사용하여 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의 n×256KB+1 바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

현재 활성 256KB 청크를 초과하는 순서가 없는 쓰기는 활성 256KB 청크가 최신 오프셋으로 재설정되고 이전 오프셋에 대한 쓰기가 실패하고 'ROFS(읽기 전용 파일 시스템)' 오류가 발생합니다. 쓰기 오프셋은 클라이언트 애플리케이션에 따라 다릅니다. WORM 추가 파일 쓰기 의미를 준수하지 않는 클라이언트는 쓰기 콘텐츠가 잘못 종료될 수 있습니다. 따라서 클라이언트가 순서가 지정되지 않은 쓰기에 대한 오프셋 제한을 따르는지 확인하거나 파일 시스템을 동기식 모드로 마운트하여 동기식 쓰기를 보장하는 것이 좋습니다.

단계

1. 적합한 명령 또는 프로그램을 사용하여 원하는 보존 시간으로 길이가 0인 파일을 생성합니다.

   UNIX 셸에서 다음 명령을 사용하여 2020년 11월 21일 오전 6:00의 보존 시간을 설정합니다 길이가 0인 파일에서 document.txt:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 읽기 전용으로 변경합니다.

UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 읽기 전용으로 만듭니다.

```
chmod 444 document.txt
```

3. 적합한 명령 또는 프로그램을 사용하여 파일의 읽기-쓰기 속성을 다시 쓰기 가능으로 변경합니다.

   파일에 데이터가 없기 때문에 이 단계는 규정 준수 위험으로 간주되지 않습니다.

   UNIX 셸에서 다음 명령을 사용하여 "document.txt"라는 파일을 쓰기 가능하게 만듭니다.

   ```
   chmod 777 document.txt
   ```

4. 적절한 명령 또는 프로그램을 사용하여 파일에 데이터 쓰기를 시작합니다.

   UNIX 셸에서 다음 명령을 사용하여 데이터를 document.txt에 씁니다.

   ```
   echo test data >> document.txt
   ```

   파일에 데이터를 더 이상 추가할 필요가 없는 경우 파일 권한을 다시 읽기 전용으로 변경합니다.

볼륨 추가 모드를 사용하여 **WORM** 추가 가능 파일을 생성합니다

ONTAP 9.3부터는 SnapLock_VOLUME APPEND MODE_(VAM) 기능을 사용하여 기본적으로 WORM 추가 가능 파일을 생성할 수 있습니다. WORM 추가 가능 파일은 로그 항목과 같이 점진적으로 기록된 데이터를 유지합니다. 데이터는 256KB 청크로 파일에 추가됩니다. 각 청크가 쓰일 때 이전 청크는 WORM으로 보호됩니다. 보존 기간이 경과할 때까지 파일을 삭제할 수 없습니다.

시작하기 전에

- WORM 추가 가능 파일이 SnapLock 볼륨에 있어야 합니다.
- SnapLock 볼륨을 마운트 해제하고 스냅샷과 사용자가 생성한 파일을 비워야 합니다.

이 작업에 대해

데이터는 활성 256KB 청크에 순차적으로 쓸 필요가 없습니다. 파일의 n×256KB+1 바이트에 데이터를 쓸 때 이전 256KB 세그먼트는 WORM으로 보호됩니다.

볼륨에 대해 자동 커밋 기간을 지정하면 자동 커밋 기간보다 긴 기간 동안 수정되지 않은 WORM 추가 가능 파일이 WORM에 커밋됩니다.

VAM은 SnapLock 감사 로그 볼륨에서 지원되지 않습니다.

단계

1. VAM 활성화:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-is-volume-append-mode

-enabled true|false *

에 대한 자세한 내용은 `volume snaplock modify` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 SVM의 볼륨 'vol1'에서 VAM이 활성화됩니다.

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. 적합한 명령 또는 프로그램을 사용하여 쓰기 권한이 있는 파일을 만듭니다.

   파일은 기본적으로 WORM-appendable입니다.

ONTAP 볼트 대상의 WORM에 스냅샷 커밋

SnapVault용 SnapLock를 사용하여 보조 스토리지에서 WORM으로 스냅샷을 보호할 수 있습니다. 볼트 대상에서 모든 기본 SnapLock 작업을 수행합니다. 대상 볼륨은 읽기 전용으로 자동 마운트되므로 WORM에 스냅샷을 명시적으로 커밋할 필요가 없습니다.

시작하기 전에

- System Manager를 사용하여 관계를 구성하려면 소스 클러스터와 대상 클러스터 모두에서 ONTAP 9.15.1 이상이 실행 중이어야 합니다.
- 대상 클러스터에서:
  - "SnapLock 라이센스를 설치합니다".
  - "준수 시계를 초기화합니다".
  - 9.10.1 이전의 ONTAP 릴리즈와 함께 CLI를 사용하는 경우, "SnapLock 애그리게이트를 생성합니다".
- 보호 정책은 "볼트" 유형이어야 합니다.
- 소스 및 타겟 애그리게이트는 64비트여야 합니다.
- 소스 볼륨은 SnapLock 볼륨일 수 없습니다.
- ONTAP CLI를 사용하는 경우 소스 볼륨과 타겟 볼륨을 에서 생성해야 합니다 "피어링된 클러스터" 및 "SVM".

이 작업에 대해

소스 볼륨은 NetApp 또는 비 NetApp 스토리지를 사용할 수 있습니다.

> WORM 상태로 커밋된 스냅샷의 이름은 변경할 수 없습니다.

SnapLock 볼륨의 클론을 생성할 수는 있지만 SnapLock 볼륨의 파일은 복제할 수 없습니다.

> LUN은 SnapLock 볼륨에서 지원되지 않습니다. LUN은 비 SnapLock 볼륨에서 생성된 스냅샷이 SnapLock 소산 관계의 일부로 보호를 위해 SnapLock 볼륨으로 전송되는 경우에만 SnapLock 볼륨에서 지원됩니다. LUN은 읽기/쓰기 SnapLock 볼륨에서 지원되지 않습니다. 하지만 변조 방지 스냅샷은 SnapMirror 소스 볼륨과 LUN이 포함된 타겟 볼륨 모두에서 지원됩니다.

ONTAP 9.10.1부터 SnapLock 및 비 SnapLock 볼륨은 동일한 애그리게이트에 존재할 수 있으므로, ONTAP 9.10.1을

사용하는 경우 더 이상 별도의 SnapLock 애그리게이트를 생성할 필요가 없습니다. '-snaplock-type' 볼륨 옵션을 사용하여 Compliance 또는 Enterprise SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리즈에서는 SnapLock 모드, 규정 준수 또는 엔터프라이즈가 aggregate에서 상속됩니다. 버전에 상관없이 유연한 타겟 볼륨이 지원되지 않습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

볼트 대상인 SnapLock 볼륨에 기본 보존 기간이 할당되어 있습니다. 이 기간의 값은 처음에 SnapLock 엔터프라이즈 볼륨의 경우 0년, SnapLock 규정 준수 볼륨의 경우 최대 30년으로 설정됩니다. 각 NetApp 스냅샷은 처음에는 이 기본 보존 기간을 사용하여 커밋됩니다. 필요한 경우 보존 기간을 나중에 연장할 수 있습니다. 자세한 내용은 을 "보존 시간 개요를 설정합니다"참조하십시오.

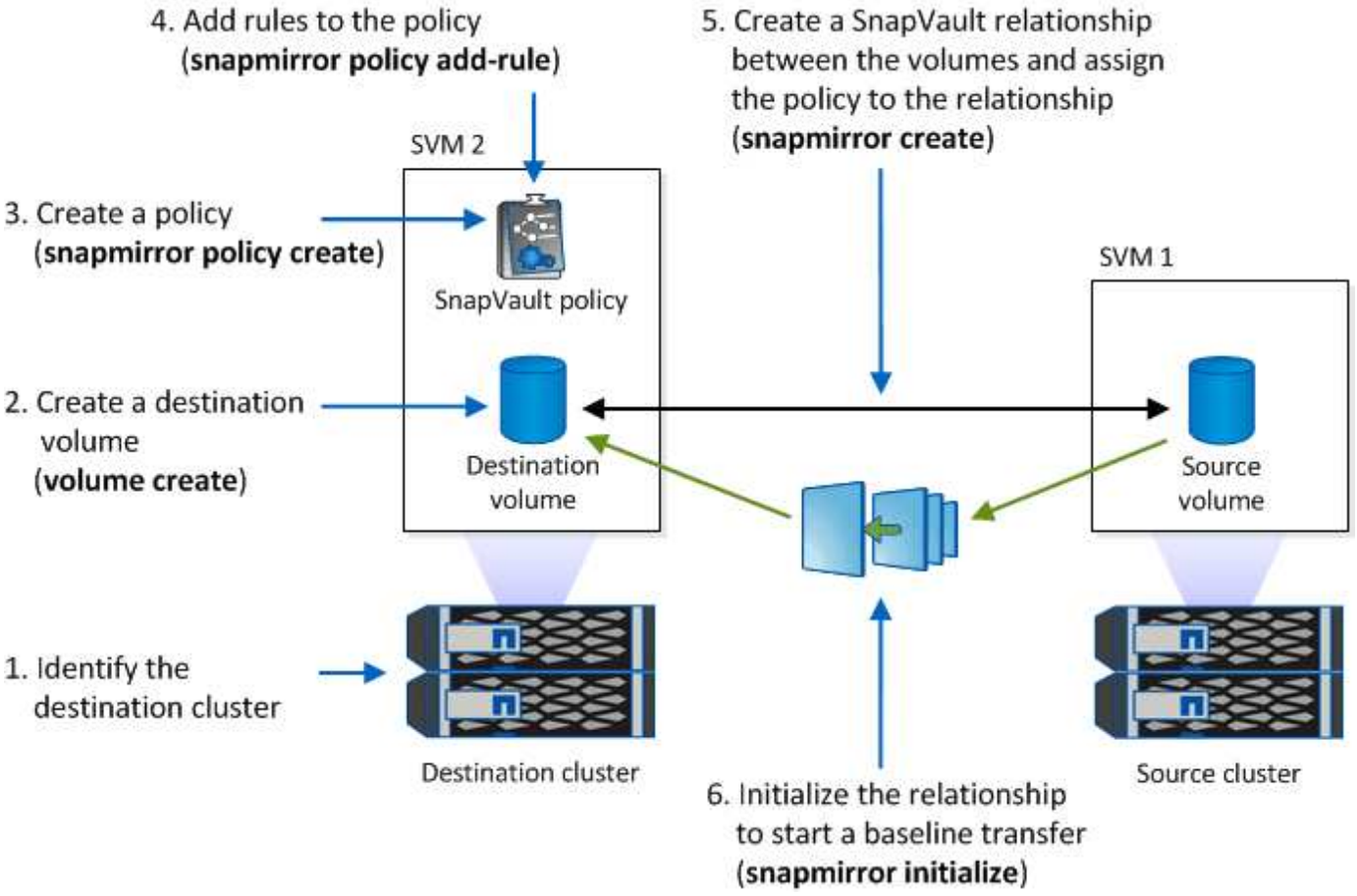
ONTAP 9.14.1부터 SnapMirror 관계의 SnapMirror 정책에서 특정 SnapMirror 레이블에 대한 보존 기간을 지정하여 소스에서 대상 볼륨으로의 복제된 스냅샷이 규칙에 지정된 보존 기간 동안 보존되도록 할 수 있습니다. 보존 기간을 지정하지 않으면 대상 볼륨의 기본 보존 기간이 사용됩니다.

ONTAP 9.13.1부터 옵션을 로 설정한 `non-snaplock` 상태로 FlexClone을 생성하고 볼륨 클론 생성 작업을 실행할 때 스냅샷을 "상위-스냅샷"으로 지정하여 SnapLock 소산 관계의 대상 SnapLock 볼륨에서 잠긴 스냅샷을 즉시 복원할 수 있습니다 `snaplock-type`. 에 대해 자세히 "SnapLock 형식으로 FlexClone 볼륨 생성"알아보십시오.

MetroCluster 구성의 경우 다음 사항에 유의해야 합니다.

- 동기식 소스 SVM과 동기식-타겟 SVM 간에는 동기식-소스 SVM 사이만이 아니라 SnapVault 관계를 생성할 수 있습니다.
- 동기화 소스 SVM의 볼륨에서 데이터 지원 SVM으로 SnapVault 관계를 생성할 수 있습니다.
- 데이터 지원 SVM의 볼륨에서 동기화 소스 SVM의 DP 볼륨으로 SnapVault 관계를 생성할 수 있습니다.

다음 그림에서는 SnapLock 볼트 관계를 초기화하는 절차를 보여 줍니다.



단계

ONTAP CLI를 사용하여 SnapLock 볼트 관계를 만들거나, ONTAP 9.15.1부터 시스템 관리자를 사용하여 SnapLock 볼트 관계를 만들 수 있습니다.

시스템 관리자

1. 볼륨이 아직 없는 경우 소스 클러스터에서 * 스토리지 > 볼륨 * 으로 이동한 후 * 추가 * 를 선택합니다.
2. Add Volume * (볼륨 추가 *) 창에서 * More Options * (추가 옵션 *)를 선택합니다.
3. 볼륨 이름, 크기, 엑스포트 정책 및 공유 이름을 입력합니다.
4. 변경 사항을 저장합니다.
5. 대상 클러스터에서 * 보호 > 관계 * 로 이동합니다.
6. 소스 * 열 위에서 * 보호 * 를 선택하고 메뉴에서 * 볼륨 * 을 선택합니다.
7. protect volumes * 창에서 보호 정책으로 * Vault * 를 선택합니다.
8. 소스 * 섹션에서 보호할 클러스터, 스토리지 VM 및 볼륨을 선택합니다.
9. 대상 * 섹션의 * 구성 세부 정보 * 에서 * 대상 스냅샷 잠금 * 을 선택한 다음 잠금 방법으로 * SnapLock for SnapVault * 를 선택합니다. * 선택한 정책 유형이 유형이 아닌 경우, SnapLock 라이센스가 설치되지 않았거나 규정 준수 클록이 초기화되지 않은 경우 * 잠금 방법 * 이 표시되지 `vault` 않습니다.
10. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
11. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 대상 클러스터에서 소스 볼륨보다 크거나 같은 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP
-size <size>
```

다음 명령을 실행하면 이름이 2GB SnapLock Compliance 볼륨이 생성됩니다 `dstvolB` 인치 `SVM2` 애그리케이트 `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. 대상 클러스터에서 "기본 보존 기간을 설정합니다".
3. "새 복제 관계를 생성합니다" 비 SnapLock 소스와 사용자가 생성한 새 SnapLock 대상 간

이 예에서는 매일 및 매주 레이블이 지정된 스냅샷을 시간별 일정에 따라 볼팅하는 정책을 사용하여 `XDPDefault` 대상 SnapLock 볼륨과의 새로운 SnapMirror 관계를 `dstvolB` 생성합니다.

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"사용자 지정 복제 정책을 생성합니다" 또는 a "사용자 지정 일정" 사용 가능한 기본값이 적합하지 않은 경우

4. 대상 SVM에서 생성된 SnapVault 관계를 초기화합니다.

```
snapmirror initialize -destination-path <destination_path>
```

다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 관계가 초기화되고 유휴 상태가 되면 대상에서 명령을 사용하여 `snapshot show` 복제된 스냅샷에 적용되는 SnapLock 만료 시간을 확인합니다.

이 예에서는 SnapMirror 레이블과 SnapLock 만료 날짜가 있는 볼륨의 스냅숏을 `dstvolB` 나열합니다.

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

관련 정보

- "클러스터 및 SVM 피어링"
- "SnapVault를 사용한 볼륨 백업"
- "SnapMirror 초기화"

ONTAP SnapMirror 사용하여 재해 복구를 위한 **WORM** 파일 미러링

SnapMirror를 사용하여 재해 복구 및 기타 목적으로 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다. 소스 볼륨과 타겟 볼륨을 모두 SnapLock에 대해 구성해야 하며 두 볼륨 모두 동일한 SnapLock 모드, Compliance 또는 Enterprise를 사용해야 합니다. 볼륨과 파일의 모든 주요 SnapLock 속성이 복제됩니다.

필수 구성 요소

피어링된 SVM이 있는 클러스터에서 소스 및 타겟 볼륨을 생성해야 합니다. 자세한 내용은 을 "클러스터 및 SVM 피어링"참조하십시오.

이 작업에 대해

- ONTAP 9.5부터 DP(데이터 보호) 유형 관계가 아닌 XDP(확장된 데이터 보호) 유형의 SnapMirror 관계로 WORM 파일을 복제할 수 있습니다. XDP 모드는 ONTAP 버전에 독립적이며 동일한 블록에 저장된 파일을 구분할 수 있으므로 복제된 Compliance 모드 볼륨을 재동기화하는 것이 훨씬 쉬워집니다. 기존 DP 유형 관계를 XDP 유형 관계로 변환하는 방법에 대한 자세한 내용은 을 참조하십시오 "데이터 보호".
- SnapLock에서 데이터 손실을 결정하면 DP 유형의 SnapMirror 관계에 대한 재동기화 작업이 Compliance-Mode 볼륨에 대해 실패합니다. 재동기화 작업이 실패하면 "volume clone create" 명령을 사용하여 대상 볼륨의 클론을 생성할 수 있습니다. 그런 다음 소스 볼륨을 클론과 다시 동기화할 수 있습니다.
- SnapLock 볼륨의 SnapMirror 관계는 다음을 지원합니다. `MirrorAllSnapshots` async-mirror 유형의 정책입니다. SnapLock 볼륨의 보존 기간은 볼륨이 보유하고 있는 모든 WORM 파일 중 최대 보존 기간에 따라

결정됩니다. 대상이 소스의 DR 복사본이므로 대상 SnapLock 볼륨의 보존 기간은 소스와 동일합니다.

- SnapLock 호환 볼륨 간의 XDP 유형의 SnapMirror 관계는 중단 후 대상의 데이터가 소스(중단 후)에서 분기된 경우에도 중단 후 재동기화를 지원합니다.

  재동기화에서 일반 스냅샷을 넘어 소스 간에 데이터 발산이 감지되면 대상에서 새 스냅샷이 잘려 이러한 발산을 캡처합니다. 새 스냅샷과 공통 스냅샷은 모두 다음과 같이 보존 시간으로 잠깁니다.

  - 대상의 볼륨 만료 시간입니다
  - 볼륨 만료 시간이 지난 시간이거나 설정되지 않은 경우 스냅샷이 30일 동안 잠깁니다
  - 대상에 법적 보류가 있는 경우 실제 볼륨 만료 기간이 마스킹되고 "무제한"으로 표시됩니다. 그러나 실제 볼륨 만료 기간 동안 스냅샷은 잠깁니다.

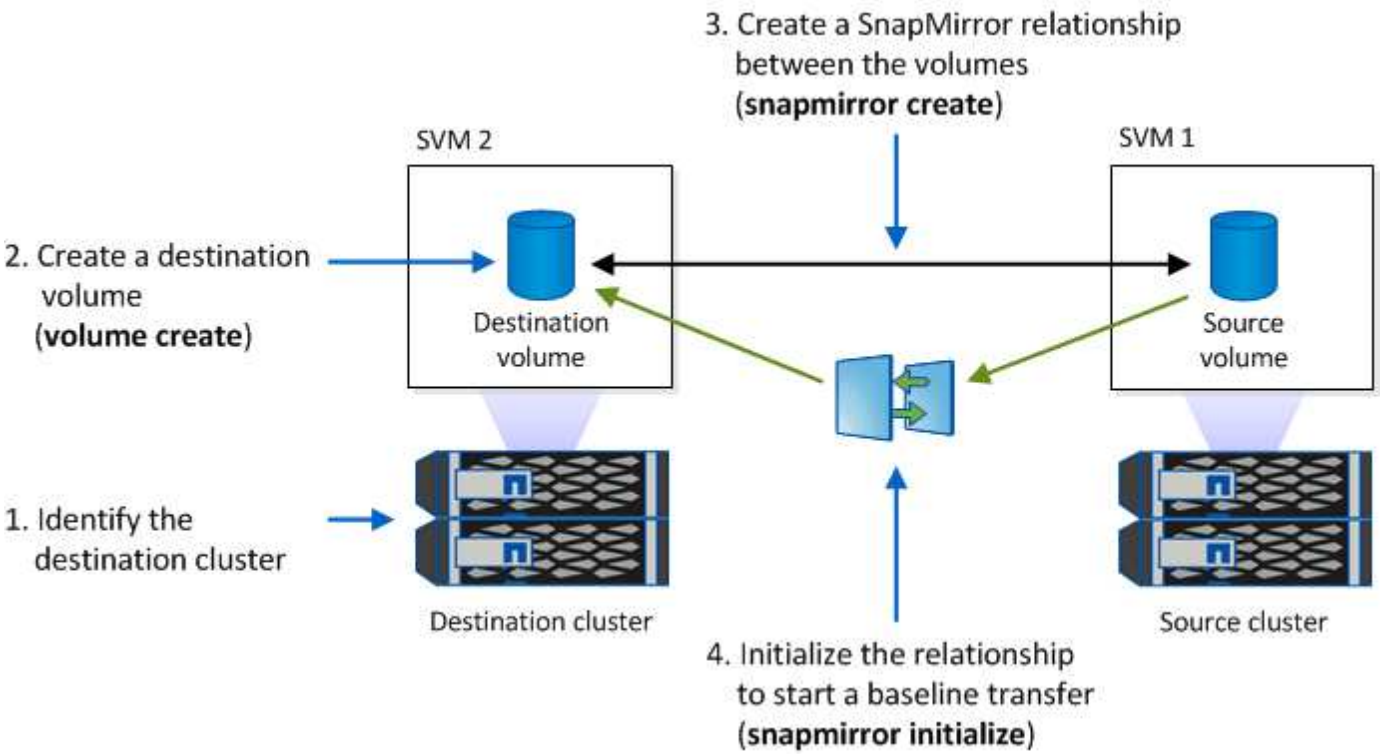
대상 볼륨의 만료 기간이 소스보다 이후인 경우 대상 만료 기간이 유지되고 재동기화 후 소스 볼륨의 만료 기간에 의해 덮어쓰이지 않습니다.

대상과 소스가 다른 법적 구속이 있는 대상에는 재동기화가 허용되지 않습니다. 재동기화를 시도하기 전에 소스와 대상에서 동일한 법적 증거 자료 보관 또는 모든 법적 고지를 해제해야 합니다.

다양한 데이터를 캡처하기 위해 생성된 대상 볼륨의 잠긴 스냅샷은 CLI를 사용하여 소스에 복사할 수 있습니다 `snapmirror update -s snapshot`. 복제된 스냅샷은 소스에서 계속 잠깁니다.

- SVM 데이터 보호 관계는 지원되지 않습니다.
- 로드 공유 데이터 보호 관계는 지원되지 않습니다.

다음 그림에서는 SnapMirror 관계를 초기화하는 절차를 보여 줍니다.



시스템 관리자

ONTAP 9.12.1부터 System Manager를 사용하여 WORM 파일의 SnapMirror 복제를 설정할 수 있습니다.

단계

1. Storage > Volumes * 로 이동합니다.
2. 표시/숨기기 * 를 클릭하고 * SnapLock 유형 * 을 선택하여 * 볼륨 * 창에 열을 표시합니다.
3. SnapLock 볼륨을 찾습니다.
4. 을 ⋮ 클릭하고 * 보호 * 를 선택합니다.
5. 대상 클러스터와 대상 스토리지 VM을 선택합니다.
6. 추가 옵션 * 을 클릭합니다.
7. 기존 정책 표시 * 를 선택하고 * DPDefault(레거시) * 를 선택합니다.
8. Destination Configuration details * 섹션에서 * Override transfer schedule * 을 선택하고 * hourly * 를 선택합니다.
9. 저장 * 을 클릭합니다.
10. 소스 볼륨 이름 왼쪽의 화살표를 클릭하여 볼륨 세부 정보를 확장하고 페이지 오른쪽의 원격 SnapMirror 보호 세부 정보를 검토합니다.
11. 원격 클러스터에서 * 보호 관계 * 로 이동합니다.
12. 관계를 찾고 대상 볼륨 이름을 클릭하여 관계 세부 정보를 봅니다.
13. 대상 볼륨 SnapLock 유형 및 기타 SnapLock 정보를 확인합니다.

CLI를 참조하십시오

1. 대상 클러스터를 식별합니다.
2. 대상 클러스터에서"SnapLock 라이센스를 설치합니다", "준수 시계를 초기화합니다"및 9.10.1 이전의 ONTAP 릴리즈를 사용하는 경우,"SnapLock 애그리게이트를 생성합니다"
3. 대상 클러스터에서 소스 볼륨과 크기가 같거나 더 큰 dP 유형의 SnapLock 대상 볼륨을 생성합니다.

   '* 볼륨 생성 - vserver_SVM_name_-volume_volume_name_-aggregate_aggregate_name_-snaplock-type compliance|enterprise-type dp-size_size_ *'

   > ⓘ ONTAP 9.10.1부터 SnapLock 볼륨과 SnapLock 아닌 볼륨이 동일한 집계에 존재할 수 있습니다. 따라서 ONTAP 9.10.1을 사용하는 경우 별도의 SnapLock 집계를 만들 필요가 없습니다. 볼륨 -snaplock-type 옵션을 사용하여 규정 준수 또는 엔터프라이즈 SnapLock 볼륨 유형을 지정합니다. ONTAP 9.10.1 이전의 ONTAP 릴리스에서는 SnapLock 모드(규정 준수 또는 엔터프라이즈)가 집계에서 상속되었습니다. 대상 볼륨의 언어 설정은 소스 볼륨의 언어 설정과 일치해야 합니다.

   다음 명령을 실행하면 node01_aggr 집계 'sVM2'에 dstvolB라는 이름의 2GB SnapLock 'Compliance' 볼륨이 생성됩니다.

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. 대상 SVM에서 SnapMirror 정책을 생성합니다.

   `snapmirror policy create -vserver SVM_name -policy policy_name`

   다음 명령을 실행하면 SVM 전체의 정책 'VM1-mirror'가 생성됩니다.

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. 대상 SVM에서 SnapMirror 일정을 생성합니다.

   '* 작업 일정 cron create-name_schedule_name_-DayOfWeek_day_of_week_-hour_hour_-minute_minute_*'

   다음 명령을 실행하면 "weekendcron"이라는 SnapMirror 스케줄이 생성됩니다.

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. 대상 SVM에서 SnapMirror 관계 생성:

   `snapmirror create -source-path source_path -destination-path destination_path -type XDP|DP -policy policy_name -schedule schedule_name`

   다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 SnapMirror 관계가 생성되고 정책 'VM1-mirror'와 스케줄 'weekendcron'이 할당됩니다.

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   > XDP 유형은 ONTAP 9.5 이상에서 사용할 수 있습니다. ONTAP 9.4 이전 버전에서 DP 유형을 사용해야 합니다.

7. 대상 SVM에서 SnapMirror 관계를 초기화합니다.

   `snapmirror initialize -destination-path destination_path`

   초기화 프로세스는 대상 볼륨에 대해 _baseline 전송_을 수행합니다. SnapMirror는 소스 볼륨의 스냅샷을 만든 다음 복사본과 이 복사본이 타겟 볼륨에 참조하는 모든 데이터 블록을 전송합니다. 또한 소스 볼륨의 다른 모든 스냅샷을 대상 볼륨으로 전송합니다.

   다음 명령을 실행하면 'VM1'의 소스 볼륨 'rcvolA'와 'VM2'의 대상 볼륨 'dstvolB'의 관계가 초기화됩니다.

   ```
   SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

관련 정보

- "클러스터 및 SVM 피어링"
- "볼륨 재해 복구 준비"
- "데이터 보호"
- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 정책 생성"

ONTAP SnapLock Legal Hold를 사용하여 소송 중 **WORM** 파일 보관

ONTAP 9.3부터는 *Legal Hold* 기능을 사용하여 소송 기간 동안 준수 모드 WORM 파일을 보존할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.

  "SnapLock 관리자 계정을 만듭니다"

- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

법적 증거 자료 보관 아래에 있는 파일은 무기한 보존 기간이 있는 WORM 파일처럼 작동합니다. 법적 증거 자료 보관 기간이 끝나는 시기를 지정하는 것은 귀하의 책임입니다.

법적 증거 자료 보관 아래에 넣을 수 있는 파일 수는 볼륨에서 사용 가능한 공간에 따라 다릅니다.

단계

1. 법적 증거 자료 보관 시작:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   다음 명령은 'vol1'의 모든 파일에 대해 법적 대기를 시작합니다.

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. 법적 증거 자료 보관 종료:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   다음 명령은 'vol1'의 모든 파일에 대해 법적 보류를 종료합니다.

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

관련 정보

- "SnapLock 법적 증거 자료 보관 이 시작됩니다"
- "SnapLock 법적 증거 자료 보관 종료"

ONTAP SnapLock 사용하여 **WORM** 파일 삭제

권한 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다. 이 기능을 사용하려면 먼저 SnapLock 관리자 계정을 만든 다음 계정을 사용하여 기능을 활성화해야 합니다.

SnapLock 관리자 계정을 만듭니다

권한 있는 삭제를 수행하려면 SnapLock 관리자 권한이 있어야 합니다. 이러한 권한은 vsadmin-SnapLock 역할에 정의되어 있습니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 SnapLock 관리자 역할을 가진 SVM 관리자 계정을 만들도록 요청할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

단계

1. SnapLock 관리자 역할을 사용하여 SVM 관리자 계정을 생성합니다.

   '* 보안 로그인 create-vserver_SVM_name_-user-or-group-name_user_or_group_name_-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_*'

   다음 명령을 실행하면 사전 정의된 "vsadmin-snaplock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 'VM1'에 액세스할 수 있습니다.

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

권한 있는 삭제 기능을 활성화합니다

삭제하려는 WORM 파일이 포함된 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 명시적으로 활성화해야 합니다.

이 작업에 대해

'-privileged-delete' 옵션의 값은 권한 있는 삭제 활성화 여부를 결정합니다. 가능한 값은 '사용', '사용 안 함', '영구 사용 안 함'입니다.

영구 불활성 상태가 단자다. 상태를 "영구 비활성화"로 설정한 후에는 볼륨에 대한 권한 있는 삭제를 활성화할 수 없습니다.

단계

1. SnapLock 엔터프라이즈 볼륨에 대한 권한 있는 삭제 활성화:

   '* volume SnapLock modify -vserver_SVM_name_-volume_volume_name_-privileged-delete disabled|enabled|permanently-disabled *

   다음 명령을 실행하면 'VM1'의 엔터프라이즈 볼륨 'dataVol'에 대한 권한 있는 삭제 기능이 활성화됩니다.

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

엔터프라이즈 모드 **WORM** 파일을 삭제합니다

권한이 있는 삭제 기능을 사용하여 보존 기간 동안 엔터프라이즈 모드 WORM 파일을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 SnapLock 관리자여야 합니다.
- SnapLock 감사 로그를 생성하고 엔터프라이즈 볼륨에서 권한 있는 삭제 기능을 활성화해야 합니다.

이 작업에 대해

만료된 WORM 파일을 삭제하려면 권한이 있는 삭제 작업을 사용할 수 없습니다. 명령을 사용하여 `volume file retention show` 삭제하려는 WORM 파일의 보존 시간을 볼 수 있습니다. 에 대한 자세한 내용은 `volume file retention show` "ONTAP 명령 참조입니다"을 참조하십시오.

단계

1. 엔터프라이즈 볼륨에서 WORM 파일 삭제:

   '* 볼륨 파일 권한이 있는-삭제-vserver_SVM_name_-file_file_path_*'

   다음 명령을 실행하면 SVM 'sVM1'에서 파일 '/vol/dataVol/F1'이 삭제됩니다.

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

ONTAP SnapLock 볼륨 이동

ONTAP 9.8부터 SnapLock 볼륨을 엔터프라이즈부터 규정 준수까지 동일한 유형의 대상 Aggregate로 이동할 수 있습니다. SnapLock 볼륨을 이동하려면 SnapLock 보안 역할이 할당되어야 합니다.

SnapLock 보안 관리자 계정을 만듭니다

SnapLock 볼륨 이동을 수행하려면 SnapLock 보안 관리자 권한이 있어야 합니다. 이 권한은 ONTAP 9.8에 도입된 _SnapLock_역할을 통해 부여됩니다. 해당 역할이 아직 할당되지 않은 경우 클러스터 관리자에게 이 SnapLock 보안 역할을 가진 SnapLock 보안 사용자를 만들도록 요청할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.
- 보안 연결(SSH, 콘솔 또는 ZAPI)에 로그인해야 합니다.

이 작업에 대해

SnapLock 역할은 데이터 SVM과 연결된 vsadmin-SnapLock 역할과는 달리 관리 SVM과 연결됩니다.

단계

1. SnapLock 관리자 역할을 사용하여 SVM 관리자 계정을 생성합니다.

   '* 보안 로그인 create-vserver_SVM_name_-user-or-group-name_user_or_group_name_-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_*'

   다음 명령을 실행하면 미리 정의된 "SnapLock" 역할을 사용하여 SVM 관리자 계정 'napLockAdmin'에서 암호를 사용하여 admin SVM 'cluster1'에 액세스할 수 있습니다.

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

SnapLock 볼륨을 이동합니다

'volume move' 명령을 사용하여 SnapLock 볼륨을 대상 애그리게이트로 이동할 수 있습니다.

시작하기 전에

- SnapLock 볼륨 이동을 수행하기 전에 SnapLock으로 보호되는 감사 로그를 생성해야 합니다.

  "감사 로그를 생성합니다".

- ONTAP 9.10.1 이전 버전의 ONTAP를 사용하는 경우 대상 애그리게이트는 이동할 SnapLock 볼륨과 동일한 SnapLock 유형이어야 합니다. Compliance to Compliance 또는 Enterprise to Enterprise입니다. ONTAP 9.10.1부터는 이러한 제한이 없어지기 때문에 aggregate에 Compliance 및 Enterprise SnapLock 볼륨과 비 SnapLock 볼륨이 모두 포함될 수 있습니다.
- SnapLock 보안 역할을 가진 사용자여야 합니다.

단계

1. 보안 연결을 사용하여 ONTAP 클러스터 관리 LIF에 로그인합니다.

   ' * ssh SnapLock_user@cluster_mgmt_ip *'

2. SnapLock 볼륨 이동:

'* volume move start -vserver_SVM_name_-volume_snaplock_volume_name_-destination -aggregate_destination_name_*'

3. 볼륨 이동 작업의 상태를 확인합니다.

   '* 볼륨 이동 표시 -volume_snaplock_volume_name_-vserver_SVM_name_-필드 볼륨, 단계, SVM*

랜섬웨어 공격으로부터 보호하기 위해 **ONTAP** 스냅샷 잠금

ONTAP 9.12.1부터 비 SnapLock 볼륨에서 스냅샷을 잠가 랜섬웨어 공격으로부터 보호할 수 있습니다. 스냅샷을 잠그면 실수로 또는 악의적으로 삭제할 수 없습니다.

만료 시간에 도달할 때까지 스냅샷을 삭제할 수 없도록 SnapLock Compliance 시계 기능을 사용하여 지정된 기간 동안 스냅샷을 잠급니다. 스냅샷을 잠그면 무단 변경이 방지되어 랜섬웨어 위협으로부터 보호할 수 있습니다. 볼륨이 랜섬웨어 공격에 의해 손상된 경우 잠긴 스냅샷을 사용하여 데이터를 복구할 수 있습니다.

ONTAP 9.14.1부터 스냅샷 잠금은 SnapLock 볼트 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 장기 보존 스냅샷을 지원합니다. 에 연결된 SnapMirror 정책 규칙을 사용하여 보존 기간을 설정하여 스냅샷 잠금을 기존 정책 레이블설정할 수 있습니다. 이 규칙은 볼륨에 설정된 기본 보존 기간을 재정의합니다. SnapMirror 레이블과 연결된 보존 기간이 없으면 볼륨의 기본 보존 기간이 사용됩니다.

변조 방지 스냅샷 요구사항 및 고려사항

- ONTAP CLI를 사용하는 경우 클러스터의 모든 노드에서 ONTAP 9.12.1 이상을 실행해야 합니다. System Manager를 사용하는 경우 모든 노드에서 ONTAP 9.13.1 이상을 실행해야 합니다.
- "SnapLock 라이센스가 클러스터에 설치되어 있어야 합니다".. 이 라이센스는 에 "ONTAP 1 을 참조하십시오 "포함되어 있습니다.
- "클러스터의 규정 준수 클록을 초기화해야 합니다"..
- 볼륨에 스냅샷 잠금이 설정되어 있으면 클러스터를 ONTAP 9.12.1 이후의 ONTAP 버전으로 업그레이드할 수 있지만, 잠긴 스냅샷이 모두 만료 날짜에 도달하여 삭제되고 스냅샷 잠금이 해제될 때까지 이전 버전의 ONTAP로 되돌릴 수 없습니다.
- 스냅샷이 잠기면 볼륨 만료 시간이 스냅샷의 만료 시간으로 설정됩니다. 두 개 이상의 스냅샷이 잠겨 있는 경우 볼륨 만료 시간은 모든 스냅샷 중에서 가장 긴 만료 시간을 반영합니다.
- 잠긴 스냅샷의 보존 기간이 스냅샷 유지 수보다 우선합니다. 즉, 잠긴 스냅샷에 대한 스냅샷 보존 기간이 만료되지 않은 경우에는 유지 수 제한이 적용되지 않습니다.
- SnapMirror 관계에서 미러 볼트 정책 규칙에 보존 기간을 설정할 수 있으며 대상 볼륨에 스냅샷 잠금이 활성화된 경우 대상에 복제된 스냅샷에 보존 기간이 적용됩니다. 보존 기간이 유지 수보다 우선합니다. 예를 들어 만료 기간이 경과하지 않은 스냅샷은 유지 수를 초과하더라도 유지됩니다.
- 비 SnapLock 볼륨에서 스냅샷 이름을 바꿀 수 있습니다. SnapMirror 관계의 운영 볼륨에 대한 스냅샷 이름 바꾸기 작업은 정책이 MirrorAllSnapshots인 경우에만 보조 볼륨에 반영됩니다. 다른 정책 유형의 경우 이름이 바뀐 스냅샷은 업데이트 중에 전파되지 않습니다.
- ONTAP CLI를 사용하는 경우 잠긴 스냅샷이 가장 최근의 스냅샷인 경우에만 명령을 사용하여 잠긴 스냅샷을 복구할 수 `volume snapshot restore` 있습니다. 복구 중인 스냅샷보다 나중에 만료되지 않은 스냅샷이 있는 경우 스냅샷 복구 작업이 실패합니다.

변조 방지 스냅샷에서 지원되는 기능

- "Cloud Volumes ONTAP"

- FlexGroup 볼륨

  스냅샷 잠금은 FlexGroup 볼륨에 대해 지원됩니다. 스냅샷 잠금은 루트 구성 요소 스냅샷에서만 발생합니다. FlexGroup 볼륨은 루트 구성 요소 만료 시간이 경과한 경우에만 삭제할 수 있습니다.

- FlexVol에서 FlexGroup로의 변환

  잠긴 스냅샷이 있는 FlexVol volume를 FlexGroup 볼륨으로 변환할 수 있습니다. 변환 후에도 스냅샷은 잠긴 상태로 유지됩니다.

- SnapMirror 비동기

  소스와 대상 모두에서 컴플라이언스 클록을 초기화해야 합니다.

- SVM 데이터 이동성(소스 클러스터에서 타겟 클러스터로 SVM을 마이그레이션 또는 재배치하는 데 사용)

  ONTAP 9.14.1부터 지원됩니다.

- 를 사용하는 SnapMirror 정책 규칙입니다 `-schedule` 매개 변수
- SVM DR

  소스와 대상 모두에서 컴플라이언스 클록을 초기화해야 합니다.

- 볼륨 클론 및 파일 클론

  잠긴 스냅샷에서 볼륨 클론 및 파일 클론을 생성할 수 있습니다.

- FlexCache 볼륨

  ONTAP 9.16.1부터 지원됩니다.

지원되지 않는 기능입니다

다음 기능은 현재 변조 방지 스냅샷에서 지원되지 않습니다.

- 정합성 보장 그룹
- "FabricPool"

  변조 방지 스냅샷은 삭제할 수 없는 변경 불가능한 보호를 제공합니다. FabricPool에는 데이터 삭제 기능이 필요하므로 동일한 볼륨에서 FabricPool 및 스냅샷 잠금을 활성화할 수 없습니다.

- SMTape
- SnapMirror 활성 동기화
- SnapMirror 동기식

볼륨을 생성할 때 스냅샷 잠금을 설정합니다

ONTAP 9.12.1부터 새 볼륨을 생성할 때 또는 CLI에서 및 `volume modify` 명령의 옵션을 `volume create` 사용하여 기존 볼륨을 수정할 때 스냅샷 잠금을 설정할 수 있습니다 `-snapshot-locking-enabled`. ONTAP 9.13.1부터 System Manager를 사용하여 스냅샷 잠금을 설정할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동하고 * Add * 를 선택합니다.
2. Add Volume * (볼륨 추가 *) 창에서 * More Options * (추가 옵션 *)를 선택합니다.
3. 볼륨 이름, 크기, 엑스포트 정책 및 공유 이름을 입력합니다.
4. 스냅샷 잠금 사용 * 을 선택합니다. SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.
5. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
6. 변경 사항을 저장합니다.
7. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
8. SnapLock 스냅샷 잠금 * 이 * 사용 * 으로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 새 볼륨을 생성하고 스냅샷 잠금을 설정하려면 다음 명령을 입력합니다.

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   다음 명령을 실행하면 vol1이라는 새 볼륨에 대한 스냅샷 잠금이 설정됩니다.

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

기존 볼륨에 대한 스냅샷 잠금을 설정합니다

ONTAP 9.12.1부터 ONTAP CLI를 사용하여 기존 볼륨에 대한 스냅샷 잠금을 설정할 수 있습니다. ONTAP 9.13.1부터 System Manager를 사용하여 기존 볼륨에 대한 스냅샷 잠금을 설정할 수 있습니다.

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 ⋮ 선택하고 * 편집 > 볼륨 * 을 선택합니다.
3. 볼륨 편집 * 창에서 스냅샷(로컬) 설정 섹션을 찾아 * 스냅샷 잠금 활성화 * 를 선택합니다.

   SnapLock 라이센스가 설치되지 않은 경우에는 이 선택 항목이 표시되지 않습니다.

4. 아직 활성화되지 않은 경우 * SnapLock 준수 클럭 초기화 * 를 선택합니다.
5. 변경 사항을 저장합니다.
6. 볼륨 * 창에서 업데이트한 볼륨을 선택하고 * 개요 * 를 선택합니다.
7. * SnapLock 스냅샷 잠금*이 *활성화*로 표시되는지 확인합니다.

CLI를 참조하십시오

1. 기존 볼륨을 수정하여 스냅샷 잠금을 설정하려면 다음 명령을 입력합니다.

```
volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
-locking-enabled true
```

잠긴 스냅샷 정책을 생성하고 보존을 적용합니다

ONTAP 9.12.1부터 스냅샷 정책을 생성하여 스냅샷 보존 기간을 적용하고 볼륨에 정책을 적용하여 지정된 기간 동안 스냅샷을 잠글 수 있습니다. 보존 기간을 수동으로 설정하여 스냅샷을 잠글 수도 있습니다. ONTAP 9.13.1부터 System Manager를 사용하여 스냅샷 잠금 정책을 생성하여 볼륨에 적용할 수 있습니다.

스냅샷 잠금 정책을 생성합니다

시스템 관리자

1. 스토리지 > 스토리지 VM * 으로 이동하여 스토리지 VM을 선택합니다.
2. 설정 * 을 선택합니다.
3. Snapshot Policies * 를 찾아 선택합니다 →.
4. 스냅샷 정책 추가 * 창에서 정책 이름을 입력합니다.
5. 를 선택합니다 + Add .
6. 스케줄 이름, 유지할 최대 스냅샷 및 SnapLock 보존 기간을 포함한 스냅샷 스케줄 세부 정보를 제공합니다.
7. SnapLock 보존 기간 * 열에 스냅샷을 보존할 시간, 일, 월 또는 년 수를 입력합니다. 예를 들어 보존 기간이 5일인 스냅샷 정책은 스냅샷이 생성된 시점부터 5일 동안 스냅샷을 잠그며, 이 시간 동안에는 삭제할 수 없습니다. 다음과 같은 보존 기간 범위가 지원됩니다.
   - 연도: 0-100
   - 월: 0-1200
   - 일 수: 0 - 36500
   - 시간: 0-24
8. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 스냅샷 정책을 생성하려면 다음 명령을 입력합니다.

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   다음 명령을 실행하면 스냅샷 잠금 정책이 생성됩니다.

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   활성 보존 상태인 스냅샷은 대체되지 않습니다. 즉, 아직 만료되지 않은 잠긴 스냅샷이 있는 경우에는 보존 횟수가 유지되지 않습니다.

볼륨에 잠금 정책을 적용합니다

시스템 관리자

1. Storage > Volumes * 로 이동합니다.
2. 를 ⋮ 선택하고 * 편집 > 볼륨 * 을 선택합니다.
3. 볼륨 편집 * 창에서 * 스냅샷 예약 * 을 선택합니다.
4. 목록에서 스냅샷 잠금 정책을 선택합니다.
5. 스냅샷 잠금이 아직 활성화되지 않은 경우 * Enable snapshot locking * 을 선택합니다.
6. 변경 사항을 저장합니다.

CLI를 참조하십시오

1. 기존 볼륨에 스냅샷 잠금 정책을 적용하려면 다음 명령을 입력합니다.

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

수동 스냅샷 생성 중에 보존 기간을 적용합니다

스냅샷을 수동으로 생성할 때 스냅샷 보존 기간을 적용할 수 있습니다. 볼륨에 대해 스냅샷 잠금을 설정해야 합니다. 그렇지 않으면 보존 기간 설정이 무시됩니다.

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 * 탭을 선택합니다.
3. 를 선택합니다 + Add .
4. 스냅샷 이름과 SnapLock 만료 시간을 입력합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
5. 변경 사항을 저장합니다.
6. 볼륨 > 스냅샷 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 스냅샷을 수동으로 생성하고 잠금 보존 기간을 적용하려면 다음 명령을 입력합니다.

```
volume snapshot create -volume <volume_name> -snapshot <snapshot name>
-snaplock-expiry-time <expiration_date_time>
```

다음 명령을 실행하면 새 스냅샷이 생성되고 보존 기간이 설정됩니다.

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

시스템 관리자

1. Storage > Volumes * 로 이동하여 볼륨을 선택합니다.
2. 볼륨 세부 정보 페이지에서 * 스냅샷 * 탭을 선택합니다.
3. 스냅샷을 선택하고 를 선택한 다음 * SnapLock 만료 시간 수정 * 을 선택합니다. 보존 만료 날짜 및 시간을 선택할 달력을 선택할 수 있습니다.
4. 변경 사항을 저장합니다.
5. 볼륨 > 스냅샷 * 페이지에서 * 표시/숨기기 * 를 선택하고 * SnapLock 만료 시간 * 을 선택하여 * SnapLock 만료 시간 * 열을 표시하고 보존 시간이 설정되었는지 확인합니다.

CLI를 참조하십시오

1. 기존 스냅샷에 보존 기간을 수동으로 적용하려면 다음 명령을 입력합니다.

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   다음 예에서는 기존 스냅샷에 보존 기간을 적용합니다.

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

기존 정책을 수정하여 장기 보존을 적용합니다

SnapMirror 관계에서 미러 볼트 정책 규칙에 보존 기간을 설정할 수 있으며 대상 볼륨에 스냅샷 잠금이 활성화된 경우 대상에 복제된 스냅샷에 보존 기간이 적용됩니다. 보존 기간이 유지 수보다 우선합니다. 예를 들어 만료 기간이 경과하지 않은 스냅샷은 유지 수를 초과하더라도 유지됩니다.

ONTAP 9.14.1부터 스냅샷의 장기 보존을 설정하는 규칙을 추가하여 기존 SnapMirror 정책을 수정할 수 있습니다. 이 규칙은 SnapLock 소산 대상 및 비 SnapLock SnapMirror 대상 볼륨에서 기본 볼륨 보존 기간을 재정의하는 데 사용됩니다.

1. 기존 SnapMirror 정책에 규칙 추가:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   다음 예에서는 "LockVault"라는 기존 정책에 6개월의 보존 기간을 적용하는 규칙을 만듭니다.

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   에 대한 자세한 내용은 `snapmirror policy add-rule` "ONTAP 명령 참조입니다"을 참조하십시오.

정합성 보장 그룹

ONTAP 일관성 그룹에 대해 알아보세요

정합성 보장 그룹은 단일 유닛으로 관리되는 볼륨의 모음입니다. ONTAP에서 일관성 그룹을 사용하면 여러 볼륨에 걸쳐 있는 애플리케이션 워크로드를 손쉽게 관리하고 보호할 수 있습니다.

일관성 그룹을 사용하면 스토리지 관리를 간소화할 수 있습니다. 20개의 LUN을 아우르는 중요한 데이터베이스가 있다고 상상해 보십시오. LUN을 개별적으로 관리하거나 단일 정합성 보장 그룹으로 구성하여 LUN을 단일 데이터 세트로 처리할 수 있습니다.

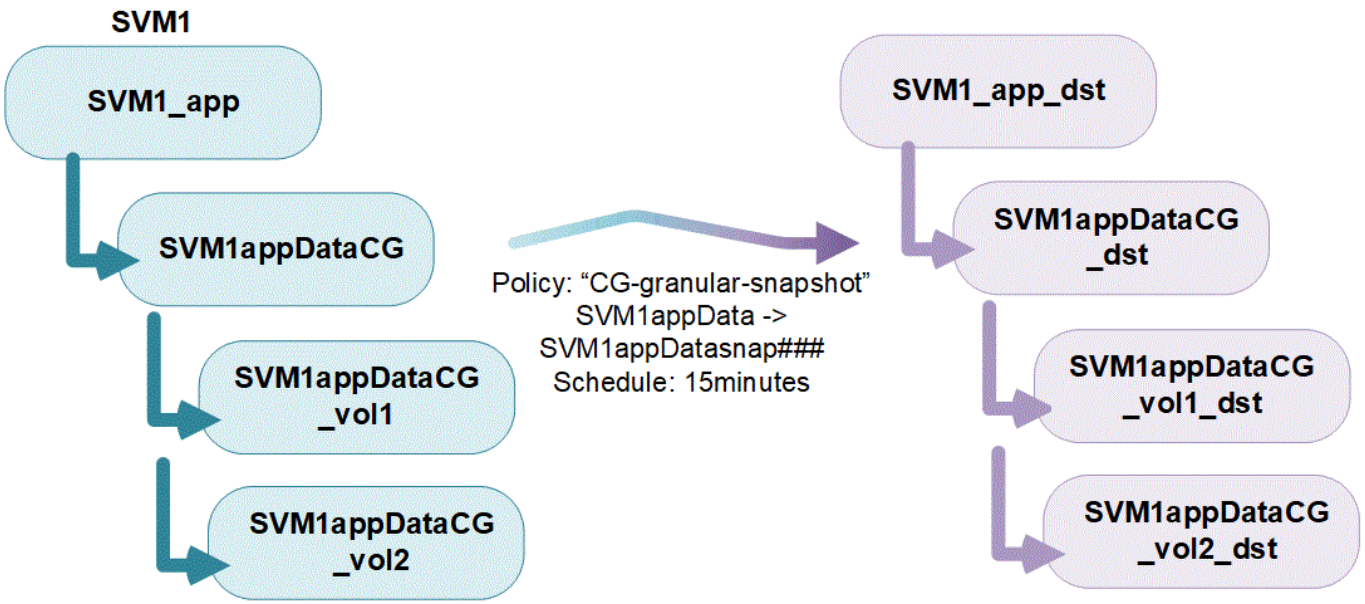
정합성 보장 그룹은 애플리케이션 워크로드 관리를 용이하게 하여, 쉽게 구성된 로컬 및 원격 보호 정책과 특정 시점에 볼륨 컬렉션에 대해 장애 발생 시 정합성이 보장되거나 애플리케이션 정합성이 보장되는 동시 스냅샷을 제공합니다. 일관성 그룹의 스냅샷을 사용하면 전체 애플리케이션 워크로드를 복구할 수 있습니다.

일관성 그룹에 대해 알아봅니다

일관성 그룹은 프로토콜(NAS, SAN 또는 NVMe)에 관계없이 모든 FlexVol 볼륨을 지원하며, ONTAP REST API를 통해 또는 System Manager의 * 스토리지 > 일관성 그룹 * 메뉴 항목에서 관리할 수 있습니다. ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹을 관리할 수 있습니다.

정합성 보장 그룹은 개별 엔터티(볼륨 컬렉션) 또는 다른 정합성 보장 그룹으로 구성된 계층적 관계로 존재할 수 있습니다. 개별 볼륨은 고유한 볼륨 세부 스냅샷 정책을 가질 수 있습니다. 또한 정합성 보장 그룹 전체의 스냅샷 정책이 있을 수 있습니다. 일관성 그룹에는 전체 일관성 그룹을 복구하는 데 사용할 수 있는 SnapMirror 활성 동기화 관계 및 공유 SnapMirror 정책이 하나만 있을 수 있습니다.

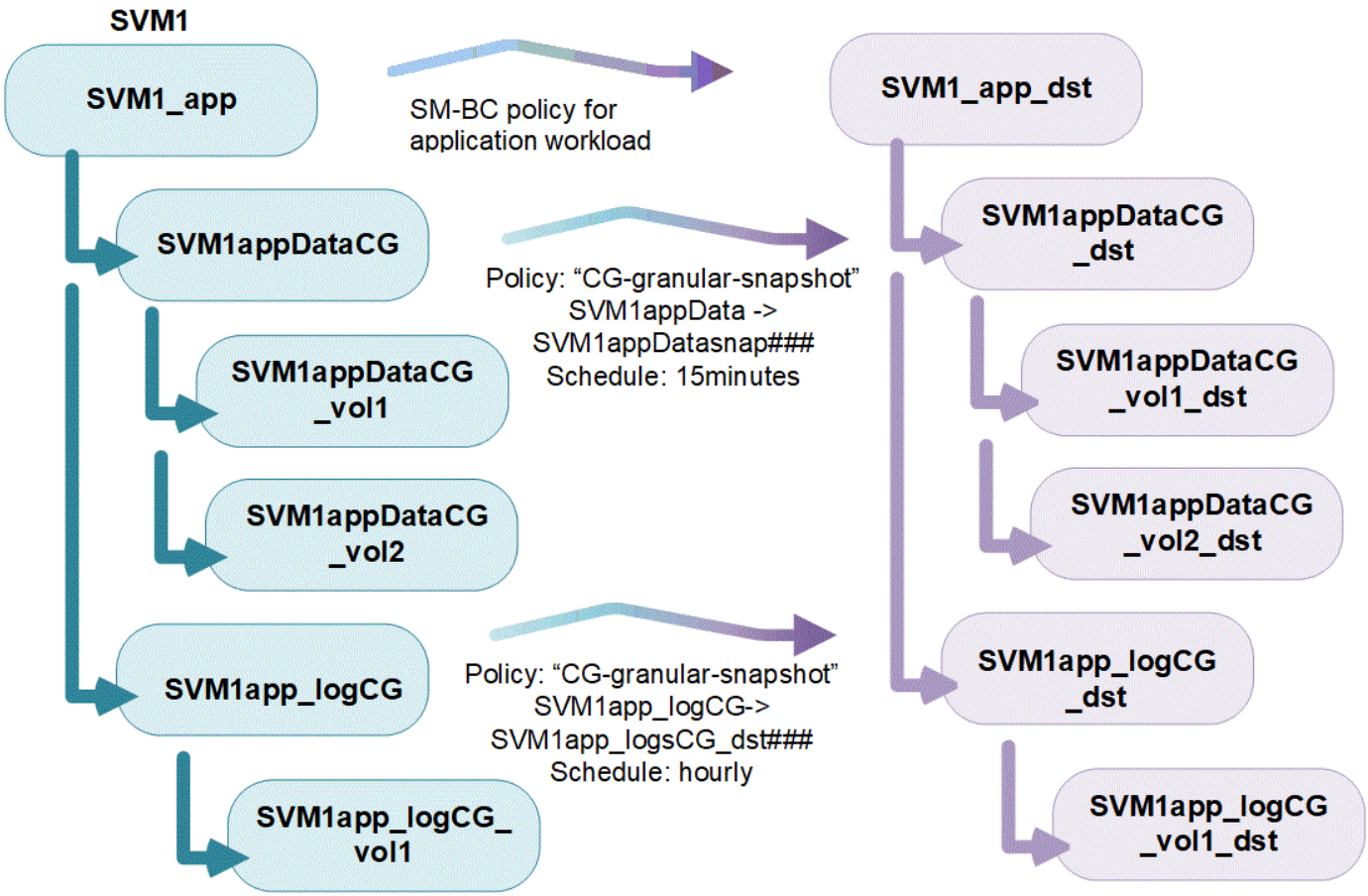
다음 다이어그램에서는 개별 일관성 그룹을 사용하는 방법을 보여 줍니다. 에서 호스팅되는 응용 프로그램의 데이터는 `SVM1` 및 의 두 볼륨에 걸쳐 `vol1` 있습니다. `vol2` 정합성 보장 그룹의 스냅샷 정책은 15분마다 데이터의 스냅샷을 캡처합니다.



애플리케이션 워크로드가 클수록 여러 개의 일관성 그룹이 필요할 수 있습니다. 이 경우 단일 일관성 그룹이 부모 일관성 그룹의 하위 구성요소가 되는 계층적 일관성 그룹을 생성할 수 있습니다. 상위 일관성 그룹에는 최대 5개의 하위 일관성 그룹이 포함될 수 있습니다. 개별 정합성 보장 그룹과 마찬가지로 원격 SnapMirror 활성 동기화 보호 정책을 정합성

보장 그룹(상위 및 하위)의 전체 구성에 적용하여 애플리케이션 워크로드를 복구할 수 있습니다.

다음 예제에서 응용 프로그램은 에서 호스팅됩니다. `SVM1` 관리자가 부모 일관성 그룹을 생성했으며 여기에는 `SVM1_app` 데이터와 `SVM1app_logCG` 로그에 대한 두 개의 하위 일관성 그룹이 `SVM1appDataCG` 포함됩니다. 각 하위 정합성 보장 그룹에는 고유한 스냅샷 정책이 있습니다. 의 볼륨 스냅샷은 `SVM1appDataCG` 15분마다 생성됩니다. 의 스냅샷은 `SVM1app_logCG` 매시간 생성됩니다. 부모 정합성 보장 그룹에는 `SVM1_app` 재해 발생 시 서비스를 지속할 수 있도록 데이터를 복제하는 SnapMirror 활성 동기화 정책이 있습니다.



ONTAP 9.12.1부터 정합성 보장 그룹이 지원됩니다 클론 복제 를 사용하여 정합성 보장 구성 구성원을 수정합니다 볼륨 추가 또는 제거 System Manager 및 ONTAP REST API 모두에서 ONTAP 9.12.1부터 ONTAP REST API는 다음을 지원합니다.

- 새 NFS 또는 SMB 볼륨 또는 NVMe 네임스페이스를 사용하여 일관성 그룹 생성
- 기존 일관성 그룹에 새 NFS 또는 SMB 볼륨 또는 NVMe 네임스페이스 추가

ONTAP REST API에 대한 자세한 내용은 를 참조하십시오 "ONTAP REST API 참조 설명서".

정합성 보장 그룹 모니터링

ONTAP 9.13.1부터 정합성 보장 그룹은 실시간 및 내역 용량과 성능 모니터링을 제공하여 애플리케이션 및 개별 정합성 보장 그룹의 성능에 대한 통찰력을 제공합니다.

모니터링 데이터는 5분마다 업데이트되고 최대 1년 동안 유지됩니다. 다음에 대한 메트릭을 추적할 수 있습니다.

- 성능: IOPS, 지연 시간, 처리량

- 용량: 크기, 사용된 논리적 용량, 사용 가능한 용량

System Manager의 정합성 보장 그룹 메뉴에 있는 개요 탭에서 모니터링 데이터를 보거나 REST API에 요청하여 모니터링 데이터를 볼 수 있습니다. ONTAP 9.14.1부터는 명령을 사용하여 CLI에서 일관성 그룹 메트릭을 볼 수 `consistency-group metrics show` 있습니다. 에 대한 자세한 내용은 `consistency-group metrics show` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 9.13.1에서는 REST API를 사용하여 기간별 메트릭만 검색할 수 있습니다. ONTAP 9.14.1부터 System Manager에서 기간별 메트릭을 사용할 수 있습니다.

일관성 그룹 보호

일관성 그룹은 애플리케이션 정합성 보장 보호 기능을 제공하여 여러 볼륨 또는 LIF 전체에서 데이터 정합성을 보장합니다. 일관성 그룹의 스냅샷을 생성할 때 일관성 그룹에 "fence"가 설정됩니다. 펜스는 스냅샷 작업이 완료될 때까지 입출력에 대한 대기열을 시작하여 정합성 보장 그룹의 모든 엔티티에서 데이터의 시점 정합성을 보장합니다. 펜스는 예약된 스냅샷 정책이나 System Manager를 사용하여 스냅샷 생성과 같은 스냅샷 생성 작업 중에 일시적으로 지연 시간이 급증할 수 있습니다. REST API 및 CLI 컨텍스트에 대한 자세한 내용은 및 를 "ONTAP REST API 설명서 ""ONTAP 명령 참조입니다"참조하십시오.

정합성 보장 그룹은 다음을 통해 보호 기능을 제공합니다.

- 스냅샷 정책
- SnapMirror 활성 동기화
- [mcc] (ONTAP 9.11.1부터)
- SnapMirror 비동기 (ONTAP 9.13.1부터)
- "SVM 재해 복구" (ONTAP 9.14.1부터)

일관성 그룹을 생성해도 보호가 자동으로 설정되지는 않습니다. 정합성 보장 그룹을 생성하거나 생성한 후에 로컬 및 원격 보호 정책을 설정할 수 있습니다.

일관성 그룹에 대한 보호를 구성하려면 를 참조하십시오 "일관성 그룹 보호".

원격 보호를 사용하려면 에 대한 요구 사항을 충족해야 SnapMirror 활성 동기화합니다.

NAS 액세스를 위해 마운트된 볼륨에 SnapMirror 활성 동기화 관계를 설정할 수 없습니다.

일관성 그룹에 대한 다중 관리자 검증 지원

ONTAP 9.16.1부터 정합성 보장 그룹에 대해 MAV(다중 관리자 검증)를 사용하여 지정된 관리자의 승인 후에만 일관성 그룹 생성, 수정 또는 삭제와 같은 특정 작업을 실행할 수 있습니다. 따라서 손상되었거나 악의적이거나 경험이 부족한 관리자가 기존 구성을 원하지 않는 방식으로 변경하지 못하게 됩니다.

"자세한 정보"

MetroCluster 구성의 일관성 그룹

ONTAP 9.11.1부터 MetroCluster 구성 내에서 클러스터의 새 볼륨에 정합성 보장 그룹을 프로비저닝할 수 있습니다. 이러한 볼륨은 미러링된 Aggregate에 프로비저닝됩니다.

볼륨이 프로비저닝되면 미러링된 Aggregate와 미러링되지 않은 애그리게이트 간에 일관성 그룹에 연결된 볼륨을 이동할 수 있습니다. 따라서 일관성 그룹에 연결된 볼륨은 미러링된 애그리게이트, 미러링되지 않은 애그리게이트 또는 둘 다에 위치할 수 있습니다. 일관성 그룹에 연결된 볼륨이 포함된 미러링된 애그리게이트를 수정하여 미러링되지 않은 상태로 만들 수 있습니다. 마찬가지로, 정합성 보장 그룹과 연결된 볼륨이 포함된 미러링되지 않은 애그리게이트를 수정하여 미러링을 활성화할 수 있습니다.

미러링된 애그리게이트에 배치된 일관성 그룹과 연결된 볼륨 및 스냅샷은 원격 사이트(사이트 B)에 복제됩니다. 사이트 B의 볼륨 콘텐츠는 정합성 보장 그룹에 대한 쓰기 순서 보증을 제공하므로 재해 발생 시 사이트 B에서 복구할 수 있습니다. ONTAP 9.11.1 이상을 실행하는 클러스터에서 REST API 및 System Manager의 일관성 그룹을 사용하여 일관성 그룹 스냅샷에 액세스할 수 있습니다. ONTAP 9.14.1부터 ONTAP CLI를 사용하여 스냅샷에 액세스할 수도 있습니다.

일관성 그룹에 연결된 볼륨 중 일부 또는 모두가 현재 액세스할 수 없는 미러링되지 않은 애그리게이트에 있는 경우, 일관성 그룹의 가져오기 또는 삭제 작업은 로컬 볼륨 또는 호스팅 애그리게이트가 오프라인 상태인 것처럼 동작합니다.

복제에 대한 정합성 보장 그룹 구성

사이트 B에서 ONTAP 9.10.1 이하 버전을 실행하는 경우 미러링된 Aggregate에 있는 일관성 그룹과 연결된 볼륨만 사이트 B에 복제됩니다 정합성 보장 그룹 구성은 두 사이트가 모두 ONTAP 9.11.1 이상을 실행하는 경우 사이트 B에만 복제됩니다. 사이트 B를 ONTAP 9.11.1로 업그레이드한 후 사이트 A의 정합성 보장 그룹에 대한 모든 관련 볼륨이 미러링된 Aggregate에 배치된 데이터가 사이트 B에 복제됩니다

> 최적의 스토리지 성능과 가용성을 위해 미러링된 집계에 최소 20%의 여유 공간을 유지하는 것이 좋습니다. 미러링되지 않은 집계의 경우 권장 사항은 10%이지만, 추가된 10%의 공간은 파일 시스템에서 증분 변경 사항을 흡수하는 데 사용될 수 있습니다. ONTAP의 쓰기 시 리디렉션 스냅샷 기반 아키텍처로 인해 증분적 변경으로 인해 미러링된 집계의 공간 활용도가 높아집니다. 이러한 모범 사례를 준수하지 않으면 성과에 부정적인 영향을 미칠 수 있습니다.

업그레이드 고려 사항

ONTAP 9 ONTAP 9 .8 및 9.9.1에서 SnapMirror 활성 동기화(이전의 SnapMirror 비즈니스 연속성)로 생성된 일관성 그룹은 자동으로 업그레이드되고 시스템 관리자 또는 ONTAP REST API의 * 스토리지 > 일관성 그룹 * 에서 관리할 수 있습니다. ONTAP 9 .8 또는 9.9.1에서 업그레이드하는 방법에 대한 자세한 내용은 을 참조하십시오."SnapMirror 활성 동기화 업그레이드 및 되돌리기 고려 사항"

REST API에서 생성된 정합성 보장 그룹 스냅샷은 System Manager의 정합성 보장 그룹 인터페이스와 정합성 보장 그룹 REST API 엔드포인트를 통해 관리할 수 있습니다. ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹 스냅샷을 관리할 수도 있습니다.

> ONTAPI 명령을 사용하여 생성된 스냅샷은 `cg-start` `cg-commit` 일관성 그룹 스냅샷으로 인식되지 않으므로 System Manager의 일관성 그룹 인터페이스 또는 ONTAP REST API의 일관성 그룹 엔드포인트를 통해 관리할 수 없습니다. ONTAP 9.14.1부터 SnapMirror 비동기 정책을 사용하는 경우 이러한 스냅샷을 대상 볼륨에 미러링할 수 있습니다. 자세한 내용은 을 SnapMirror 비동기 구성참조하십시오.

릴리즈별 지원 기능

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
계층적 일관성 그룹	✓	✓	✓	✓	✓	✓	✓
스냅샷을 통한 로컬 보호	✓	✓	✓	✓	✓	✓	✓

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
SnapMirror 활성 동기화	✓	✓	✓	✓	✓	✓	✓
MetroCluster 지원	✓	✓	✓	✓	✓	✓	
2단계 커밋(REST API만 해당)	✓	✓	✓	✓	✓	✓	
응용 프로그램 및 구성 요소 태그	✓	✓	✓	✓	✓		
클론 정합성 보장 그룹	✓	✓	✓	✓	✓		
볼륨 추가 및 제거	✓	✓	✓	✓	✓		
새 NAS 볼륨으로 CG를 생성합니다	✓	✓	✓	✓	REST API만 해당		
새로운 NVMe 네임스페이스를 사용하여 CG를 생성합니다	✓	✓	✓	✓	REST API만 해당		
하위 일관성 그룹 간에 볼륨을 이동합니다	✓	✓	✓	✓			
정합성 보장 그룹 지오메트리를 수정합니다	✓	✓	✓	✓			
모니터링	✓	✓	✓	✓			
다중 관리 검증	✓						
SnapMirror 비동기식(단일 일관성 그룹만 해당)	✓	✓	✓	✓			
SVM 재해 복구(단일 일관성 그룹만 해당)	✓	✓	✓				
CLI 지원	✓	✓	✓				

일관성 그룹에 대해 자세히 알아보십시오

관련 정보

- "ONTAP 자동화 설명서"
- SnapMirror 활성 동기화
- SnapMirror 비동기식 재해 복구 기본 사항
- "MetroCluster 설명서"
- "다중 관리 검증"
- "ONTAP 명령 참조입니다"

ONTAP 일관성 그룹 제한에 대해 알아보세요

일관성 그룹을 계획 및 관리할 때는 클러스터와 부모 또는 자식 일관성 그룹 모두의 범위에서 개체 제한을 고려합니다.

적용된 제한

다음 표에는 일관성 그룹의 제한이 나와 있습니다. SnapMirror 액티브 동기화를 사용하는 일관성 그룹에 대해서는 별도의 제한 사항이 적용됩니다. 자세한 내용은 을 참조하십시오 "SnapMirror 활성 동기화 제한".

제한	범위	최소	최대
정합성 보장 그룹 수입니다	클러스터	0	클러스터 * 의 최대 볼륨 수와 동일합니다
상위 일관성 그룹의 수입니다	클러스터	0	클러스터의 최대 볼륨 수와 동일합니다

개별 및 상위 일관성 그룹의 수입니다	클러스터	0	클러스터의 최대 볼륨 수와 동일합니다
일관성 그룹에 있는 볼륨의 수입니다	단일 일관성 그룹	볼륨 1개	80개 볼륨
비동기식 SnapMirror를 사용하는 일관성 그룹에 있는 볼륨 수입니다	단일 일관성 그룹	볼륨 1개	• ONTAP 9.15.1 이상: 80개 볼륨 • ONTAP 9.13.1 및 9.14.1:16 볼륨
상위 일관성 그룹의 하위 볼륨에 있는 볼륨 수입니다	부모 일관성 그룹	볼륨 1개	80개 볼륨
하위 일관성 그룹의 볼륨 수입니다	하위 일관성 그룹	볼륨 1개	80개 볼륨
부모 일관성 그룹에 있는 하위 일관성 그룹의 수입니다	부모 일관성 그룹	일관성 그룹 1개	5개의 일관성 그룹
일관성 그룹이 있는 SVM 재해 복구 관계의 수(ONTAP 9.14.1부터 사용 가능)	클러스터	0	32

* SnapMirror 비동기로 설정된 최대 50개의 일관성 그룹을 클러스터에서 호스팅할 수 있습니다.

시행되지 않은 제한

정합성 보장 그룹에 대해 지원되는 최소 스냅샷 스케줄은 30분입니다. 이는 "FlexGroup 볼륨 테스트"정합성 보장 그룹과 동일한 스냅샷 인프라를 공유하는 을 기반으로 합니다.

단일 **ONTAP** 일관성 그룹 구성

일관성 그룹은 ONTAP 버전에 따라 기존 볼륨 또는 새 LUN이나 볼륨으로 생성할 수 있습니다. 볼륨 또는 LUN은 한 번에 하나의 일관성 그룹에만 연결할 수 있습니다.

이 작업에 대해

- ONTAP 9.10.1 ~ 9.11.1에서는 일관성 그룹이 생성된 후 해당 그룹의 구성원 볼륨을 수정할 수 없습니다.

  ONTAP 9.12.1부터 일관성 그룹의 구성원 볼륨을 수정할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 참조하십시오 일관성 그룹 수정.

- ONTAP 9.17.1부터 SnapMirror Active Sync 구성에서 VMware 워크로드에 대한 호스트를 NVMe 하위 시스템에 매핑하기 위해 NVMe 프로토콜을 선택할 수 있습니다.

새 **LUN** 또는 볼륨이 있는 일관성 그룹을 생성합니다

ONTAP 9.10.1 ~ 9.12.1에서는 새 LUN을 사용하여 일관성 그룹을 생성할 수 있습니다. 또한 ONTAP 9.13.1부터 System Manager에서는 새로운 NVMe 네임스페이스 또는 새 NAS 볼륨으로 일관성 그룹을 생성할 수 있습니다. (ONTAP 9.12.1부터 시작되는 ONTAP REST API에서도 지원됩니다.)

시스템 관리자(**ONTAP 9.16.1** 및 이전 버전)

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.

   ONTAP 9.10.1 ~ 9.12.1에서 새 스토리지 객체에 대한 유일한 옵션은 새 **LUN** 사용 입니다. ONTAP 9.13.1부터 System Manager는 새로운 NVMe 네임스페이스와 새로운 NAS 볼륨이 있는 일관성 그룹을 생성할 수 있도록 지원합니다.

3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN의 수와 볼륨 또는 LUN당 용량을 지정합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하여 정합성 보장 그룹을 생성하려면 * 기타 * 를 사용해야 합니다.
   b. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   c. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   d. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
4. 보호 정책을 구성하거나 하위 일관성 그룹을 추가하거나 액세스 권한을 부여하려면 * 추가 옵션 * 을 선택합니다.
5. 저장 * 을 선택합니다.
6. 작업이 완료되면 표시되는 기본 정합성 보장 그룹 메뉴로 돌아가 정합성 보장 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하면 해당 정책, 원격 또는 로컬 아래에 녹색 방패 가 표시될 때 해당 정책이 적용되었음을 알 수 있습니다.

시스템 관리자(**ONTAP 9.17.1** 이상)

단계

1. *보호 > 일관성 그룹*을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.
3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN 수와 볼륨 또는 LUN당 용량을 지정합니다. 애플리케이션 유형: 애플리케이션 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 일관성 그룹에 기타 유형이 지정됩니다. 태그 일관성에 대해 자세히 알아보기 응용 프로그램 및 구성 요소 태그. 원격 보호 정책으로 일관성 그룹을 만들 계획이라면 *기타*를 사용해야 합니다
   a. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   b. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   c. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
4. 보호 정책을 구성하거나 하위 일관성 그룹을 추가하거나 액세스 권한을 부여하려면 * 추가 옵션 * 을 선택합니다.
5. 저장 * 을 선택합니다.
6. 작업이 완료되면 표시되는 기본 정합성 보장 그룹 메뉴로 돌아가 정합성 보장 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하면 해당 정책, 원격 또는 로컬 아래에 녹색 방패 가 표시될 때 해당 정책이 적용되었음을 알 수 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 새 볼륨으로 새로운 일관성 그룹을 생성할 수 있습니다. 특정 매개 변수는 볼륨이 SAN, NVMe 또는 NFS 볼륨에 따라 다릅니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

NFS 볼륨으로 일관성 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

SAN 볼륨으로 정합성 보장 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

NVMe 네임스페이스로 일관성 그룹을 생성합니다

1. 정합성 보장 그룹을 생성합니다.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

모두 끝냈군요

1. 를 사용하여 일관성 그룹이 생성되었는지 확인합니다 `consistency-group show` 명령.

에 대한 자세한 내용은 `consistency-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 볼륨이 있는 일관성 그룹을 생성합니다

기존 볼륨을 사용하여 일관성 그룹을 생성할 수 있습니다.

시스템 관리자(**ONTAP 9.16.1** 및 이전 버전)

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. * + 추가 * 를 선택한 다음 * 기존 볼륨 사용 * 을 선택합니다.
3. 일관성 그룹의 이름을 지정하고 스토리지 VM을 선택합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 일관성 그룹에 SnapMirror 액티브 동기화 관계가 있는 경우 * 기타 * 를 사용해야 합니다.

   ⓘ ONTAP 9.15.1 이전의 ONTAP 버전에서는 SnapMirror 액티브 동기화를 SnapMirror 비즈니스 연속성이라고 합니다.

4. 포함할 기존 볼륨을 선택합니다. 정합성 보장 그룹에 아직 포함되지 않은 볼륨만 선택할 수 있습니다.

   ⓘ 기존 볼륨으로 일관성 그룹을 생성하는 경우 일관성 그룹은 FlexVol 볼륨을 지원합니다. 또는 SnapMirror 동기식 또는 SnapMirror 비동기식 관계가 있는 볼륨을 일관성 그룹에 추가할 수 있지만 일관성 그룹을 인식하지 않습니다. 일관성 그룹은 S3 버킷 또는 SVMDR 관계가 있는 스토리지 VM을 지원하지 않습니다.

5. 저장 * 을 선택합니다.
6. ONTAP 작업이 완료된 후 표시되는 기본 일관성 그룹 메뉴로 돌아가서 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 선택한 경우 메뉴에서 일관성 그룹을 선택하여 정책이 올바르게 설정되었는지 확인합니다. 보호 정책을 설정하는 경우 해당 정책(원격 또는 로컬)에서 찾기에 녹색 실드가 표시되면 해당 정책이 적용되었음을 알 수 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 기존 볼륨과 함께 일관성 그룹을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 를 발행합니다 `consistency-group create` 명령. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 를 사용하여 일관성 그룹을 확인합니다 `consistency-group show` 명령.

   에 대한 자세한 내용은 `consistency-group show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 일관성 그룹 보호
- 일관성 그룹 수정
- 일관성 그룹의 클론을 생성합니다

계층적 **ONTAP** 일관성 그룹 구성

계층적 일관성 그룹을 사용하여 여러 볼륨에 걸쳐 있는 대규모 워크로드를 관리할 수 있으므로 하위 일관성 그룹에 대한 우산 역할을 하는 부모 일관성 그룹을 생성할 수 있습니다.

계층적 일관성 그룹에는 최대 5개의 개별 일관성 그룹을 포함할 수 있는 부모가 있습니다. 계층적 정합성 보장 그룹은 정합성 보장 그룹 또는 개별 볼륨에 걸쳐 서로 다른 로컬 스냅샷 정책을 지원할 수 있습니다. 원격 보호 정책을 사용하는 경우 전체 계층 일관성 그룹(상위 및 하위)에 적용됩니다.

ONTAP 9.13.1부터 가능합니다 일관성 그룹의 구조를 수정합니다 및 하위 일관성 그룹 간에 볼륨을 이동합니다.

일관성 그룹의 개체 제한은 를 참조하십시오 일관성 그룹에 대한 개체 제한.

새 **LUN** 또는 볼륨이 있는 계층적 일관성 그룹을 생성합니다

계층적 일관성 그룹을 생성할 때 새 LUN으로 이를 채울 수 있습니다. ONTAP 9.13.1부터 새로운 NVMe 네임스페이스와 NAS 볼륨을 사용할 수도 있습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. Add * 를 선택한 다음 스토리지 객체에 대한 프로토콜을 선택합니다.

   ONTAP 9.10.1 ~ 9.12.1에서 새 스토리지 객체에 대한 유일한 옵션은 새 **LUN** 사용 입니다. ONTAP 9.13.1부터 System Manager는 새로운 NVMe 네임스페이스와 새로운 NAS 볼륨이 있는 일관성 그룹을 생성할 수 있도록 지원합니다.

3. 일관성 그룹의 이름을 지정합니다. 볼륨 또는 LUN의 수와 볼륨 또는 LUN당 용량을 지정합니다.
   a. 응용 프로그램 유형: ONTAP 9.12.1 이상을 사용하는 경우 응용 프로그램 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하려는 경우 * 기타 * 를 선택해야 합니다.
4. 호스트 운영 체제 및 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   a. 새 LUN**: 호스트 운영 체제와 LUN 형식을 선택합니다. 호스트 이니시에이터 정보를 입력합니다.
   b. 새 **NAS** 볼륨: SVM의 NAS 구성에 따라 적절한 내보내기 옵션(NFS 또는 SMB/CIFS)을 선택합니다.
   c. 새 NVMe 네임스페이스**: 호스트 운영 체제와 NVMe 하위 시스템을 선택합니다.
5. 하위 일관성 그룹을 추가하려면 * 더 많은 옵션 * 을 선택한 다음 * + 하위 일관성 그룹 추가 * 를 선택합니다.
6. LUN 또는 볼륨당 성능 수준, LUN 또는 볼륨 수, 용량을 선택합니다. 사용 중인 프로토콜에 따라 적절한 내보내기 구성 또는 운영 체제 정보를 지정합니다.
7. 필요에 따라 로컬 스냅샷 정책을 선택하고 액세스 권한을 설정합니다.
8. 최대 5개의 하위 일관성 그룹에 대해 반복합니다.
9. 저장 * 을 선택합니다.
10. ONTAP 작업이 완료되면 표시되는 기본 일관성 그룹 메뉴로 돌아가 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 설정하는 경우 해당 정책, 원격 또는 로컬 아래에서 녹색 차폐가 체크 표시와 함께 표시되어야 합니다.

CLI를 참조하십시오

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

CLI에서 새 볼륨으로 계층적 정합성 보장 그룹을 생성할 때는 각 하위 정합성 보장 그룹을 개별적으로 생성해야 합니다.

단계

1. 를 사용하여 새 일관성 그룹을 생성합니다 `consistency-group create` 명령.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
```

```
-count <number_of_volumes> -size <size>
```

2. CLI에서 메시지가 표시되면 새 부모 일관성 그룹을 생성할지 확인합니다. 를 `y`입력합니다.
3. 필요한 경우 1단계를 반복하여 하위 정합성 보장 그룹을 추가로 생성합니다.

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

기존 볼륨을 포함하는 계층적 일관성 그룹을 생성합니다

기존 볼륨을 계층적 일관성 그룹으로 구성할 수 있습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. * + 추가 * 를 선택한 다음 * 기존 볼륨 사용 * 을 선택합니다.
3. 스토리지 VM을 선택합니다.
4. 포함할 기존 볼륨을 선택합니다. 정합성 보장 그룹에 아직 포함되지 않은 볼륨만 선택할 수 있습니다.
5. 하위 일관성 그룹을 추가하려면 * + 하위 일관성 그룹 추가 * 를 선택합니다. 필요한 일관성 그룹을 생성합니다. 이 그룹의 이름은 자동으로 지정됩니다.
   a. 구성 요소 유형: ONTAP 9.12.1 이상을 사용하는 경우 "data", "logs" 또는 "other"의 구성 요소 유형을 선택합니다. 값을 선택하지 않으면 기본적으로 정합성 보장 그룹에 기타 유형이 할당됩니다. 에서 일관성 태그 지정에 대해 자세히 알아보십시오 응용 프로그램 및 구성 요소 태그. 원격 보호 정책을 사용하려는 경우 * 기타 * 를 사용해야 합니다.
6. 각 일관성 그룹에 기존 볼륨을 할당합니다.
7. 필요한 경우 로컬 스냅샷 정책을 선택합니다.
8. 최대 5개의 하위 일관성 그룹에 대해 반복합니다.
9. 저장 * 을 선택합니다.
10. ONTAP 작업이 완료되면 표시되는 기본 일관성 그룹 메뉴로 돌아가 일관성 그룹이 생성되었는지 확인합니다. 보호 정책을 선택한 경우 메뉴에서 정합성 보장 그룹을 선택하여 정책이 올바르게 설정되었는지 확인합니다. 해당 정책 유형 아래에 녹색 차폐가 있고 확인 표시가 있습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 계층적 일관성 그룹을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 새 부모 정합성 보장 그룹을 프로비저닝하고 새 하위 정합성 보장 그룹에 볼륨을 할당합니다.

```
consistency-group create -vserver <svm_name> -consistency-group
<child_consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volumes <volume_names>
```

2. 를 입력합니다 `y` 새 부모 및 자식 일관성 그룹을 생성하려면 다음을 수행합니다.

   에 대한 자세한 내용은 `consistency-group create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 일관성 그룹의 구조를 수정합니다
- 일관성 그룹 수정

- 일관성 그룹 보호

ONTAP 일관성 그룹 보호

일관성 그룹은 여러 볼륨에 걸쳐 있는 SAN, NAS 및 NVMe 애플리케이션에 대해 쉽게 관리되는 로컬 및 원격 보호를 제공합니다.

일관성 그룹을 생성해도 보호가 자동으로 설정되지는 않습니다. 보호 정책은 생성 시 또는 일관성 그룹을 생성한 후에 설정할 수 있습니다. 다음을 사용하여 일관성 그룹을 보호할 수 있습니다.

- 로컬 스냅샷
- SnapMirror 액티브 동기화(9.15.1 이전의 ONTAP 버전에서는 SnapMirror 비즈니스 연속성이라고 함)
- MetroCluster(9.11.1부터)
- SnapMirror 비동기식(9.13.1부터)
- 비동기식 SVM 재해 복구(9.14.1부터)

중첩된 일관성 그룹을 사용하는 경우 상위 및 하위 일관성 그룹에 대해 서로 다른 보호 정책을 설정할 수 있습니다.

ONTAP 9.11.1부터 정합성 보장 그룹이 2단계 정합성 보장 그룹 스냅샷 생성제공합니다. 2단계 스냅샷 작업은 사전 검사를 실행하여 스냅샷이 성공적으로 캡처되었는지 확인합니다.

전체 정합성 보장 그룹, 계층적 구성의 단일 정합성 보장 그룹 또는 정합성 보장 그룹 내의 개별 볼륨에 대해 복구가 수행될 수 있습니다. 복구할 정합성 보장 그룹을 선택하고 스냅샷 유형을 선택한 다음 복구를 기반으로 할 스냅샷을 식별하여 복구할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 "이전 스냅샷에서 볼륨을 복원합니다"참조하십시오.

로컬 스냅샷 정책을 구성합니다

로컬 스냅샷 보호 정책을 설정하면 정합성 보장 그룹의 모든 볼륨을 포괄하는 정책을 생성할 수 있습니다.

이 작업에 대해

정합성 보장 그룹에 대해 지원되는 최소 스냅샷 스케줄은 30분입니다. 이는 "FlexGroup 볼륨 테스트"정합성 보장 그룹과 동일한 스냅샷 인프라를 공유하는 을 기반으로 합니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
3. 일관성 그룹의 개요 페이지 오른쪽 위에서 * 편집 * 을 선택합니다.
4. 스냅샷 예약(로컬) 옆에 있는 상자를 선택하세요.
5. 스냅샷 정책을 선택합니다. 새 사용자 지정 정책을 구성하려면 을 "사용자 지정 데이터 보호 정책을 생성합니다"참조하십시오.
6. 저장 * 을 선택합니다.
7. 일관성 그룹 개요 메뉴로 돌아갑니다. 왼쪽 열의 * Snapshots (Local) * 아래에서 상태는 옆에 보호됨으로 표시됩니다. 

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹의 보호 정책을 수정할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 다음 명령을 실행하여 보호 정책을 설정하거나 수정합니다.

   하위 정합성 보장의 보호 정책을 수정하는 경우 를 사용하여 부모 정합성 보장 그룹을 식별해야 합니다 `-parent-consistency-group` *`parent_consistency_group_name`* 매개 변수.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

필요 시 스냅샷을 생성합니다

일반적으로 예약된 정책 외에 일관성 그룹의 스냅샷을 생성해야 하는 경우 필요에 따라 생성할 수 있습니다.

시스템 관리자

단계

1. 스토리지 * > * Consistency groups * 로 이동합니다.
2. 필요 시 스냅샷을 생성할 정합성 보장 그룹을 선택합니다.
3. Snapshot 복사본 * 탭으로 전환한 다음 * + 추가 * 를 선택합니다.
4. 이름 * 및 * SnapMirror 레이블 * 을 제공하십시오. 정합성 * 드롭다운 메뉴에서 * 애플리케이션 정합성 * 또는 * 충돌 정합성 보장 * 을 선택합니다.
5. 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹의 주문형 스냅샷을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 스냅샷 생성:

   기본적으로 스냅샷 유형은 충돌 일치입니다. 선택적 매개 변수를 사용하여 스냅샷 유형을 수정할 수 `-type` 있습니다.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

2단계 정합성 보장 그룹 스냅샷을 생성합니다

ONTAP 9.11.1부터 일관성 그룹은 CG(정합성 보장 그룹) 스냅샷 생성을 위한 2단계 커밋을 지원하며, 이 커밋은 스냅샷을 커밋하기 전에 사전 점검을 실행합니다. 이 기능은 ONTAP REST API에서만 사용할 수 있습니다.

2단계 CG 스냅샷 생성은 정합성 보장 그룹을 프로비저닝하거나 정합성 보장 그룹을 복구하는 것이 아니라 스냅샷 생성에만 사용할 수 있습니다.

2단계 CG 스냅샷은 스냅샷 생성 프로세스를 다음 두 단계로 나눕니다.

1. 첫 번째 단계에서는 API가 사전 검사를 실행하고 스냅샷 생성을 트리거합니다. 첫 번째 단계에는 스냅샷이 성공적으로 커밋될 시간을 지정하는 시간 제한 매개 변수가 포함됩니다.
2. 1단계의 요청이 성공적으로 완료되면 첫 번째 단계에서 지정된 간격 내에 두 번째 단계를 호출하여 스냅샷을 적절한 끝점에 커밋할 수 있습니다.

시작하기 전에

- 2단계 CG 스냅샷 생성을 사용하려면 클러스터의 모든 노드에서 ONTAP 9.11.1 이상을 실행해야 합니다.
- 정합성 보장 그룹 스냅샷 작업의 활성 호출은 한 번에 하나의 정합성 보장 그룹 인스턴스에서만 지원됩니다(1단계 또는 2단계). 다른 작업이 진행 중인 동안 스냅샷 작업을 호출하려고 하면 오류가 발생합니다.

- 스냅샷 생성을 호출할 때 옵션 시간 초과 값을 5초에서 120초 사이로 설정할 수 있습니다. 시간 초과 값을 제공하지 않으면 기본 값인 7초로 작업이 시간 초과됩니다. API에서 매개 변수를 사용하여 시간 초과 값을 `action_timeout` 설정합니다. CLI에서 `-timeout` 플래그를 사용합니다.

단계

REST API 또는 ONTAP 9.14.1부터 ONTAP CLI를 사용하여 2단계 스냅샷을 완료할 수 있습니다. 이 작업은 System Manager에서 지원되지 않습니다.

> API를 사용하여 스냅샷 생성을 호출하는 경우 API를 사용하여 스냅샷을 커밋해야 합니다. CLI를 사용하여 스냅샷 생성을 호출하는 경우 CLI를 사용하여 스냅샷을 커밋해야 합니다. 혼합 방법은 지원되지 않습니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 2단계 스냅샷을 생성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 스냅샷을 시작합니다.

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. 스냅샷이 생성되었는지 확인합니다.

   ```
   consistency-group snapshot show
   ```

3. 스냅샷 커밋:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API를 참조하십시오

1. 스냅샷 생성을 호출합니다. 매개 변수를 사용하여 정합성 보장 그룹 끝점에 POST 요청을 `action=start` 보냅니다.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. POST 요청이 성공하면 출력에 snapshot uid가 포함됩니다. 해당 uuid를 사용하여 스냅샷을 커밋할 패치 요청을 제출합니다.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

정합성 보장 그룹에 대한 원격 보호를 설정합니다

정합성 보장 그룹은 SnapMirror Active Sync 및 ONTAP 9.13.1, SnapMirror Asynchronous를 통해 원격 보호를 제공합니다.

SnapMirror 활성 동기화로 보호를 구성합니다

SnapMirror 활성 동기화를 사용하여 정합성 보장 그룹에 생성된 정합성 보장 그룹의 스냅샷이 대상으로 복제되도록 할 수 있습니다. SnapMirror 활성 동기화에 대한 자세한 내용 또는 CLI를 사용하여 SnapMirror 활성 동기화를 구성하는 방법에 대한 자세한 내용은 을 참조하십시오.무중단 업무 운영을 위한 보호 구성

시작하기 전에

- NAS 액세스를 위해 마운트된 볼륨에 SnapMirror 활성 동기화 관계를 설정할 수 없습니다.
- 소스 및 대상 클러스터의 정책 레이블이 일치해야 합니다.
- SnapMirror 활성 동기화는 SnapMirror 레이블이 있는 규칙이 미리 정의된 정책에 추가되고 해당 레이블을 사용하여 스냅샷이 생성되지 않는 한 스냅샷을 기본적으로 복제하지 않습니다. `AutomatedFailOver`

  이 프로세스에 대한 자세한 내용은 을 참조하십시오 "SnapMirror 액티브 동기화로 보호".

- 다중 구간 구축 SnapMirror 액티브 동기화에서는 지원되지 않습니다.
- ONTAP 9.13.1부터 무중단으로 업그레이드할 수 있습니다 볼륨을 일관성 그룹에 추가합니다 활성 SnapMirror 활성 동기화 관계가 있습니다. 일관성 그룹에 대한 다른 변경 사항은 SnapMirror 활성 동기화 관계를 해제하고 일관성 그룹을 수정한 다음 관계를 다시 설정하고 재동기화해야 합니다.

CLI를 사용하여 SnapMirror 활성 동기화를 구성하려면 를 참조하십시오 SnapMirror 액티브 동기화로 보호.

System Manager를 위한 단계

1. 을(를) 충족하는지 확인합니다 "SnapMirror 액티브 동기화 사용을 위한 사전 요구사항".
2. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
3. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
4. 개요 페이지 오른쪽 상단에서 * 자세히 * 를 선택한 다음 * 보호 * 를 선택합니다.
5. System Manager는 소스 측 정보를 자동으로 채웁니다. 대상에 적합한 클러스터 및 스토리지 VM을 선택합니다.

보호 정책을 선택합니다. Initialize relationship * 이 선택되어 있는지 확인합니다.

6. 저장 * 을 선택합니다.
7. 정합성 보장 그룹을 초기화하고 동기화해야 합니다. 정합성 보장 그룹 * 메뉴로 돌아가 동기화가 성공적으로 완료되었는지 확인합니다. SnapMirror (원격) * 상태가 `Protected` 옆에 표시됩니다.

SnapMirror 비동기 구성

ONTAP 9.13.1부터 단일 일관성 그룹에 대해 SnapMirror 비동기식 보호를 구성할 수 있습니다. ONTAP 9.14.1부터 SnapMirror 비동기식을 사용하여 일관성 그룹 관계를 사용하여 볼륨 세분화 스냅샷을 타겟 클러스터에 복제할 수 있습니다.

이 작업에 대해

볼륨 세분화 스냅샷을 복제하려면 ONTAP 9.14.1 이상을 실행해야 합니다. MirrorAndVault 및 Vault 정책의 경우, 볼륨 세분화 스냅샷 정책의 SnapMirror 레이블은 일관성 그룹의 SnapMirror 정책 규칙과 일치해야 합니다. 볼륨 세분화 스냅샷은 일관성 그룹 스냅샷과 관계없이 계산되는 일관성 그룹의 SnapMirror 정책의 Keep 값을 준수합니다. 예를 들어 대상에 두 개의 스냅샷을 유지하는 정책이 있는 경우 볼륨 세분화 스냅샷 두 개와 정합성 보장 그룹 스냅샷 두 개를 만들 수 있습니다.

SnapMirror 관계를 볼륨 세분화 스냅샷과 재동기화할 때 플래그로 볼륨 세분화 스냅샷을 보존할 수 `-preserve` 있습니다. 정합성 보장 그룹 스냅샷보다 최신 볼륨 세분화 스냅샷은 보존됩니다. 정합성 보장 그룹 스냅샷이 없는 경우 재동기화 작업에서 볼륨 세분화 스냅샷을 전송할 수 없습니다.

시작하기 전에

- SnapMirror 비동기식 보호는 단일 일관성 그룹에만 사용할 수 있습니다. 계층적 일관성 그룹에는 지원되지 않습니다. 계층적 일관성 그룹을 단일 일관성 그룹으로 변환하려면 을 참조하십시오 정합성 보장 그룹 아키텍처 수정.
- 소스 및 대상 클러스터의 정책 레이블이 일치해야 합니다.
- 무중단으로 확장 가능합니다 볼륨을 일관성 그룹에 추가합니다 활성 SnapMirror 비동기식 관계를 통해 원격 백업 기능을 지원합니다. 일관성 그룹이 변경되면 SnapMirror 관계를 중단시키고 일관성 그룹을 수정한 다음, 관계를 다시 설정하고 다시 동기화해야 합니다.
- SnapMirror 비동기 사용 시 보호되도록 설정된 일관성 그룹에는 제한 사항이 다릅니다. 자세한 내용은 을 참조하십시오 정합성 보장 그룹 제한.
- 여러 개별 볼륨에 대해 SnapMirror 비동기식 보호 관계를 구성한 경우 기존 스냅샷을 유지하면서 해당 볼륨을 정합성 보장 그룹으로 변환할 수 있습니다. 볼륨을 성공적으로 변환하려면 다음을 수행합니다.
  - 볼륨의 공통 스냅샷이 있어야 합니다.
  - 기존 SnapMirror 관계를 해제해야 합니다. 단일 일관성 그룹에 볼륨을 추가합니다그런 다음 다음 다음 다음 워크플로를 사용하여 관계를 다시 동기화합니다.

단계

1. 대상 클러스터에서 * 스토리지 > 일관성 그룹 * 을 선택합니다.
2. 정합성 보장 그룹 메뉴에서 생성한 정합성 보장 그룹을 선택합니다.
3. 개요 페이지 오른쪽 상단에서 * 자세히 * 를 선택한 다음 * 보호 * 를 선택합니다.
4. System Manager는 소스 측 정보를 자동으로 채웁니다. 대상에 적합한 클러스터 및 스토리지 VM을 선택합니다. 보호 정책을 선택합니다. Initialize relationship * 이 선택되어 있는지 확인합니다.

   비동기 정책을 선택할 때 전송 일정 재정의 옵션을 사용할 수 있습니다.

SnapMirror 비동기식을 사용하는 일관성 그룹에서 지원되는 최소 일정(복구 시점 목표 또는 RPO)은 30분입니다.

5. 저장 * 을 선택합니다.
6. 정합성 보장 그룹을 초기화하고 동기화해야 합니다. 정합성 보장 그룹 * 메뉴로 돌아가 동기화가 성공적으로 완료되었는지 확인합니다. SnapMirror (원격) * 상태가 `Protected` 옆에 표시됩니다.

SVM 재해 복구 구성

ONTAP 9.14.1부터 는 SVM 재해 복구일관성 그룹을 지원하므로 일관성 그룹 정보를 소스에서 타겟 클러스터로 미러링할 수 있습니다.

이미 일관성 그룹이 포함된 SVM에서 SVM 재해 복구를 사용하도록 설정하려면 의 SVM 구성 워크플로우를 따릅니다 시스템 관리자 또는 을 누릅니다 ONTAP CLI를 참조하십시오.

활성 및 정상 상태의 SVM 재해 복구 관계에 있는 SVM에 일관성 그룹을 추가하려면 대상 클러스터에서 SVM 재해 복구 관계를 업데이트해야 합니다. 자세한 내용은 을 참조하십시오 복제 관계를 수동으로 업데이트합니다. 일관성 그룹을 확장할 때는 언제든지 관계를 업데이트해야 합니다.

제한 사항

- SVM 재해 복구는 계층적 일관성 그룹을 지원하지 않습니다.
- SVM 재해 복구는 비동기식 SnapMirror로 보호되는 일관성 그룹을 지원하지 않습니다. SVM 재해 복구를 구성하기 전에 SnapMirror 관계를 해제해야 합니다.
- 두 클러스터에서 모두 ONTAP 9.14.1 이상을 실행해야 한다.
- 일관성 그룹이 포함된 SVM 재해 복구 구성에는 팬아웃 관계가 지원되지 않습니다.
- 기타 제한 사항은 를 참조하십시오 정합성 보장 그룹 제한.

관계를 시각화합니다

System Manager는 * Protection > Relationships * 메뉴에서 LUN 맵을 시각화합니다. 소스 관계를 선택하면 System Manager에서 소스 관계를 시각화합니다. 볼륨을 선택하면 이러한 관계를 자세히 살펴보고 포함된 LUN 및 이니시에이터 그룹 관계의 목록을 볼 수 있습니다. 이 정보는 개별 볼륨 보기에서 Excel 통합 문서로 다운로드할 수 있으며 다운로드 작업은 백그라운드에서 실행됩니다.

관련 정보

- "일관성 그룹의 클론을 생성합니다"
- "스냅샷을 구성합니다"
- "사용자 지정 데이터 보호 정책을 생성합니다"
- "스냅샷에서 복구합니다"
- "이전 스냅샷에서 볼륨을 복원합니다"
- "SnapMirror Active Sync 개요"
- "ONTAP 자동화 설명서"
- SnapMirror 비동기식 재해 복구 기본 사항

ONTAP 일관성 그룹의 멤버 볼륨 수정

ONTAP 9.12.1부터 볼륨을 제거하거나 볼륨을 추가(정합성 보장 그룹 확장)하여 정합성 보장 그룹을 수정할 수 있습니다. ONTAP 9.13.1부터 하위 정합성 보장 그룹이 공통 부모를 공유하는 경우 볼륨을 이동할 수 있습니다.

볼륨을 일관성 그룹에 추가합니다

ONTAP 9.12.1부터는 일관성 그룹에 볼륨을 무중단으로 추가할 수 있습니다.

이 작업에 대해

- 다른 일관성 그룹에 연결된 볼륨은 추가할 수 없습니다.
- 일관성 그룹은 NAS, SAN 및 NVMe 프로토콜을 지원합니다.
- 조정이 전체 내에 있는 경우 일관성 그룹에 한 번에 최대 16개의 볼륨을 추가할 수 있습니다 정합성 보장 그룹 제한.
- ONTAP 9.13.1부터 활성 SnapMirror 활성 동기화 또는 SnapMirror 비동기 보호 정책을 사용하여 운영 중단 없이 일관성 그룹에 볼륨을 추가할 수 있습니다.
- SnapMirror 액티브 동기화로 보호되는 일관성 그룹에 볼륨을 추가하면 새 볼륨에 대해 미러링 및 보호가 구성될 때까지 SnapMirror 액티브 동기화 관계 상태가 "확장"으로 변경됩니다. 이 프로세스가 완료되기 전에 운영 클러스터에서 재해가 발생하면 페일오버 작업의 일부로 정합성 보장 그룹이 원래 구성으로 되돌아갑니다.
- ONTAP 9.12.1 이하 버전에서는 SnapMirror 활성 동기화 관계의 일관성 그룹에 볼륨을 추가할 수 _ 없습니다. 먼저 SnapMirror 액티브 동기화 관계를 삭제하고 일관성 그룹을 수정한 다음 SnapMirror 액티브 동기화로 보호를 복원해야 합니다.
- ONTAP 9.12.1부터 ONTAP REST API는 정합성 보장 그룹에 *new* 또는 기존 볼륨을 추가할 수 있도록 지원합니다. ONTAP REST API에 대한 자세한 내용은 를 참조하십시오 "ONTAP REST API 참조 설명서".

  ONTAP 9.13.1부터 이 기능은 System Manager에서 지원됩니다.

- 정합성 보장 그룹을 확장할 때 수정 전에 캡처한 정합성 보장 그룹의 스냅샷은 부분적으로 간주됩니다. 해당 스냅샷을 기반으로 하는 모든 복구 작업은 스냅샷 시점에 정합성 보장 그룹을 반영합니다.
- ONTAP 9.10.1 ~ 9.11.1을 사용하는 경우 일관성 그룹을 수정할 수 없습니다. ONTAP 9.10.1 또는 9.11.1에서 일관성 그룹의 구성을 변경하려면 일관성 그룹을 삭제한 다음, 포함할 볼륨으로 새 일관성 그룹을 생성해야 합니다.
- ONTAP 9.14.1부터 SnapMirror 비동기식을 사용할 경우 볼륨 세분화 스냅샷을 대상 클러스터에 복제할 수 있습니다. SnapMirror 비동기식을 사용하여 일관성 그룹을 확장하는 경우, SnapMirror 정책이 MirrorAll 또는 MirrorAndVault일 때 정합성 보장 그룹을 확장한 후에만 볼륨 세부 스냅샷이 복제됩니다. 기본 정합성 보장 그룹 스냅샷보다 최신 볼륨 세분화 스냅샷만 복제됩니다.
- SVM 재해 복구 관계(ONTAP 9.14.1부터 지원)의 일관성 그룹에 볼륨을 추가하는 경우, 일관성 그룹을 확장한 후 대상 클러스터에서 SVM 재해 복구 관계를 업데이트해야 합니다. 자세한 내용은 다음을 참조하십시오. 복제 관계를 수동으로 업데이트합니다 .
- ONTAP 9.17.1에서 NVMe를 사용하는 경우 일관성 그룹을 수정할 수 없습니다.

예 **2.** 단계

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 수정할 일관성 그룹을 선택합니다.
3. 단일 일관성 그룹을 수정하는 경우 * Volumes * 메뉴 맨 위에서 * 더 보기 * 를 선택한 다음 * 확장 * 을 선택하여 볼륨을 추가합니다.

   하위 일관성 그룹을 수정할 경우 수정할 부모 일관성 그룹을 식별합니다. > * 버튼을 선택하여 하위 일관성 그룹을 표시한 다음, 수정할 하위 일관성 그룹의 이름 옆에 있는 을 선택합니다 ⋮ . 해당 메뉴에서 * Expand * 를 선택합니다.

4. 정합성 보장 그룹에 추가할 볼륨을 최대 16개까지 선택합니다.
5. 저장 * 을 선택합니다. 작업이 완료되면 정합성 보장 그룹의 * Volumes * 메뉴에서 새로 추가된 볼륨을 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 일관성 그룹에 볼륨을 추가할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

기존 볼륨을 추가합니다

1. 다음 명령을 실행합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 목록을 사용할 수 있습니다.

   만 포함합니다 `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개 변수입니다.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

새 볼륨을 추가합니다

새 볼륨을 추가하는 절차는 사용 중인 프로토콜에 따라 다릅니다.

다음만 포함합니다. `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개변수입니다.

- 새 볼륨을 내보내지 않고 추가하려면 다음을 수행합니다.

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  ```

volume_name -size *size*

- 새 NFS 볼륨 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- 새 SAN 볼륨 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- 새 NVMe 네임스페이스 추가하기:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

일관성 그룹에서 볼륨을 제거합니다

일관성 그룹에서 제거된 볼륨은 삭제되지 않습니다. 클러스터에서 활성 상태로 유지됩니다.

이 작업에 대해

- SnapMirror 활성 동기화 또는 SVM 재해 복구 관계의 일관성 그룹에서 볼륨을 제거할 수는 없습니다. 먼저 SnapMirror 액티브 동기화 관계를 삭제하여 일관성 그룹을 수정한 다음 관계를 다시 설정해야 합니다.
- 제거 작업 후 일관성 그룹에 볼륨이 없으면 일관성 그룹이 삭제됩니다.
- 볼륨이 일관성 그룹에서 제거되면 일관성 그룹의 기존 스냅샷은 그대로 유지되지만 유효하지 않은 것으로 간주됩니다. 기존 스냅샷을 사용하여 정합성 보장 그룹의 컨텐츠를 복구할 수 없습니다. 볼륨 세분화 스냅샷은 유효합니다.
- 클러스터에서 볼륨을 삭제하면 해당 볼륨이 일관성 그룹에서 자동으로 제거됩니다.
- ONTAP 9.10.1 또는 9.11.1에서 일관성 그룹의 구성을 변경하려면 일관성 그룹을 삭제한 다음 원하는 구성원 볼륨을 가진 새 일관성 그룹을 생성해야 합니다.
- 클러스터에서 볼륨을 삭제하면 일관성 그룹에서도 자동으로 제거됩니다.

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 수정할 단일 또는 하위 일관성 그룹을 선택합니다.
3. Volumes * 메뉴에서 일관성 그룹에서 제거할 개별 볼륨 옆의 확인란을 선택합니다.
4. 정합성 보장 그룹에서 볼륨 제거 * 를 선택합니다.
5. 볼륨을 제거하면 정합성 보장 그룹의 모든 스냅샷이 무효화된다는 것을 이해했는지 확인하고 * Remove * 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 CLI를 사용하여 일관성 그룹에서 볼륨을 제거할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

단계

1. 볼륨을 제거합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 목록을 사용할 수 있습니다.

   만 포함합니다 `-parent-consistency-group` 일관성 그룹이 계층적 관계에 있는 경우 매개 변수입니다.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

일관성 그룹 간에 볼륨 이동

ONTAP 9.13.1부터 부모 항목을 공유하는 하위 일관성 그룹 간에 볼륨을 이동할 수 있습니다.

이 작업에 대해

- 동일한 상위 일관성 그룹 아래에 중첩된 일관성 그룹 간에만 볼륨을 이동할 수 있습니다.
- 기존 일관성 그룹 스냅샷이 잘못되어 일관성 그룹 스냅샷으로 더 이상 액세스할 수 없습니다. 개별 볼륨 스냅샷은 유효한 상태로 유지됩니다.
- 부모 정합성 보장 그룹의 스냅샷은 유효한 상태로 유지됩니다.
- 모든 볼륨을 하위 일관성 그룹 밖으로 이동하면 해당 일관성 그룹이 삭제됩니다.
- 정합성 보장 그룹에 대한 수정 사항은 을 준수해야 합니다 정합성 보장 그룹 제한.

시스템 관리자

ONTAP 9.12.1부터 System Manager로 이 작업을 수행할 수 있습니다.

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 이동할 볼륨이 포함된 상위 일관성 그룹을 선택합니다. 하위 일관성 그룹을 찾은 다음 볼륨 메뉴를 확장합니다. 이동할 볼륨을 선택합니다.
3. 이동을 선택합니다.
4. 볼륨을 새 일관성 그룹 또는 기존 그룹으로 이동할지 여부를 선택합니다.
   a. 기존 일관성 그룹으로 이동하려면 기존 자식 일관성 그룹을 선택한 다음 드롭다운 메뉴에서 일관성 그룹의 이름을 선택합니다.
   b. 새 일관성 그룹으로 이동하려면 새 하위 일관성 그룹을 선택합니다. 새 하위 일관성 그룹의 이름을 입력하고 구성 요소 유형을 선택합니다.
5. 이동을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 일관성 그룹 간에 볼륨을 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

볼륨을 새 하위 정합성 보장 그룹으로 이동합니다

1. 다음 명령을 실행하면 지정된 볼륨이 포함된 새 하위 정합성 보장 그룹이 생성됩니다.

   새 일관성 그룹을 생성할 때 새 스냅샷, QoS 및 계층화 정책을 지정할 수 있습니다.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

볼륨을 기존 하위 정합성 보장 그룹으로 이동합니다

1. 볼륨을 재할당합니다. 를 클릭합니다 `-volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

관련 정보

- 정합성 보장 그룹 제한
- 일관성 그룹의 클론을 생성합니다

ONTAP 일관성 그룹 지오메트리 수정

ONTAP 9.13.1부터 정합성 보장 그룹의 지오메트리를 수정할 수 있습니다. 정합성 보장 그룹의 구조를 수정하면 지속적인 입출력 작업을 중단하지 않고 하위 또는 상위 정합성 보장 그룹의 구성을 변경할 수 있습니다.

정합성 보장 그룹 구조를 수정하면 정합성 보장 그룹의 기존 스냅샷에 영향을 줍니다. 자세한 내용은 수행하려는 지오메트리의 특정 수정 사항을 참조하십시오.

원격 보호 정책으로 구성된 정합성 보장 그룹의 구조는 수정할 수 없습니다. 먼저 보호 관계를 끊은 후 지오메트리를 수정한 다음 원격 보호를 복원해야 합니다.

새 하위 일관성 그룹을 추가합니다

ONTAP 9.13.1부터 새 하위 일관성 그룹을 기존 부모 일관성 그룹에 추가할 수 있습니다.

이 작업에 대해

- 부모 일관성 그룹에는 최대 5개의 자식 일관성 그룹이 포함될 수 있습니다. 을 참조하십시오 정합성 보장 그룹 제한 기타 제한.
- 단일 일관성 그룹에는 하위 일관성 그룹을 추가할 수 없습니다. 먼저 해야 합니다 [승격] 그러면 일관성 그룹을 자식 일관성 그룹에 추가할 수 있습니다.
- 확장 작업 전에 캡처된 정합성 보장 그룹의 기존 스냅샷은 부분적으로 간주됩니다. 해당 스냅샷을 기반으로 하는 모든 복구 작업은 스냅샷 시점에 정합성 보장 그룹을 반영합니다.

예 **3.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

새 하위 일관성 그룹을 추가합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 하위 일관성 그룹을 추가할 상위 일관성 그룹을 선택합니다.
3. 부모 일관성 그룹의 이름 옆에 있는 자세히 를 선택한 다음 새 자식 일관성 그룹 추가 를 선택합니다.
4. 일관성 그룹의 이름을 입력합니다.
5. 새 볼륨이나 기존 볼륨을 추가할지 여부를 선택합니다.
   a. 기존 볼륨을 추가하는 경우 **existing volumes** 를 선택한 다음 드롭다운 메뉴에서 볼륨을 선택합니다.
   b. 새 볼륨을 추가하는 경우 새 볼륨 을 선택한 다음 볼륨 수와 해당 크기를 지정합니다.
6. 추가 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 하위 정합성 보장 그룹을 추가할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

새 볼륨이 포함된 하위 정합성 보장 그룹을 추가합니다

1. 새 일관성 그룹을 생성합니다. 일관성 그룹 이름, 볼륨 접두사, 볼륨 수, 볼륨 크기, 스토리지 서비스 등의 값을 입력합니다. 및 엑스포트 정책 이름:

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

기존 볼륨이 있는 하위 정합성 보장 그룹을 추가합니다

1. 새 일관성 그룹을 생성합니다. 를 클릭합니다 `volumes` 매개 변수에는 쉼표로 구분된 볼륨 이름 목록을 사용할 수 있습니다.

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

하위 일관성 그룹을 분리합니다

ONTAP 9.13.1부터 부모 일관성 그룹을 제거하여 개별 일관성 그룹으로 변환할 수 있습니다.

이 작업에 대해

- 하위 정합성 보장 그룹을 분리하면 부모 정합성 보장 그룹의 스냅샷이 무효화되고 액세스할 수 없게 됩니다. 볼륨 세분화 스냅샷은 유효한 상태로 유지됩니다.
- 개별 정합성 보장 그룹의 기존 스냅샷은 유효한 상태로 유지됩니다.
- 분리할 하위 정합성 보장 그룹과 이름이 같은 기존 단일 정합성 보장 그룹이 있는 경우 이 작업이 실패합니다. 이 시나리오가 발생한 경우 일관성 그룹을 분리할 때 일관성 그룹의 이름을 변경해야 합니다.

예 **4.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 분리합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 분리할 자식이 포함된 부모 일관성 그룹을 선택합니다.
3. 분리하려는 하위 일관성 그룹 옆에 있는 자세히 를 선택한 다음 부모에서 분리 를 선택합니다.
4. 선택적으로 일관성 그룹의 이름을 바꾸고 애플리케이션 유형을 선택합니다.
5. 분리 를 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 하위 정합성 보장 그룹을 분리할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 분리합니다

1. 정합성 보장 그룹을 분리합니다. 필요한 경우 분리된 정합성 보장 그룹의 이름을 로 변경합니다 `-new-name` 매개 변수.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

부모 일관성 그룹 아래에서 기존 단일 일관성 그룹을 이동합니다

ONTAP 9.13.1부터 기존 단일 일관성 그룹을 하위 일관성 그룹으로 변환할 수 있습니다. 이동 작업 중에 일관성 그룹을 기존 부모 일관성 그룹 아래로 이동하거나 새 부모 일관성 그룹을 생성할 수 있습니다.

이 작업에 대해

- 상위 일관성 그룹의 하위 항목이 4개 이하가 되어야 합니다. 부모 일관성 그룹에는 최대 5개의 자식 일관성 그룹이 포함될 수 있습니다. 을 참조하십시오 정합성 보장 그룹 제한 기타 제한.
- 이 작업을 수행하기 전에 캡처한 _parent_consistency 그룹의 기존 스냅샷은 부분적으로 간주됩니다. 이러한 스냅샷 중 하나를 기반으로 하는 복구 작업은 스냅샷의 특정 시점에 정합성 보장 그룹을 반영합니다.

- 단일 일관성 그룹의 기존 일관성 그룹 스냅샷은 유효한 상태를 유지합니다.

예 **5.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

부모 일관성 그룹 아래에서 기존 단일 일관성 그룹을 이동합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 변환할 일관성 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 다른 정합성 보장 그룹 아래로 이동** 을 선택합니다.
4. 선택적으로 일관성 그룹의 새 이름을 입력하고 구성요소 유형을 선택합니다. 기본적으로 부품 유형은 다른 유형입니다.
5. 기존 부모 일관성 그룹으로 마이그레이션하거나 새 부모 일관성 그룹을 생성할지 선택합니다.
   a. 기존 부모 일관성 그룹으로 마이그레이션하려면 기존 일관성 그룹을 선택한 다음 드롭다운 메뉴에서 일관성 그룹을 선택합니다.
   b. 새 부모 일관성 그룹을 생성하려면 새 일관성 그룹을 선택한 다음 새 일관성 그룹의 이름을 제공합니다.
6. 이동을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 단일 일관성 그룹을 부모 일관성 그룹 아래로 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 새 부모 일관성 그룹 아래로 이동합니다

1. 새 부모 일관성 그룹을 생성합니다. 를 클릭합니다 `-consistency-groups` 매개 변수는 기존 일관성 그룹을 새 부모로 마이그레이션합니다.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

기존 일관성 그룹 아래에서 일관성 그룹을 이동합니다

1. 정합성 보장 그룹 이동:

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

하위 일관성 그룹을 승격합니다

ONTAP 9.13.1부터 단일 일관성 그룹을 부모 일관성 그룹으로 승격할 수 있습니다. 단일 일관성 그룹을 상위 일관성 그룹으로 승격하면 원래의 단일 일관성 그룹에 있는 모든 볼륨을 상속하는 새 하위 일관성 그룹도 생성됩니다.

이 작업에 대해

- 하위 일관성 그룹을 부모 일관성 그룹으로 변환하려면 먼저 해야 합니다 [detach] 그런 다음 하위 일관성 그룹을 이 절차에 따릅니다.
- 정합성 보장 그룹을 프로모션한 후에도 정합성 보장 그룹의 기존 스냅샷은 유효한 상태로 유지됩니다.

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 승격합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 상향 이동할 정합성 보장 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 부모 일관성 그룹으로 승격** 을 선택합니다.
4. 이름 을 입력하고 자식 일관성 그룹에 대한 구성 요소 형식 을 선택합니다.
5. 승격을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터는 ONTAP CLI를 사용하여 단일 일관성 그룹을 부모 일관성 그룹 아래로 이동할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

하위 일관성 그룹을 승격합니다

1. 정합성 보장 그룹을 승격합니다. 이 명령은 부모 정합성 보장 그룹 하나와 자식 정합성 보장 그룹 하나를 생성합니다.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

상위 항목을 단일 일관성 그룹으로 강등합니다

ONTAP 9.13.1부터 부모 일관성 그룹을 단일 일관성 그룹으로 강등할 수 있습니다. 모체를 강등하면 정합성 보장 그룹의 계층 구조가 평평하여 연결된 모든 자식 일관성 그룹이 제거됩니다. 일관성 그룹의 모든 볼륨은 새로운 단일 일관성 그룹에 유지됩니다.

이 작업에 대해

- parent_consistency 그룹의 기존 스냅샷은 단일 정합성 보장으로 하향 이동한 후에도 유효한 상태로 유지됩니다. 해당 부모의 associated_child_consistency 그룹 중 하나라도 강등 시 기존 스냅샷이 유효하지 않게 됩니다. 하위 정합성 보장 그룹 내의 개별 볼륨 스냅샷은 볼륨 세분화 스냅샷으로 계속 액세스할 수 있습니다.

예 **6.** 단계

시스템 관리자

ONTAP 9.13.1부터 System Manager로 이 작업을 수행할 수 있습니다.

일관성 그룹을 강등합니다

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 강등할 상위 일관성 그룹을 선택합니다.
3. 더 보기 를 선택한 다음 단일 정합성 보장 그룹으로 하향 이동** 을 선택합니다.
4. 연결된 모든 하위 정합성 보장 그룹이 삭제되고 해당 볼륨이 새 단일 정합성 보장 그룹 아래로 이동된다는 경고 메시지가 표시됩니다. 하향 이동 을 선택하여 충격 이해 여부를 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 일관성 그룹을 강등할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 강등합니다

1. 정합성 보장 그룹을 강등합니다. 옵션 을 사용합니다 `-new-name` 일관성 그룹의 이름을 바꾸는 매개 변수입니다.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

ONTAP 일관성 그룹 애플리케이션 및 구성 요소 태그 수정

ONTAP 9.12.1부터 정합성 보장 그룹은 구성 요소 및 애플리케이션 태그 지정을 지원합니다. 애플리케이션 및 구성 요소 태그는 관리 툴로서 일관성 그룹의 다양한 워크로드를 필터링하고 식별할 수 있습니다.

이 작업에 대해

정합성 보장 그룹은 다음 두 가지 유형의 태그를 제공합니다.

- 응용 프로그램 태그: 이러한 태그는 개별 및 부모 일관성 그룹에 적용됩니다. 애플리케이션 태그는 MongoDB, Oracle, SQL Server와 같은 워크로드에 대한 레이블링을 제공합니다. 일관성 그룹의 기본 애플리케이션 태그는 기타입니다.
- 구성 요소 태그: 계층적인 정합성 보장 그룹의 하위 요소에는 응용 프로그램 태그 대신 구성 요소 태그가 있습니다. 구성 요소 태그에 대한 옵션은 "데이터", "로그" 또는 "기타"입니다. 기본값은 기타 입니다.

일관성 그룹을 생성하거나 일관성 그룹을 생성한 후에 태그를 적용할 수 있습니다.

일관성 그룹에 SnapMirror 활성 동기화 관계가 있는 경우 * 기타 * 를 애플리케이션 또는 구성 요소 태그로 사용해야 합니다.

단계

ONTAP 9.12.1부터 System Manager를 사용하여 응용 프로그램 및 구성 요소 태그를 수정할 수 있습니다. ONTAP 9.14.1부터 ONTAP CLI를 사용하여 응용 프로그램 및 구성 요소 태그를 수정할 수 있습니다.

시스템 관리자

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 태그를 수정할 일관성 그룹을 선택합니다. 일관성 그룹 이름 옆의 를 선택하고 * Edit * 를 선택합니다 .
3. 드롭다운 메뉴에서 적절한 응용 프로그램 또는 구성 요소 태그를 선택합니다.
4. 저장 * 을 선택합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 ONTAP CLI를 사용하여 기존 일관성 그룹의 애플리케이션 또는 구성 요소 태그를 수정할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

응용 프로그램 태그를 수정합니다

1. 애플리케이션 태그에는 제한된 수의 사전 설정 문자열을 사용할 수 있습니다. 허용되는 문자열 목록을 보려면 다음 명령을 실행합니다.
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. 출력에서 적절한 문자열을 선택하고 정합성 보장 그룹을 수정합니다.
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

부품 태그를 수정합니다

1. 부품 유형을 수정합니다. 구성 요소 유형은 데이터, 로그 또는 기타일 수 있습니다. SnapMirror 액티브 동기화를 사용 중인 경우 "기타"여야 합니다.
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

ONTAP 일관성 그룹 복제

ONTAP 9.12.1부터는 일관성 그룹을 클론 복제하여 일관성 그룹 및 해당 콘텐츠의 복사본을 생성할 수 있습니다. 일관성 그룹을 클론 복제하면 일관성 그룹 구성의 복사본, 애플리케이션 유형과 같은 메타데이터, 파일, 디렉토리, LUN 또는 NVMe 네임스페이스와 같은 모든 볼륨과 해당 콘텐츠의 복사본이 생성됩니다.

이 작업에 대해

일관성 그룹을 클론 복제할 때는 현재 구성으로 클론을 생성할 수 있지만 볼륨 콘텐츠를 그대로 사용하거나 기존 일관성 그룹 스냅샷을 기반으로 클론을 생성할 수 있습니다.

일관성 그룹의 클론은 전체 일관성 그룹에 대해서만 지원됩니다. 계층적 관계에서 개별 하위 일관성 그룹을 클론 복제할 수 없습니다. 전체 일관성 그룹 구성만 클론 복제할 수 있습니다.

일관성 그룹을 클론 복제할 때 다음 구성 요소는 클론 복제되지 않습니다.

- iGroup
- LUN 매핑
- NVMe 하위 시스템
- NVMe 네임스페이스 서브시스템 맵

시작하기 전에

- 일관성 그룹을 클론 복제할 때 공유 이름이 지정되지 않은 경우 ONTAP은 클론 복제된 볼륨에 대한 SMB 공유를 생성하지 않습니다. * 접합 경로가 지정되지 않은 경우 클론 생성된 정합성 보장 그룹이 마운트되지 않습니다.
- 정합성 보장 그룹의 현재 구성 볼륨을 반영하지 않는 스냅샷을 기반으로 정합성 보장 그룹을 클론 복제하려고 하면 작업이 실패합니다.
- 일관성 그룹의 클론을 생성한 후에는 적절한 매핑 작업을 수행해야 합니다.

  을 참조하십시오 여러 LUN에 igroup 매핑 또는 NVMe 네임스페이스를 하위 시스템에 매핑합니다 를 참조하십시오.

- 일관성 그룹의 클론 복제는 SnapMirror 액티브 동기화 관계의 일관성 그룹 또는 관련 DP 볼륨의 일관성 그룹에 대해 지원되지 않습니다.

시스템 관리자

단계

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 일관성 그룹 * 메뉴에서 클론 복제할 일관성 그룹을 선택합니다.
3. 일관성 그룹의 개요 페이지 오른쪽 위에서 * Clone * 을 선택합니다.
4. 클론 복제된 새 일관성 그룹의 이름을 입력하거나 기본 이름을 그대로 사용합니다.
   a. 활성화 여부를 선택합니다 "* 씬 프로비저닝 *".
   b. 소스에서 정합성 보장 그룹을 분리시키고 클론 정합성 보장 그룹에 추가 디스크 공간을 할당하려면 * 클론 분할 * 을 선택합니다.
5. 일관성 그룹을 현재 상태로 복제하려면 *새 스냅샷 추가*를 선택합니다.

   스냅샷을 기반으로 일관성 그룹을 클론 복제하려면 * Use an existing snapshot * 을 선택합니다. 이 옵션을 선택하면 새 하위 메뉴가 열립니다. 클론 작업의 기준으로 사용할 스냅샷을 선택합니다.
6. 클론 * 을 선택합니다.
7. 정합성 보장 그룹 * 메뉴로 돌아가 정합성 보장 그룹의 클론이 생성되었는지 확인합니다.

CLI를 참조하십시오

ONTAP 9.14.1부터 클러스터 관리자 자격 증명과 함께 CLI를 사용하여 일관성 그룹을 클론 복제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹의 클론을 생성합니다

1. 이 `consistency-group clone create` 명령은 일관성 그룹의 현재 시점 상태를 복제합니다. 스냅샷을 기반으로 클론 작업의 기준을 설정하려면 `-source-snapshot` 매개 변수를 포함합니다.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   에 대한 자세한 내용은 `consistency-group clone create` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 단계

- 여러 LUN에 igroup 매핑
- NVMe 네임스페이스를 하위 시스템에 매핑합니다

ONTAP 일관성 그룹 삭제

일관성 그룹이 더 이상 필요하지 않다고 결정한 경우 삭제할 수 있습니다.

이 작업에 대해

- 일관성 그룹을 삭제하면 일관성 그룹의 인스턴스가 삭제되며 구성 볼륨 또는 LUN에 영향을 주지 않습니다. 정합성 보장 그룹을 삭제해도 각 볼륨에 있는 스냅샷은 삭제되지 않지만 정합성 보장 그룹 스냅샷으로는 더 이상 액세스할 수 없습니다. 하지만 스냅샷은 일반 볼륨 세분화 스냅샷처럼 계속 관리할 수 있습니다.
- ONTAP은 일관성 그룹에 있는 볼륨이 모두 삭제된 경우 일관성 그룹을 자동으로 삭제합니다.
- 부모 일관성 그룹을 삭제하면 연결된 모든 하위 일관성 그룹이 삭제됩니다.
- 9.10.1 ~ 9.12.0 사이의 ONTAP 버전을 사용하는 경우 볼륨 자체가 삭제된 경우에만 정합성 보장 그룹에서 볼륨을 제거할 수 있으며, 이 경우 볼륨이 정합성 보장 그룹에서 자동으로 제거됩니다. ONTAP 9.12.1부터 일관성 그룹을 삭제하지 않고도 일관성 그룹에서 볼륨을 제거할 수 있습니다. 이 프로세스에 대한 자세한 내용은 을 참조하십시오 일관성 그룹 수정.

예 **7.** 단계

시스템 관리자

1. 스토리지 > 정합성 보장 그룹 * 을 선택합니다.
2. 삭제할 일관성 그룹을 선택합니다.
3. 일관성 그룹 이름 옆의 * Delete * 를 차례로 선택합니다 ⋮ .

CLI를 참조하십시오

ONTAP 9.14.1부터 CLI를 사용하여 일관성 그룹을 삭제할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 admin 권한 수준이어야 합니다.
- ONTAP 9.15.1부터 관리자 권한 수준의 모든 사용자가 이 작업을 수행할 수 있습니다. ONTAP 9.14.1에서는 클러스터 또는 SVM 관리자만 이 작업을 수행할 수 있습니다.

일관성 그룹을 삭제합니다

1. 정합성 보장 그룹 삭제:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror 활성 동기화

소개

ONTAP SnapMirror Active Sync에 대해 알아보세요

SnapMirror Active Sync는 SnapMirror Business Continuity(SM-BC)라고도 하며, 사이트 전체에 장애가 발생하더라도 비즈니스 서비스가 계속 작동할 수 있도록 합니다. 이 기술을 사용하면 수동 개입이나 사용자 정의 스크립팅 없이도 애플리케이션이 원활하게 보조 복사본으로 장애 조치될 수 있습니다.

NetApp SnapMirror Active Sync(SM-as)는 자동 장애 조치를 통해 보다 세분화되고 비용이 저렴하며 사용하기 쉬운

애플리케이션 수준 보호 기능을 제공하도록 설계되었습니다. SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하는 경우에도 미션 크리티컬 비즈니스 서비스가 계속 운영될 수 있습니다. SnapMirror 활성 동기화를 사용하면 지리적으로 분산된 위치의 사이트 간에 애플리케이션의 여러 볼륨을 동기식으로 복제할 수 있습니다(일관성 그룹에 추가하여). 1차 데이터베이스가 중단되는 경우 자동으로 2차 데이터베이스로 장애 조치를 취해 1계층 애플리케이션의 비즈니스 연속성을 확보할 수 있습니다.

일부 국가의 금융 기관 규정에 따라 기업은 2차 데이터 센터에서 주기적으로 서비스를 제공받아야 합니다. SnapMirror Active Sync는 고가용성 클러스터를 통해 비즈니스 연속성을 위한 이러한 데이터 센터 전환을 지원합니다.

ONTAP 9.9.1부터 사용 가능한 SnapMirror Active Sync는 AFF 및 All-Flash SAN Array(ASA) 클러스터에서 지원됩니다. 기본 클러스터와 보조 클러스터는 ASA, ASA r2 또는 AFF 중 하나와 같은 유형이어야 합니다. SnapMirror Active Sync는 iSCSI 또는 FCP LUN 또는 NVMe 네임스페이스를 사용하여 애플리케이션을 보호합니다.

SnapMirror Active Sync는 대칭 및 비대칭 구성을 모두 지원합니다. ONTAP 9.15.1에서는 대칭적 액티브/액티브에 대한 지원이 도입되었습니다. 대칭적 활성/활성 구성을 사용하면 보호된 LUN의 두 사본 모두 양방향 동기 복제를 통해 읽기 및 쓰기 I/O 작업을 수행할 수 있으므로 각 LUN 사본이 로컬 I/O 요청을 처리할 수 있습니다.

2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 문서와 통합되었습니다. 이제 ONTAP SnapMirror 액티브 동기화 문서에 _TR-4878: SnapMirror active sync_의 콘텐츠가 포함되어 있습니다.

이점

SnapMirror 액티브 동기화는 다음과 같은 이점을 제공합니다.

- 비즈니스 크리티컬 애플리케이션을 위한 지속적인 가용성:
- 주요 애플리케이션을 운영 사이트와 보조 사이트에서 교대로 호스팅할 수 있습니다.
- 정합성 보장 그룹을 사용하여 애플리케이션 관리를 간소화하여 종속 쓰기 순서 정합성 보장
- 각 애플리케이션의 장애 조치를 테스트하는 기능
- 애플리케이션 가용성에 영향을 주지 않고 미러 클론을 즉시 생성
- 동일한 ONTAP 클러스터에 보호된 워크로드와 보호되지 않은 워크로드를 구축할 수 있습니다.
- LUN, NVMe 네임스페이스, NVMe 하위 시스템 또는 스토리지 장치 ID는 동일하게 유지되므로 애플리케이션은 이를 공유 가상 장치로 인식합니다.
- 2차 클러스터를 유연하게 재사용하여 애플리케이션 성능 또는 가용성에 영향을 주지 않고 개발 테스트, UAT 또는 보고용으로 애플리케이션 사용을 위한 즉각적인 클론을 생성할 수 있습니다.

SnapMirror 액티브 싱크를 사용하면 데이터 LUN 또는 NVMe 네임스페이스를 보호하여 재해 발생 시 비즈니스 연속성을 위해 애플리케이션을 투명하게 페일오버할 수 있습니다. 자세한 내용은 다음을 참조하세요. "사용 사례" .

주요 개념

SnapMirror Active Sync는 일관성 그룹을 사용하여 데이터가 복제되도록 보장합니다. SnapMirror Active Sync는 ONTAP Mediator를 사용하거나 ONTAP 9.17.1부터는 Cloud Mediator를 사용하여 자동 장애 조치를 수행하여 재해 발생 시에도 데이터가 제공되도록 보장합니다. SnapMirror Active Sync 배포를 계획할 때는 SnapMirror Active Sync의 핵심 개념과 아키텍처를 이해하는 것이 중요합니다.

비대칭 및 대칭

대칭형 액티브/액티브 구성에서는 두 사이트 모두 액티브 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다. 대칭형 액티브/액티브 구성은 VMware vMSC, SQL 기반 Windows 장애 조치 클러스터, Oracle RAC를 포함한 클러스터형

애플리케이션에 최적화되어 있습니다.

비대칭 액티브/액티브 구성에서는 보조 사이트의 데이터가 LUN, 네임스페이스 또는 스토리지 장치에 프록시됩니다.

자세한 내용은 을 참조하십시오 SnapMirror 액티브 동기화 아키텍처.

일관성 그룹

AFF 및 ASA 시스템의 경우 "일관성 그룹" 비즈니스 연속성을 위해 보호해야 하는 애플리케이션 워크로드에 대한 일관성을 보장하는 FlexVol 볼륨의 집합입니다. ASA r2 시스템에서 일관성 그룹은 스토리지 유닛의 집합입니다.

일관성 그룹의 목적은 볼륨 또는 스토리지 유닛 컬렉션의 스냅샷 이미지를 동시에 생성하여 특정 시점에 해당 컬렉션의 충돌 발생 시에도 일관된 복사본을 유지하는 것입니다. 일관성 그룹은 데이터세트의 모든 볼륨이 정지되었다가 정확히 동일한 시점에 스냅샷되도록 보장합니다. 이를 통해 데이터세트를 지원하는 볼륨 또는 스토리지 유닛 전반에 걸쳐 데이터 일관성이 유지되는 복원 지점을 제공합니다. 따라서 일관성 그룹은 종속 쓰기 순서 일관성을 유지합니다. 비즈니스 연속성을 위해 애플리케이션을 보호하려는 경우, 해당 애플리케이션에 해당하는 볼륨 또는 스토리지 유닛 그룹을 일관성 그룹에 추가하여 소스 일관성 그룹과 대상 일관성 그룹 간에 데이터 보호 관계를 설정해야 합니다. 소스 일관성 그룹과 대상 일관성 그룹에는 동일한 개수와 유형의 볼륨이 포함되어야 합니다.

구성 요소

SnapMirror 활성 동기화 관계에서 보호되는 일관성 그룹의 일부인 개별 볼륨, LUN 또는 NVMe 네임스페이스(ONTAP 9.17.1부터 시작).

ONTAP 중재자

그만큼 "ONTAP 중재자" 피어링된 ONTAP 클러스터 및 노드에 대한 상태 정보를 수신하여 두 클러스터 간 오케스트레이션을 수행하고 각 노드/클러스터가 정상 작동 중인지 확인합니다. ONTAP Mediator는 다음에 대한 상태 정보를 제공합니다.

- 피어 ONTAP 클러스터
- 피어 ONTAP 클러스터 노드입니다
- 일관성 그룹(SnapMirror 활성 동기화 관계에서 페일오버 유닛을 정의). 각 일관성 그룹에 대해 다음 정보가 제공됩니다.
  - 복제 상태: 초기화되지 않음, 동기화 중 또는 동기화 중단
  - 운영 복제본을 호스팅하는 클러스터
  - 작업 컨텍스트(계획된 페일오버에 사용됨)

이 ONTAP 중재자 상태 정보를 통해 클러스터는 서로 다른 유형의 장애를 구별하고 자동 페일오버를 수행할지 여부를 결정할 수 있습니다. ONTAP mediator는 ONTAP 클러스터(기본 및 보조) 모두와 함께 SnapMirror 액티브 동기화 쿼럼의 세 가지 파티 중 하나입니다. 합의에 도달하기 위해서는 정족수 중 적어도 두 당사자가 일정한 운영에 합의하여야 한다.

ONTAP 9.15.1부터 System Manager는 두 클러스터의 SnapMirror 활성 동기화 관계 상태를 표시합니다. System Manager의 두 클러스터 중 하나에서 ONTAP 중재자의 상태를 모니터링할 수도 있습니다. 이전 ONTAP 릴리즈에서는 소스 클러스터의 SnapMirror 활성 동기화 관계 상태가 System Manager에 표시됩니다.

ONTAP 클라우드 중재자

ONTAP Cloud Mediator는 ONTAP 9.17.1부터 사용할 수 있습니다. ONTAP Cloud Mediator는 NetApp 콘솔을 사용하여 클라우드에서 호스팅된다는 점을 제외하면 ONTAP Mediator와 동일한 서비스를 제공합니다.

계획된 페일오버

SnapMirror 활성 동기화 관계에서 복사본의 역할을 변경하기 위한 수동 작업입니다. 운영 사이트는 2차 사이트가 되고 2차 사이트는 1차 사이트가 됩니다.

자동 비계획 페일오버**(AUFO)**

미러 복제본에 대한 페일오버를 수행하는 자동 작업입니다. 이 작업은 ONTAP 중재자의 도움을 받아 운영 복제본을 사용할 수 없음을 감지해야 합니다.

1차 **- 1**차 및 **1**차 편향

SnapMirror 액티브 동기화는 네트워크 파티션 시 I/O를 제공하기 위해 기본 복사본을 우선적으로 사용하는 기본 원칙을 사용합니다.

Primary-bias는 SnapMirror Active Sync Protected 데이터 세트의 가용성을 개선하는 특별한 쿼럼 구현입니다. 운영 복사본을 사용할 수 있는 경우 두 클러스터 모두에서 ONTAP 중재자에 연결할 수 없을 때 운영 바이어스가 적용됩니다.

Primary-first 및 primary bias는 ONTAP 9.15.1부터 SnapMirror 액티브 동기화에서 지원됩니다. 1차 복사본은 System Manager에서 지정되고 REST API 및 CLI를 사용하여 출력됩니다.

동기화 중단**(OOS)**

응용 프로그램 입출력이 보조 스토리지 시스템으로 복제되지 않으면** 비동기 상태로 보고됩니다. 동기화 중단 상태는 보조 볼륨이 기본(소스)과 동기화되지 않았으며 SnapMirror 복제가 발생하지 않음을 의미합니다.

미러 상태가 `Snapmirrored` 이는 SnapMirror 관계가 설정되었고 데이터 전송이 완료되었음을 나타냅니다. 즉, 대상 볼륨이 소스 볼륨과 최신 상태임을 의미합니다.

SnapMirror 액티브 동기화는 자동 재동기화를 지원하여 복사본이 InSync 상태로 돌아갈 수 있도록 합니다.

ONTAP 9.15.1부터 SnapMirror 액티브 동기화가 지원됩니다 "팬아웃 구성의 자동 재구성".

균일 및 비균일 설정

- 호스트 액세스 균일 두 사이트의 호스트가 두 사이트의 스토리지 클러스터에 대한 모든 경로에 접속되어 있음을 의미합니다. 사이트 간 경로가 거리 전체에 걸쳐 확장됩니다.
- 비균일 호스트 액세스 각 사이트의 호스트가 동일한 사이트의 클러스터에만 연결되어 있음을 의미합니다. 사이트 간 경로 및 확장 경로가 연결되지 않았습니다.

모든 SnapMirror 액티브 동기식 배포에 대해 통일된 호스트 액세스가 지원되며, 비균일 호스트 액세스는 대칭 액티브/액티브 구축에만 지원됩니다.

제로 **RPO**

RPO는 지정된 기간 동안 허용되는 데이터 손실량인 복구 시점 목표를 나타냅니다. RPO가 0이면 데이터 손실이 허용되지 않습니다.

즉각적인 **RTO**

RTO는 복구 시간 목표를 나타냅니다. 이 시간은 운영 중단, 장애 또는 기타 데이터 손실 이벤트가 발생한 후 애플리케이션이 운영 중단 없이 정상 작업으로 돌아가도록 허용할 수 있는 시간입니다. RTO가 0이면 가동 중지 시간이 허용되지 않는다는 의미입니다.

ONTAP 버전에서 **SnapMirror Active Sync** 구성 지원

SnapMirror Active Sync에 대한 지원은 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	지원되는 클러스터	지원되는 프로토콜	지원되는 구성
9.17.1 이상	• AFF • ASA • C 시리즈 • ASA r2	• iSCSI • FC • VMware 워크로드를 위한 NVMe	• 비대칭 활성/활성 비대칭 액티브/액티브는 ASA r2 및 NVMe를 지원하지 않습니다. NVMe 지원에 대한 자세한 내용은 "NVMe 구성, 지원 및 제한 사항"를 참조하십시오. • 대칭적인 액티브/액티브
9.16.1 이상	• AFF • ASA • C 시리즈 • ASA r2	• iSCSI • FC	• 비대칭 활성/활성 • 대칭형 액티브/액티브 대칭형 액티브/액티브 구성은 ONTAP 9.16.1 이상에서 4노드 간 클러스터를 지원합니다. ASA r2의 경우 2노드 클러스터만 지원됩니다.
9.15.1 이상	• AFF • ASA • C 시리즈	• iSCSI • FC	• 비대칭 활성/활성 • 대칭형 액티브/액티브 대칭형 액티브/액티브 구성은 ONTAP 9.15.1에서 2노드 클러스터를 지원합니다. 2노드 간 2노드 클러스터 및 4노드 간 4노드 클러스터는 ONTAP 9.16.1 이상에서 지원됩니다.

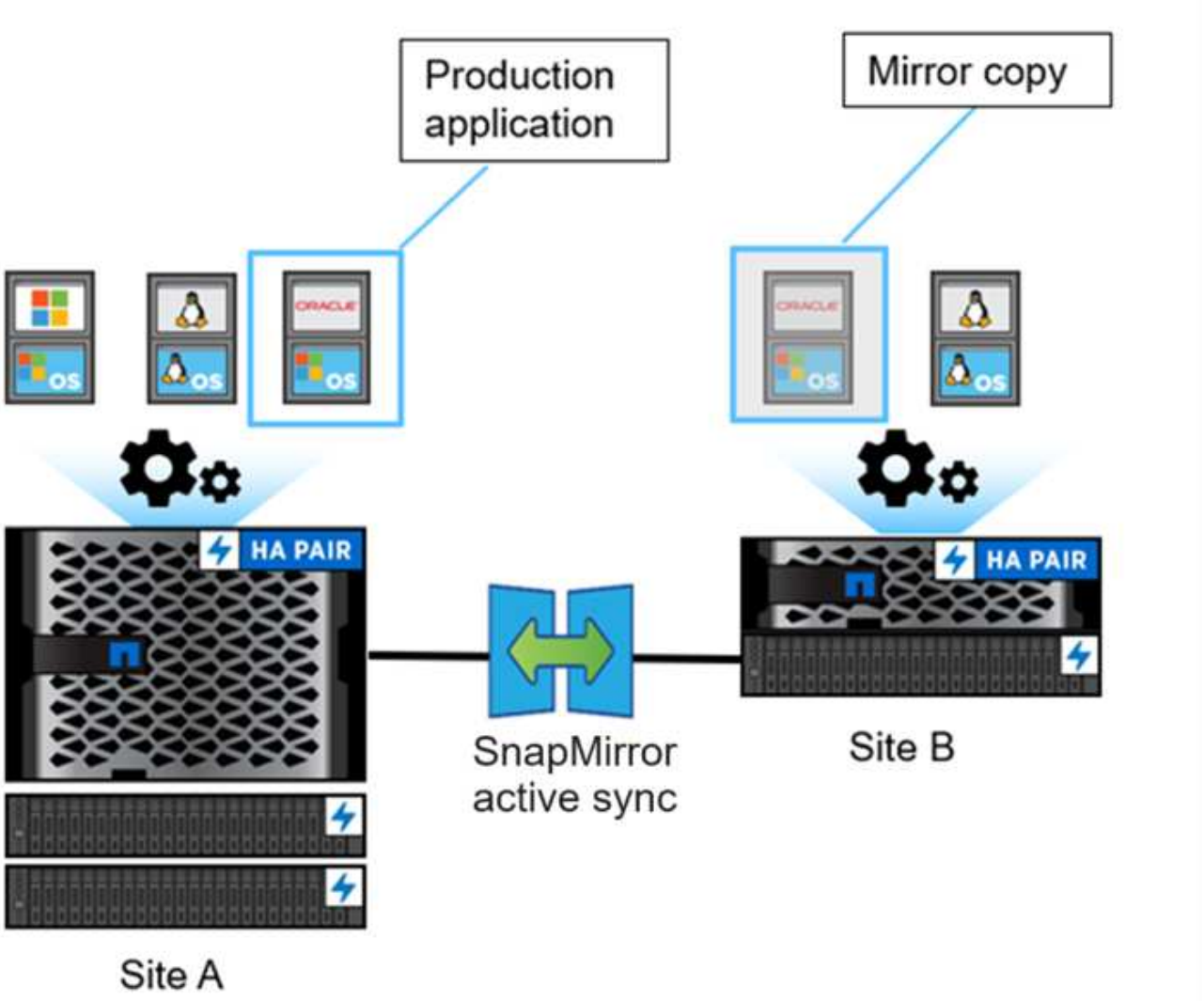
9.9.1 이상	• AFF • ASA • C 시리즈	• iSCSI • FC	비대칭 활성/활성

1차 및 2차 클러스터는 동일한 유형이어야 합니다. "ASA" , "ASA r2" , 또는 AFF.

ONTAP SnapMirror 액티브 싱크 아키텍처

SnapMirror 액티브 동기화 아키텍처는 두 클러스터 모두에서 활성 워크로드를 지원하여 기본 워크로드를 두 클러스터에서 동시에 처리할 수 있습니다. 일부 국가의 금융 기관 규정에서는 기업이 보조 데이터 센터에서도 주기적으로 서비스를 받을 수 있도록 요구합니다. 이를 "틱톡" 배포라고 하며, SnapMirror Active Sync를 통해 이를 구현할 수 있습니다.

비즈니스 연속성을 보호하기 위한 데이터 보호 관계는 스토리지 가상 머신(SVM) 내 여러 볼륨의 애플리케이션별 LUN 또는 NVMe 네임스페이스를 일관성 그룹에 추가하여 소스 스토리지 시스템과 대상 스토리지 시스템 간에 생성됩니다. 일반적인 운영 환경에서는 엔터프라이즈 애플리케이션이 기본 일관성 그룹에 데이터를 쓰고, 기본 일관성 그룹은 이 I/O를 미러 일관성 그룹에 동기적으로 복제합니다.



데이터 보호 관계에 두 개의 개별 데이터 사본이 존재하더라도 SnapMirror Active Sync는 동일한 LUN 또는 NVMe 네임스페이스 ID를 유지하므로 애플리케이션 호스트는 이를 여러 경로를 가진 공유 가상 장치로 인식하고, 한 번에 하나의 LUN 또는 NVMe 네임스페이스 사본에만 쓰기가 수행됩니다. 장애로 인해 기본 스토리지 시스템이 오프라인 상태가 되면 ONTAP 이 장애를 감지하고 Mediator를 사용하여 재확인합니다. ONTAP 과 Mediator 모두 기본 사이트에 ping을 보낼 수 없는 경우, ONTAP 자동 장애 조치(failover) 작업을 수행합니다. 이 프로세스를 통해 이전에는 장애 조치를 위해 필요했던 수동 개입이나 스크립팅 없이 특정 애플리케이션만 장애 조치할 수 있습니다.

기타 고려 사항:

- 비즈니스 연속성을 위한 보호 범위를 벗어나는 미러링되지 않은 볼륨이 지원됩니다.
- 비즈니스 연속성을 위해 보호되는 볼륨에 대해 하나의 다른 SnapMirror 비동기식 관계만 지원됩니다.
- Cascade 토폴로지는 무중단 업무 운영을 위한 보호 기능이 지원되지 않습니다.

중재자의 역할

SnapMirror Active Sync는 Mediator를 사용하여 SnapMirror Active Sync 복사본에 대한 수동 감시 역할을 합니다. 네트워크 파티션이 발생하거나 복사본 하나를 사용할 수 없는 경우, SnapMirror Active Sync는 Mediator를 사용하여 어떤 복사본이 I/O를 계속 처리할지 결정하고, 다른 복사본의 I/O는 중단합니다. 온프레미스 ONTAP Mediator 외에도 ONTAP 9.17.1부터 ONTAP Cloud Mediator를 설치하여 클라우드 배포 환경에서 동일한 기능을 제공할 수 있습니다. ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용할 수 있지만, 동시에 사용할 수는 없습니다.

Mediator는 SnapMirror 액티브 동기화 구성에서 패시브 쿼럼 감시(passive quorum witness)로서 중요한 역할을 수행하여 쿼럼 유지 관리를 보장하고 장애 발생 시 데이터 액세스를 용이하게 합니다. 이는 컨트롤러가 피어 컨트롤러의 활성 상태를 확인하는 ping 프록시 역할을 합니다. Mediator는 스위치오버 작업을 직접 트리거하지는 않지만, 네트워크 통신 문제 발생 시 생존 노드가 파트너의 상태를 확인할 수 있도록 하는 중요한 기능을 제공합니다. ONTAP Mediator는 쿼럼 감시 역할을 수행하면서 피어 클러스터에 대한 대체 경로(실제로는 프록시 역할)를 제공합니다.

또한, 클러스터가 쿼럼 프로세스의 일부로 이 정보를 얻을 수 있도록 합니다. 통신 목적으로 노드 관리 LIF와 클러스터 관리 LIF를 사용합니다. 사이트 장애와 ISL(InterSwitch Link) 장애를 구분하기 위해 여러 경로를 통해 중복 연결을 설정합니다. 이벤트로 인해 클러스터가 Mediator 소프트웨어 및 모든 노드와의 연결이 끊어지면 연결할 수 없는 것으로 간주됩니다. 이 경우 경고가 발생하고 보조 사이트의 미러 일관성 그룹으로 자동 장애 조치가 활성화되어 클라이언트의 중단 없는 I/O가 보장됩니다. 복제 데이터 경로는 하트비트 메커니즘을 사용하며, 네트워크 오류나 이벤트가 일정 기간 이상 지속되면 하트비트 장애가 발생하여 관계가 동기화되지 않을 수 있습니다. 그러나 다른 포트로의 LIF 장애 조치와 같은 중복 경로가 있으면 하트비트를 유지하고 이러한 중단을 방지할 수 있습니다.

ONTAP 중재자

ONTAP Mediator는 모니터링하는 두 개의 ONTAP 클러스터와는 별개의 세 번째 장애 도메인에 설치됩니다. 이 설정에는 세 가지 핵심 구성 요소가 있습니다.

- SnapMirror 활성 동기화 운영 정합성 보장 그룹을 호스팅하는 운영 ONTAP 클러스터입니다
- 미러 정합성 보장 그룹을 호스팅하는 보조 ONTAP 클러스터입니다
- ONTAP 중재자

ONTAP Mediator는 다음 목적으로 사용됩니다.

- 정족수를 설정한다
- 자동 페일오버(AUFO)를 통한 지속적인 가용성
- 계획된 페일오버(PFO)

ONTAP Mediator 1.7은 비즈니스 연속성을 위해 10개의 클러스터 쌍을 관리할 수 있습니다.

ONTAP Mediator를 사용할 수 없는 경우 계획된 장애 조치나 자동 장애 조치를 수행할 수 없습니다. 애플리케이션 데이터는 어떠한 중단 없이 동기적으로 복제되므로 데이터 손실이 없습니다.

ONTAP 클라우드 중재자

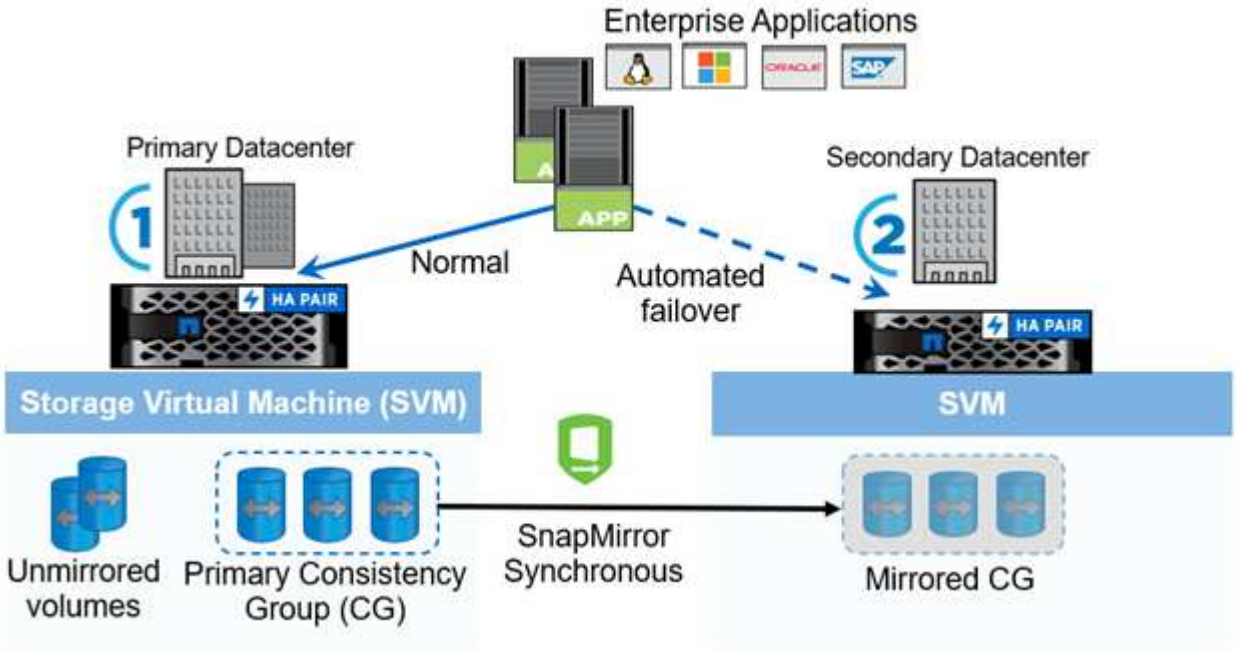
ONTAP 9.17.1부터 ONTAP Cloud Mediator는 NetApp 콘솔에서 클라우드 기반 서비스로 제공되며 SnapMirror Active Sync와 함께 사용할 수 있습니다. ONTAP Mediator와 유사하게 ONTAP Cloud Mediator는 SnapMirror 액티브 동기화 관계에서 다음과 같은 기능을 제공합니다.

- HA 또는 SnapMirror 활성 동기화 메타데이터에 대한 지속적이고 보호된 저장소를 제공합니다.
- 컨트롤러 활성을 위한 핑 프록시 역할을 합니다.
- quorum 결정에 도움이 되는 동기 노드 상태 쿼리 기능을 제공합니다.

ONTAP Cloud Mediator는 NetApp Console 클라우드 서비스를 관리할 필요가 없는 제3의 사이트로 사용하여 SnapMirror 활성 동기화 배포를 간소화하는 데 도움이 됩니다. ONTAP Cloud Mediator 서비스는 온프레미스 ONTAP Mediator와 동일한 기능을 제공하지만, 제3의 사이트 유지 관리에 따른 운영 복잡성을 줄여줍니다 . 반면, ONTAP Cloud Mediator는 패키지 형태로 제공되며, 운영을 위한 독립적인 전원 및 네트워크 인프라를 갖춘 제3의 사이트에서 실행되는 Linux 호스트에 설치해야 합니다.

SnapMirror Active Sync 작업 워크플로

다음 그림에서는 개괄적인 SnapMirror 액티브 동기화의 설계를 보여 줍니다.



이 다이어그램은 운영 데이터 센터의 SVM(스토리지 VM)에서 호스팅되는 엔터프라이즈 애플리케이션을 보여 줍니다. SVM은 볼륨 5개를 포함하며, 볼륨 3개는 일관성 그룹의 일부입니다. 일관성 그룹의 볼륨 3개가 보조 데이터 센터에 미러링됩니다. 정상적인 상황에서는 모든 쓰기 작업이 운영 데이터 센터에 수행됩니다. 실제로 이 데이터 센터는 I/O 작업의 소스로 사용되고, 보조 데이터 센터는 대상으로 작동합니다.

1차 데이터 센터에서 재해가 발생하는 경우 ONTAP 2차 데이터 센터가 1차 데이터 센터 역할을 하도록 지시하여 모든

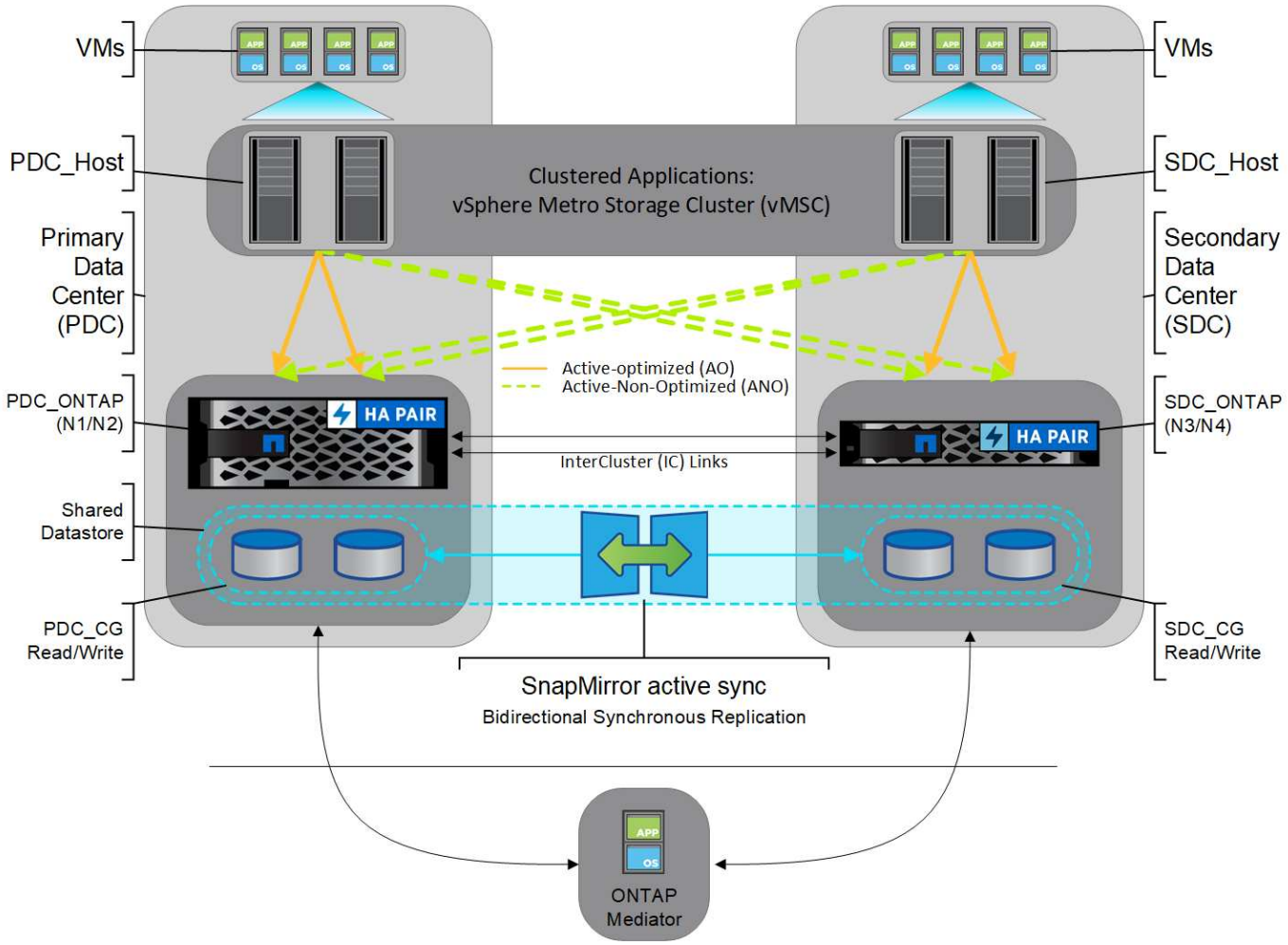
I/O 작업을 처리합니다. 일관성 그룹에 미러링된 볼륨만 제공됩니다. SVM의 다른 두 권과 관련된 모든 작업은 재해 사건의 영향을 받습니다.

대칭적인 액티브/액티브

SnapMirror Active Sync는 비대칭 솔루션 및 대칭 솔루션을 제공합니다.

_비대칭 구성_에서 기본 스토리지 사본은 활성-최적화 경로를 노출하고 클라이언트 I/O를 능동적으로 처리합니다. 보조 사이트는 I/O에 원격 경로를 사용합니다. 보조 사이트의 스토리지 경로는 활성-비최적화로 간주됩니다. 쓰기 LUN에 대한 액세스는 보조 사이트에서 프록시됩니다. NVMe 프로토콜은 비대칭 구성에서 지원되지 않습니다.

_대칭형 액티브/액티브 구성_에서는 활성 최적화 경로가 양쪽 사이트 모두에 노출되고 호스트별로 설정 가능하며 구성 가능합니다. 즉, 양쪽 호스트 모두 활성 I/O를 위해 로컬 스토리지에 액세스할 수 있습니다. ONTAP 9.16.1부터 대칭형 액티브/액티브는 2노드 클러스터와 4노드 클러스터에서 지원됩니다. SnapMirror 액티브 동기화는 2노드 클러스터 간 구성과 4노드 클러스터 간 구성을 지원합니다. 4노드 클러스터에서 2노드 클러스터로의 구성 또는 2노드 클러스터에서 4노드 클러스터로의 구성은 지원하지 않습니다. ONTAP 9.17.1부터 대칭형 액티브/액티브 구성은 2노드 클러스터에서 NVMe 프로토콜을 지원합니다.



대칭 액티브/액티브는 VMware Metro Storage Cluster, Oracle RAC, SQL을 사용한 Windows 페일오버 클러스터링을 비롯한 클러스터 애플리케이션을 대상으로 합니다.

ONTAP SnapMirror Active Sync 사용 사례

전 세계적으로 연결된 비즈니스 환경에서는 사이버 공격, 정전, 자연 재해 등의 중단이

발생하더라도 데이터 손실 없이 비즈니스에 중요한 애플리케이션 데이터를 신속하게 복구해야 한다는 요구가 있습니다. 이러한 요구는 금융 분야나 GDPR(일반 데이터 보호 규정)과 같은 규제 의무를 준수하는 분야에서 더욱 높아집니다.

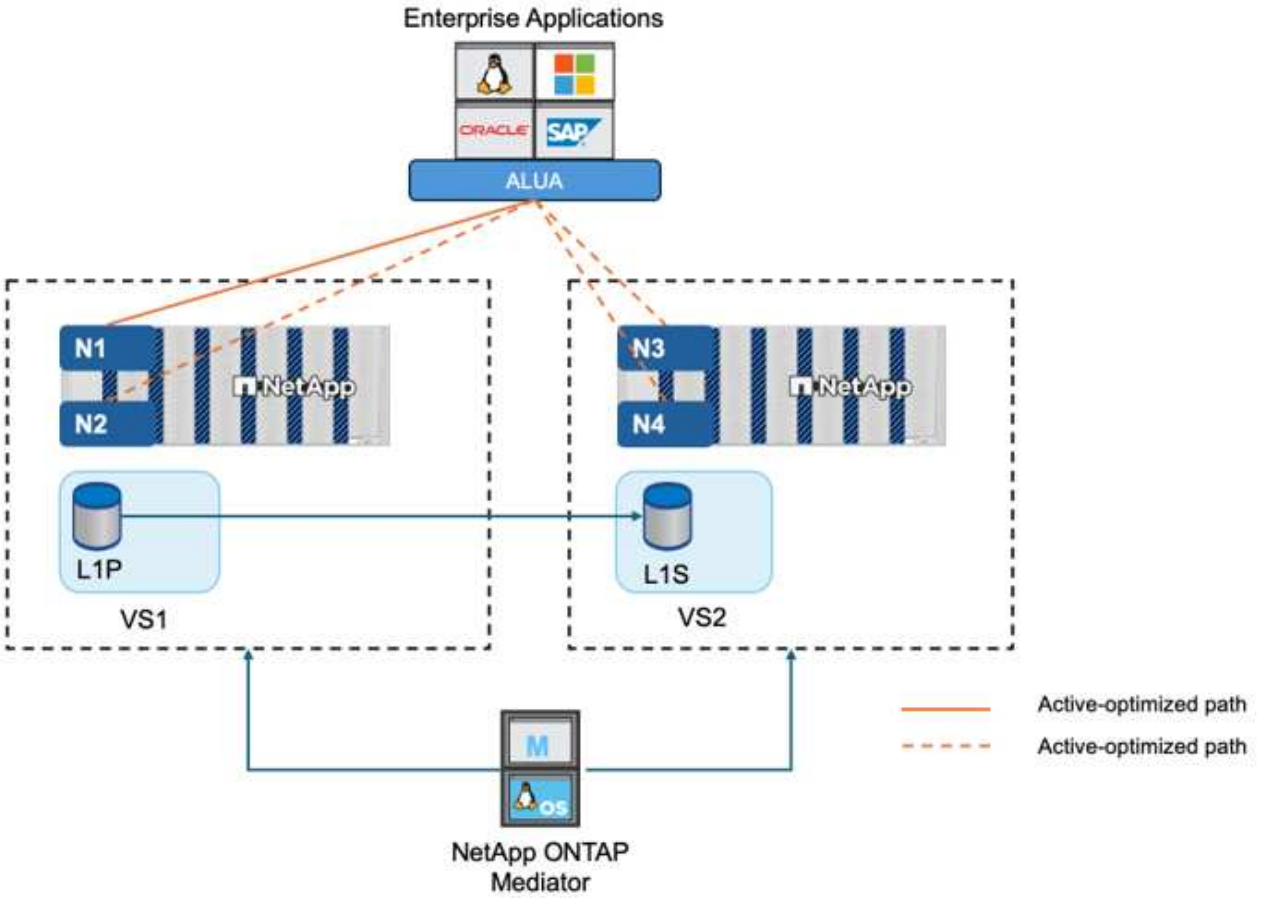
SnapMirror 액티브 동기화는 다음과 같은 사용 사례를 제공합니다.

제로 복구 시간 목표**(RTO)**를 위한 애플리케이션 구축

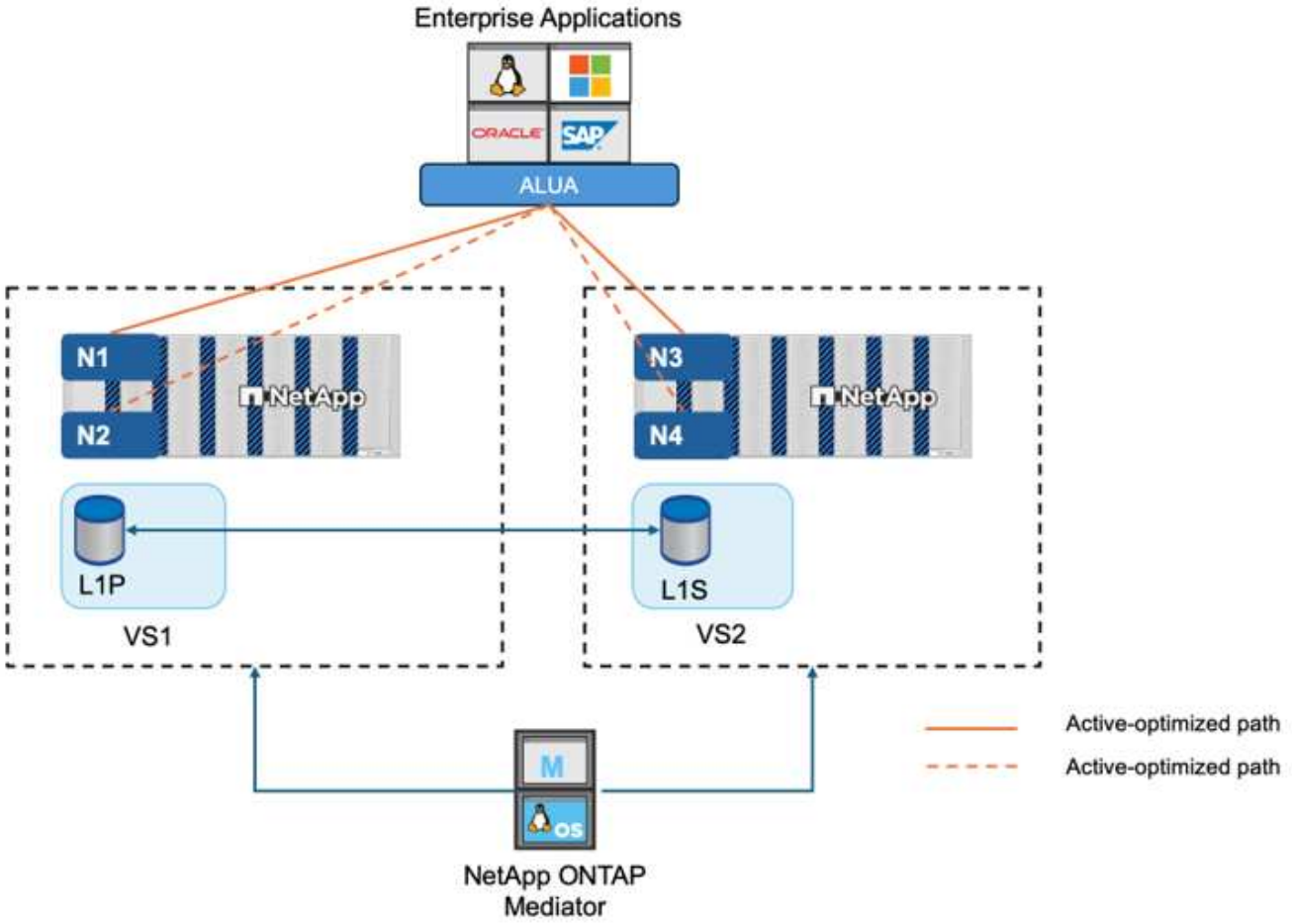
SnapMirror Active Sync 배포에는 기본 클러스터와 보조 클러스터가 있습니다. 기본 클러스터의 LUN `L1P`) 거울이 있어요 `L1S`) 보조 LUN에 있습니다. 두 LUN은 동일한 직렬 ID를 공유하며 호스트에 읽기-쓰기 LUN으로 보고됩니다. 그러나 비대칭 구성에서는 읽기 및 쓰기 작업이 기본 LUN으로만 처리됩니다. `L1P` . 미러에 대한 모든 쓰기 `L1S` 대리인을 통해 제공됩니다.

제로 **RTO** 또는 투명한 애플리케이션 페일오버**(TAF)**를 위한 애플리케이션 구축

TAF는 호스트 MPIO 소프트웨어 기반 경로 페일오버를 통해 스토리지에 대한 무중단 액세스를 구현합니다. 두 LUN 복사본(예: 기본 볼륨(L1P) 및 미러 볼륨(L1S))은 동일한 ID(일련 번호)를 가지며 호스트에 읽기/쓰기 가능으로 보고됩니다. 그러나 비대칭 구성에서는 읽기 및 쓰기가 기본 볼륨에서만 처리됩니다. 미러 볼륨에 대한 I/O는 기본 볼륨으로 프록시됩니다. 호스트에서 L1에 대한 기본 경로는 비대칭 논리 단위 액세스(ALUA) 액세스 상태가 활성 최적화(A/O)인 경우 VS1:N1입니다. ONTAP Mediator는 구축 과정의 일부로 필요하며, 주로 기본 볼륨의 스토리지 중단 시 페일오버(계획된 또는 계획되지 않은)를 수행합니다.



TAF는 자동 장애 조치(Automated Failover)와 자동 장애 조치 이중화(Automated Failover Duplex)의 두 가지 모드로 작동합니다. 자동 장애 조치를 사용하면 읽기 및 쓰기 작업이 기본 볼륨에서만 처리되므로, 자체적으로 쓰기 작업을 처리할 수 없는 미러 복사본에 대한 IO는 기본 복사본으로 프록시됩니다. 자동 장애 조치 이중화를 사용하면 기본 복사본과 보조 복사본 모두 IO를 처리할 수 있으므로 프록시가 필요하지 않습니다.



ONTAP 9.17.1에서 호스트 액세스에 NVMe를 사용하는 경우 AutomatedFailoverDuplex 정책만 지원됩니다.

SnapMirror Active Sync는 애플리케이션 호스트 다중 경로 소프트웨어에서 스토리지 어레이와의 애플리케이션 호스트 통신에 필요한 우선 순위 및 액세스 가용성을 통해 알려진 경로를 사용할 수 있도록 하는 메커니즘인 ALUA를 사용합니다. ALUA는 LUN을 소유한 컨트롤러에 대한 활성 최적화 경로를 최적화되지 않은 활성 경로로 표시하며, 기본 경로에 장애가 발생할 경우에만 사용됩니다.

NVMe 프로토콜을 사용하는 SnapMirror 액티브 동기화는 ANA(비대칭 네임스페이스 액세스)를 사용하여 애플리케이션 호스트가 보호되는 NVMe 네임스페이스에 대한 최적화된 경로와 최적화되지 않은 경로를 검색할 수 있도록 합니다. ONTAP NVMe 타겟은 적절한 경로 상태를 게시하여 애플리케이션 호스트가 보호되는 NVMe 네임스페이스에 대한 최적의 경로를 사용할 수 있도록 합니다.

클러스터된 애플리케이션

VMware Metro Storage Cluster, Oracle RAC, SQL을 사용한 Windows Failover Clustering을 포함한 클러스터형 애플리케이션은 성능 오버헤드 없이 VM을 다른 사이트로 장애 조치할 수 있도록 동시 액세스가 필요합니다. SnapMirror 액티브 싱크 대칭 액티브/액티브는 클러스터형 애플리케이션의 요구 사항을 충족하기 위해 양방향 복제를 통해 로컬로 IO를 제공합니다. ONTAP 9.16.1부터 4노드 클러스터 구성에서 대칭적 액티브/액티브가 지원되며, ONTAP 9.15.1의 2노드 클러스터 제한에서 확장되었습니다.

재해 시나리오

지리적으로 분산된 사이트 간에 애플리케이션을 위해 여러 볼륨을 동기식으로 복제합니다. 운영 중단 시 보조 복사본으로 자동으로 페일오버하여 계층 1 애플리케이션에 비즈니스 연속성을 제공할 수 있습니다. 기본 클러스터를 호스팅하는 사이트에 재해가 발생하면 호스트 다중 경로 소프트웨어는 클러스터를 통과하는 모든 경로를 중지로 표시하고 보조 클러스터의 경로를 사용합니다. 그 결과 ONTAP 중재자가 미러 복사본에 대해 무중단 페일오버를

수행합니다.

확장된 애플리케이션 지원

SnapMirror 액티브 동기화는 사용하기 쉬운 애플리케이션 수준의 세분성과 자동 장애 조치를 통해 유연성을 제공합니다. SnapMirror Active Sync는 IP 네트워크를 통한 검증된 SnapMirror 동기 복제를 사용하여 LAN이나 WAN을 통해 고속으로 데이터를 복제하여 Oracle, Microsoft SQL Server 등과 같은 비즈니스에 중요한 애플리케이션에 대한 높은 데이터 가용성과 빠른 데이터 복제를 가상 및 물리적 환경 모두에서 달성합니다.

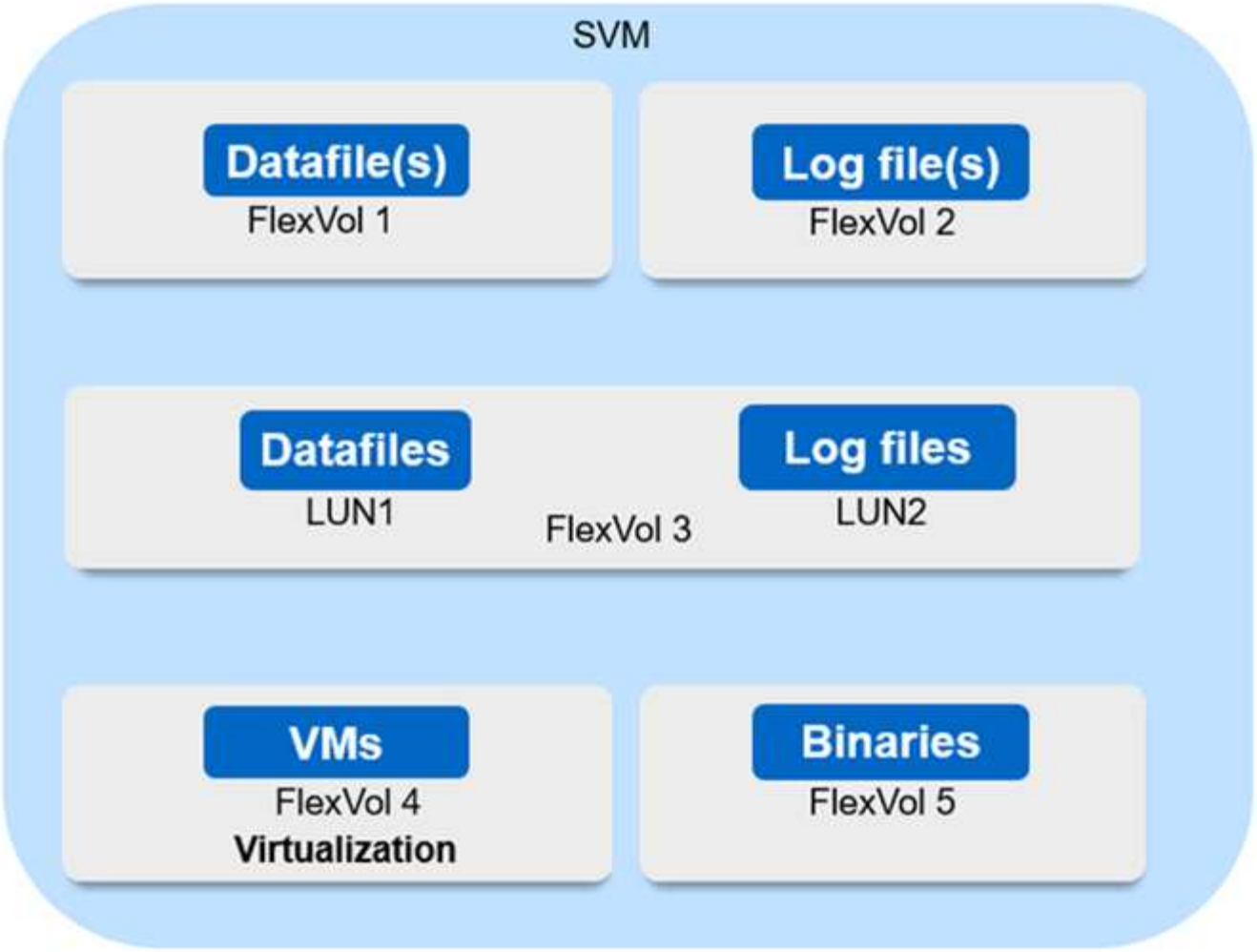
SnapMirror 액티브 동기화를 사용하면 사이트 전체에 장애가 발생하더라도 2차 복사본에 TAF를 적용하여 미션 크리티컬 비즈니스 서비스를 계속 운영할 수 있습니다. 이 장애 조치를 트리거하는 데 수동 개입이나 추가 스크립팅이 필요하지 않습니다.

ONTAP SnapMirror Active Sync를 위한 배포 전략 및 모범 사례

비즈니스 연속성을 위해 보호해야 할 워크로드를 명확하게 식별하여 데이터 보호 전략을 수립하는 것이 중요합니다. 데이터 보호 전략에서 가장 중요한 단계는 기업 애플리케이션 데이터 레이아웃을 명확히 하는 것입니다. 이를 통해 볼륨을 어떻게 분배하고 비즈니스 연속성을 보호할지 결정할 수 있습니다. 장애 조치는 애플리케이션별로 일관성 그룹 수준에서 발생하므로 일관성 그룹에 필요한 데이터 볼륨을 추가해야 합니다.

SVM 구성

다이어그램은 SnapMirror 액티브 동기화에 대한 권장 스토리지 VM(SVM) 구성을 캡처합니다.



- 데이터 볼륨의 경우:
  - 랜덤 읽기 워크로드는 순차적 쓰기에서 격리되므로, 데이터베이스 크기에 따라 데이터 및 로그 파일은 일반적으로 별도의 볼륨에 배치됩니다.
    - 대규모 중요 데이터베이스의 경우 단일 데이터 파일은 FlexVol 1에 있고 해당 로그 파일은 FlexVol 2에 있습니다.
    - 더 나은 통합을 위해 중요도가 낮은 크기의 중요하지 않은 데이터베이스는 모든 데이터 파일이 FlexVol 1에 있고 해당 로그 파일이 FlexVol 2에 있도록 그룹화됩니다. 그러나 이 그룹화를 통해 응용 프로그램 수준의 세분화가 손실됩니다.
  - 또 다른 변형은 모든 파일을 동일한 FlexVol 3 내에 두고, 데이터 파일은 lun1에, 로그 파일은 LUN 2에 저장하는 것입니다.
- 환경이 가상화되어 있으면 여러 엔터프라이즈 애플리케이션에 대한 모든 VM이 데이터 저장소에 공유됩니다. 일반적으로 VM 및 애플리케이션 바이너리는 SnapMirror를 사용하여 비동기식으로 복제됩니다.

계획

ONTAP SnapMirror Active Sync를 위한 필수 구성 요소

SnapMirror 활성 동기화 배포를 계획할 때 다양한 하드웨어, 소프트웨어 및 시스템 구성 요구 사항을 충족하는지 확인하십시오.

하드웨어

다음 표에서는 지원되는 NetApp 클러스터 구성을 간략하게 보여 줍니다.

클러스터 유형입니다	지원 모델	지원되는 기능	지원되는 최대 클러스터 노드
AFF	A-시리즈, C-시리즈	자동 페일오버 이중(대칭형 Active/Active), 자동 페일오버(비대칭형 Active/Active)	• 2 (ONTAP 9.9.1 이상) • 4 (대칭 활성/활성 구성이 있는 ONTAP 9.16.1)
ASA	A-시리즈, C-시리즈	자동 페일오버 이중(대칭형 Active/Active), 자동 페일오버(비대칭형 Active/Active)	• 2 (ONTAP 9.9.1 이상 • 4 (대칭 활성/활성 구성이 있는 ONTAP 9.16.1)
ASA r2	모두	자동 장애 조치 이중화(대칭형 액티브/액티브)	• 2 (ONTAP 9.17.1 또는 이전 버전) • 4 (ONTAP 9.18.1 이상)

아래 표에는 클러스터 유형 간 복제 기능이 간략하게 정리되어 있습니다.

클러스터 유형 1	클러스터 유형 2	복제가 지원됩니까?
AFF A-시리즈	AFF C-Series로 문의하십시오	예
ASA r2 A-시리즈	ASA r2 C-시리즈	예
AFF	ASA	아니요
ASA	ASA r2	아니요
ASA r2	ASA r2	예

소프트웨어

- ONTAP 9.9.1 이상
- ONTAP 중재자 1.2 이상
- 다음 중 하나를 실행하는 ONTAP Mediator용 Linux 서버 또는 가상 머신:

ONTAP 중재자 버전	지원되는 Linux 버전

1.11	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10 • Rocky Linux 10.1, 9.7 및 8.10 • Oracle Linux 10.0 및 9.6
1.10	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.0, 9.6, 9.4 및 8.10 • Rocky Linux 10.0, 9.6 및 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.9	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.8	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8 • Rocky Linux 9.4 및 8.10
1.7	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8 • Rocky Linux 9.3 및 8.9
1.6	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.2, 9.1, 9.0 및 8.8 • Rocky Linux 9.2 및 8.8

1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6

1. 호환 가능이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.

라이센싱

다음 SnapMirror 라이선스는 ONTAP One 라이선스 제품군의 일부로 제공되며 두 클러스터 모두에 적용해야 합니다.

- SnapMirror 동기식
- SnapMirror를 참조하십시오

> 2019년 6월 이전에 ONTAP 스토리지 시스템을 구매한 경우 다음을 참조하세요. "ONTAP 마스터 라이선스 키" 필요한 SnapMirror 동기 라이센스를 받으세요.

- vSphere Metro Storage Cluster(vMSC)의 경우 VMware vSphere 라이선스가 필요합니다.

네트워킹 환경

- 클러스터 간 지연 RTT(Round Trip Time)는 10밀리초 미만이어야 합니다.
- ONTAP 9.14.1부터 "SCSI-3 영구 예약" SnapMirror 액티브 동기화에서 지원됩니다.

지원되는 프로토콜

SnapMirror Active Sync는 SAN 프로토콜을 지원합니다.

- FC 및 iSCSI 프로토콜은 ONTAP 9.9.1부터 지원됩니다.
- NVMe 프로토콜은 ONTAP 9.17.1부터 VMware 워크로드에서 지원됩니다.

  SnapMirror Active Sync는 NVMe 프로토콜을 사용하여 다음을 지원하지 않습니다.

  - 4노드 대칭 액티브/액티브 구성
  - 비대칭 활성/활성 구성
  - 일관성 그룹 크기의 변화

SnapMirror 액티브 싱크에서 NVMe 프로토콜을 사용할 경우 일관성 그룹을 중단 없이 확장하거나 축소할 수 없습니다. SnapMirror 액티브 싱크에서 NVMe 프로토콜을 사용할 경우 일관성 그룹 확장 및 축소 작업은 중단을 수반합니다.

- 동일한 일관성 그룹에서 LUN과 네임스페이스가 공존합니다.

IPspace

SnapMirror Active Sync에서는 클러스터 피어 관계를 위해 기본 IP 공간이 필요합니다. 사용자 정의 IP 공간은 지원되지 않습니다.

NTFS 보안 스타일

SnapMirror 액티브 동기화 볼륨에서는 NTFS 보안 스타일이 * 지원되지 않음 *.

ONTAP 중재자

- ONTAP Mediator는 외부에서 프로비저닝되어야 하며 투명한 애플리케이션 장애 조치를 위해 ONTAP에 연결되어야 합니다.
- 완전한 기능을 갖추고 계획되지 않은 자동 장애 조치를 활성화하려면 외부 ONTAP Mediator를 ONTAP 클러스터로 프로비저닝하고 구성해야 합니다.
- ONTAP Mediator는 두 개의 ONTAP 클러스터와 별도로 세 번째 장애 도메인에 설치해야 합니다.
- ONTAP Mediator를 설치할 때 자체 서명된 인증서를 주요 신뢰할 수 있는 CA에서 서명한 유효한 인증서로 바꿔야 합니다.
- ONTAP Mediator에 대한 자세한 내용은 다음을 참조하세요. "ONTAP Mediator 설치 준비" .

기타 필수 구성 요소

- ONTAP 9.15.1 이전 릴리스에서는 SnapMirror 활성 동기화 관계가 읽기-쓰기 대상 볼륨(비대칭 활성-활성의 DP에서 읽기-쓰기로 변환된 볼륨)에서 지원되지 않습니다. 읽기-쓰기 볼륨을 사용하려면 먼저 볼륨 수준 SnapMirror 관계(비동기 또는 동기)를 생성한 다음 해당 관계를 삭제하여 해당 볼륨을 DP 볼륨으로 변환해야 합니다. 자세한 내용은 다음을 참조하십시오. "기존 SnapMirror 관계를 SnapMirror 활성 동기화로 변환" .
- SnapMirror Active Sync를 사용하는 스토리지 VM은 클라이언트 컴퓨터로 Active Directory에 가입할 수 없습니다.

추가 정보

- "Hardware Universe"
- "ONTAP 중재자 개요"

ONTAP SnapMirror Active Sync 상호 운용성

SnapMirror Active Sync는 다양한 운영 체제, 애플리케이션 호스트 및 ONTAP의 기타 기능과 호환됩니다.

여기에서 다루지 않은 자세한 지원 가능성 및 상호 운용성 정보는 상호 운용성 매트릭스 툴을 ("IMT"참조하십시오.

애플리케이션 호스트

SnapMirror Active Sync는 Hyper-V, ESXi, Red Hat Enterprise Linux(RHEL), Windows Server와 같은 운영 체제, vSphere Metro Storage Cluster(vMSC)와 같은 클러스터링 솔루션을 포함한 하이퍼바이저를 지원하며 ONTAP 9.14.1부터는 Windows Server Failover Cluster도 지원합니다.

운영 체제

SnapMirror Active Sync는 다음과 같은 다양한 운영 체제에서 지원됩니다.

- PVR을 통한 AIX(ONTAP 9.11.1부터)
- HP-UX(ONTAP 9.10.1 시작)
- Solaris 11.4(ONTAP 9.10.1 시작)

AIX

ONTAP 9.11.1부터 AIX는 다음 규정을 이해하는 데 동의하는 표준 엔지니어링 FPVR(Feature Policy Variance Request)을 통해 SnapMirror 액티브 동기화를 지원합니다.

- SnapMirror 액티브 동기화는 제로 RPO 데이터 보호를 제공할 수 있지만 AIX의 페일오버 프로세스에서는 경로 변경을 인식하기 위한 추가 단계가 필요합니다. 루트 볼륨 그룹에 속하지 않는 LUN은 가 될 때까지 I/O 일시 중지를 경험합니다 `cfgmgr` 명령이 실행됩니다. 이를 자동화할 수 있으며, 대부분의 애플리케이션은 추가 운영 중단 없이 운영을 재개합니다.
- 루트 볼륨 그룹에 포함된 LUN은 일반적으로 SnapMirror 활성 동기화를 통해 보호되지 않습니다. 을(를) 실행할 수 없습니다 `cfgmgr` 페일오버 후 명령입니다. 즉, SAN 경로의 변경 사항을 인식하려면 재부팅이 필요합니다. 루트 볼륨 그룹에 대해 제로 RPO 데이터 보호를 달성할 수 있지만, 페일오버는 중단을 야기합니다.

AIX와 SnapMirror active sync에 대한 자세한 내용은 NetApp 세일즈 팀에 문의하십시오.

HP-UX를 참조하십시오

ONTAP 9.10.1부터 HP-UX용 SnapMirror 액티브 동기화가 지원됩니다.

HP-UX를 사용한 자동 비계획 페일오버

기본 클러스터와 보조 클러스터 간의 연결이 끊어지고 기본 클러스터와 중재자 간의 연결도 끊어지면 이중 이벤트 실패로 인해 격리된 마스터 클러스터에서 자동 계획되지 않은 장애 조치(AUFO) 이벤트가 발생할 수 있습니다. 이는 다른 AUFO 행사와 달리 드문 행사로 간주됩니다.

- 이 시나리오에서는 HP-UX 호스트에서 입출력이 재개되는 데 120초 이상 걸릴 수 있습니다. 실행 중인 애플리케이션에 따라 I/O 중단 또는 오류 메시지가 발생할 수 없습니다.
- 문제를 해결하려면 중단 허용 시간이 120초 미만인 HP-UX 호스트에서 애플리케이션을 다시 시작해야 합니다.

Solaris

ONTAP 9.10.1부터 SnapMirror 액티브 동기화는 Solaris 11.4를 지원합니다.

SnapMirror 활성 동기화 환경에서 계획되지 않은 사이트 장애 조치(failover) 전환이 발생할 때 Solaris 클라이언트 애플리케이션이 중단되지 않도록 하려면 기본 Solaris OS 설정을 수정합니다. 권장 설정으로 Solaris를 구성하려면 다음을 참조하세요."NetApp 지식 기반: SnapMirror Active Sync에서 Solaris 호스트 지원 권장 설정" .

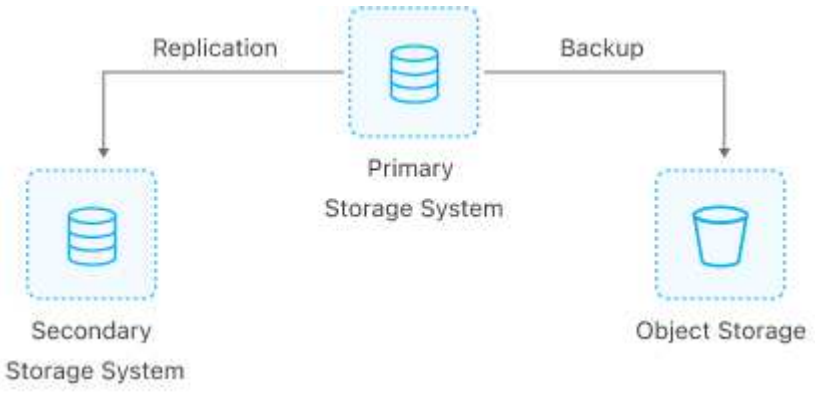
SnapMirror 액티브 동기화는 ONTAP의 구성 요소와 통합되어 데이터 보호 기능을 확장합니다.

FabricPool

SnapMirror 액티브 동기화는 없음, 스냅샷 또는 자동의 계층화 정책으로 FabricPool 애그리게이트에서 소스 및 타겟 볼륨을 지원합니다. SnapMirror 액티브 동기화는 All 의 계층화 정책을 사용하는 FabricPool 애그리게이트를 지원하지 않습니다.

팬아웃 구성

~ 안에팬아웃 구성 소스 볼륨을 SnapMirror 활성 동기화 대상 엔드포인트와 하나의 SnapMirror 비동기 관계에 미러링할 수 있습니다.



SnapMirror Active Sync는 팬아웃 구성 `MirrorAllSnapshots`ONTAP 9.11.1부터 정책 및 `MirrorAndVault` 정책을 지원합니다. 정책을 사용하는 SnapMirror 활성 동기화에서는 팬아웃 구성이 지원되지 `XDPDefault` 않습니다.

ONTAP 9.15.1부터 SnapMirror 액티브 동기화는 페일오버 이벤트 후 팬아웃 구간의 자동 재구성을 지원합니다. 운영 사이트에서 보조 사이트로 페일오버가 성공하면 보조 사이트를 소스로 처리하도록 3차 사이트가 자동으로 다시 구성됩니다. 비동기 팬아웃 구간은 정합성 보장 그룹 관계 또는 독립 볼륨 관계일 수 있습니다. 두 경우 모두 재구성을 수행할 수 있습니다. 재구성이 계획된 또는 계획되지 않은 페일오버에 의해 트리거됩니다. 운영 사이트로 페일백할 때도 재구성이 수행됩니다.

이전 릴리스의 ONTAP에서 팬아웃 구성을 관리하는 방법에 대한 자세한 내용은 을 참조하십시오 팬아웃 구성에서 보호를 재개합니다.

NDMP 복구입니다

ONTAP 9.13.1부터 SnapMirror 활성 동기화와 함께 을 사용할 수 NDMP를 사용하여 데이터를 복제하고 복구합니다있습니다. NDMP를 사용하면 데이터를 SnapMirror 활성 동기화 소스로 이동하여 보호를 일시 중지하지 않고 복원을 완료할 수 있습니다. 이 기능은 특히 팬아웃 구성에 유용합니다.

SnapCenter

SnapMirror 활성 동기화는 부터 SnapCenter에서 "SnapCenter 5.0 을 참조하십시오"지원됩니다. SnapCenter를 사용하면 애플리케이션 및 가상 머신을 보호하고 복구하는 데 사용할 수 있는 스냅샷을 생성할 수 있으므로, 애플리케이션 레벨 세분화로 상시 사용 가능한 스토리지 솔루션을 사용할 수 있습니다.

SnapRestore

SnapMirror 활성 동기화는 부분 및 단일 파일 SnapRestore를 지원합니다.

단일 파일 SnapRestore

ONTAP 9.11.1부터 단일 파일 SnapRestoreSnapMirror 활성 동기화 볼륨에 대해 이 지원됩니다. SnapMirror 활성 동기화 소스에서 대상으로 복제된 스냅샷에서 단일 파일을 복구할 수 있습니다. 볼륨에는 하나 이상의 LUN이 포함될 수 있으므로 이 기능을 사용하면 중단이 적은 복원 작업을 구현하고 다른 LUN을 중단하지 않고 하나의 LUN을 세부적으로 복원할 수 있습니다. Single File SnapRestore에는 데이터 이동 없는 것과 원본 이동 없는 두 가지 옵션이 있습니다.

부분 파일 SnapRestore

ONTAP 9.12.1부터 "부분 LUN 복원"SnapMirror 활성 동기화 볼륨에 대해 이 지원됩니다. SnapMirror 활성 동기화 소스(볼륨)와 대상(스냅샷) 볼륨 간에 복제된 응용 프로그램 생성 스냅샷에서 데이터를 복원할 수 있습니다. 여러 데이터베이스를 동일한 LUN에 저장하는 호스트에서 데이터베이스를 복구해야 하는 경우 부분 LUN 또는 파일 복구가 필요할 수 있습니다. 이 기능을 사용하려면 데이터 및 바이트 수의 시작 바이트 오프셋을 알고 있어야 합니다.

변조 방지 스냅샷

SnapMirror 활성 동기화에서는 변조 방지 스냅샷이 지원되지 않습니다.

대용량 LUN 및 대용량 볼륨

대용량 LUN 및 대용량 볼륨(100TB 이상)에 대한 지원은 사용 중인 ONTAP 버전과 플랫폼에 따라 다릅니다.

ONTAP 9.12.1P2 이상

- ONTAP 9.12.1 P2 이상의 경우 SnapMirror Active Sync는 ASA 및 AFF(A 시리즈 및 C 시리즈)에서 100TB보다 큰 대용량 LUN과 볼륨을 지원합니다. 운영 클러스터와 2차 클러스터의 유형은 ASA 또는 AFF 중 하나여야 합니다. AFF A-Series에서 AFF C-Series로, 또는 그 반대로 복제가 지원됩니다.

> ONTAP 릴리즈 9.12.1P2 이상의 경우 운영 클러스터와 보조 클러스터가 모두 ASA(All-Flash SAN Array) 또는 AFF(All-Flash Array)인지, 둘 다 ONTAP 9.12.1 P2 이상이 설치되어 있는지 확인해야 합니다. 보조 클러스터가 ONTAP 9.12.1P2 이전 버전을 실행 중이거나 스토리지 유형이 운영 클러스터와 동일하지 않은 경우 운영 볼륨이 100TB 이상 증가할 경우 동기식 관계가 동기화되지 않을 수 있습니다.

ONTAP 9.9.1 - 9.12.1P1

- ONTAP 9.9.1 ~ 9.12.1 P1(포함) 사이의 ONTAP 릴리즈의 경우 100TB를 초과하는 대형 LUN과 대용량 볼륨은 All-Flash SAN 어레이에서만 지원됩니다. AFF A-Series에서 AFF C-Series로, 또는 그 반대로 복제가 지원됩니다.

> ONTAP 9.9.9.1과 9.12.1 P2 사이의 ONTAP 릴리즈의 경우 기본 클러스터와 보조 클러스터가 All-Flash SAN 어레이여야 하며 둘 다 ONTAP 9.9.1 이상이 설치되어 있어야 합니다. 2차 클러스터에서 ONTAP 9.9.1 이전 버전을 실행 중이거나 All-Flash SAN 어레이가 아닌 경우 운영 볼륨이 100TB보다 커지면 동기식 관계가 동기화되지 않을 수 있습니다.

추가 정보

- "SnapMirror 액티브 동기화에 대해 AIX 호스트를 구성하는 방법"

ONTAP SnapMirror Active Sync에 대한 개체 제한

SnapMirror 액티브 동기화를 사용하기 위한 준비를 할 때는 다음 개체 제한에 유의하십시오.

클러스터의 일관성 그룹

SnapMirror 액티브 동기화가 있는 클러스터의 일관성 그룹 제한은 관계에 따라 계산되며 사용되는 ONTAP 버전에 따라 달라집니다. 제한은 플랫폼에 독립적입니다.

ONTAP 버전입니다	최대 관계 수
ONTAP 9.11.1 이상	50 *
ONTAP 9.10.1	20
ONTAP 9.9.1	5

* ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터에서는 100개의 일관성 그룹이 지원됩니다.

정합성 보장 그룹당 볼륨

SnapMirror 활성 동기화가 있는 일관성 그룹당 최대 볼륨 수는 플랫폼과는 별개입니다.

ONTAP 버전입니다	일관성 그룹 관계에서 지원되는 최대 볼륨 수입니다
ONTAP 9.15.1 이상	80
ONTAP 9.10.1 - 9.14.1	16
ONTAP 9.9.1	12

볼륨

SnapMirror 활성 동기화의 볼륨 제한은 관계 수가 아닌 끝점 수를 기준으로 계산됩니다. 12개의 볼륨이 있는 일관성 그룹은 운영 클러스터와 보조 클러스터 모두에서 12개의 엔드포인트를 지원합니다. SnapMirror 활성 동기화와 SnapMirror 동기식 관계는 모두 총 엔드포인트 수에 기여합니다.

이러한 제한은 FAS, AFF 및 ASA 시스템에 적용됩니다. ASA r2 시스템(ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 또는 ASA A20)을 사용하는 경우 다음을 참조하십시오. "ASA r2 설명서" .

플랫폼당 최대 엔드포인트는 다음 표에 나와 있습니다.

플랫폼	**SnapMirror** 활성 동기화에 대한 **HA**당 엔드포인트			**HA**당 전체 동기화 및 **SnapMirror** 활성 동기화 엔드포인트		
	ONTAP 9.11.1 이상	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 이상	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400 *	200	60	400	200	80
ASA	400 *	200	60	400	200	80

* ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터의 총 제한은 800개입니다.

SAN 오브젝트 제한

SAN 오브젝트 제한사항은 다음 표에 나와 있습니다. 이 제한은 플랫폼에 관계없이 적용됩니다.

SnapMirror 활성 동기화 관계의 개체	카운트
볼륨당 LUN	• 256(ONTAP 9.9.1 - ONTAP 9.15.0) • 512(ONTAP 9.15.1 이상)
2 x 2 SnapMirror Active Sync 솔루션당 고유한 LUN, 네임스페이스 또는 스토리지 유닛 수	4,096개
4 x 4 SnapMirror 액티브 동기화 솔루션당 고유한 LUN, 네임스페이스 또는 스토리지 유닛 수(ONTAP 9.16.1부터 사용 가능)	6,144
SVM당 LIF(SnapMirror 활성 동기화 관계에 볼륨이 하나 이상 있는 경우)	256
노드당 클러스터 간 LIF	4
클러스터당 클러스터 간 LIF	8

NVMe 객체 제한

ONTAP 9.17.1부터 SnapMirror Active Sync는 NVMe 프로토콜을 지원합니다. NVMe 객체 제한은 다음 표에 포함되어 있습니다.

SnapMirror 활성 동기화 관계의 최대 개체 수	카운트
노드당 네임스페이스 맵 수	4K
클러스터 크기	2개의 노드
HA 쌍당 일관성 그룹 수	50
단일 NVMe SnapMirror 활성 동기화 일관성 그룹의 볼륨 수	80
HA 쌍의 볼륨 수	400
일관성 그룹당 NVMe 서브시스템	16
일관성 그룹당 네임스페이스 맵	256

관련 정보

- "Hardware Universe"
- "정합성 보장 그룹 제한"

구성

SnapMirror 활성 동기화를 위한 ONTAP 클러스터 구성

SnapMirror 액티브 싱크는 장애 조치 발생 시 데이터를 보호하기 위해 피어링된 클러스터를 사용합니다. SnapMirror 액티브 싱크를 위해 ONTAP Mediator 또는 ONTAP Cloud

Mediator를 구성하기 전에 먼저 클러스터가 올바르게 구성되었는지 확인해야 합니다.

시작하기 전에

ONTAP Mediator 또는 ONTAP Cloud Mediator를 구성하기 전에 다음 사항을 확인해야 합니다.

1. 클러스터 간에는 클러스터 피어링 관계가 존재합니다.

   > 클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.

   "클러스터 피어 관계 생성"

2. SVM은 각 클러스터에 생성됩니다.

   "SVM 생성"

3. 각 클러스터의 SVM 사이에는 피어 관계가 존재합니다.

   "SVM 피어링 관계 생성"

4. 볼륨은 LUN에 대해 존재합니다.

   "볼륨을 생성하는 중입니다"

5. 두 클러스터의 각 노드에 최소한 하나의 SAN LIF(해당되는 경우 FC 또는 iSCSI)가 생성됩니다.

   "클러스터 SAN 환경에서 LIF에 대한 고려 사항"

   "LIF 생성"

6. 필요한 LUN이 생성되어 igroup에 매핑됩니다. igroup은 LUN을 애플리케이션 호스트의 개시자에 매핑하는 데 사용됩니다.

   "LUN을 생성하고 igroup을 매핑합니다"

7. 새로운 LUN을 발견하기 위해 애플리케이션 호스트를 다시 검사합니다.

SnapMirror Active Sync를 위한 **ONTAP Mediator** 구성

SnapMirror 액티브 동기화는 장애 조치 시나리오 발생 시 피어링된 클러스터를 사용하여 데이터를 보호합니다. ONTAP Mediator는 각 클러스터의 상태를 모니터링하여 비즈니스 연속성을 보장하는 핵심 리소스입니다. SnapMirror 액티브 동기화를 구성하려면 먼저 ONTAP Mediator를 설치하고 기본 및 보조 클러스터가 올바르게 구성되었는지 확인해야 합니다.

ONTAP Mediator를 설치하고 클러스터를 구성한 후, 자체 서명 인증서를 사용하여 SnapMirror Active Sync용 ONTAP Mediator 초기화 . 그런 다음 해야 SnapMirror 활성 동기화에 대한 일관성 그룹을 생성, 초기화 및 매핑합니다합니다.

ONTAP 중재자

ONTAP Mediator는 SnapMirror 활성 동기화 관계에서 ONTAP 클러스터가 사용하는 고가용성(HA) 메타데이터에

대한 지속적이고 펜싱된 저장소를 제공합니다. 또한 ONTAP Mediator는 쿼럼 확인을 지원하는 동기식 노드 상태 쿼리 기능을 제공하고 컨트롤러 활성화 감지를 위한 Ping 프록시 역할을 합니다.

각 클러스터 피어 관계는 단일 ONTAP 중재자 인스턴스와만 연결할 수 있습니다. HA 중재자 인스턴스는 지원되지 않습니다. 클러스터가 다른 클러스터와 여러 피어 관계에 있는 경우 다음과 같은 ONTAP 중재자 옵션을 사용할 수 있습니다.

- 각 관계에 SnapMirror 활성 동기화가 구성되어 있는 경우 각 클러스터 피어 관계마다 고유한 ONTAP 중재자 인스턴스가 있을 수 있습니다.
- 클러스터는 모든 피어 관계에 대해 동일한 ONTAP 중재자 인스턴스를 사용할 수 있습니다.

예를 들어 클러스터 B가 클러스터 A, 클러스터 C 및 클러스터 D와 피어 관계에 있는 경우 각 관계에 SnapMirror Active Sync가 구성되어 있을 때 세 클러스터 피어 관계 모두 고유한 연결된 ONTAP 중재자 인스턴스를 가질 수 있습니다. 또는, 클러스터 B는 3개의 피어 관계 모두에 동일한 ONTAP 중재자 인스턴스를 사용할 수 있습니다. 이 시나리오에서는 클러스터에 대해 ONTAP mediator의 동일한 인스턴스가 세 번 나열되어 있습니다.

ONTAP 9.17.1부터 다음을 구성할 수 있습니다. "ONTAP 클라우드 중재자" SnapMirror Active Sync 구성에서 클러스터의 상태를 모니터링하려면 두 개의 Mediator를 동시에 사용할 수 없습니다.

ONTAP 9.17.1과 함께 SnapMirror Active Sync 및 ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용하는 경우 다음에서 *알려진 문제 및 제한 사항*을 검토해야 합니다."ONTAP 릴리즈 노트" 이러한 구성에 대한 중요한 정보는 다음을 참조하세요.

ONTAP 중재자 전제 조건

- ONTAP Mediator에는 자체적인 필수 구성 요소가 포함되어 있습니다. ONTAP Mediator를 설치하기 전에 이러한 필수 구성 요소를 충족해야 합니다.

  자세한 내용은 다음을 참조하세요. "ONTAP Mediator 서비스 설치를 준비하세요" .

- 기본적으로 ONTAP Mediator는 TCP 포트 31784를 통해 서비스를 제공합니다. ONTAP 클러스터와 ONTAP Mediator 사이에서 포트 31784가 열려 있고 사용 가능한지 확인해야 합니다.

ONTAP Mediator를 설치하고 클러스터 구성을 확인하세요**.**

ONTAP Mediator를 설치하고 클러스터 구성을 확인하려면 다음 단계를 각각 수행하세요. 각 단계에 대해 특정 구성이 수행되었는지 확인해야 합니다. 각 단계에는 따라야 할 특정 절차에 대한 링크가 포함되어 있습니다.

단계

1. 소스 및 대상 클러스터가 올바르게 구성되었는지 확인하기 전에 ONTAP Mediator를 설치하세요.

   ONTAP Mediator 설치 또는 업그레이드 준비

2. 클러스터 피어링 관계가 클러스터 간에 존재하는지 확인합니다.

   클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.

   "SnapMirror 활성 동기화를 위한 ONTAP 클러스터 구성"

ONTAP Mediator를 설치하고 클러스터 구성을 확인한 후, 클러스터 모니터링을 위해 ONTAP Mediator를 초기화해야 합니다. System Manager 또는 ONTAP CLI를 사용하여 ONTAP Mediator를 초기화할 수 있습니다.

시스템 관리자

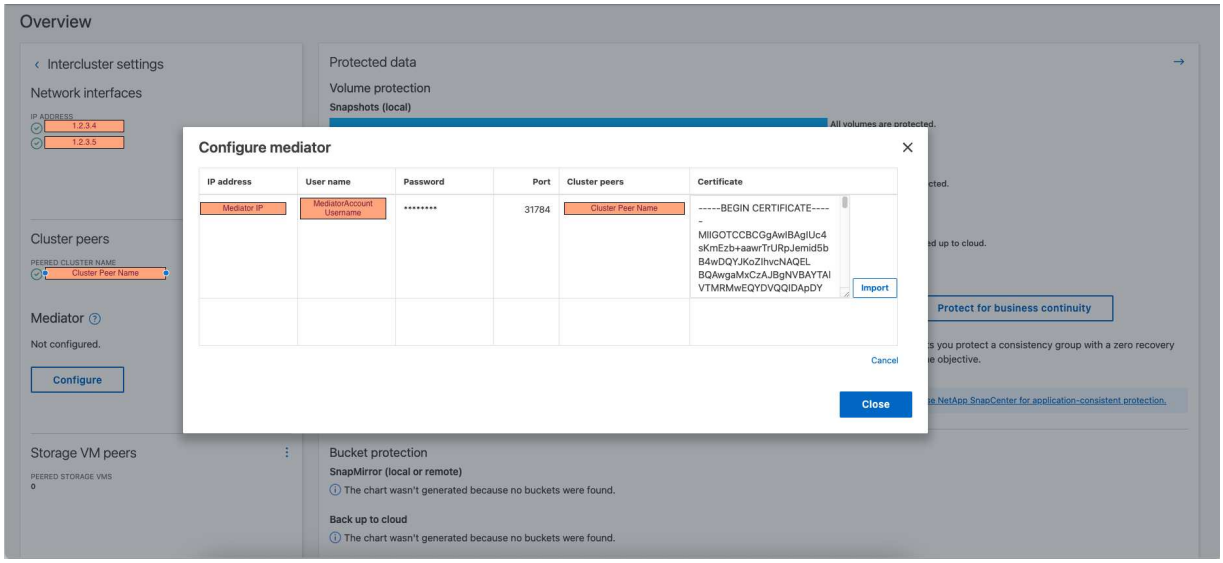
System Manager를 사용하면 ONTAP Mediator를 자동 장애 조치로 구성할 수 있습니다. 자체 서명된 SSL 및 CA를 타사 인증 SSL 인증서 및 CA로 대체할 수도 있습니다(아직 수행하지 않은 경우).

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

ONTAP 중재자 **1.9** 이상

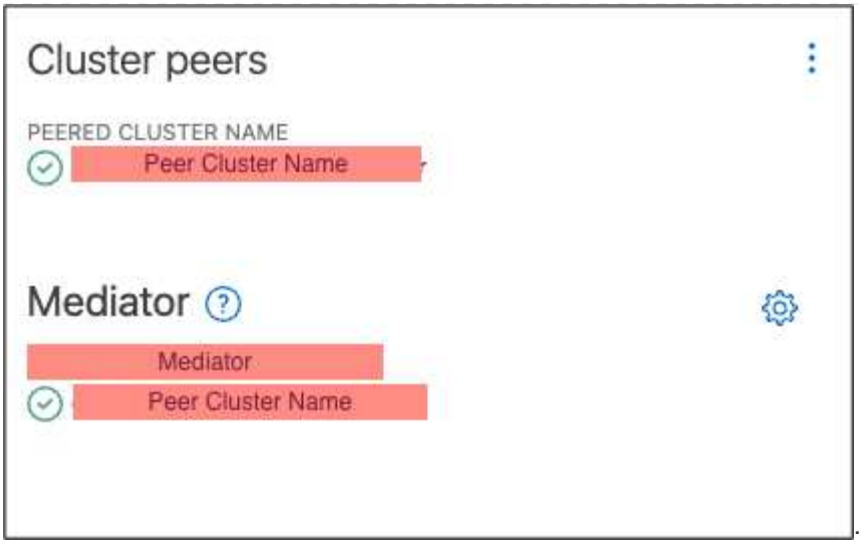
1. 보호 > 개요 > 중재자 > 구성 * 으로 이동합니다.
2. *추가*를 선택하고 다음 ONTAP Mediator 정보를 입력합니다.
   - IPv4 주소입니다
   - 사용자 이름
   - 암호
   - 인증서
3. 다음과 같은 두 가지 방법으로 인증서 입력을 제공할 수 있습니다.
   - * option (a) *: * Import * 를 선택하여 `intermediate.crt` 파일을 탐색하고 가져옵니다.
   - * option (b) *: 파일의 내용을 `intermediate.crt` 복사하여 * Certificate * 필드에 붙여 넣습니다.

   모든 세부 정보가 올바르게 입력되면 제공된 인증서가 모든 피어 클러스터에 설치됩니다.



인증서 추가가 완료되면 ONTAP Mediator가 ONTAP 클러스터에 추가됩니다.

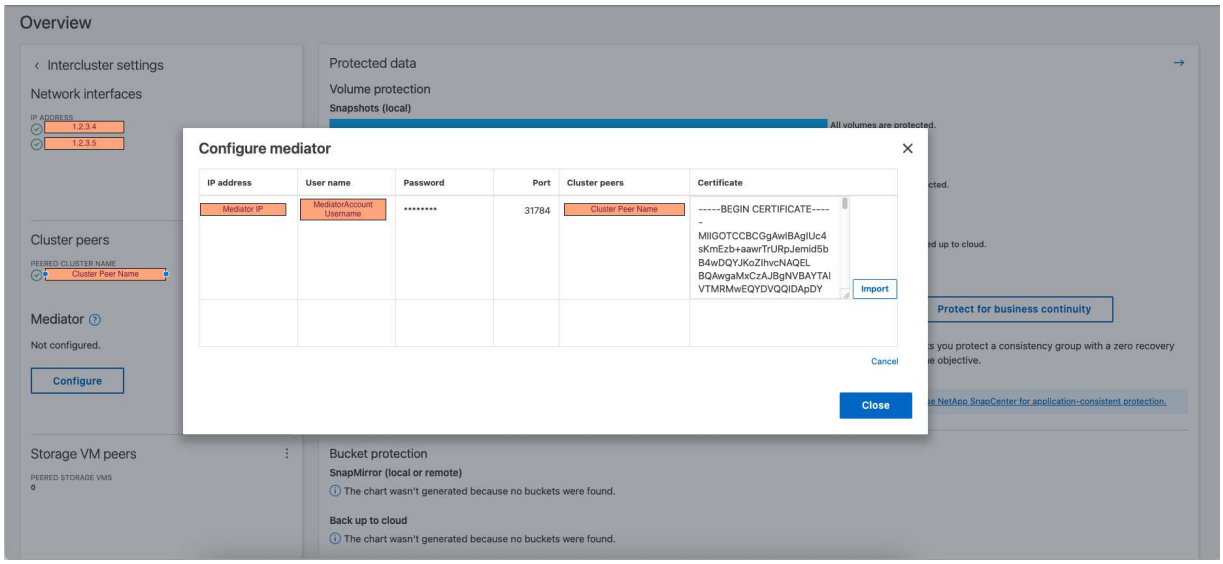
다음 이미지는 성공적인 ONTAP 중재자 구성을 보여줍니다.



ONTAP 중재자 **1.8** 이하

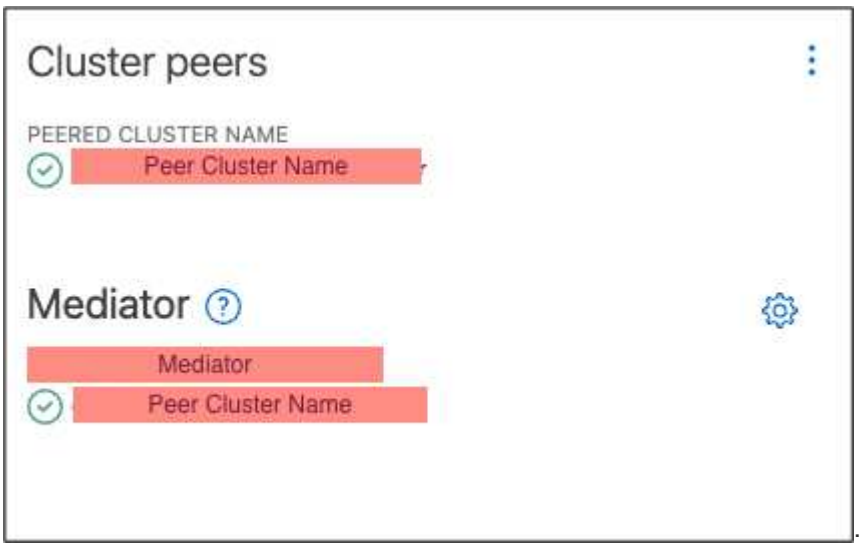
1. 보호 > 개요 > 중재자 > 구성 * 으로 이동합니다.
2. *추가*를 선택하고 다음 ONTAP Mediator 정보를 입력합니다.
   - IPv4 주소입니다
   - 사용자 이름
   - 암호
   - 인증서
3. 다음과 같은 두 가지 방법으로 인증서 입력을 제공할 수 있습니다.
   - * option (a) *: * Import * 를 선택하여 `ca.crt` 파일을 탐색하고 가져옵니다.
   - * option (b) *: 파일의 내용을 `ca.crt` 복사하여 * Certificate * 필드에 붙여 넣습니다.

   모든 세부 정보가 올바르게 입력되면 제공된 인증서가 모든 피어 클러스터에 설치됩니다.



인증서 추가가 완료되면 ONTAP Mediator가 ONTAP 클러스터에 추가됩니다.

다음 이미지는 성공적인 ONTAP 중재자 구성을 보여줍니다.



CLI를 참조하십시오

ONTAP CLI를 사용하여 기본 또는 보조 클러스터에서 ONTAP Mediator를 초기화할 수 있습니다 . `mediator add` 한 클러스터에서 명령을 실행하면 다른 클러스터에 ONTAP Mediator가 자동으로 추가됩니다.

ONTAP Mediator를 사용하여 SnapMirror 활성 동기화 관계를 모니터링하는 경우, 유효한 자체 서명 인증서 또는 인증 기관(CA) 인증서 없이는 ONTAP에서 ONTAP Mediator를 초기화할 수 없습니다. 피어링된 클러스터에 대한 인증서 저장소에 유효한 인증서를 추가합니다. ONTAP Mediator를 사용하여 MetroCluster IP 시스템을 모니터링하는 경우, 초기 구성 후 HTTPS가 사용되지 않으므로 인증서가 필요하지 않습니다.

ONTAP 중재자 **1.9** 이상

1. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 ONTAP 중재자 CA 인증서를 찾습니다 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. 피어링된 클러스터의 인증서 저장소에 유효한 인증 기관을 추가합니다.

   예:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. ONTAP 중재자 CA 인증서를 ONTAP 클러스터에 추가합니다. 메시지가 표시되면 ONTAP Mediator에서 받은 CA 인증서를 삽입하세요. 모든 피어 클러스터에서 단계를 반복합니다.

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   예:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 생성된 인증서 이름을 사용하여 설치된 자체 서명된 CA 인증서를 봅니다.

   `security certificate show -common-name <common_name>`

   예:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 클러스터 중 하나에서 ONTAP Mediator를 초기화합니다. 다른 클러스터에는 ONTAP Mediator가 자동으로 추가됩니다.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 선택적으로 작업 ID 상태를 `job show -id` 확인하여 SnapMirror mediator add 명령이 성공적인지 확인합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAP 중재자 구성의 상태를 점검한다.

스냅미러 중재자 쇼

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` SnapMirror 일관성 그룹 관계가 ONTAP Mediator와 동기화되는지 여부를 나타냅니다. `true` 동기화가 성공했음을 나타냅니다.

ONTAP 중재자 **1.8** 이하

1. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 ONTAP 중재자 CA 인증서를 찾습니다 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. 피어링된 클러스터의 인증서 저장소에 유효한 인증 기관을 추가합니다.

   예:

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. ONTAP 중재자 CA 인증서를 ONTAP 클러스터에 추가합니다. 메시지가 표시되면 ONTAP 중재자로부터 얻은 CA 인증서를 삽입합니다. 모든 피어 클러스터에서 단계를 반복합니다.

   `security certificate install -type server-ca -vserver <vserver_name>`

   예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 생성된 인증서 이름을 사용하여 설치된 자체 서명된 CA 인증서를 봅니다.

   `security certificate show -common-name <common_name>`

   예:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 클러스터 중 하나에서 ONTAP Mediator를 초기화합니다. 다른 클러스터에는 ONTAP Mediator가 자동으로 추가됩니다.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 선택적으로 작업 ID 상태를 `job show -id` 확인하여 SnapMirror mediator add 명령이 성공적인지 확인합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. ONTAP 중재자 구성의 상태를 점검한다.

스냅미러 중재자 쇼

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` SnapMirror 일관성 그룹 관계가 ONTAP Mediator와 동기화되는지 여부를 나타냅니다. `true` 동기화가 성공했음을 나타냅니다.

타사 인증서로 **ONTAP** 중재자를 다시 초기화합니다

ONTAP Mediator를 다시 초기화해야 할 수도 있습니다. ONTAP Mediator IP 주소 변경, 인증서 만료 등 ONTAP Mediator를 다시 초기화해야 하는 상황이 발생할 수 있습니다.

다음 절차에서는 자체 서명된 인증서를 타사 인증서로 대체해야 하는 특정 경우에 대해 ONTAP 중재자를 다시 초기화하는 방법을 보여 줍니다.

이 작업에 대해

SnapMirror Active Sync 클러스터의 자체 서명 인증서를 타사 인증서로 교체하고 ONTAP에서 ONTAP Mediator 구성을 제거한 다음 ONTAP Mediator를 추가해야 합니다.

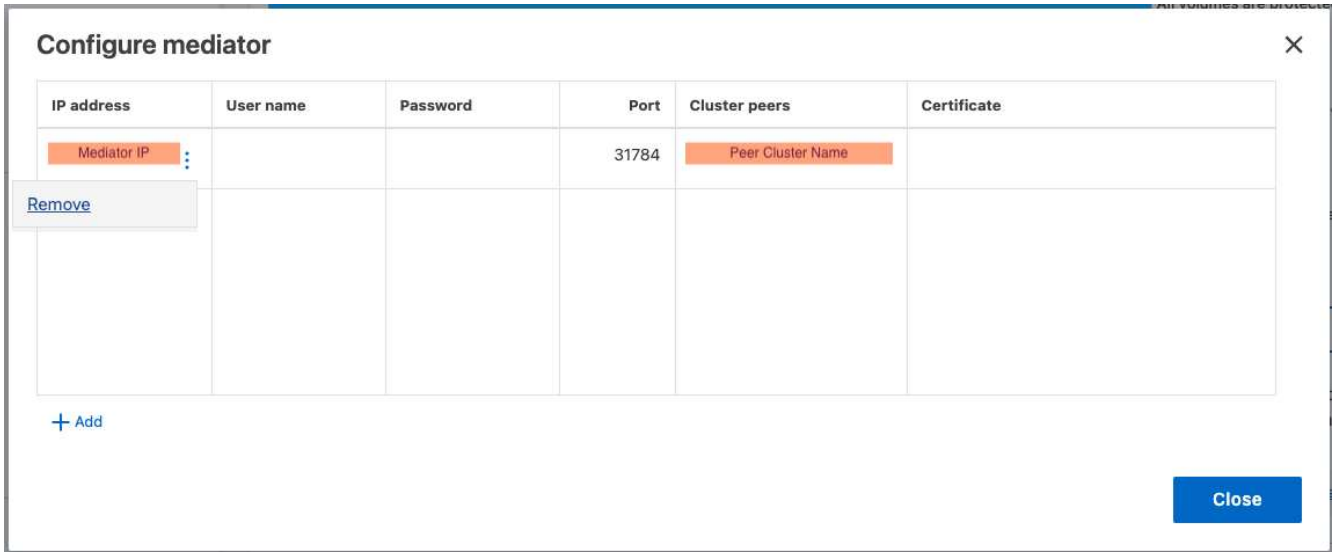
시스템 관리자

System Manager를 사용하여 ONTAP 클러스터에서 이전 자체 서명 인증서로 구성된 ONTAP Mediator 버전을 제거하고 새로운 타사 인증서로 ONTAP 클러스터를 다시 구성해야 합니다.

단계

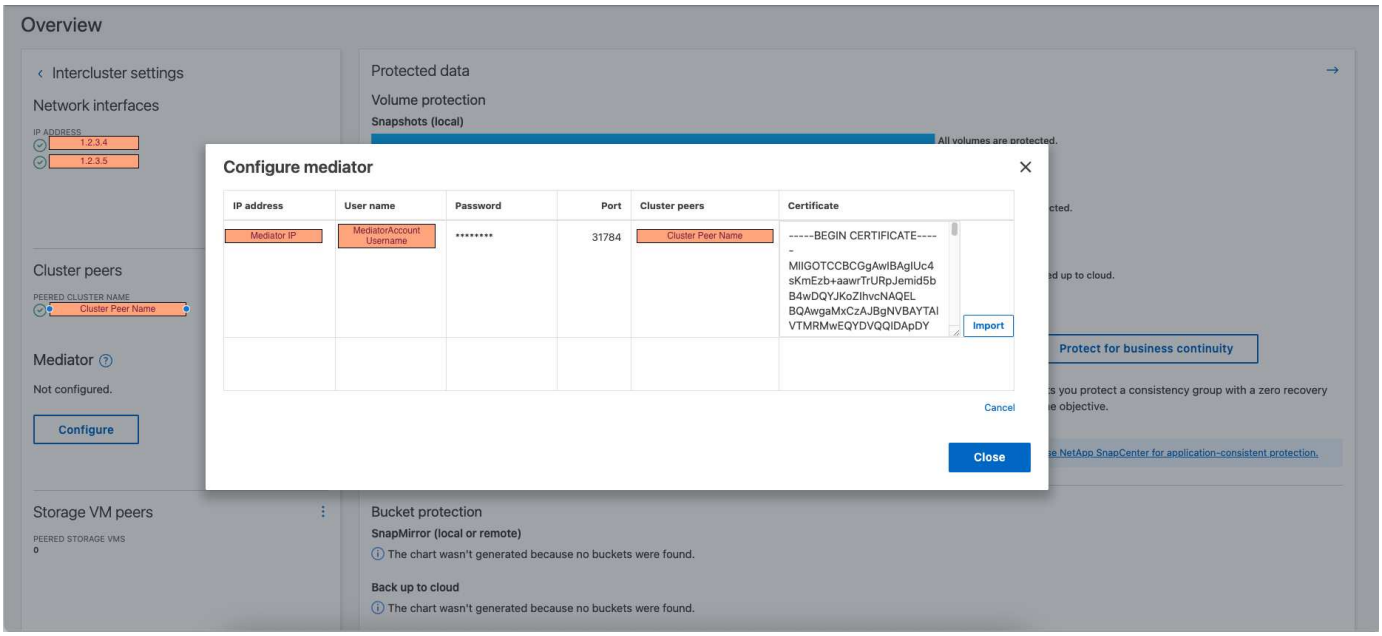
1. 메뉴 옵션 아이콘을 선택하고 *제거*를 선택하여 ONTAP Mediator를 제거하세요.

ⓘ 이 단계에서는 자체 서명된 server-ca를 ONTAP 클러스터에서 제거하지 않습니다. NetApp에서는 타사 인증서를 추가하기 위해 다음 단계를 수행하기 전에 * Certificate * 탭으로 이동하여 수동으로 제거할 것을 권장합니다.



2. 올바른 인증서로 ONTAP Mediator를 다시 추가합니다.

ONTAP Mediator는 이제 새로운 타사 자체 서명 인증서로 구성되었습니다.



CLI를 참조하십시오

ONTAP CLI를 사용하여 자체 서명된 인증서를 타사 인증서로 대체하여 기본 또는 보조 클러스터에서 ONTAP Mediator를 다시 초기화할 수 있습니다.

ONTAP 중재자 **1.9** 이상

1. 모든 클러스터에 대해 자체 서명된 인증서를 사용할 때 이전에 설치한 자체 서명된 `intermediate.crt` 인증서를 제거합니다. 아래 예에서는 두 개의 클러스터가 있습니다.

   예:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 다음을 사용하여 이전에 구성된 ONTAP 중재자를 SnapMirror 활성 동기화 클러스터에서 제거합니다. `-force true`

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 하위 CA에서 인증서를 가져오는 방법에 대한 지침은 `intermediate.crt` 에 설명된 단계를 "자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다"참조하십시오. 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

에는 `intermediate.crt` 파일에 정의된 PKI 권한으로 전송되어야 하는 요청에서 파생되는 특정 속성이 있습니다 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 새 타사 ONTAP 중재자 CA 인증서를 `intermediate.crt` 추가합니다.

   예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt`피어링된 클러스터에 파일을 추가합니다. 모든 피어 클러스터에 대해 이 단계를 반복합니다.

   예:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. SnapMirror 활성 동기화 클러스터에서 이전에 구성한 ONTAP 중재자를 제거합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator를 다시 추가합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` SnapMirror 일관성 그룹 관계가 중재자와의 동기화 여부, 즉 상태를 나타냅니다 `true` 동기화가 성공했음을 나타냅니다.

ONTAP 중재자 **1.8** 이하

1. 모든 클러스터에 대해 자체 서명된 인증서를 사용할 때 이전에 설치한 자체 서명된 `ca.crt` 인증서를 제거합니다. 아래 예에서는 두 개의 클러스터가 있습니다.

   예:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 다음을 사용하여 이전에 구성된 ONTAP 중재자를 SnapMirror 활성 동기화 클러스터에서 제거합니다. `-force true`

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 하위 CA에서 인증서를 가져오는 방법에 대한 지침은 `ca.crt` 에 설명된 단계를 "자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다"참조하십시오. 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

   에는 `ca.crt` 파일에 정의된 PKI 권한으로 전송되어야 하는 요청에서 파생되는 특정 속성이 있습니다 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. ONTAP 중재자 Linux VM/호스트 소프트웨어 설치 위치에서 새 타사 ONTAP 중재자 CA 인증서를 `ca.crt` 추가합니다.

예:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. `intermediate.crt`피어링된 클러스터에 파일을 추가합니다. 모든 피어 클러스터에 대해 이 단계를 반복합니다.

   예:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. SnapMirror 활성 동기화 클러스터에서 이전에 구성한 ONTAP 중재자를 제거합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator를 다시 추가합니다.

   예:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` SnapMirror 일관성 그룹 관계가 중재자와의 동기화 여부, 즉 상태를 나타냅니다 `true` 동기화가 성공했음을 나타냅니다.

관련 정보

- "작업 표시"
- "보안 인증서 삭제"
- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "스냅미러 중재자 추가"
- "스냅미러 중재자 제거"

- "스냅미러 중재자 쇼"

ONTAP Cloud Mediator 구성을 준비하세요

당신 전에 "ONTAP Cloud Mediator 구성" , 전제 조건이 충족되었는지 확인해야 합니다.

방화벽 요구 사항

도메인 컨트롤러의 방화벽 설정은 HTTPS 트래픽을 허용해야 합니다. `api.bluexp.netapp.com` 두 클러스터 모두에서.

프록시 서버 요구 사항

SnapMirror Active Sync에 프록시 서버를 사용하는 경우 프록시 서버가 생성되었고 다음 프록시 서버 정보가 있는지 확인하세요.

- HTTPS 프록시 IP
- 포트
- 사용자 이름
- 암호

숨어 있음

NetApp 콘솔 클라우드 서버와 SnapMirror Active Sync 클러스터 피어 간의 권장 ping 지연 시간은 200ms 미만입니다.

루트 **CA** 인증서

클러스터에서 인증서를 확인하세요

ONTAP 에는 잘 알려진 루트 CA 인증서가 미리 설치되어 있으므로 대부분의 경우 NetApp 콘솔 서버의 루트 CA 인증서를 설치할 필요가 없습니다. ONTAP Cloud Mediator 구성을 시작하기 전에 클러스터를 확인하여 인증서가 있는지 확인할 수 있습니다.

예:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
```

```
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

설치된 인증서에 대한 프록시 서버를 확인하세요

NetApp 콘솔에서 ONTAP Cloud Mediator 서비스에 연결하기 위해 프록시를 사용하는 경우 프록시 서버의 루트 CA 인증서가 ONTAP 에 설치되어 있는지 확인하세요.

예:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

CA 인증서를 다운로드하세요:

필요한 경우 인증 기관 웹사이트에서 루트 CA 인증서를 다운로드하여 클러스터에 설치할 수 있습니다.

예:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

SnapMirror Active Sync를 위한 **ONTAP Cloud Mediator** 구성

ONTAP 9.17.1부터 ONTAP Cloud Mediator를 사용하여 각 클러스터의 상태를 모니터링하여 비즈니스 연속성을 확보할 수 있습니다. ONTAP Cloud Mediator는 클라우드 기반 서비스입니다. SnapMirror 활성 동기화와 함께 ONTAP Cloud Mediator를 사용하는 경우 먼저 NetApp 콘솔 서비스와 클라이언트 정보가 구성되어 있는지 확인하고 적절한 클러스터 피어링을 보장해야 합니다.

ONTAP Mediator와 마찬가지로 ONTAP Cloud Mediator는 SnapMirror 활성 동기화 관계에서 ONTAP 클러스터가 사용하는 고가용성(HA) 메타데이터를 위한 영구적이고 펜싱된 저장소를 제공합니다. ONTAP Cloud Mediator는 쿼럼 결정을 지원하는 동기식 노드 상태 쿼리 기능을 제공하고, 컨트롤러 활성 상태 감지를 위한 ping 프록시 역할을 합니다.

ONTAP 9.17.1과 함께 SnapMirror Active Sync 및 ONTAP Mediator 또는 ONTAP Cloud Mediator를 사용하는 경우 다음에서 *알려진 문제 및 제한 사항*을 검토해야 합니다."ONTAP 릴리즈 노트" 이러한 구성에 대한 중요한 정보는 다음을 참조하세요.

시작하기 전에

ONTAP Cloud Mediator를 구성하기 전에 다음 정보를 확인해야 합니다.

- 클러스터가 구성되었습니다.

  "SnapMirror 활성 동기화를 위한 ONTAP 클러스터 구성"

- NetApp 콘솔에서 NetApp 콘솔 조직 ID를 복사하고 ONTAP Cloud Mediator를 구성할 때 사용할 콘솔 구성원 서비스 계정을 생성했습니다. 서비스 계정을 생성할 때 조직은 ONTAP Cloud Mediator를 구성한 구독으로 설정해야 합니다. 범주는 *애플리케이션*으로, 역할 유형은 * ONTAP Mediator 설정 역할*로 설정해야 합니다. 역할을 생성할 때 클라이언트 ID와 클라이언트 비밀번호를 저장해야 합니다.

  "NetApp 콘솔 멤버 및 서비스 계정 추가"

단계

System Manager나 ONTAP CLI를 사용하여 ONTAP Cloud Mediator를 추가할 수 있습니다.

시스템 관리자

1. *보호 > 개요 > 중재자*로 이동하여 *추가*를 선택합니다.
2. 중개자 추가 창에서 중개자 유형으로 *클라우드*를 선택하고 다음 정보를 입력합니다.
   - NetApp 콘솔 조직 ID
   - NetApp 콘솔 클라이언트 ID
   - NetApp 콘솔 클라이언트 비밀번호
3. 클러스터 피어를 선택하세요.
4. HTTP 프록시를 사용 중이고 아직 구성하지 않은 경우 로컬 및 원격 호스트에 대한 HTTP 프록시 정보를 입력합니다.

   각 클러스터 피어에 대해 다른 프록시 서버를 사용하는 것이 좋습니다.

5. 선택 사항: 특히 프록시 서버를 사용하는 경우 ONTAP 에 루트 CA 인증서를 설치해야 하는 경우 제공된 텍스트 상자에 인증서를 붙여넣습니다.
6. 추가 * 를 선택합니다.
7. *보호 > 개요*로 이동하여 SnapMirror Active Sync 클러스터와 ONTAP Cloud Mediator 간의 관계 상태를 확인합니다.

CLI를 참조하십시오

1. ONTAP Cloud Mediator 구성:
   `snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp -org-id <NetApp Console Organization ID> -service-account-client-id <Service Account Client ID> -use-http-proxy-local <true|false> -use-http -proxy-remote <true|false>`
2. ONTAP Cloud Mediator 상태 확인:
   `snapmirror mediator show`

   예:

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
0.0.0.0          C2_cluster       connected         true
cloud
```

ONTAP SnapMirror Active Sync로 보호하세요

SnapMirror 액티브 동기화는 ONTAP 9.15.1부터 대칭 액티브/액티브 보호까지 비대칭 보호를 제공합니다.

SnapMirror 활성 동기화를 사용하여 비대칭 보호를 구성하려면 ONTAP 소스 클러스터에서 LUN을 선택하고 일관성 그룹에 추가해야 합니다.

시작하기 전에

- SnapMirror 동기식 라이센스가 있어야 합니다.
- 클러스터 또는 스토리지 VM 관리자여야 합니다.
- 일관성 그룹의 모든 구성 볼륨은 단일 스토리지 VM(SVM)에 있어야 합니다.
  - LUN은 서로 다른 볼륨에 상주할 수 있습니다.
- 소스 클러스터와 대상 클러스터는 같을 수 없습니다.
- ASA 클러스터 및 비 ASA 클러스터에 걸쳐 SnapMirror 활성 동기화 일관성 그룹 관계를 설정할 수 없습니다.
- 클러스터 피어 관계를 위한 SnapMirror 액티브 동기화에 기본 IPspace가 필요합니다. 사용자 지정 IPspace는 지원되지 않습니다.
- 일관성 그룹의 이름은 고유해야 합니다.
- 보조(대상) 클러스터의 볼륨은 DP 유형이어야 합니다.
- 운영 SVM과 2차 SVM은 피어링된 관계에 있어야 합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 일관성 그룹을 구성할 수 있습니다.

ONTAP 9.10.1부터 ONTAP System Manager에서 일관성 그룹 엔드포인트와 메뉴를 제공하여 추가 관리 유틸리티를 제공합니다. ONTAP 9.10.1 이상을 사용하는 경우 다음을 참조하십시오. "일관성 그룹을 구성합니다" 그 다음에 "보호 구성" SnapMirror 활성 동기화 관계를 생성합니다.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

시스템 관리자

1. 운영 클러스터에서 * 보호 > 개요 > 무중단 업무 운영 보호 > LUN 보호 * 로 이동합니다.
2. 보호할 LUN을 선택하고 보호 그룹에 추가합니다.
3. 대상 클러스터와 SVM을 선택합니다.
4. 기본적으로 * 관계 초기화 * 가 선택됩니다. 보호를 시작하려면 * 저장 * 을 클릭합니다.
5. 대시보드 > 성능 * 으로 이동하여 LUN의 IOPS 활동을 확인합니다.
6. 대상 클러스터에서 System Manager를 사용하여 비즈니스 연속성 관계에 대한 보호가 동기화 상태인지 확인합니다. * 보호 > 관계 *.

CLI를 참조하십시오

1. 타겟 클러스터에서 일관성 그룹 관계를 생성합니다.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   를 사용하여 구성 볼륨을 최대 12개까지 매핑할 수 있습니다 `cg-item-mappings` 의 매개 변수입니다 `snapmirror create` 명령.

   다음 예에서는 두 개의 일관성 그룹을 생성합니다. `cg_src_ on the source with `vol1` 및 `vol2` 미러링된 타겟 정합성 보장 그룹, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. 대상 클러스터에서 일관성 그룹을 초기화합니다.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. 초기화 작업이 성공적으로 완료되었는지 확인하십시오. 상태는 InSync가 되어야 합니다.

   스냅미러 쇼

4. 각 클러스터에서 igroup을 생성하여 애플리케이션 호스트의 이니시에이터에 LUN을 매핑할 수 있습니다.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   에 대한 자세한 내용은 `lun igroup create` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 각 클러스터에서 LUN을 igroup에 매핑합니다.

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. 에서 LUN 매핑이 성공적으로 완료되었는지 확인합니다 `lun map` 명령. 그런 다음 애플리케이션 호스트에서 새 LUN을 검색할 수 있습니다.

System Manager 또는 ONTAP CLI를 사용하여 대칭 보호를 설정할 수 있습니다. 두 인터페이스 모두에서 에 대한 단계가 다릅니다 균일 및 비균일 설정.

시작하기 전에

- 두 클러스터에서 모두 ONTAP 9.15.1 이상을 실행해야 한다.
- 대칭 액티브/액티브 구성에는 이 필요합니다 `AutomatedFailoverDuplex` 보호 정책. 또는, 가능합니다 사용자 지정 SnapMirror 정책을 생성합니다 제공함 `-type` 있습니다 `automated-failover-duplex`.
- ONTAP 9.15.1에서 대칭 액티브/액티브는 2노드 클러스터에서만 지원됩니다.
- ONTAP 9.16.1 GA부터 SnapMirror 액티브 동기화는 4노드 클러스터에서 대칭 액티브/액티브 구성을 지원합니다.
  - 4노드 클러스터에서 SnapMirror 액티브 동기화를 사용하려면 ONTAP 9.16.1 GA 이상을 실행해야 합니다.
  - 4노드 구성을 배포하기 전에 먼저 해야 클러스터 피어 관계를 생성합니다합니다.
  - 4노드 클러스터의 경우 를 제한검토합니다.
  - 2노드 클러스터로 되돌리는 경우 되돌리기 전에 클러스터에서 SnapMirror 액티브 동기화 관계를 제거해야 합니다.
  - 4노드 구성을 사용하여 스토리지와 컨트롤러를 업그레이드할 수 있습니다. 이 프로세스는 무중단 작업으로, 볼륨을 새 노드로 이동하는 동안 클러스터를 확장합니다. 자세한 내용은 을 "클러스터를 새로 고칩니다 "참조하십시오.
- ONTAP 9.17.1부터 두 클러스터 모두 ONTAP 9.17.1 이상을 실행하는 경우에만 NVMe 네임스페이스에서 대칭적 액티브/액티브 보호를 구성할 수 있습니다.

SCSI SnapMirror 활성 동기화 구성을 사용하여 대칭 활성/활성 보호 구성

단계

시스템 관리자나 ONTAP CLI를 사용하여 SCSI 프로토콜 호스트 매핑을 사용하여 대칭적 활성/활성 보호를 구성할 수 있습니다.

시스템 관리자

균일 설정에 대한 단계

1. 운영 사이트에서 "새 LUN을 사용하여 일관성 그룹을 생성합니다."
   a. 일관성 그룹을 생성할 때 호스트 이니시에이터를 지정하여 igroup을 생성합니다.
   b. 확인란을 선택하여 **SnapMirror** 활성화 를 선택한 다음 을 선택합니다 `AutomatedFailoverDuplex` 정책.
   c. 표시되는 대화 상자에서 **Replicate initiator groups** 확인란을 선택하여 igroup을 복제합니다. 근접 설정 편집** 에서 호스트의 근접 SVM을 설정합니다.
   d. 저장을 선택합니다.

비균일 설정에 대한 단계

1. 운영 사이트에서 "새 LUN을 사용하여 일관성 그룹을 생성합니다."
   a. 일관성 그룹을 생성할 때 호스트 이니시에이터를 지정하여 igroup을 생성합니다.
   b. 확인란을 선택하여 **SnapMirror** 활성화 를 선택한 다음 을 선택합니다 `AutomatedFailoverDuplex` 정책.
   c. LUN, 일관성 그룹, igroup, SnapMirror 관계 및 igroup 매핑을 생성하려면 저장을 선택합니다.
2. 2차 사이트에서 igroup을 생성하고 LUN을 매핑합니다.
   a. **Hosts> SAN Initiator Groups** 로 이동합니다.
   b. 새 igroup을 생성하려면 **+** 추가 를 선택하십시오.
   c. 이름 제공, 호스트 운영 체제 를 선택한 다음 이니시에이터 그룹 구성원 을 선택합니다.
   d. 관계를 초기화하려면 저장 을 선택합니다.
3. 새로운 igroup을 대상 LUN에 매핑합니다.
   a. 스토리지 **>** LUN** 으로 이동합니다.
   b. igroup에 매핑할 모든 LUN을 선택합니다.
   c. 추가 를 선택한 다음 이니시에이터 그룹에 매핑** 을 선택합니다.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 애플리케이션의 모든 볼륨을 그룹화하는 새로운 SnapMirror 관계를 생성합니다. 를 지정했는지 확인합니다 `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예: 다음 예에서는 두 개의 일관성 그룹을 만듭니다. 소스에 vol1 및 vol2가 있는 cg_src와 대상에 미러링된 일관성 그룹인 cg_dst입니다.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. SnapMirror 관계 초기화:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   `snapmirror show -destination-path <destination_path>`
4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. igroup 구성을 설정합니다. 로컬 클러스터에서 이니시에이터에 대한 기본 경로를 설정합니다. 역선호도를 위해 피어 클러스터로 구성을 복제하는 옵션을 지정합니다.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   ONTAP 9.16.1부터 `-proximal-vserver local` 이 명령의 매개 변수를 사용합니다.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   ONTAP 9.16.1부터 `-proximal-vserver peer` 이 명령의 매개 변수를 사용합니다.
6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN으로 연결되는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

비균일 설정에 대한 단계

1. 애플리케이션의 모든 볼륨을 그룹화하는 새로운 SnapMirror 관계를 생성합니다. 를 지정했는지 확인합니다 `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예: 다음 예에서는 두 개의 일관성 그룹을 만듭니다. 소스에 vol1 및 vol2가 있는 cg_src와 대상에 미러링된 일관성 그룹인 cg_dst입니다.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
   AutomatedFailOverDuplex
   ```

2. SnapMirror 관계 초기화:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. 소스 및 대상 클러스터 모두에서 igroup 구성을 설정합니다.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN으로 연결되는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

NVMe SnapMirror 활성 동기화 구성을 사용하여 대칭 활성/활성 보호 구성

시작하기 전에

대칭적 액티브/액티브 보호를 구성하는 데 필요한 요구 사항 외에도 NVMe 프로토콜을 사용할 때 지원되는 구성과 지원되지 않는 구성을 알고 있어야 합니다.

- 일관성 그룹에는 하나 이상의 하위 시스템이 있을 수 있습니다.
- 일관성 그룹 내의 볼륨은 여러 하위 시스템의 네임스페이스 맵을 가질 수 있습니다.
- 하위 시스템은 두 개 이상의 일관성 그룹에 속하는 네임스페이스 맵을 가질 수 없습니다.
- 하위 시스템은 일관성 그룹에 속하는 일부 네임스페이스 맵과 일관성 그룹에 속하지 않는 일부 네임스페이스 맵을 가질 수 없습니다.
- 하위 시스템에는 동일한 일관성 그룹에 속하는 네임스페이스 맵이 있어야 합니다.

단계

ONTAP 9.17.1부터 System Manager나 ONTAP CLI를 사용하여 일관성 그룹을 만들고 NVMe 프로토콜 호스트 매핑을 사용하여 대칭적 활성/활성 보호를 구성할 수 있습니다.

시스템 관리자

1. 기본 사이트에서 "새로운 볼륨이나 NVMe 네임스페이스를 사용하여 일관성 그룹을 만듭니다."
2. *+추가*를 선택하고 *새 NVMe 네임스페이스 사용*을 선택합니다.
3. 일관성 그룹 이름을 입력하세요.
4. *더보기*를 선택하세요.
5. 보호 섹션에서 * SnapMirror 활성화*를 선택한 다음 다음을 선택합니다. `AutomatedFailoverDuplex` 정책.
6. 호스트 매핑 섹션에서 기존 **NVMe** 하위 시스템 또는 *새 NVMe 하위 시스템*을 선택합니다.
7. 근위 SVM을 변경하려면 *근접*을 선택하세요. 기본적으로 소스 SVM이 선택됩니다.
8. 필요한 경우 다른 NVMe 하위 시스템을 추가합니다.

CLI를 참조하십시오

1. 애플리케이션에서 사용하는 모든 NVMe 네임스페이스를 포함하는 모든 볼륨을 그룹화하는 새 SnapMirror 관계를 생성합니다 . `AutomatedFailOverDuplex` 양방향 동기화 복제를 설정하는 정책입니다.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   예:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. SnapMirror 관계 초기화:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   예:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. 을(를) 기다리면 작업이 성공적으로 수행되었는지 확인합니다 `Mirrored State` 를 눌러 로 표시합니다 `SnapMirrored` 및 `Relationship Status` 현재 `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

   기본 볼륨의 NVMe 네임스페이스와 연결된 NVMe 하위 시스템은 자동으로 보조 클러스터에 복제됩니다.

4. 호스트에서 필요에 따라 각 클러스터에 대한 액세스를 통해 호스트 연결을 구성합니다.
5. 각 호스트에 인접한 SVM을 지정하세요. 이렇게 하면 호스트가 기본 클러스터의 경로를 사용하여 NVMe 네임스페이스에 액세스할 수 있습니다. 이는 기본 클러스터의 SVM 또는 DR 클러스터의 SVM일 수 있습니다.

다음 명령은 SVM VS_A가 호스트 H1에 근접해 있고 VS_A를 근접 SVM으로 설정함을 나타냅니다.

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

다음 명령은 SVM VS_B가 호스트 H2에 근접해 있음을 나타내며 VS_B를 근접 SVM으로 설정합니다.

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. 호스트에서 경로를 검색하고 호스트에 기본 클러스터의 스토리지로 가는 활성/최적화된 경로가 있는지 확인합니다.
7. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산하여 필요한 로드 밸런싱을 수행합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 초기화"
- "스냅미러 쇼"

기존 ONTAP SnapMirror 관계를 SnapMirror Active Sync 관계로 변환

SnapMirror 보호를 구성한 경우 관계를 SnapMirror 액티브 동기화로 변환할 수 있습니다. ONTAP 9.15.1부터 대칭 액티브/액티브 보호를 사용하도록 관계를 변환할 수 있습니다.

기존 iSCSI 또는 FC SnapMirror 관계를 비대칭 SnapMirror Active Sync 관계로 변환

소스 클러스터와 대상 클러스터 간에 기존 iSCSI 또는 FC SnapMirror 동기 관계가 있는 경우, 이를 비대칭 SnapMirror 활성 동기화 관계로 변환할 수 있습니다. 이를 통해 미러링된 볼륨을 일관성 그룹과 연결하여 다중 볼륨 워크로드에서 RPO를 0으로 유지할 수 있습니다. 또한 SnapMirror 활성 동기화 관계 설정 이전 시점으로 되돌려야 하는 경우 기존 SnapMirror 스냅샷을 보존할 수 있습니다.

이 작업에 대해

- Primary 및 Secondary 클러스터에서 클러스터 및 SVM 관리자여야 합니다.
- SnapMirror 정책을 변경하여 제로 RPO를 제로 RTO 동기화로 변환할 수 없습니다.
- 를 실행하기 전에 LUN이 매핑 해제되었는지 확인해야 합니다 `snapmirror create` 명령.

  2차 볼륨의 기존 LUN이 매핑되어 있는 경우 `AutomatedFailover` 정책이 구성되어 있습니다 `snapmirror create` 명령이 오류를 트리거합니다.

시작하기 전에

- 기본 클러스터와 보조 클러스터 사이에는 0 RPO SnapMirror 동기 관계가 존재해야 합니다.
- 제로 RTO SnapMirror 관계를 생성하기 전에 대상 볼륨의 모든 LUN을 매핑 해제해야 합니다.
- SnapMirror 액티브 동기화는 SAN 프로토콜만 지원합니다(NFS/CIFS 제외). NAS 액세스를 위해 정합성 보장 그룹의 구성 요소 가 마운트되지 않았는지 확인합니다.
- "ONTAP 중재자" SnapMirror Active Sync에 맞게 구성해야 합니다.

단계

1. 보조 클러스터에서 기존 관계에 대한 SnapMirror 업데이트를 수행합니다.

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirror 업데이트가 성공적으로 완료되었는지 확인합니다.

```
SiteB::>snapmirror show
```

3. 각 제로 RPO 동기식 관계를 일시 중지합니다.

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. 각 제로 RPO 동기식 관계 삭제:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. 소스 SnapMirror 관계를 해제하지만 공통 스냅샷은 보존합니다.

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. 제로 RTO SnapMirror 동기식 관계 생성:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. 정합성 보장 그룹을 다시 동기화합니다.

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

기존 **iSCSI** 또는 **FC SnapMirror** 관계를 대칭 활성/활성으로 변환

ONTAP 9.15.1부터 기존 iSCSI 또는 FC SnapMirror 관계를 SnapMirror 활성 동기화 대칭 활성/활성 관계로 변환할 수 있습니다.

시작하기 전에

- ONTAP 9.15.1 이상을 실행 중이어야 합니다.
- 운영 클러스터와 2차 클러스터 사이에 제로 RPO SnapMirror 동기화 관계가 있어야 합니다.
- 제로 RTO SnapMirror 관계를 생성하기 전에 대상 볼륨의 모든 LUN을 매핑 해제해야 합니다.

- SnapMirror 액티브 동기화는 SAN 프로토콜만 지원합니다(NFS/CIFS 제외). NAS 액세스를 위해 정합성 보장 그룹의 구성 요소 가 마운트되지 않았는지 확인합니다.
- "ONTAP 중재자" SnapMirror Active Sync에 맞게 구성해야 합니다.

단계

1. 보조 클러스터에서 기존 관계에 대한 SnapMirror 업데이트를 수행합니다.

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. SnapMirror 업데이트가 성공적으로 완료되었는지 확인합니다.

```
SiteB::>snapmirror show
```

3. 각 제로 RPO 동기식 관계를 일시 중지합니다.

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. 각 제로 RPO 동기식 관계 삭제:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. 소스 SnapMirror 관계를 해제하지만 공통 스냅샷은 보존합니다.

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. AutomatedFailoverDuplex 정책을 사용하여 제로 RTO SnapMirror 동기식 관계를 생성합니다.

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. 기존 호스트가 로컬 운영 클러스터인 경우 보조 클러스터에 호스트를 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
8. 2차 사이트에서 원격 호스트와 연결된 igroup에서 LUN 매핑을 삭제합니다.

   igroup에 복제되지 않은 LUN에 대한 맵이 포함되어 있지 않은지 확인합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. 운영 사이트에서 기존 호스트의 이니시에이터 구성을 수정하여 로컬 클러스터의 이니시에이터에 대한 근위 경로를 설정합니다.

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 선호도를 해당 로컬 사이트에 근접하게 설정합니다. Ennable igroup replication으로 구성을 복제하고 원격 클러스터에서 호스트 인접성을 반전합니다.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
12. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.
13. 정합성 보장 그룹을 다시 동기화합니다.

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "SnapMirror 중지"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"
- "스냅미러 쇼"

ONTAP SnapMirror 활성 동기화 관계 유형 변환

ONTAP 9.15.1부터 비대칭에서 대칭 액티브/액티브로, 또는 그 반대로 SnapMirror 액티브 동기화 보호 유형 간에 전환할 수 있습니다.

대칭 액티브/액티브 관계로 변환합니다

비대칭 보호 기능이 있는 iSCSI 또는 FC SnapMirror 활성 동기화 관계를 대칭 활성/활성으로 변환할 수 있습니다.

시작하기 전에

- 두 클러스터에서 모두 ONTAP 9.15.1 이상을 실행해야 한다.
- 대칭 액티브/액티브 구성에는 이 필요합니다 `AutomatedFailoverDuplex` 보호 정책. 또는, 가능합니다 사용자 지정 SnapMirror 정책을 생성합니다 제공함 `-type` 있습니다 `automated-failover-duplex`.

시스템 관리자

균일 설정에 대한 단계

1. 대상 igroup 제거:
   a. 대상 클러스터에서 **Hosts** > **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
2. SnapMirror 활성 동기화 관계를 편집합니다.
   a. 보호> 관계 로 이동합니다.
   b. 수정할 관계 옆에 있는 kabob 메뉴를 선택한 다음 편집 을 선택합니다.
   c. 보호 정책을 AutomatedFailoverDuplex로 수정합니다.
   d. 선택 `AutoMatedFailoverDuplex` 호스트 근접 설정을 수정할 수 있는 대화 상자를 표시합니다. 초기자에 대해 초기자 근위에서부터 그리고 저장에 대한 적절한 옵션을 선택합니다.
   e. 저장을 선택합니다.
3. 보호 메뉴에서 관계가 로 표시될 때 작업이 성공했는지 확인합니다 `InSync`.

비균일 설정에 대한 단계

1. 대상 igroup 제거:
   a. 보조 사이트에서 **Hosts** > **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
2. 새로운 igroup 작성:
   a. 대상 사이트의 **SAN Initiator Groups** 메뉴에서 **Add** 를 선택합니다.
   b. 이름 제공, 호스트 운영 체제 를 선택한 다음 이니시에이터 그룹 구성원 을 선택합니다.
   c. 저장을 선택합니다.
3. 새로운 igroup을 대상 LUN에 매핑합니다.
   a. 스토리지 **>** LUN** 으로 이동합니다.
   b. igroup에 매핑할 모든 LUN을 선택합니다.
   c. 추가 를 선택한 다음 이니시에이터 그룹에 매핑** 을 선택합니다.
4. SnapMirror 활성 동기화 관계를 편집합니다.
   a. 보호> 관계 로 이동합니다.
   b. 수정할 관계 옆에 있는 kabob 메뉴를 선택한 다음 편집 을 선택합니다.
   c. 보호 정책을 AutomatedFailoverDuplex로 수정합니다.
   d. AutoMatedFailoverDuplex 를 선택하면 호스트 근접 설정을 수정하는 옵션이 시작됩니다. 초기자에 대해 초기자 근위에서부터 그리고 저장에 대한 적절한 옵션을 선택합니다.
   e. 저장을 선택합니다.

5. 보호 메뉴에서 관계가 로 표시될 때 작업이 성공했는지 확인합니다 `InSync`.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 에서 SnapMirror 정책을 수정합니다 `AutomatedFailover` 를 선택합니다 `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. 정책을 수정하면 재동기화가 트리거됩니다. 다시 동기화가 완료될 때까지 기다린 다음 관계가 인지 확인합니다 `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. 기존 호스트가 로컬 운영 클러스터인 경우 호스트를 두 번째 클러스터에 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
4. 2차 사이트에서 원격 호스트와 연결된 igroup에서 LUN 매핑을 삭제합니다.

   igroup에 복제되지 않은 LUN에 대한 맵이 포함되어 있지 않은지 확인합니다.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

5. 운영 사이트에서 권한 수준을 다음과 같이 설정합니다 `advanced`.

   ```
   SiteA::> set -privilege advanced
   ```

6. 기존 호스트의 이니시에이터 구성을 수정하여 로컬 클러스터의 이니시에이터에 대한 근위 경로를 설정합니다.

   ```
   SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
   -initiator <host> -proximal-vserver <server>
   ```

   이 단계를 완료한 후 권한 수준을 admin으로 다시 설정할 수 있습니다.

7. 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 선호도를 해당 로컬 사이트에 근접하게 설정합니다. Ennable igroup replication으로 구성을 복제하고 원격 클러스터에서 호스트 인접성을 반전합니다.

   ```
   SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
   SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
   host2 -proximal-vserver vsB
   ```

8. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
9. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.

비균일 설정에 대한 단계

1. 에서 SnapMirror 정책을 수정합니다 `AutomatedFailover` 를 선택합니다 `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. 정책을 수정하면 재동기화가 트리거됩니다. 다시 동기화가 완료될 때까지 기다린 다음 관계가 인지 확인합니다 `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. 기존 호스트가 운영 클러스터에 로컬인 경우 호스트를 두 번째 클러스터에 추가하고 각 클러스터에 대한 각 액세스 권한을 사용하여 연결을 설정합니다.
4. 2차 사이트에서 새로운 호스트에 대한 새로운 igroup 및 이니시에이터를 추가하고 호스트 유사성을 로컬 사이트에 설정합니다. LUN을 igroup에 매핑합니다.

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

5. 호스트에서 경로를 검색하고 호스트에 기본 클러스터에서 스토리지 LUN에 대한 활성/최적화 경로가 있는지 확인합니다
6. 애플리케이션을 배포하고 VM 워크로드를 클러스터 전체에 분산합니다.

대칭형 액티브/액티브 관계에서 비대칭형 **iSCSI** 또는 **FC** 관계로 변환

iSCSI 또는 FC를 사용하여 대칭적 액티브/액티브 보호를 구성한 경우 ONTAP CLI를 사용하여 해당 관계를 비대칭적 보호로 변환할 수 있습니다.

단계

1. 모든 VM 워크로드를 소스 클러스터의 로컬 호스트로 이동합니다.
2. VM 인스턴스를 관리하지 않는 호스트에 대한 igroup 구성을 제거한 다음 igroup 구성을 수정하여 igroup 복제를 종료합니다.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. 보조 사이트에서 LUN 매핑을 해제합니다.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. 보조 사이트에서 대칭 액티브/액티브 관계를 삭제합니다.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. 운영 사이트에서 대칭 액티브/액티브 관계를 해제합니다.
   `SiteA::> snapmirror release -destination-path <destination_path> -relationship -info-only true`

6. 보조 사이트에서 정책을 사용하여 동일한 볼륨 세트에 대한 관계를 생성하여 `AutomatedFailover` 관계를 다시 동기화합니다.

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
<policy_type>
```

> 관계를 다시 생성하기 전에 보조 사이트의 정합성 보장 그룹이 "삭제할 수 있습니다"필요합니다. 대상 볼륨"DP 유형으로 변환해야 합니다" 볼륨을 DP로 변환하려면, `MirrorAllSnapshots` 또는 `Sync` 가 아닌 정책과 함께 명령을-`AutomatedFailover` 수행합니다 `snapmirror resync`. `MirrorAndVault`

7. 미러 상태 관계가 인지 확인합니다 `Snapmirrored` 관계 상태는 입니다 `Insync`.

```
snapmirror show -destination-path destination_path
```

8. 호스트에서 경로를 다시 검색합니다.

관련 정보

- "SnapMirror 삭제"
- "SnapMirror 수정"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"
- "스냅미러 쇼"

SnapMirror 활성 동기화를 관리하고 데이터를 보호합니다

ONTAP 일관성 그룹 간에 공통 스냅샷을 만듭니다.

정기적으로 예약된 스냅샷 작업 외에도 운영 SnapMirror 정합성 보장 그룹의 볼륨과 보조 SnapMirror 정합성 보장 그룹의 볼륨 간에 공통을 수동으로 생성할 수 "스냅샷"있습니다.

이 작업에 대해

예약된 스냅샷 생성 간격은 12시간입니다.

시작하기 전에

- SnapMirror 그룹 관계가 동기화되어 있어야 합니다.

단계

1. 일반 스냅샷 생성:

대상 경로 **VS1_DST:/CG/CG_DST**'의 경우, '목적지
> SnapMirror update-destination-path VS1_DST:/CG/CG_DST'

2. 업데이트 진행 상황 모니터링:

```
destination::>snapmirror show -fields newest-snapshot
```

관련 정보

- "스냅미러 쇼"

SnapMirror 활성 동기화 관계에서 **ONTAP** 클러스터의 계획된 장애 조치를 수행합니다**.**

SnapMirror 액티브 동기화 관계에서 ONTAP 클러스터의 계획된 페일오버에서는 운영 및 2차 클러스터의 역할을 전환하여 2차 클러스터가 운영 클러스터에서 페일오버되도록 합니다. 페일오버 중에 보조 클러스터는 클라이언트 작업을 중단하지 않고 로컬에서 입력 및 출력 요청을 처리합니다.

계획된 페일오버를 수행하여 재해 복구 구성의 상태를 테스트하거나 운영 클러스터에 대한 유지 관리를 수행할 수 있습니다.

이 작업에 대해

계획된 페일오버는 보조 클러스터의 관리자가 시작합니다. 이 작업을 수행하려면 운영 및 2차 역할을 전환하여 2차 클러스터가 운영 클러스터에서 대신 수행하게 해야 합니다. 그러면 새로운 운영 클러스터가 클라이언트 작업을 중단하지 않고 로컬에서 입력 및 출력 요청 처리를 시작할 수 있습니다.

시작하기 전에

- SnapMirror 활성 동기화 관계가 동기화되어 있어야 합니다.
- 무중단 운영이 진행 중인 경우에는 계획된 페일오버를 시작할 수 없습니다. 무중단 운영에는 볼륨 이동, 애그리게이트 재배치, 스토리지 페일오버가 포함됩니다.
- ONTAP 중재자는 구성, 연결 및 쿼럼에 있어야 합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 계획된 페일오버를 수행할 수 있습니다.

시스템 관리자

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

1. System Manager에서 보호 > 개요 > 관계 를 선택합니다.
2. 페일오버할 SnapMirror 활성 동기화 관계를 확인합니다. 이름 옆에 있는 을 선택합니다 … 관계의 이름 옆에 있는 장애 조치 를 선택합니다.
3. 페일오버 상태를 모니터링하려면 를 사용합니다 `snapmirror failover show` ONTAP CLI에서

CLI를 참조하십시오

1. 대상 클러스터에서 페일오버 작업을 시작합니다.

   대상 경로 VS1_DST:/CG/CG_DST'에 대한 오류 수정:::> SnapMirror 페일오버 시작 대상 경로 VS1_DST:/CG/CG_DST

2. 페일오버 진행률을 모니터링합니다.

   대상::> SnapMirror failover show'

3. 페일오버 작업이 완료되면 대상에서 SnapMirror 동기식 보호 관계 상태를 모니터링할 수 있습니다.

   목적지::> SnapMirror 쇼

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 쇼"

계획되지 않은 자동 **ONTAP** 클러스터 장애 조치 작업에서 복구

자동 비계획 장애 조치(AUFO) 작업은 기본 클러스터가 다운되거나 격리될 때 발생합니다. ONTAP Mediator는 장애 조치가 발생할 때 이를 감지하고 보조 클러스터에 대한 자동적인 계획되지 않은 장애 조치를 실행합니다. 이 작업은 ONTAP Mediator의 도움을 받아서만 수행됩니다. 보조 클러스터는 기본 클러스터로 전환되어 클라이언트 서비스를 시작합니다. 이 작업은 ONTAP 중재자의 지원을 받아야만 수행됩니다.

예기치 않은 자동 페일오버 후에는 입출력 경로가 손실되지 않도록 호스트 LUN 입출력 경로를 재검색해야 합니다.

계획되지 않은 페일오버 후에 보호 관계를 다시 설정합니다

System Manager 또는 ONTAP CLI를 사용하여 보호 관계를 다시 설정할 수 있습니다.

시스템 관리자

단계

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

1. *보호 > 관계*로 이동하여 관계 상태가 "동기화되지 않음"으로 표시될 때까지 기다립니다.
2. 원래 소스 클러스터에서 작업을 재개하려면 를 ⋮ 클릭하고 * Failover * 를 선택합니다.

CLI를 참조하십시오

를 사용하여 자동 비계획 페일오버 상태를 모니터링할 수 있습니다 `snapmirror failover show` 명령.

예를 들면 다음과 같습니다.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

페일오버 후 팬아웃 구성에서 보호를 재개합니다

ONTAP 9.15.1부터 SnapMirror 액티브 동기화는 페일오버 이벤트 후 팬아웃 구간의 자동 재구성을 지원합니다. 비동기 팬아웃 구간은 정합성 보장 그룹 관계 또는 독립 볼륨 관계일 수 있습니다. 자세한 내용은 을 "팬아웃 구성"참조하십시오.

ONTAP 9.14.1 이하를 사용 중이고 SnapMirror 활성 동기화 관계에서 2차 클러스터에서 페일오버가 발생한 경우 SnapMirror 비동기 대상이 비정상 상태가 됩니다. SnapMirror 비동기식 엔드포인트와의 관계를 삭제하고 다시 생성하여 보호를 수동으로 복원해야 합니다.

단계

1. 페일오버 작업이 성공적으로 완료되었는지 확인합니다. '스냅샷 페일오버 표시'입니다
2. SnapMirror 비동기 끝점에서 팬 아웃 끝점을 삭제합니다.
   `snapmirror delete -destination-path` *`destination_path`*
3. 세 번째 사이트에서 새로운 SnapMirror 액티브 동기식 운영 볼륨과 비동기 팬아웃 타겟 볼륨 간에 SnapMirror 비동기식 관계를 생성합니다.
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*

4. 관계 재동기화:
   `snapmirror resync -destination-path destination_path`
5. 관계 상태 및 상태 확인: '스냅샷 표시

관련 정보

- "SnapMirror 생성"
- "SnapMirror 삭제"
- "스냅미러 페일오버 쇼"
- "스냅미러 재동기화"
- "스냅미러 쇼"

ONTAP SnapMirror 활성 동기화 작업 모니터링

다음 SnapMirror 활성 동기화 작업을 모니터링하여 SnapMirror 활성 동기화 구성의 상태를 확인할 수 있습니다.

- ONTAP 중재자
- 계획된 페일오버 작업
- 계획되지 않은 페일오버 작업을 자동으로 수행합니다
- SnapMirror 활성 동기화 가용성

ONTAP 9.15.1부터 System Manager는 두 클러스터의 SnapMirror 활성 동기화 관계 상태를 표시합니다. System Manager의 두 클러스터 중 하나에서 ONTAP 중재자의 상태를 모니터링할 수도 있습니다.

ONTAP 중재자

정상 작동 중에는 ONTAP 중재자 상태가 연결되어야 합니다. 다른 상태에 있는 경우 오류 상태를 나타낼 수 있습니다. 를 검토할 수 있습니다 "EMS(이벤트 관리 시스템) 메시지" 오류 및 적절한 수정 조치를 확인합니다.

계획된 페일오버 작업

'napmirror failover show' 명령을 사용하여 계획된 페일오버 작업의 상태 및 진행률을 모니터링할 수 있습니다. 예를 들면 다음과 같습니다.

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

페일오버 작업이 완료되면 새 대상 클러스터에서 SnapMirror 보호 상태를 모니터링할 수 있습니다. 예를 들면 다음과 같습니다.

```
ClusterA::> snapmirror show
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

계획되지 않은 자동 페일오버 중에 를 사용하여 작업 상태를 모니터링할 수 있습니다 `snapmirror failover show` 명령.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
          Source Path: vs1:/cg/scg3
     Destination Path: vs3:/cg/dcg3
      Failover Status: completed
         Error Reason:
             End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

을 참조하십시오 "EMS 참조" 이벤트 메시지 및 수정 조치에 대해 알아보십시오.

SnapMirror 활성 동기화 가용성

운영 클러스터, 2차 클러스터 또는 둘 다에서 일련의 명령을 사용하여 SnapMirror 액티브 동기화 관계의 가용성을 확인할 수 있습니다.

사용하는 명령에는 1차 및 2차 클러스터 모두에 대한 'napmirror 중재자 표시' 명령을 사용하여 연결 및 쿼럼 상태, 'napmirror show' 명령 및 'volume show' 명령을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 중재자 쇼"

ONTAP 일관성 그룹에 볼륨 추가 또는 제거

애플리케이션 워크로드의 요구사항이 변경됨에 따라 비즈니스 연속성을 보장하기 위해 일관성 그룹에서 볼륨을 추가하거나 제거해야 할 수 있습니다. 활성 SnapMirror 활성 동기화 관계에서

볼륨을 추가 및 제거하는 프로세스는 사용 중인 ONTAP의 버전에 따라 다릅니다.

대부분의 경우 이 프로세스는 운영 중단을 야기하여 SnapMirror 관계를 삭제하고 일관성 그룹을 수정한 다음 보호를 재개해야 합니다. ONTAP 9.13.1부터 활성 SnapMirror 관계가 있는 일관성 그룹에 볼륨을 추가하는 것은 무중단 작업입니다.

이 작업에 대해

- ONTAP 9.9.1에서는 ONTAP CLI를 사용하여 일관성 그룹에 볼륨을 추가하거나 제거할 수 있습니다.
- ONTAP 9.10.1.1부터는 를 관리하는 것이 좋습니다 "정합성 보장 그룹" System Manager 또는 ONTAP REST API를 통해

  볼륨을 추가하거나 제거하여 일관성 그룹의 구성을 변경하려면 먼저 원래 관계를 삭제한 다음 새 구성도를 사용하여 일관성 그룹을 다시 생성해야 합니다.

- ONTAP 9.13.1부터 소스 또는 대상에서 활성 SnapMirror 관계가 있는 일관성 그룹에 중단 없이 볼륨을 추가할 수 있습니다. 이 작업은 NVMe 프로토콜에서는 지원되지 않습니다.

  볼륨 제거는 중단을 야기하는 작업입니다. 볼륨을 제거하기 전에 SnapMirror 관계를 삭제해야 합니다.

ONTAP 9.9.1-9.13.0

시작하기 전에

- 에 있는 동안에는 일관성 그룹을 수정할 수 없습니다 `InSync` 상태.
- 대상 볼륨은 DP 유형이어야 합니다.
- 정합성 보장 그룹을 확장하기 위해 추가하는 새 볼륨에는 소스 볼륨과 대상 볼륨 사이에 공통 스냅샷 쌍이 있어야 합니다.

단계

두 볼륨 매핑에 표시된 예는 다음과 같습니다. `vol_src1 ←→ vol_dst1` 및 `vol_src2 ←→ vol_dst2`정합성 보장 그룹 관계에서 최종 지점 간의 관계를 나타냅니다 `vs1_src:/cg/cg_src` 및 `vs1_dst:/cg/cg_dst`.

1. 소스 및 대상 클러스터에서 명령을 사용하여 소스와 대상 클러스터 간에 공통 스냅샷이 있는지 확인합니다 `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   'source::> snapshot show -vserver vs1_src -volume vol_src3 -snapshot SnapMirror *'

   대상::> snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror *

2. 공통 스냅샷이 없는 경우 FlexVol SnapMirror 관계를 생성하고 초기화합니다.

   대상 경로 VS1_Dst:vol_dst3'이라는 메시지가 나타납니다

3. 정합성 보장 그룹 관계를 삭제합니다.

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로::::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

4. 소스 SnapMirror 관계를 해제하고 공통 스냅샷을 보존합니다.

   'source::> snapmirror release-relationship-info-only true-destination-path vs1_dst:vol_dst3'

5. LUN 매핑을 해제하고 기존 일관성 그룹 관계를 삭제합니다.

   대상::> LUN 매핑 삭제 - vserver vs1_dst -path <lun_path> -igroup <igroup_name>'

   > 대상 LUN은 매핑 해제되지만 운영 복제본의 LUN은 계속해서 호스트 입출력을 처리합니다

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로::::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

   '소스::> SnapMirror release-destination-path vs1_dst:/cg/cg_dst-relationship-info-only true'

6. **ONTAP 9.10.1~9.13.0**을 사용하는 경우 소스에서 정합성 보장 그룹을 삭제하고 올바른 구성으로 다시 만드십시오. 의 단계를 따르"일관성 그룹을 삭제합니다" 십시오"단일 일관성 그룹을 구성합니다". ONTAP ONTAP 는 없습니다.

   ONTAP 9.9.1을 사용하는 경우 다음 단계로 건너뜁니다.

7. 새 컴포지션을 사용하여 대상에 새 일관성 그룹을 생성합니다.

   대상 경로 VS1_Dst:/CG/CG_src-destination-path vs1_dst:/cg/cg_dst-item-mapping vol_src1:@vol_dst1, vol_src2:@vol_dst2, vol_src3:@vol_dst3

8. 제로급 RTO 정합성 보장 그룹 관계를 재동기화하여 동기화되도록 합니다.

   대상 경로 VS1_DST:/CG/CG_DST'를 다시 동기화하십시오

9. 5단계에서 매핑되지 않은 LUN을 다시 매핑합니다.

   ```
   destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
   ```

10. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

ONTAP 9.13.1 이상

ONTAP 9.13.1부터 활성 SnapMirror 활성 동기화 관계가 있는 일관성 그룹에 볼륨을 중단 없이 추가할 수 있습니다. SnapMirror 액티브 동기화에서는 소스 또는 대상 모두에서 볼륨을 추가할 수 있습니다.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

소스 정합성 보장 그룹에서 볼륨을 추가하는 방법에 대한 자세한 내용은 를 참조하십시오 일관성 그룹 수정.

타겟 클러스터에서 볼륨을 추가합니다

1. 대상 클러스터에서 보호 > 관계를 선택합니다.
2. 볼륨을 추가할 SnapMirror 구성을 찾습니다. 를 선택한 다음 확장 을 선택합니다 ⋮ .
3. 정합성 보장 그룹에 볼륨을 추가할 볼륨 관계를 선택합니다
4. **Expand**(확장**)를 선택합니다.

관련 정보

- "SnapMirror 삭제"
- "SnapMirror 초기화"
- "SnapMirror 릴리즈"
- "스냅미러 재동기화"

ONTAP SnapMirror Active Sync로 업그레이드하고 되돌리기

SnapMirror 액티브 동기화는 ONTAP 9.9.1부터 지원됩니다. ONTAP 클러스터 또는 컨트롤러의 업그레이드와 되돌리기는 업그레이드하거나 되돌리려는 ONTAP 버전에 따라 SnapMirror 활성 동기화 관계에 영향을 미칩니다.

클러스터를 새로 고칩니다

ONTAP 9.16.1부터 SnapMirror 액티브 동기화는 대칭 액티브/액티브 구성의 4노드 클러스터를 지원합니다. 4노드 클러스터를 사용하여 컨트롤러와 스토리지를 업그레이드할 수 있습니다.

시작하기 전에

- 를 검토합니다. "4노드 클러스터의 요구사항"
- 기술 업데이트 프로세스 중에 비대칭 구성을 만들 수 있지만 새로 고침을 완료한 후에는 대칭 구성으로 돌아가야 합니다.
- 이러한 지침은 50개 이하의 일관성 그룹과 400개 이하의 볼륨 엔드포인트를 가진 기존 4노드 구성에 적용됩니다.

단계

1. "모든 SnapMirror 활성 동기화 볼륨을 _single_high-availability(HA) 쌍으로 이동합니다"..
2. "클러스터에서 사용되지 않는 노드를 제거합니다"..
3. "클러스터에 새 노드를 추가합니다"..
4. "모든 볼륨을 이동합니다" 새 노드로 이동할 수 있습니다.
5. "클러스터에서 사용되지 않는 노드를 제거합니다" 그런 다음 교체합니다"새로운 노드로".

SnapMirror 활성 동기화로 ONTAP 업그레이드

SnapMirror 액티브 동기화를 사용하려면 소스 및 대상 클러스터의 모든 노드에서 ONTAP 9.9.1 이상을 실행해야 합니다.

활성 SnapMirror 활성 동기화 관계를 사용하여 ONTAP를 업그레이드할 때는 를 사용해야 합니다 자동 무중단 업그레이드(ANDU). ANDU를 사용하면 SnapMirror 활성 동기화 관계가 동기화되고 업그레이드 프로세스 중에 정상 상태가 됩니다.

ONTAP 업그레이드를 위해 SnapMirror 액티브 동기화 배포를 준비하기 위한 구성 단계가 없습니다. 그러나 업그레이드 전후에 다음 사항을 확인하는 것이 좋습니다.

- SnapMirror 활성 동기화 관계가 동기화됩니다.
- 이벤트 로그에 SnapMirror와 관련된 오류가 없습니다.
- 중재자는 온라인 상태이며 두 클러스터에서 모두 정상입니다.
- 모든 호스트는 LUN을 보호하기 위해 모든 경로를 올바르게 볼 수 있습니다.

ONTAP 9.9.1 또는 9.9.1에서 ONTAP 9.10.1 이상으로 클러스터를 업그레이드하면 ONTAP에서 새로운 을 생성합니다 정합성 보장 그룹 소스 및 대상 클러스터 모두에서 System Manager를 사용하여 SnapMirror 활성 동기화 관계를 구성할 수 있습니다.

를 클릭합니다 `snapmirror quiesce` 및 `snampirror resume` SnapMirror 활성 동기화에서는 명령이 지원되지 않습니다.

ONTAP 9.10.1에서 ONTAP 9.9.1로 되돌립니다

관계를 9.10.1에서 9.9.1로 되돌리려면 SnapMirror 활성 동기화 관계를 삭제한 다음 9.10.1 일관성 그룹 인스턴스를 따라야 합니다. 활성 SnapMirror 활성 동기화 관계가 있는 일관성 그룹은 삭제할 수 없습니다. 9.9.1 이전 버전에서 다른 스마트 컨테이너 또는 엔터프라이즈 앱과 이전에 연결된 9.10.1로 업그레이드된 FlexVol 볼륨은 더 이상 복원 시 연결되지 않습니다. 일관성 그룹을 삭제해도 구성 볼륨 또는 볼륨 세부 스냅샷은 삭제되지 않습니다. 을 참조하십시오 "일관성 그룹을 삭제합니다" ONTAP 9.10.1 이상에서 이 작업에 대한 자세한 내용을 확인하십시오.

ONTAP 9.9.1 이전 릴리즈보다 SnapMirror 활성 동기화는 혼합 ONTAP 클러스터에 지원되지 않습니다.

ONTAP 9.1.1에서 이전 버전의 ONTAP으로 되돌리는 경우 다음에 대해 알아야 합니다.

- 클러스터가 SnapMirror 활성 동기화 대상을 호스팅하는 경우 관계가 끊어져 삭제될 때까지 ONTAP 9.8 이전 버전으로 되돌릴 수 없습니다.
- 클러스터가 SnapMirror 액티브 동기화 소스를 호스팅하는 경우 관계가 해제될 때까지 ONTAP 9.8 이하로 되돌릴 수 없습니다.
- 사용자가 생성한 모든 맞춤형 SnapMirror 활성 동기화 정책을 삭제한 후 ONTAP 9.8 이하로 되돌려야 합니다.

이러한 요구 사항을 충족하려면 를 참조하십시오 "SnapMirror 활성 동기화 구성을 제거합니다".

단계

1. SnapMirror 활성 동기화 관계의 클러스터 중 하나에서 다음 명령을 입력하여 되돌릴 준비가 되었는지 확인합니다.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   다음 샘플 출력에서는 정리 명령으로 되돌릴 준비가 되지 않은 클러스터를 보여 줍니다.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
   ```

```
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. 복원 검사의 요구 사항을 충족하면 을 참조하십시오 "ONTAP를 되돌립니다".

관련 정보

- "네트워크 인터페이스"
- "SnapMirror가 깨졌습니다"
- "스냅미러 정책 삭제"
- "스냅미러 정책 보기"
- "SnapMirror 중지"
- "스냅미러 쇼"

ONTAP SnapMirror Active Sync 구성 제거

더 이상 제로 RTO SnapMirror 동기식 보호가 필요하지 않은 경우 SnapMirror 액티브 동기화 관계를 삭제할 수 있습니다.

비대칭 구성을 제거합니다

- SnapMirror 액티브 동기화 관계를 삭제하기 전에 대상 클러스터의 모든 LUN을 매핑 해제해야 합니다.
- LUN이 매핑 해제되었고 호스트가 다시 스캔되면 SCSI 타겟은 LUN 인벤토리가 변경되었음을 호스트에 알립니다. 제로 RTO 2차 볼륨의 기존 LUN은 제로 RTO 관계가 삭제된 후 새 ID를 반영하도록 변경됩니다. 호스트는 소스 볼륨 LUN과 관계가 없는 새 LUN으로 보조 볼륨 LUN을 검색합니다.
- 관계가 삭제된 후 보조 볼륨은 DP 볼륨으로 유지됩니다. 을(를) 실행할 수 있습니다 `snapmirror break` 읽기/쓰기로 변환하는 명령입니다.
- 관계가 반대로 설정되지 않은 경우 페일오버된 상태에서는 관계를 삭제할 수 없습니다.

단계

1. 보조 클러스터에서 소스 끝점과 대상 끝점 간의 SnapMirror 활성 동기화 일관성 그룹 관계를 제거합니다.

   대상 경로 VS1_DST:/CG/CG_DST'의 경우, "대상 경로:::> SnapMirror delete-destination-path VS1_DST:/CG/CG_DST"

2. 운영 클러스터에서 정합성 보장 그룹 관계 및 관계에 대해 생성된 스냅샷을 해제합니다.

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. 호스트 재검색을 수행하여 LUN 인벤토리를 업데이트합니다.
4. ONTAP 9.10.1부터 SnapMirror 관계를 삭제해도 일관성 그룹은 삭제되지 않습니다. 일관성 그룹을 삭제하려면 시스템 관리자 또는 ONTAP REST API를 사용해야 합니다. 을 참조하십시오 일관성 그룹을 삭제합니다 를 참조하십시오.

iSCSI 또는 **FC** 대칭 활성/활성 구성 제거

System Manager 또는 ONTAP CLI를 사용하여 대칭 구성을 제거할 수 있습니다. 두 인터페이스 모두에서 에 대한 단계가 다릅니다 균일 및 비균일 설정.

시스템 관리자

균일 설정에 대한 단계

1. 운영 사이트에서 igroup에서 원격 호스트를 제거하고 복제를 종료합니다.
   a. **Hosts**> * SAN Initiator Groups * 로 이동합니다.
   b. 수정할 igroup을 선택한 다음 편집 을 선택합니다.
   c. 원격 이니시에이터를 제거하고 igroup 복제를 종료합니다. 저장을 선택합니다.
2. 보조 사이트에서 LUN 매핑을 해제하여 복제된 관계를 삭제합니다.
   a. **Hosts**> **SAN Initiator Groups** 로 이동합니다.
   b. SnapMirror 관계가 있는 igroup을 선택한 다음 삭제 를 선택합니다.
   c. 대화 상자에서 연결된 **LUN** 매핑 해제 상자를 선택한 다음 삭제 를 선택합니다.
   d. 보호> 관계 로 이동합니다.
   e. SnapMirror 활성 동기화 관계를 선택한 다음 릴리즈 를 선택하여 관계를 삭제합니다.

비균일 설정에 대한 단계

1. 운영 사이트에서 igroup에서 원격 호스트를 제거하고 복제를 종료합니다.
   a. **Hosts**> * SAN Initiator Groups * 로 이동합니다.
   b. 수정할 igroup을 선택한 다음 편집 을 선택합니다.
   c. 원격 이니시에이터를 제거하고 igroup 복제를 종료합니다. 저장을 선택합니다.
2. 2차 사이트에서 SnapMirror 활성 동기화 관계를 제거합니다.
   a. 보호> 관계 로 이동합니다.
   b. SnapMirror 활성 동기화 관계를 선택한 다음 릴리즈 를 선택하여 관계를 삭제합니다.

CLI를 참조하십시오

균일 설정에 대한 단계

1. 모든 VM 워크로드를 SnapMirror 활성 동기화의 소스 클러스터로 호스트 로컬 이동합니다.
2. 소스 클러스터에서 igroup에서 이니시에이터를 제거하고 igroup 구성을 수정하여 igroup 복제를 종료합니다.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. 2차 사이트에서 LUN 매핑을 삭제하고 igroup 구성을 제거합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 2차 사이트에서 SnapMirror 활성 동기화 관계를 삭제합니다.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. 기본 사이트에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

비균일 설정에 대한 단계

1. 모든 VM 워크로드를 SnapMirror 활성 동기화의 소스 클러스터로 호스트 로컬 이동합니다.
2. 소스 클러스터의 이니시에이터를 igroup에서 제거합니다.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. 2차 사이트에서 LUN 매핑을 삭제하고 igroup 구성을 제거합니다.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 2차 사이트에서 SnapMirror 활성 동기화 관계를 삭제합니다.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. 기본 사이트에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

NVMe 대칭 활성/활성 구성 제거

시스템 관리자

단계

1. 소스 클러스터에서 *보호 > 복제*로 이동합니다.
2. 제거하려는 관계를 찾아 선택하세요. ⋮ *삭제*를 선택하세요.

CLI를 참조하십시오

1. 대상 클러스터에서 SnapMirror 활성 동기화 관계를 삭제합니다.

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   예:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   하위 시스템과 해당 네임스페이스가 보조 클러스터에서 제거됩니다.

2. 소스 클러스터에서 기본 사이트의 SnapMirror 활성 동기화 관계를 해제합니다.

   ```
   snapmirror release -destination-path <destination_path>
   ```

   예:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. 경로를 다시 검색하여 호스트에서 로컬 경로만 사용할 수 있는지 확인합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "SnapMirror 삭제"
- "SnapMirror 릴리즈"

ONTAP Mediator 또는 **ONTAP Cloud Mediator** 제거

ONTAP 클러스터에서 기존 ONTAP Mediator 또는 ONTAP Cloud Mediator 구성을 제거하려면 다음을 사용할 수 있습니다. `snapmirror mediator remove` 예 를 들어, 한 번에 한 가지 유형의 Mediator만 사용할 수 있으므로 다른 인스턴스를 설치하기 전에 기존 인스턴스를 제거해야 합니다.

단계

다음 단계 중 하나를 완료하여 ONTAP Mediator 또는 ONTAP Cloud Mediator를 제거할 수 있습니다.

ONTAP 중재자

1. ONTAP 중재자 제거:

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   예:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP 클라우드 중재자

1. ONTAP Cloud Mediator 제거:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   예:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

관련 정보

- "스냅미러 중재자 제거"

문제 해결

ONTAP SnapMirror 삭제 작업이 테이크오버 상태에서 실패합니다**.**

다음 정보를 사용하십시오. `snapmirror delete` SnapMirror 활성 동기화 일관성 그룹 관계가 인수 상태인 경우 명령이 실패합니다.

문제:

ONTAP 9.9.1이 클러스터에 설치되면 다음을 실행합니다. `snapmirror delete` SnapMirror 활성 동기화 일관성 그룹 관계가 인수 상태인 경우 명령이 실패합니다.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

해결 방법

SnapMirror 활성 동기화 관계에 있는 노드가 인수 상태인 경우 "-force" 옵션을 true로 설정하여 SnapMirror 삭제 및 해제 작업을 수행합니다.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

관련 정보

- "SnapMirror 삭제"

ONTAP SnapMirror 관계 생성 및 일관성 그룹 초기화 실패

SnapMirror 관계 생성 및 일관성 그룹 초기화에 실패하는 경우 다음 정보를 사용합니다.

문제:

SnapMirror 관계 및 일관성 그룹 초기화가 실패합니다.

솔루션:

클러스터당 일관성 그룹 제한을 초과하지 않았는지 확인합니다. SnapMirror 활성 동기화의 일관성 그룹 제한은 플랫폼과는 독립적이며 ONTAP 버전에 따라 다릅니다. 을 참조하십시오 "개체 제한" ONTAP 버전 관련 지침을 참조하십시오.

오류:

정합성 보장 그룹의 초기화가 중단된 경우 ONTAP REST API, System Manager 또는 'show-Expand' 명령을 사용하여 정합성 보장 그룹 초기화의 상태를 확인하십시오.

ONTAP 9.14.1부터 9.8까지 SnapMirror 액티브 동기화는 SnapMirror 비즈니스 연속성(SM-BC)이라고 합니다.

솔루션:

일관성 그룹이 초기화되지 않은 경우 SnapMirror 활성 동기화 관계를 제거하고 일관성 그룹을 삭제한 다음 관계를 다시 생성한 후 초기화합니다. 이 워크플로는 사용 중인 ONTAP 버전에 따라 다릅니다.

ONTAP 9.9.9.1을 사용하는 경우	ONTAP 9.10.1 이상을 사용하는 경우

1. "SnapMirror 활성 동기화 구성을 제거합니다" 2. "일관성 그룹 관계를 생성한 다음 일관성 그룹 관계를 초기화합니다"	1. 보호 > 관계 * 에서 일관성 그룹에서 SnapMirror 활성 동기화 관계를 찾습니다. ⋮를 선택한 다음 * Delete * 를 선택하여 SnapMirror 활성 동기화 관계를 제거합니다. 2. "일관성 그룹을 삭제합니다" 3. "일관성 그룹을 구성합니다"

계획된 **ONTAP** 클러스터 장애 조치가 실패했습니다.

계획된 장애 조치 작업이 실패한 경우 다음 정보를 사용하세요.

문제:

'napmirror failover start' 명령을 실행한 후 'napmirror failover show' 명령의 출력에 무중단 작업이 진행 중임을 나타내는 메시지가 표시됩니다.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                                08:35:04
08:35:04
```

원인:

볼륨 이동, 애그리게이트 재배치, 스토리지 페일오버 등 무중단 운영이 진행 중인 경우에는 계획된 페일오버를 시작할 수 없습니다.

솔루션:

무중단 운영이 완료될 때까지 기다린 후 페일오버 작업을 다시 시도하십시오.

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"

ONTAP Mediator 또는 **ONTAP Cloud Mediator**에 연결할 수 없거나 **Mediator** 쿼럼 상태가 거짓입니다.

ONTAP Mediator 또는 ONTAP Cloud Mediator에 접근할 수 없거나 Mediator 쿼럼 상태가 거짓인 경우 다음 정보를 사용하세요.

문제:

실행 후 `snapmirror failover start` 명령, 출력 `snapmirror failover show` 명령은 ONTAP Mediator 또는 ONTAP Cloud Mediator가 구성되지 않았음을 나타내는 메시지를 표시합니다.

보다 "활성 동기화에 대해 ONTAP 중재자 및 클러스터를 구성합니다" 또는 "SnapMirror Active Sync를 위한 ONTAP Cloud Mediator 구성" .

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

원인:

중재자가 구성되지 않았거나 네트워크 연결 문제가 있습니다.

솔루션:

ONTAP 중재자가 구성되지 않은 경우 SnapMirror 활성 동기화 관계를 설정하기 전에 ONTAP 중재자를 구성해야 합니다. 네트워크 연결 문제를 해결합니다. SnapMirror 중재자 show 명령을 사용하여 중재자가 연결되어 있고 소스 사이트와 대상 사이트 모두에서 쿼럼 상태가 true 인지 확인합니다. 자세한 내용은 을 참조하십시오 "ONTAP 중재자를 구성합니다".

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

관련 정보

- "스냅미러 페일오버 쇼"
- "스냅미러 페일오버 시작"
- "스냅미러 중재자 쇼"

ONTAP Cloud Mediator에 접속 가능하지만 응답이 느립니다**.**

ONTAP Cloud Meditor가 ping 지연 시간이 권장 지연 시간보다 높다는 오류로 인해 실패하는 경우 다음 정보를 사용하세요.

문제:

시스템 관리자: Cloud Mediator 서비스에 접속할 수는 있지만 응답 속도가 느립니다.

CLI: `mediator add` 명령이 다음 오류로 인해 실패합니다.
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

원인:

클러스터가 NetApp 콘솔 클라우드 근처에 위치하지 않았거나 네트워크 경로 병목 현상이 있을 수 있습니다.

솔루션:

- NetApp Console 클라우드(미국 동부)의 지리적 위치와 근접성을 확인하세요.
- 네트워크 경로를 최적화하거나 병목 현상을 해결합니다.
- 네트워크 도구를 사용하여 왕복 시간(RTT)을 측정하고 지연 시간을 권장 한도 내로 줄입니다.
- HTTP 프록시를 사용하여 성능을 향상시키세요.

보다 "SnapMirror Active Sync를 위한 ONTAP Cloud Mediator 및 클러스터 구성" .

사이트 **B**에서 예기치 않은 자동 페일오버가 트리거되지 않습니다

사이트 A에서 장애가 발생해도 사이트 B에서 계획되지 않은 장애 조치가 발생하지 않는 경우 다음 정보를 사용합니다.

문제:

사이트 A에서 장애가 발생해도 사이트 B에서 계획되지 않은 페일오버가 트리거되지 않습니다

가능한 원인 **#1:**

ONTAP Mediator 또는 ONTAP Cloud Mediator가 구성되지 않았습니다. 이것이 원인인지 확인하려면 다음을 실행하세요. `snapmirror mediator show` 사이트 B 클러스터에 대한 명령입니다.

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

이 예는 Mediator가 사이트 B에 구성되지 않았음을 나타냅니다.

솔루션:

두 클러스터 모두에 Mediator가 구성되어 있고, 상태가 연결됨이고, 쿼럼이 True로 설정되어 있는지 확인하세요.

가능한 원인 **#2:**

SnapMirror 일관성 그룹이 동기화되지 않았습니다. 이 문제가 원인인지 확인하려면 이벤트 로그를 보고 사이트 장애 발생 시 정합성 보장 그룹이 동기화되어 있는지 확인합니다.

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

솔루션:

사이트 B에서 강제 대체 작동을 수행하려면 다음 단계를 완료합니다

1. 사이트 B에서 정합성 보장 그룹에 속한 모든 LUN 매핑을 해제합니다
2. "강제" 옵션을 사용하여 SnapMirror 일관성 그룹 관계를 삭제합니다.
3. 정합성 보장 그룹 구성 볼륨의 '스냅샷 중단' 명령을 입력하여 볼륨을 DP에서 R/W로 변환한 후 사이트 B에서 입출력을 활성화합니다
4. 사이트 A 노드를 부팅하여 사이트 B에서 사이트 A로 RTO 관계가 0이 되도록 합니다
5. 사이트 A에서 정합성 보장 그룹을 해제하여 `relationship-info-only` 공통 스냅샷을 유지하고 정합성 보장 그룹에 속한 LUN의 매핑을 해제합니다.
6. Sync 정책 또는 Async 정책을 사용하여 볼륨 레벨 관계를 설정하여 사이트 A의 볼륨을 R/W에서 DP로 변환합니다.
7. 관계를 동기화하기 위해 '스냅샷 재동기화'를 실행합니다.
8. 사이트 A의 동기화 정책과 SnapMirror 관계를 삭제합니다
9. 사이트 B에서 'lationship-info-only true'를 사용하여 동기화 정책과 SnapMirror 관계를 해제합니다
10. 사이트 B에서 사이트 A로 일관성 그룹 관계를 생성합니다
11. 사이트 A에서 일관성 그룹 재동기화를 수행한 다음 일관성 그룹이 동기화 중인지 확인합니다.
12. 호스트 LUN 입출력 경로를 재검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 중재자 쇼"
- "스냅미러 재동기화"

사이트 **B**와 **ONTAP Mediator** 간의 링크가 끊어지고 사이트 **A**가 끊어졌습니다**.**

ONTAP Mediator 또는 ONTAP Cloud Mediator의 연결을 확인하려면 다음을 사용하세요. `snapmirror mediator show` 명령입니다. 연결 상태가 "접근 불가"이고 사이트 B가 사이트 A에 접속할 수 없는 경우, 아래와 비슷한 출력이 표시됩니다. 해결 방법에 따라 연결을 복원하세요.

예:

ONTAP Cloud Mediator 출력 `snapmirror mediator show` 명령을 사용합니다.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

ONTAP Mediator 출력 `snapmirror mediator show` 명령을 사용합니다.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

해결 방법

사이트 B에서 입출력을 사용하도록 페일오버를 강제 실행한 다음 사이트 B에서 사이트 A로 RTO 관계를 0으로 설정합니다 사이트 B에서 강제 대체 작동을 수행하려면 다음 단계를 완료합니다

1. 사이트 B에서 일관성 그룹에 속한 모든 LUN의 매핑을 해제합니다. 이 작업은 실패하므로 먼저 igroup을 수정하여 복제 피어 SVM을 제거한 다음 LUN 맵을 삭제해야 합니다.

예:

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_1                        igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
1 entries were displayed.
```

1. 강제 옵션을 사용하여 SnapMirror 일관성 그룹 관계를 삭제합니다.
2. SnapMirror break 명령을 입력합니다 (`snapmirror break -destination_path` *svm*`:_volume_`) 정합성 보장 그룹 구성 볼륨에서 볼륨을 DP에서 RW로 변환하여 사이트 B의 입출력을 활성화합니다

   일관성 그룹의 각 관계에 대해 SnapMirror break 명령을 실행해야 합니다. 예를 들어, 일관성 그룹에 볼륨이 3개인 경우 각 볼륨에 대해 명령을 실행합니다.

3. 사이트 A 노드를 부팅하여 사이트 B에서 사이트 A로 RTO 관계가 0이 되도록 합니다
4. 사이트 A에서 relationship-info-only를 사용하여 정합성 보장 그룹을 해제하여 공통 스냅샷을 유지하고 정합성 보장 그룹에 속하는 LUN의 매핑을 해제합니다.

5. 동기화 정책 또는 비동기 정책을 사용하여 볼륨 수준 관계를 설정하여 사이트 A의 볼륨을 RW에서 DP로 변환합니다.
6. 를 발행합니다 `snapmirror resync` 관계를 동기화하는 명령입니다.
7. 사이트 A에서 동기화 정책이 적용된 SnapMirror 관계를 삭제합니다
8. 사이트 B에서 relationship-info만 true를 사용하여 동기 정책과 SnapMirror 관계를 해제합니다
9. 사이트 B와 사이트 A 간의 정합성 보장 그룹 관계를 생성합니다
10. 소스 클러스터에서 정합성 보장 그룹을 다시 동기화합니다. 정합성 보장 그룹 상태가 동기화되어 있는지 확인합니다.
11. 호스트 LUN 입출력 경로를 다시 검색하여 LUN에 대한 모든 경로를 복구합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 중재자 쇼"
- "스냅미러 재동기화"
- "스냅미러 쇼"

사이트 **A**와 **ONTAP Mediator** 간의 링크가 다운되고 사이트 **B**가 다운되었습니다**.**

SnapMirror 액티브 동기화를 사용할 경우 ONTAP 중재자 또는 피어링된 클러스터 간에 연결이 끊어질 수 있습니다. SnapMirror 활성 동기화 관계의 여러 부분에 대한 연결, 가용성 및 합의 상태를 확인한 다음 강제로 연결을 다시 시작하여 문제를 진단할 수 있습니다.

확인할 사항	**CLI** 명령	표시기
사이트 A의 중재자	스냅미러 중재자 쇼	연결 상태는 로 표시됩니다 `unreachable`
사이트 B 연결	클러스터 피어 쇼	사용 가능 여부는 로 표시됩니다 `unavailable`
SnapMirror 활성 동기화 볼륨의 합의 상태입니다	'volume show_volume_name_-fields smbc-Consensus'	를 클릭합니다 `sm-bc consensus` 필드가 표시됩니다 `Awaiting-consensus`

이 문제를 진단하고 해결하는 방법에 대한 추가 정보는 다음을 참조하십시오."NetApp 기술 자료: SnapMirror Active Sync를 사용할 때 사이트 A와 Mediator 간의 링크가 끊어지고 사이트 B가 끊어짐" .

관련 정보

- "클러스터 피어 쇼"
- "스냅미러 중재자 쇼"

대상 볼륨에 펜스가 설정된 경우 **ONTAP SnapMirror** 삭제 작업이 실패합니다**.**

대상 볼륨에 리디렉션 펜스가 설정되어 있는 경우 SnapMirror 삭제 작업이 실패하면 다음 정보를 사용합니다.

문제:

대상 볼륨에 리디렉션 펜스 세트가 있으면 SnapMirror 삭제 작업이 실패합니다.

해결 방법

다음 작업을 수행하여 리디렉션을 재시도하고 대상 볼륨에서 Fence를 제거합니다.

- SnapMirror 재동기화
- SnapMirror 업데이트

ONTAP 기본이 다운되면 볼륨 이동 작업이 중단됩니다**.**

SnapMirror 활성 동기화 관계에서 기본 사이트가 다운되어 볼륨 이동 작업이 컷오버 지연 상태로 무기한 중단되는 경우 다음 정보를 사용합니다.

문제:

SnapMirror 활성 동기화 관계에서 운영 사이트가 다운되면 볼륨 이동 작업이 컷오버가 지연된 상태로 무기한 중단됩니다.
운영 사이트가 다운되면 보조 사이트가 자동 예상치 못한 장애 조치(AUFO)를 수행합니다. AUFO가 트리거될 때 볼륨 이동 작업이 진행 중이면 볼륨 이동이 중단됩니다.

솔루션:

중단된 볼륨 이동 인스턴스를 중단하고 볼륨 이동 작업을 다시 시작하십시오.

스냅샷을 삭제할 수 없을 때 **ONTAP SnapMirror** 릴리스가 실패합니다**.**

스냅샷을 삭제할 수 없어 SnapMirror 릴리스 작업이 실패하는 경우 다음 정보를 사용하세요.

문제:

스냅샷을 삭제할 수 없으면 SnapMirror 릴리즈 작업이 실패합니다.

솔루션:

스냅샷에 임시 태그가 있습니다. `snapshot delete`임시 스냅샷을 제거하려면 옵션과 함께 명령을 `-ignore-owners` 사용합니다.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

'napmirror release' 명령을 재시도합니다.

관련 정보

- "SnapMirror 릴리즈"

볼륨 이동 참조 스냅샷이 **ONTAP SnapMirror** 관계에 대한 최신 정보로 표시됩니다**.**

볼륨 이동 작업 후 SnapMirror 관계에 대해 볼륨 이동 참조 스냅샷이 최신으로 표시되는 경우 다음 정보를 사용합니다.

문제:

정합성 보장 그룹 볼륨에서 볼륨 이동 작업을 수행한 후 볼륨 이동 참조 스냅샷이 SnapMirror 관계의 최신 스냅샷으로

잘못 표시될 수 있습니다.

다음 명령을 사용하여 최신 스냅샷을 볼 수 있습니다.

'스냅샷 표시-필드 최신-스냅샷 상태-확장'을 선택합니다

솔루션:
수동으로 '스냅샷 미러 재동기화'를 수행하거나 볼륨 이동 작업이 완료된 후 다음 자동 재동기화 작업을 기다리십시오.

관련 정보

- "스냅미러 재동기화"
- "스냅미러 쇼"

MetroCluster 및 SnapMirror Active Sync를 위한 ONTAP Mediator

ONTAP 중재자에 대해 자세히 알아보십시오

이 문서는 ONTAP Mediator의 온프레미스 버전을 참조합니다. ONTAP 9.17.1부터 제공되는 ONTAP Cloud Mediator에 대한 자세한 내용은 다음을 참조하십시오. "SnapMirror Active Sync 설명서" .

ONTAP Mediator는 ONTAP 기능에 대한 다양한 기능을 제공합니다.

- HA 메타데이터에 대한 영구적이고 울타리 저장소를 제공합니다.
- 컨트롤러 활성을 위한 핑 프록시 역할을 합니다.
- quorum 결정에 도움이 되는 동기 노드 상태 쿼리 기능을 제공합니다.

ONTAP Mediator는 두 가지 추가 systemctl 서비스를 제공합니다.

- **`ontap_mediator.service`**

  ONTAP 관계를 관리하기 위한 REST API 서버를 유지 관리합니다.

- **`mediator-scst.service`**

  SCST(iSCSI 모듈)의 시작 및 종료를 제어합니다.

시스템 관리자를 위해 제공되는 도구

시스템 관리자를 위해 제공되는 도구:

- **`/usr/local/bin/mediator_change_password`**

  현재 API 사용자 이름과 암호를 제공할 때 새 API 암호를 설정합니다.

- **`/usr/local/bin/mediator_change_user`**

현재 API 사용자 이름 및 암호를 제공할 때 새 API 사용자 이름을 설정합니다.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  NetApp 고객 지원 커뮤니케이션하기 위해 필요한 모든 유용한 지원 정보를 포함하는 로컬 tgz 파일을 생성합니다. 여기에는 애플리케이션 구성, 로그 및 일부 시스템 정보가 포함됩니다. 번들은 로컬 디스크에 생성되고 필요에 따라 수동으로 전송할 수 있습니다. 스토리지 위치:/opt/netapp/data/support_bundle/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  ONTAP 중재자 패키지와 SCST 커널 모듈을 제거합니다. 여기에는 모든 구성, 로그 및 메일박스 데이터가 포함됩니다.

- **`/usr/local/bin/mediator_unlock_user`**

  인증 재시도 한도에 도달하면 API 사용자 계정의 잠금을 해제합니다. 이 기능은 무차별 암호 대입(brute force password derivation)을 방지하는 데 사용됩니다. 사용자에게 올바른 사용자 이름과 암호를 묻는 메시지가 표시됩니다.

- **`/usr/local/bin/mediator_add_user`**

  (지원만 해당) 설치 시 API 사용자를 추가하는 데 사용됩니다.

특별 참고 사항

ONTAP mediator는 SCST에 의존하여 iSCSI를 제공합니다(참조 http://scst.sourceforge.net/index.html). 이 패키지는 커널 전용으로 설치하는 동안 컴파일되는 커널 모듈입니다. 커널에 대한 업데이트를 수행하려면 SCST를 다시 설치해야 할 수 있습니다. 또는 ONTAP Mediator를 제거한 다음 다시 설치하고 ONTAP 관계를 다시 구성하세요.

ⓘ 서버 OS 커널에 대한 모든 업데이트는 ONTAP의 유지 관리 창과 조율되어야 합니다.

ONTAP Mediator의 새로운 기능

ONTAP Mediator는 각 릴리스마다 새로운 기능 향상을 제공합니다. 새로운 기능

향상된 기능

SCST 버전 정보는 를 SCST 지원 매트릭스참조하십시오.

ONTAP 중재자 버전	향상된 기능

1.11	• RHEL 지원: ◦ 호환성: 9.5. ◦ 권장 버전: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10. • Rocky Linux 10.1, 9.7 및 8.10을 지원합니다. • Oracle Linux 10.0 및 9.6 지원. • MetroCluster IP 구성에 IPv6에 대한 지원을 추가합니다. • fapolicyd에 대한 지원을 추가합니다.
1.10	• RHEL 지원: ◦ 호환성: 9.5. ◦ 권장 버전: 10.0, 9.6, 9.4, 8.10. • Rocky Linux 10.0, 9.6 및 8.10을 지원합니다. • 기본 Python 버전을 Python 3.9에서 Python 3.12로 업그레이드합니다.
1.9.1	• RHEL 지원: ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8. • Rocky Linux 9.5 및 8.10 지원. • 코드 서명 검증을 위한 새로운 인증서를 추가합니다. • 다음을 사용하여 코드 서명 확인 건너뛰기에 대한 지원이 추가되었습니다. `-skip -code-signature-check` 깃발. • 설치 프로그램은 만료된 코드 서명 인증서를 감지하면 경고를 표시합니다.
1.9	• RHEL 지원: ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8. • Rocky Linux 9.5 및 8.10 지원. • RHEL 및 Rocky Linux에 대한 FIPS 지원 • 확장성 향상을 위해 성능 향상 추가 • 파일 이름이 향상되어 PKI 서명 인증서의 설정이 간편해졌습니다.
1.8	• RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8. • Rocky Linux 9.4 및 8.10 지원.

1.7	• RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8. • Rocky Linux 9.3 및 8.9 지원. • 자체 서명된 인증서 및 타사 서명 인증서의 SAN(주체 대체 이름) 데이터 지원
1.6	• Python 3.9 업데이트. • RHEL 지원: ◦ 호환 가능 버전: 8.7, 8.6, 8.5, 8.4. ◦ 권장 버전: 9.2, 9.1, 9.0, 8.8. • Rocky Linux 9.2 및 8.8 지원. • RHEL 7.x/CentOS 모든 릴리스에 대한 지원이 중단되었습니다.
1.5	• RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • RHEL 7.x/CentOS 7.x에 대한 중단 경고를 포함합니다 • 대규모 SnapMirror 액티브 동기화 시스템에 맞게 속도 최적화 • 설치 프로그램에 암호화 코드 서명이 추가되었습니다.
1.4	• RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • UFEI 기반 펌웨어의 보안 부팅(SB) 지원이 추가되었습니다.
1.3	• RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원.
1.2	• RHEL 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6을 지원합니다. • CentOS 7.9, 7.8, 7.7 및 7.6 지원. • HTTPS 사서함 지원. • ONTAP 9.8 + MCC-IP AUSO 및 SnapMirror 액티브 동기화 ZRTO와 함께 사용
1.1	• RHEL 8.0 및 7.6 지원. • CentOS 7.6 지원. • Perl 종속성을 제거합니다.

1.0	• iSCSI 메일박스 지원 • ONTAP 9.7+ MCC-IP AUSO와 함께 사용. • RHEL/CentOS 7.6 지원

OS 지원 매트릭스

ONTAP 중재자를 위한 OS	1.11	1.10	1.9.1	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
RHEL 10.1	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 10.0	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.7	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.6	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.5 를 참조하십시오	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.4 를 참조하십시오	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.3 을 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.2	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.1	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 9.0	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요

RHEL 8.10을 참조하십시오	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.9 를 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.8	아니요	아니요	예	예	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.7	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.6을 참조하십시오	아니요	아니요	호환 가능	호환 가능	예	예	예	아니요	아니요	아니요	아니요	아니요	아니요
RHEL 8.5	아니요	아니요	호환 가능	호환 가능	예	예	예	예	예	아니요	아니요	아니요	아니요
RHEL 8.4	아니요	아니요	호환 가능	호환 가능	예	예	예	예	예	아니요	아니요	아니요	아니요
RHEL 8.3	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	아니요	아니요	아니요
RHEL 8.2	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	아니요	아니요	아니요
RHEL 8.1	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 8.0	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	예	아니요
RHEL 및 CentOS 7.9	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	호환 가능	아니요	아니요

RHEL 및 CentOS 7.8	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 및 CentOS 7.7	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	아니요	아니요
RHEL 및 CentOS 7.6	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	사용되지 않음	예	예	예	예	예	예(RHEL에만 해당)
CentOS 8 및 스트림	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	해당 없음	해당 없음	해당 없음
로키 리눅스 10.0	예	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
록키 리눅스 9	예	예	예	예	예	예	예	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
Rocky Linux 8	예	예	예	예	예	예	예	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
오라클 리눅스 10.0	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요
오라클 리눅스 9	예	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요	아니요

- "예"는 ONTAP 중재자 설치에 OS가 권장되며 완전히 호환되고 지원됨을 의미합니다.
- "아니요"는 OS 및 ONTAP 중재자가 호환되지 않음을 의미합니다.
- "호환"이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.
- ONTAP Mediator 1.6에서는 Rocky Linux 9 및 8에 대한 지원이 추가되었습니다.
- ONTAP 중재자 1.5는 RHEL 7.x 지사 운영 체제에서 마지막으로 지원되는 릴리스입니다.
- 재분개로 인해 모든 릴리스에 대해 CentOS 8이 제거되었습니다. CentOS Stream은 적합한 운영 대상 OS가 아닌

것으로 간주됩니다. 지원은 계획되어 있지 않습니다.

SCST 지원 매트릭스

다음 표는 ONTAP mediator의 각 버전에 대해 지원되는 SCST 버전을 보여줍니다.

ONTAP 중재자 버전	지원되는 SCST 버전입니다
ONTAP 중재자 1.11	scst-3.9.tar.gz
ONTAP 중재자 1.10	scst-3.9.tar.gz
ONTAP 중재자 1.9.1	scst-3.8.0.tar.bz2
ONTAP 중재자 1.9	scst-3.8.0.tar.bz2
ONTAP 중재자 1.8	scst-3.8.0.tar.bz2
ONTAP 중재자 1.7	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.6	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.5	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.4	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.3	scst - 3.5.0.tar.bz2
ONTAP 중재자 1.2	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.1	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.0	scst - 3.3.0.tar.bz2

설치 또는 업그레이드

ONTAP Mediator 설치 워크플로 요약

ONTAP Mediator를 설치하는 과정에는 설치 준비, 저장소 액세스 제공, 설치 패키지 다운로드, 코드 서명 확인, ONTAP Mediator 패키지 설치, 설치 후 구성 작업 수행이 포함됩니다.

1. **"ONTAP Mediator 설치 또는 업그레이드 준비"**

ONTAP Mediator를 설치하거나 업그레이드하려면 모든 필수 구성 요소가 충족되었는지 확인해야 합니다.

2. **"호스트 OS 및 중재자 업그레이드"**

ONTAP Mediator의 기존 버전을 업그레이드하는 경우, 먼저 이전 버전을 제거한 후 새 버전을 설치해야 합니다. ONTAP Mediator를 처음 설치하는 경우 이 단계를 건너뛸 수 있습니다.

3. "저장소 액세스 제공"

설치 과정에서 ONTAP Mediator가 필요한 패키지에 액세스할 수 있도록 저장소에 대한 액세스를 활성화해야 합니다.

4 **"ONTAP 중재자 설치 패키지를 다운로드합니다"**

ONTAP Mediator 다운로드 페이지에서 ONTAP Mediator 설치 패키지를 다운로드하세요.

5 **"ONTAP Mediator 설치 패키지의 코드 서명을 확인하세요."**

NetApp에서는 ONTAP Mediator 설치 패키지를 설치하기 전에 ONTAP Mediator 코드 서명을 확인할 것을 권장합니다.

6 **"ONTAP Mediator 설치"**

ONTAP Mediator를 설치하려면 설치 패키지를 받아서 호스트에서 설치 프로그램을 실행해야 합니다.

7 **"ONTAP Mediator 설치 확인"**

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

8 "설치 후 구성 작업 수행"

ONTAP Mediator를 설치하고 실행한 후에는 ONTAP Mediator 기능을 사용하기 위해 추가 구성 작업을 수행해야 합니다.

ONTAP Mediator 설치 또는 업그레이드

ONTAP Mediator를 설치하거나 업그레이드하려면 모든 필수 구성 요소를 충족하고, 설치 패키지를 다운로드한 다음 호스트에서 설치 프로그램을 실행해야 합니다.

- ONTAP 9.8부터는 모든 버전의 ONTAP Mediator를 사용하여 SnapMirror 활성 동기화 관계를 모니터링할 수 있습니다.
- ONTAP Mediator의 모든 버전을 사용하여 MetroCluster IP 구성을 모니터링할 수 있습니다.

설치 및 업그레이드 고려 사항

ONTAP Mediator를 업그레이드하거나 설치하기 전에 다음 사항을 검토하세요.

ONTAP Mediator 1.8 및 이전 버전은 Red Hat Enterprise Linux(RHEL) FIPS 모드와 호환되지 않아 성공적으로 설치할 수 없습니다. FIPS 모드가 활성화되어 있는지 확인하려면 다음을 사용하세요. `fips-mode-setup --check` 명령. 다음을 사용하여 FIPS 모드를 비활성화할 수 있습니다. `fips-modesetup --disable` 명령. ONTAP Mediator 1.8 또는 이전 버전을 성공적으로 설치하려면 FIPS 모드를 비활성화한 후 재부팅하세요.

- ONTAP Mediator를 최신 버전으로 업그레이드해야 합니다. 이전 버전은 모든 ONTAP 릴리스에서 여전히 작동하지만 최신 버전에는 타사 구성 요소에 대한 보안 패치가 포함되어 있습니다.
- 새 ONTAP 중재자 버전으로 업그레이드할 때 더 높은 버전을 사용할 수 없는 경우 설치 관리자는 자동으로 권장 SCST 버전으로 업그레이드합니다. 더 높은 SCST 버전을 수동으로 설치하는 방법은 을 참조하십시오"ONTAP 중재자 관리". 지원되는 버전은 를 "SCST 지원 매트릭스"참조하십시오.

- 설치에 실패하면 ONTAP Mediator의 최신 버전으로 업그레이드해야 할 수도 있습니다.
- 2025년 6월 15일부터 코드 서명 인증서가 만료되어 ONTAP Mediator 1.9 및 1.8을 설치하거나 업그레이드할 수 없습니다. 설치나 업그레이드가 실패하면 대신 ONTAP Mediator 1.9.1 패치 버전을 사용하세요.

- 를 설치하는 경우 `yum-utils` 패키지를 사용하면 을 사용할 수 있습니다 `needs-restarting` 명령.
- ONTAP Mediator 1.11부터 MetroCluster IP 구성에 IPv6가 지원됩니다.

호스트 요구 사항

RHEL 또는 Rocky Linux를 설치하고 관련 저장소를 구성할 때 다음 요구 사항을 따르세요.

설치 또는 구성 프로세스를 수정하는 경우 추가 단계를 수행해야 할 수 있습니다.

Linux 배포 요구 사항

- Red Hat의 모범 사례에 따라 RHEL 또는 Rocky Linux를 설치합니다. CentOS 8.x의 지원이 종료되었으므로, CentOS 8.x와 호환되는 버전은 권장되지 않습니다.
- ONTAP Mediator를 설치할 때 설치 프로그램이 모든 필수 소프트웨어 종속성을 검색하여 설치할 수 있도록 시스템이 필수 저장소에 액세스할 수 있는지 확인하세요.
- yum 설치 관리자가 RHEL 리포지토리에서 종속 소프트웨어를 찾을 수 있도록 하려면 설치 중 또는 이후에 유효한 Red Hat 서브스크립션을 사용하여 시스템을 등록합니다.

  자세한 내용은 Red Hat 서브스크립션 관리자 설명서를 참조하십시오.

네트워킹 요구 사항

다음 포트가 ONTAP 중재자에 사용 가능하고 사용되지 않는지 확인합니다.

포트/서비스	출처	방향	목적지	목적
22/TCP	관리 호스트	인바운드	ONTAP 중재자	(선택 사항) SSH/ONTAP 중재자 관리
31784/TCP	cluster-mgmt 및 node-mgmt LIF	인바운드	ONTAP 중재자 웹 서버	(필수) REST API(HTTPS)
3260/tcp	노드 관리 LIF	인바운드	ONTAP는 iSCSI 대상을 중재합니다	(MetroCluster IP 구성에 필요) 사서함에 대한 iSCSI 데이터 연결

SMBC 고객의 경우 ONTAP는 포트 3260을 활성화 또는 연결할 필요가 없습니다.

- 타사 방화벽을 사용하는 경우 다음을 참조하세요."ONTAP 중재자를 위한 방화벽 요구 사항" .
- 인터넷에 액세스할 수 없는 Linux 호스트의 경우 로컬 리포지토리에서 필요한 패키지를 사용할 수 있는지 확인합니다.

Linux 환경에서 LACP(Link Aggregation Control Protocol)를 사용하는 경우 커널을 구성하고 `sysctl net.ipv4.conf.all.arp_ignore` 을 로 `2`설정합니다.

OS 요구 사항

OS는 다음 요구 사항을 충족해야 합니다.

- 64비트 물리적 설치 또는 가상 머신
- 8GB RAM
- 1GB 디스크 공간(응용 프로그램 설치, 서버 로그 및 데이터베이스에 사용됨)
- 사용자: 루트 액세스

다음 표는 ONTAP mediator 버전별로 지원되는 운영 체제를 보여줍니다.

ONTAP 중재자 버전	지원되는 Linux 버전
1.11	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.1, 10.0, 9.7, 9.6, 9.4, 8.10 • Rocky Linux 10.1, 9.7 및 8.10 • Oracle Linux 10.0 및 9.6
1.10	• Red Hat Enterprise Linux ◦ 호환 가능: 9.5 [1] ◦ 권장: 10.0, 9.6, 9.4 및 8.10 • Rocky Linux 10.0, 9.6 및 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.9	• Red Hat Enterprise Linux ◦ 호환 가능 버전: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.5, 9.4, 9.2, 9.0, 8.10, 8.8 • Rocky Linux 9.5 및 8.10
1.8	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, 8.8 • Rocky Linux 9.4 및 8.10

1.7	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.3, 9.2, 9.1, 9.0, 8.9, 8.8 • Rocky Linux 9.3 및 8.9
1.6	• Red Hat Enterprise Linux: ◦ 호환 가능: 8.7, 8.6, 8.5, 8.4 [1] ◦ 권장: 9.2, 9.1, 9.0 및 8.8 • Rocky Linux 9.2 및 8.8
1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 및 7.6 • CentOS: 7.9, 7.8, 7.7 및 7.6

1. 호환 가능이란 Red Hat이 더 이상 이러한 RHEL 버전을 지원하지 않지만 ONTAP Mediator는 여전히 해당 버전에 설치할 수 있음을 의미합니다.

OS 필수 패키지

ONTAP Mediator에는 다음 패키지가 필요합니다.

패키지는 사전 설치되거나 ONTAP 중재자 설치 프로그램에 의해 자동으로 설치됩니다.

모든 RHEL/CentOS 버전	RHEL 10.x / Rocky Linux 10용 추가 패키지	RHEL 9.x/Rocky Linux 9용 추가 패키지	RHEL 8.x/Rocky Linux 8용 추가 패키지

• OpenSSL • OpenSSL - devel • kernel-devel-$(uname-r) • GCC 를 참조하십시오 • 만듭니다 • libselinux-utils • 패치 • bzip2 • Perl - 데이터 - 덤프 • Perl-ExtUtils-MakeMaker • efootmgr • mokutil	• 파이썬3.12 • 파이썬3.12-개발	• elfutils -libelf -devel • 정책 코어 유틸리티 - 비톤 - 유틸리티 • 3단계 • python3-devel	• elfutils -libelf -devel • 정책 코어 유틸리티 - 비톤 - 유틸리티 • redhat-LSB-core를 참조하십시오 • python39 • 피톤39-데블

중재자 설치 패키지는 다음을 포함하는 자동 압축 tar 파일입니다.

- 지원되는 릴리즈의 리포지토리에서 가져올 수 없는 모든 종속성을 포함하는 RPM 파일입니다.
- 설치 스크립트

유효한 SSL 인증서를 권장합니다.

OS 업그레이드 고려 사항 및 커널 호환성

- 커널을 제외한 모든 라이브러리 패키지를 업데이트할 수 있지만 ONTAP Mediator에서 변경 사항을 적용하려면 재부팅이 필요할 수 있습니다. 재부팅이 필요한 경우 가동 중지 시간을 예약하세요.
- OS 커널을 최신 상태로 유지해야 합니다. 커널 코어를 지원되는 버전으로 업그레이드하세요."ONTAP 중재자 버전 매트릭스" . 시스템을 재부팅해야 하므로, 정전에 대비한 유지 관리 기간을 계획하세요.
  - 재부팅하기 전에 SCST 커널 모듈을 제거한 다음 나중에 다시 설치하세요.
  - 커널 OS 업그레이드를 시작하기 전에 지원되는 SCST 버전을 준비하여 다시 설치하세요.

- 커널 버전이 운영 체제 버전과 일치해야 합니다.
- 테스트된 SCST 모듈이 작동하지 않을 수 있으므로 ONTAP Mediator 릴리스에 대해 지원되는 OS 버전 이상으로 커널을 업그레이드하지 마세요.

UEFI 보안 부팅이 활성화된 경우 **ONTAP mediator**를 설치합니다

ONTAP mediator는 UEFI 보안 부팅이 활성화되어 있거나 활성화되지 않은 시스템에 설치할 수 있습니다.

이 작업에 대해

필요하지 않거나 ONTAP mediator 설치 문제를 해결하는 경우 ONTAP mediator를 설치하기 전에 UEFI 보안 부팅을 사용하지 않도록 선택할 수 있습니다. 시스템 설정에서 UEFI 보안 부팅 옵션을 비활성화합니다.

UEFI 보안 부팅을 비활성화하는 방법에 대한 자세한 지침은 호스트 OS 설명서를 참조하십시오.

UEFI 보안 부팅이 활성화된 ONTAP Mediator를 설치하려면 서비스를 시작하기 전에 보안 키를 등록해야 합니다. 이 키는 SCST 설치의 컴파일 단계 중에 생성되며 컴퓨터에 개인 공개 키 쌍으로 저장됩니다. 유틸리티를 사용하여 `mokutil` 공개 키를 UEFI 펌웨어에 컴퓨터 소유자 키(Mok)로 추가하여 시스템이 서명된 모듈을 신뢰하고 로드할 수 있도록 합니다. `mokutil`Mok를 활성화하기 위해 시스템을 재부팅할 때 필요하므로 암호를 안전한 위치에 저장합니다.

단계

1. 시스템에서 UEFI 보안 부팅이 활성화되어 있는지 확인합니다.

```
mokutil --sb-state
```

결과는 이 시스템에서 UEFI 보안 부팅이 활성화되었는지 여부를 나타냅니다.

만약…	이동…
UEFI 보안 부팅이 활성화되었습니다	
UEFI 보안 부팅이 비활성화되었습니다	"호스트 운영 체제를 업그레이드한 다음 ONTAP Mediator를 업그레이드합니다."

- 보안 위치에 저장해야 하는 암호를 만들라는 메시지가 표시됩니다. UEFI 부팅 관리자에서 키를 활성화하려면 이 암호가 필요합니다.
- ONTAP 중재자 1.2.0 및 이전 버전은 이 모드를 지원하지 않습니다.

2. 유틸리티가 설치되어 있지 않으면 `mokutil` 다음 명령을 실행합니다.

```
yum install mokutil
```

호스트 **OS** 및 **ONTAP** 중재자를 업그레이드합니다

ONTAP 중재자를 위한 호스트 OS를 최신 버전으로 업그레이드하려면 먼저 ONTAP 중재자를 제거해야 합니다.

이 작업에 대해

leapp-upgrade 도구를 사용하여 ONTAP Mediator의 호스트 OS를 업그레이드하기 전에 ONTAP Mediator를 제거하세요. 이 도구는 등록된 저장소에서 새로운 RPM 버전을 확인합니다.

ONTAP Mediator 설치 프로그램은 .rpm 파일을 설치하고, leapp-upgrade 도구는 이 파일을 검색에 포함합니다. 설치 프로그램이 등록된 저장소에서 파일을 다운로드하는 대신 압축을 풀기 때문에 도구에서 업그레이드를 찾을 수 없습니다. 패키지를 제거하려면 leapp-upgrade 도구를 사용해야 합니다.

단계

1. 로그 파일을 백업하세요.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. leapp-upgrade 도구를 사용하여 업그레이드를 수행합니다.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediator를 다시 설치하세요:

로그 파일 손실을 방지하기 위해 ONTAP 중재자를 재설치한 후 바로 나머지 단계를 수행하십시오.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. ontap_mediator 중지:

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. 로그 파일을 교체합니다.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. ontap_mediator를 시작합니다:

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. 모든 ONTAP 클러스터를 업그레이드된 ONTAP Mediator에 다시 연결합니다.

IP를 통한 MetroCluster

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirror 활성 동기화

SnapMirror Active Sync의 경우 /opt/netapp 외부에 저장된 TLS 인증서를 다시 설치할 필요가 없습니다. /opt/netapp에 저장된 인증서를 백업하고 복원합니다.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                         ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

```
The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

관련 정보

- "보안 인증서 삭제"
- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "스냅미러 중재자 추가"
- "스냅미러 중재자 제거"
- "스토리지 iSCSI 이니시에이터 표시"

ONTAP 중재자 설치를 위한 리포지토리 액세스를 제공합니다

설치 과정에서 ONTAP Mediator가 필요한 패키지에 액세스할 수 있도록 저장소에 대한 액세스를 활성화해야 합니다.

단계

1. 다음 표와 같이 액세스해야 하는 리포지토리를 결정합니다.

운영 체제가…	이러한 리포지토리에 대한 액세스를 제공해야 합니다…
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x를 참조하십시오	• RHEL-9-for-x86_64-baseos-rpms • RHEL-9-for-x86_64-appstream-rpms
RHEL 8.x를 참조하십시오	• RHEL-8-for-x86_64-baseos-rpms • RHEL-8-for-x86_64-appstream-rpms
RHEL 7.x를 참조하십시오	• RHEL-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - 기본 리포지토리입니다
로키 리눅스 10	• 애플리케이션 스트림 • 베이스코스
록키 리눅스 9	• 애플리케이션 스트림 • 베이스코스
Rocky Linux 8	• 애플리케이션 스트림 • 베이스코스

2. 다음 절차 중 하나를 사용하여 위에 나열된 리포지토리에 액세스할 수 있으므로 ONTAP 중재자가 설치 프로세스 중에 필요한 패키지에 액세스할 수 있습니다.

ONTAP Mediator에 "추가" 및 "선택" 저장소에 있는 Python 모듈에 대한 종속성이 있는 경우 액세스해야 할 수 있습니다. `rhel-X-for-x86_64-extras-rpms` 그리고 `rhel-X-for-x86_64-optional-rpms` 파일.

RHEL 10.x 운영 체제에 대한 절차

운영 체제가 *RHEL 10.x*인 경우 다음 절차를 사용하여 저장소에 대한 액세스를 활성화하세요.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 9.x 운영 체제에 대한 절차

운영 체제가 * RHEL 9.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 8.x 운영 체제에 대한 절차

운영 체제가 * RHEL 8.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. yum repolist 명령을 실행합니다.

새로 가입된 리포지토리가 목록에 나타납니다.

RHEL 7.x 운영 체제에 대한 절차

운영 체제가 * RHEL 7.x * 인 경우 다음 절차를 사용하여 리포지토리에 액세스할 수 있습니다.

단계

1. 필요한 리포지토리 구독:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

다음 예제에서는 이 명령의 실행을 보여 줍니다.

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. yum repolist 명령을 실행합니다.

다음 예제에서는 이 명령의 실행을 보여 줍니다. "rhel-7-server-optional-rpms" 리포지토리가 목록에 나타나야 합니다.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                    repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

CentOS 7.x 운영 체제에 대한 절차

운영 체제가 * CentOS 7.x * 인 경우 리포지토리에 대한 액세스를 활성화하려면 다음 절차를 따르십시오.

다음 예는 CentOS 7.6의 리포지토리를 보여 주고 있으며 다른 CentOS 버전에서는 작동하지 않을 수 있습니다. 사용 중인 CentOS 버전에 대한 기본 리포지토리를 사용합니다.

단계

1. C7.6.1810-Base 리포지토리를 추가합니다. C7.6.1810 - 기본 볼트 리포지토리에는 ONTAP 중재자를 위해 필요한 "kernel-devel" 패키지가 포함되어 있습니다.
2. /etc/yum.repos.d/CentOS-Vault.repo에 다음 줄을 추가합니다.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. yum repolist 명령을 실행합니다.

   다음 예제에서는 이 명령의 실행을 보여 줍니다. CentOS-7.6.1810-기본 리포지토리가 목록에 나타나야 합니다.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Rocky Linux 10, 9 또는 **8** 운영 체제에 대한 절차

운영 체제가 **Rocky Linux 10**, **Rocky Linux 9** 또는 *Rocky Linux 8*인 경우 다음 절차를 사용하여 저장소에 대한 액세스를 활성화하세요.

단계

1. 필요한 리포지토리 구독:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. 을 수행합니다 `clean` 작동:

```
dnf clean all
```

3. 리포지토리 목록을 확인합니다.

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                          repo name
appstream                        Rocky Linux 8 - AppStream
baseos                           Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

ONTAP 중재자 설치 패키지를 다운로드합니다

ONTAP Mediator 설치 패키지를 다운로드하여 설치하세요.

단계

1. ONTAP Mediator 다운로드 페이지에서 ONTAP Mediator 설치 패키지를 다운로드하세요.

   "ONTAP 중재자 다운로드 페이지"

2. Mediator 설치 패키지를 현재 작업 디렉토리에 넣었는지 확인하세요.

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   ⓘ ONTAP 중재자 버전 1.4 및 이전 버전의 경우 설치 관리자의 이름이 지정됩니다 `ontap-mediator`.

   시스템에 인터넷 접속이 불가능한 경우, 설치 프로그램이 필요한 패키지에 접근할 수 있는지 확인하세요.

3. 필요한 경우 Mediator 설치 패키지를 설치 디렉터리로 이동합니다.
4. 설치 프로그램 패키지의 압축을 풉니다.

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

ONTAP 중재자 코드 서명을 확인합니다

NetApp 설치 전에 ONTAP Mediator 코드 서명을 확인할 것을 권장합니다. 이 단계는 선택 사항입니다.

시작하기 전에

ONTAP Mediator 코드 서명을 확인하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하세요.

- 2025년 6월 15일부터 코드 서명 검증 인증서가 만료되어 ONTAP Mediator 1.9 및 1.8를 설치하거나 업그레이드할 수 없습니다. 대신 ONTAP Mediator 1.11 또는 1.10을 설치하거나 업그레이드하세요.
- 시스템이 아래 요구 사항을 충족하지 않는 경우 확인 프로세스가 필요하지 않으며 로 직접 이동할 수 있습니다"ONTAP 중재자 설치 패키지를 설치합니다".

- 기본 검증을 위한 OpenSSL 버전 1.0.2에서 3.0까지
- TSA(Time Stamping Authority) 작업을 위한 OpenSSL 버전 1.1.0 이상
- OCSP 검증을 위한 공용 인터넷 액세스

다운로드 패키지에는 다음 파일이 포함되어 있습니다.

파일	설명
`ONTAP-Mediator-production.pub`	서명을 확인하는 데 사용되는 공개 키입니다
`csc-prod-chain-ONTAP-Mediator.pem`	공공 인증 CA 신뢰 체인
`csc-prod-ONTAP-Mediator.pem`	키를 생성하는 데 사용되는 인증서입니다
`ontap-mediator-1.11.0`	버전 1.11에 대한 제품 설치 실행 파일
`ontap-mediator-1.11.0.sig`	SHA-256 해시된 후 csc-prod 키를 사용하여 RSA에 서명하여 설치 관리자를 서명합니다

ontap-mediator-1.11.0.sig.tsr	설치 관리자의 서명에 OCSCP가 사용할 해지 요청입니다
ontap-mediator-1.11.0.tsr	타임스탬프 서명 요청 파일입니다
tsa-prod-ONTAP-Mediator.pem	TSR의 공개 인증서
tsa-prod-chain-ONTAP-Mediator.pem	TSR의 공개 인증서 CA 체인

단계

1. 에 대해 해지 확인을 수행합니다 `csc-prod-ONTAP-Mediator.pem` 온라인 인증서 상태 프로토콜(OCSP)을 사용합니다.

   a. 인증서의 OCSP URL을 찾으세요. 개발자 인증서는 URI를 제공하지 않을 수 있습니다.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. 인증서에 대한 OCSP 요청을 생성합니다.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. OCSP Manager에 연결하여 OCSP 요청을 보냅니다.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. CSC의 신뢰 체인과 로컬 호스트에 대한 만료 날짜를 확인합니다.

   `openssl verify`

   를 클릭합니다 `openssl` 경로의 버전에 유효한 값이 있어야 합니다 `cert.pem` (자체 서명 안 됨).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. 확인하다 `ontap-mediator-1.11.0.sig.tsr` 그리고 `ontap-mediator-1.11.0.tsr` 연관된 인증서를 사용하는 파일:

오픈SSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
```

오픈SSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

ⓘ `.tsr`파일에는 설치 프로그램과 관련된 타임스탬프 응답과 코드 서명이 포함되어 있습니다. 처리 과정에서는 타임스탬프에 TSA의 유효한 서명이 있고 입력 파일이 변경되지 않았음을 확인합니다. 귀하의 기기는 로컬에서 검증을 수행합니다. TSA 서버에 접속할 필요가 없습니다.

4. 키에 대한 서명 확인:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

ONTAP 중재자 설치 패키지를 설치합니다

ONTAP Mediator를 설치하려면 설치 패키지를 받아서 호스트에서 설치 프로그램을 실행해야 합니다.

단계

1. 설치 프로그램을 실행하고 필요에 따라 프롬프트에 응답합니다.

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

설치 중에 서명 확인을 건너뛰려면 다음 명령을 사용하세요. `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code-signature-check`

설치 프로그램은 필요한 계정을 생성하고 필요한 패키지를 설치합니다. Mediator가 이미 설치되어 있는 경우 업그레이드하라는 메시지가 표시됩니다.

ONTAP 중재자 설치의 예(콘솔 출력)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]#./ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes



Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                              50 k
 gcc
x86_64                                            14.2.1-7.el10
AppStream                                              37 M
 kernel-devel
x86_64                                            6.12.0-55.9.1.el10_0
AppStream                                              22 M
 make
x86_64                                            1:4.4.1-9.el10
BaseOS                                                591 k
 openssl-devel
x86_64                                            1:3.2.2-16.el10
AppStream                                             3.9 M
 patch
x86_64                                            2.7.6-26.el10
AppStream                                             134 k
 perl-ExtUtils-MakeMaker
noarch                                            2:7.70-513.el10
AppStream                                              297 k
 python3-devel
x86_64                                            3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                            23.3.2-7.el10
AppStream                                             3.2 M
Installing dependencies:
 annobin-docs
noarch                                            12.92-1.el10
AppStream                                              94 k
 annobin-plugin-gcc
x86_64                                            12.92-1.el10
AppStream                                             985 k
 bison
x86_64                                            3.8.2-9.el10
AppStream                                             1.0 M
 cmake-filesystem
x86_64                                            3.30.5-2.el10
AppStream                                              29 k
 cpp
x86_64                                            14.2.1-7.el10
AppStream                                              12 M
 dwz
x86_64                                            0.15-7.el10
AppStream                                             139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64                go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

UEFI 보안 부팅을 위한 보안 키 등록

ONTAP Mediator 1.4부터 UEFI 시스템에서 보안 부팅 메커니즘이 활성화됩니다. 보안 부팅이 활성화된 경우 설치 후 보안 키를 등록하기 위한 추가 단계를 거쳐야 합니다.

단계

1. SCST 커널 모듈에 서명하려면 README 파일의 지침을 따르세요.

   ```
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
   signing
   ```

2. 필요한 키를 찾습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

설치 후 시스템 출력에는 README 파일과 키 위치가 제공됩니다.

3. Mok 목록에 공개 키를 추가합니다.

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

개인 키는 기본 위치에 두거나 안전한 위치로 옮길 수 있습니다. 부트 관리자가 공개 키를 사용할 수 있도록 공개 키를 기존 위치에 보관해야 합니다. 자세한 내용은 README.module-signing 파일을 참조하세요.

```
[root@hostname ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
```

4. 호스트를 재부팅하고 장치의 UEFI 부팅 관리자를 사용하여 새 MOK를 승인합니다. 제공된 암호 문구가 필요합니다. `mokutil` 유용성"UEFI 보안 부팅이 활성화된 경우 ONTAP mediator를 설치합니다" .

SCST 커널 모듈 서명

ONTAP Mediator가 설치된 후 systemctl status가 `mediator-scst` 실패(비활성)로 표시되는 경우 다음 단계에 따라 SCST 커널 모듈에 서명하세요.

단계

1. 빌드 프로세스 중에 공개/비공개 키 쌍이 생성됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` 다음 명령을 사용하여 디렉토리로 이동합니다.

```
[root@mediator-host ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
[root@mediator-host ~]#
```

2. 다음 명령을 실행하여 UEFI 키 저장소로 공개 키를 가져오는 프로세스를 시작합니다.

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
input password:
input password again:

[root@mediator-host ~]#
```

3. mokutil 소프트웨어는 가져오기 프로세스 중에 이 키에 사용할 임시 비밀번호를 요청합니다.
4. 가져오기 프로세스가 시작되었는지 확인하십시오. `mokutil --list-new` 그리고 시스템을 재부팅하세요.

부트로더는 EFI MOK 관리자를 시작합니다.

5. 화면의 메뉴를 사용하여 SCST 커널 모듈 키를 켭니다. 부팅 후 실행 `systemctl status mediator-scst`. 서비스가 시작되면 SCST 커널 모듈이 서명됩니다.

ONTAP 중재자 설치 상태를 확인합니다

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

단계

1. ONTAP Mediator의 상태를 확인하세요:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator에서 사용하는 포트를 확인하세요.

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

설치 후 **ONTAP** 중재자 구성

ONTAP Mediator를 설치하고 실행한 후에는 ONTAP Mediator 기능을 사용하기 위해 ONTAP 스토리지 시스템에서 추가 구성 작업을 수행해야 합니다.

- MetroCluster IP 구성에서 ONTAP Mediator를 사용하려면 다음을 참조하세요. "MetroCluster IP 구성에서 ONTAP Mediator 구성" .
- SnapMirror 활성 동기화를 사용하려면 을 참조하십시오"ONTAP Mediator를 설치하고 ONTAP 클러스터 구성을 확인하세요.".

ONTAP 중재자 보안 정책을 구성합니다

ONTAP Mediator는 여러 가지 구성 가능한 보안 설정을 지원합니다. 모든 설정의 기본값은 `low_space_threshold_mib: 10` 읽기 전용 파일로 제공됩니다.

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

에 배치된 모든 값 `ontap_mediator.user_config.yaml` 는 기본값을 무시하고 모든 ONTAP 중재자 업그레이드에 대해 유지됩니다.

수정 후 `ontap_mediator.user_config.yaml` , ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP 중재자 특성을 수정합니다

필요한 경우 이 섹션에 설명된 ONTAP 중재자 속성을 수정할 수 있습니다.

> ONTAP 중재자 업그레이드 중에 수정된 값이 유지되지 않으므로 의 다른 기본값은 `ontap_mediator.config.yaml` 변경되지 않아야 합니다.

필요한 변수를 파일에 복사하여 기본 설정을 재정의하여 ONTAP 중재자 특성을 `ontap_mediator.user_config.yaml` 수정합니다.

타사 SSL 인증서를 설치합니다

자체 서명된 기본 인증서를 타사 SSL 인증서로 대체해야 하는 경우 다음 파일에서 특정 특성을 수정합니다.

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

이러한 파일의 변수는 ONTAP Mediator에서 사용되는 인증서 파일을 제어하는 데 사용됩니다.

ONTAP 중재자 **1.9** 이상

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 있습니다.

변수	경로
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` 클라이언트 인증서의 만료를 설정하는 데 사용됩니다. 최대값은 3년(1095일)입니다.
- `x509_passin_pwd` 은 서명된 클라이언트 인증서의 암호입니다.

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 있습니다.

변수	경로
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP 중재자 **1.8** 이하

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 있습니다.

변수	경로
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` 클라이언트 인증서의 만료를 설정하는 데 사용됩니다. 최대값은 3년(1095일)입니다.
- `x509_passin_pwd` 은 서명된 클라이언트 인증서의 암호입니다.

다음 표에 나열된 기본 변수가 파일에 포함되어 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 있습니다.

변수	경로
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

이러한 속성을 수정한 경우 ONTAP Mediator를 다시 시작하여 변경 사항을 적용하세요. 기본 인증서를 타사 인증서로 교체하는 방법에 대한 자세한 지침은 을 참조하십시오"자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다".

암호 공격 보호

다음 설정은 무차별 암호 추측 공격에 대한 보호 기능을 제공합니다.

기능을 활성화하려면 및 `retry_limit` 의 값을 `window_seconds` 설정합니다.

예:

- 추측을 위한 5분 창을 제공한 다음 이 수를 0으로 재설정합니다.

```
authentication_lock_window_seconds: 300
```

- 기간 내에 5번의 장애가 발생할 경우 계정을 잠급니다.

```
authentication_retry_limit: 5
```

- 각 시도를 거부하기 전에 발생하는 지연을 설정하여 무차별 암호 추측 공격의 영향을 줄입니다.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

암호 복잡성 규칙

다음 필드는 ONTAP 중재자 API 사용자 계정의 암호 복잡성 규칙을 제어합니다.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

사용 가능한 공간 제어

디스크에 필요한 여유 공간을 제어하는 설정이 `/opt/netapp/lib/ontap_mediator` 있습니다.

공간이 설정된 임계값보다 낮으면 서비스에서 경고 이벤트를 실행합니다.

```
low_space_threshold_mib: 10
```

예약 로그 공간을 제어합니다

reserve_log_space는 특정 설정에 의해 제어됩니다. 기본적으로 ONTAP Mediator 설치 시 로그를 위한 별도의 디스크 공간이 생성됩니다. 설치 프로그램은 ONTAP Mediator 로깅에 명시적으로 사용할 총 700MB의 디스크 공간을 가진 새로운 고정 크기 파일을 생성합니다.

이 기능을 비활성화하고 기본 디스크 공간을 사용하려면 다음 단계를 수행하십시오.

1. 다음 파일에서 reserve_log_space 값을 1에서 0으로 변경합니다.

   `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

2. 중재자 다시 시작:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

이 기능을 다시 활성화하려면 값을 0에서 1로 변경하고 중재자를 다시 시작하십시오.

디스크 공간 간에 전환하면 기존 로그가 지워지지 않습니다. 이전 로그는 모두 백업된 다음 중재자를 전환하고 다시 시작한 후 현재 디스크 공간으로 이동합니다.

ONTAP 중재자 관리

사용자 자격 증명 변경, 서비스 중지 및 재활성화, 서비스 상태 확인, 호스트 유지 관리를 위한 SCST 설치 또는 제거를 포함하여 ONTAP Mediator를 관리합니다. 또한 자체 서명된 인증서 다시 생성, 신뢰할 수 있는 타사 인증서로 대체, 인증서 관련 문제 해결 등의 인증서를 관리할 수 있습니다.

사용자 이름을 변경합니다

다음 절차를 사용하여 사용자 이름을 변경할 수 있습니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/중재자_username'

단계

다음 옵션 중 하나를 선택하여 사용자 이름을 변경합니다.

- * option (a) * : 명령을 실행합니다 `mediator_change_user` 를 클릭하고 다음 예에 표시된 프롬프트에 응답합니다.

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- * option(b) *: 다음 명령을 실행합니다.

  MDIATOR_USERNAME=중재자_PASSWORD=mediator2 MEDIATOR_NEW_USERNAME=mediatoradmin 중재자_CHANGE_USER

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

암호를 변경합니다

다음 절차를 사용하여 암호를 변경할 수 있습니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/중재자_change_password'

단계

다음 옵션 중 하나를 선택하여 암호를 변경합니다.

- * option (a) * : 를 실행합니다 `mediator_change_password` 다음 예에 표시된 대로 명령을 실행하고 프롬프트에 응답합니다.

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
             Old Password:
             New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- * option(b) *: 다음 명령을 실행합니다.

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

이 예제에서는 암호가 "mediator1"에서 "mediator2"로 변경되었음을 보여 줍니다.

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

ONTAP 중재자 중단

ONTAP Mediator를 중지하려면 다음 단계를 수행하세요.

단계

1. ONTAP 중재자 중단:

```
systemctl stop ontap_mediator
```

2. SCST 중지:

```
systemctl stop mediator-scst
```

3. ONTAP Mediator 및 SCST 비활성화:

```
systemctl disable ontap_mediator mediator-scst
```

ONTAP Mediator 다시 활성화

ONTAP Mediator를 다시 활성화하려면 다음 단계를 수행하세요.

단계

1. ONTAP Mediator 및 SCST 활성화:

```
systemctl enable ontap_mediator mediator-scst
```

2. SCST 시작:

```
systemctl start mediator-scst
```

3. ONTAP 중재자 시작:

```
systemctl start ontap_mediator
```

ONTAP Mediator가 정상인지 확인하세요

ONTAP Mediator를 설치한 후 성공적으로 실행되는지 확인하세요.

단계

1. ONTAP Mediator의 상태를 확인하세요:

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. ONTAP Mediator에서 사용하는 포트를 확인하세요.

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

ONTAP Mediator 제거

필요한 경우 ONTAP Mediator를 제거할 수 있습니다.

시작하기 전에

ONTAP을 제거하기 전에 ONTAP Mediator와 ONTAP의 연결을 해제해야 합니다.

이 작업에 대해

ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.

이 명령에 액세스할 수 없는 경우 다음 예에 표시된 대로 전체 경로를 사용하여 명령을 실행해야 할 수 있습니다.

'/usr/local/bin/uninstall_ontap_중재자'

단계

1. ONTAP Mediator 제거:

   uninstall_ontap_중재자

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

자체 서명된 임시 인증서를 다시 생성합니다

ONTAP mediator 1.7부터 다음 절차에 따라 자체 서명된 임시 인증서를 다시 생성할 수 있습니다.

이 절차는 ONTAP mediator 1.7 이상을 실행하는 시스템에서만 지원됩니다.

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- ONTAP Mediator를 설치한 후 호스트 이름이나 호스트의 IP 주소가 변경되어 생성된 자체 서명 인증서가 더 이상 사용되지 않는 경우에만 이 작업을 수행할 수 있습니다.
- 임시 자체 서명된 인증서가 신뢰할 수 있는 타사 인증서로 대체되면 이 작업을 사용하여 인증서를 다시 생성합니다. 자체 서명된 인증서가 없으면 이 절차가 실패합니다.

단계

현재 호스트에 대해 자체 서명된 새 임시 인증서를 다시 생성하려면 다음 단계를 수행하십시오.

1. ONTAP Mediator를 다시 시작하세요:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

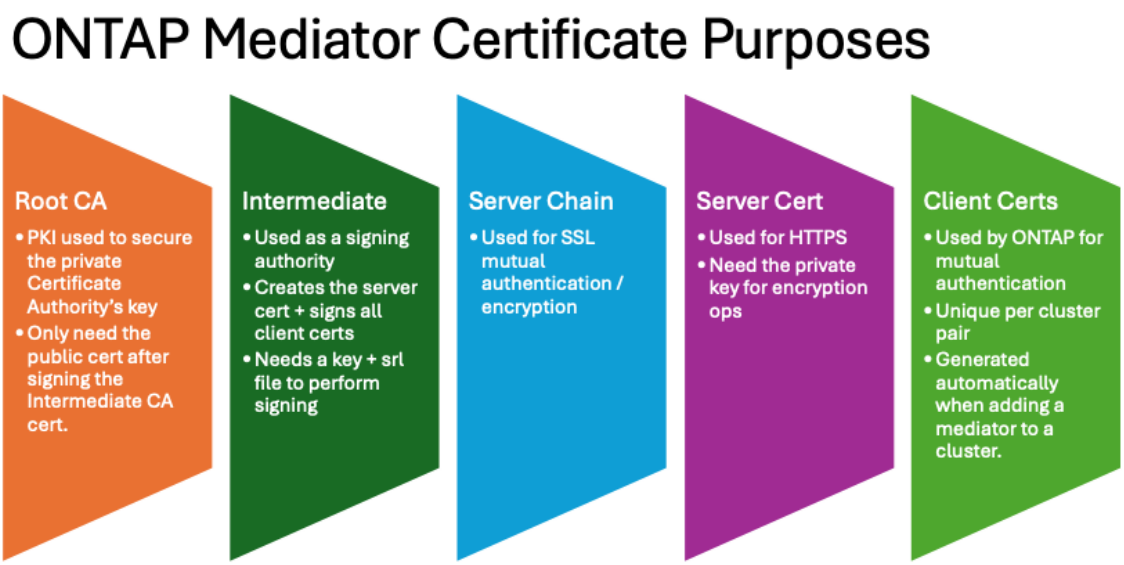
자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿉니다

지원되는 경우 자체 서명된 인증서를 신뢰할 수 있는 타사 인증서로 바꿀 수 있습니다.

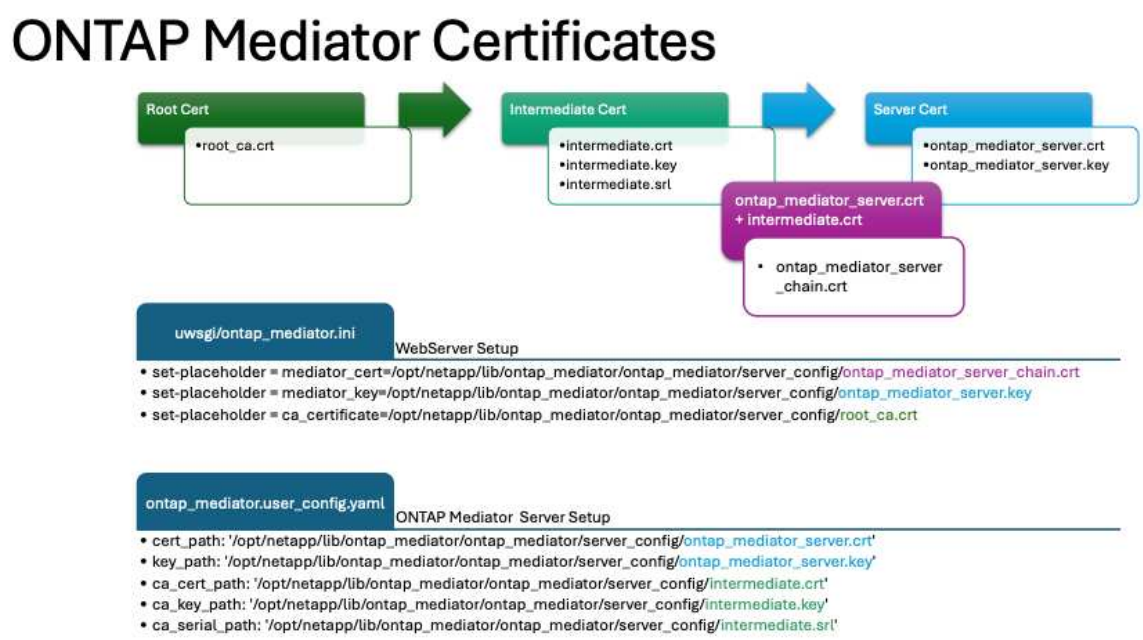
- 타사 인증서는 ONTAP 9.16.1 및 일부 이전 ONTAP 패치 릴리스에서만 지원됩니다. 을 "NetApp 버그 온라인 버그 ID CONTAP-243278"참조하십시오.
- 타사 인증서는 ONTAP mediator 1.7 이상을 실행하는 시스템에서만 지원됩니다.

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- 생성된 자체 서명된 인증서를 신뢰할 수 있는 하위 CA(인증 기관)에서 가져온 인증서로 교체해야 하는 경우 이 작업을 수행할 수 있습니다. 이렇게 하려면 신뢰할 수 있는 PKI(공개 키 인프라) 권한에 액세스할 수 있어야 합니다.
- 다음 이미지는 각 ONTAP 중재자 인증서의 용도를 보여 줍니다.



- 다음 이미지는 웹 서버 설정과 ONTAP Mediator 설정에 대한 구성을 보여줍니다.



1단계: **CA** 인증서를 발급하는 타사로부터 인증서를 얻습니다

다음 절차를 사용하여 PKI 기관으로부터 인증서를 얻을 수 있습니다.

다음 예제에서는 자체 서명된 인증서 액터를 에 있는 타사 인증서 액터로 바꾸는 방법을 보여 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/` 줍니다.

이 예는 ONTAP Mediator에 필요한 인증서에 대한 필수 기준을 보여줍니다. 이 절차와 다른 방법으로 PKI 기관으로부터 인증서를 얻을 수 있습니다. 비즈니스 요구에 따라 절차를 조정합니다.

ONTAP 중재자 **1.9** 이상

1. PKI 기관에서 인증서를 생성하기 위해 사용할 개인 키와 구성 파일을 `openssl_ca.cnf` 만듭니다 `intermediate.key`.

   a. 개인 키를 `intermediate.key`생성합니다.

      ▪ 예 *

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. 구성 파일 `openssl_ca.cnf` (에 위치 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`)은 생성된 인증서에 있어야 하는 속성을 정의합니다.

2. 개인 키 및 구성 파일을 사용하여 인증서 서명 요청을 만듭니다 `intermediate.csr`.

   ◦ 예: *

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. PKI 기관에 인증서 서명 요청을 보내 `intermediate.csr` 서명을 받습니다.

   PKI 기관은 요청을 검증하고 서명합니다. `.csr` , 인증서 생성 `intermediate.crt` . 또한 다음을 얻어야 합니다. `root_ca.crt` 서명한 인증서 `intermediate.crt` PKI 기관의 인증서.

   SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서. 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

ONTAP 중재자 **1.8** 이하

1. PKI 기관에서 인증서를 생성하기 위해 사용할 개인 키와 구성 파일을 `openssl_ca.cnf` 만듭니다 `ca.key`.

   a. 개인 키를 `ca.key`생성합니다.

      ▪ 예 *

```
openssl genrsa -aes256 -out ca.key 4096
```

   a. 구성 파일 `openssl_ca.cnf` (에 위치 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.c`

nf)은 생성된 인증서에 있어야 하는 속성을 정의합니다.

2. 개인 키 및 구성 파일을 사용하여 인증서 서명 요청을 만듭니다 ca.csr.

   ◦ 예: *

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. PKI 기관에 인증서 서명 요청을 보내 ca.csr 서명을 받습니다.

   PKI 권한은 요청을 확인하고 에 서명하여 .csr`인증서를 `ca.crt`생성합니다. 또한 PKI 기관으로부터 인증서를 얻어야 `root_ca.crt that signed the `ca.crt 합니다.

   SM-BC(SnapMirror Business Continuity) 클러스터의 경우 및 인증서를 ONTAP 클러스터에 추가해야 ca.crt root_ca.crt 합니다. 을 "SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성"참조하십시오.

2단계**:** 타사 **CA** 인증서로 서명하여 서버 인증서를 생성합니다

ONTAP 중재자 **1.9** 이상

서버 인증서는 개인 키 및 타사 인증서로 `intermediate.crt` 서명해야 `intermediate.key` 합니다. 또한 구성 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` 파일에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 특성이 포함되어 있습니다.

다음 명령을 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 CSR(인증서 서명 요청)을 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSR에서 서버 인증서를 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

> 이러한 파일은 PKI 기관에서 가져왔습니다. 다른 인증서 이름을 사용하는 경우 `intermediate.crt` 및 를 `intermediate.key` 관련 파일 이름으로 바꿉니다.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

◦ 이 `-CAcreateserial` 옵션은 파일을 생성하는 데 `intermediate.srl` 사용됩니다.

ONTAP 중재자 **1.8** 이하

서버 인증서는 개인 키 및 타사 인증서로 `ca.crt` 서명해야 `ca.key` 합니다. 또한 구성 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` 파일에는 OpenSSL에서 발급한 서버 인증서에 필요한 속성을 지정하는 특정 특성이 포함되어 있습니다.

다음 명령을 사용하여 서버 인증서를 생성할 수 있습니다.

단계

1. 서버 CSR(인증서 서명 요청)을 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. CSR에서 서버 인증서를 생성하려면 폴더에서 다음 명령을 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` 실행합니다.

> 이러한 파일은 PKI 기관에서 가져왔습니다. 다른 인증서 이름을 사용하는 경우 `ca.crt` 및 를 `ca.key` 관련 파일 이름으로 바꿉니다.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- 이 `-CAcreateserial` 옵션은 파일을 생성하는 데 `ca.srl` 사용됩니다.

3단계**: ONTAP** 중재자 구성에서 새로운 타사 **CA** 인증서와 서버 인증서를 교체합니다

ONTAP Mediator 1.10 이상

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 및 `key_path` 서버 인증서 변수입니다.
- `ca_cert_path`, `ca_key_path`, 및 `ca_serial_path` CA 인증서 변수입니다.

단계

1. 모든 `intermediate.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `intermediate.crt` `ontap_mediator_server.crt` 생성합니다.

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. 업데이트 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` 파일.

   값을 업데이트합니다 `ssl_keyfile` , `ssl_certfile` , 그리고 `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

- 그만큼 `ssl_keyfile` 값은 키 경로입니다 `ontap_mediator_server.crt` 파일입니다 `ontap_mediator_server.key` .
- 그만큼 `ssl_certfile` 값은 경로입니다 `ontap_mediator_server_chain.crt` 파일.
- 그만큼 `ssl_ca_certs` 값은 경로입니다 `root_ca.crt` 파일.

4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
   - Linux 그룹 소유자: `netapp:netapp`
   - Linux 권한: `600`
5. ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 및 `key_path` 서버 인증서 변수입니다.
- `ca_cert_path`, `ca_key_path`, 및 `ca_serial_path` CA 인증서 변수입니다.

단계

1. 모든 `intermediate.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `intermediate.crt` `ontap_mediator_server.crt` 생성합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 mediator_cert mediator_key `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

    - mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt
    - mediator_key value`는 파일의 키 경로입니다. `ontap_mediator_server.crt ontap_mediator_server.key
    - ca_certificate`값은 파일의 경로입니다. `root_ca.crt

4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
    - Linux 그룹 소유자: netapp:netapp
    - Linux 권한: 600
5. ONTAP Mediator를 다시 시작하세요:

```
systemctl restart ontap_mediator
```

ONTAP 중재자 **1.8** 이하

인증서 구성은 다음 위치에 있는 구성 파일에서 ONTAP Mediator에 제공됩니다. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml . 이 파일에는 다음과 같은 속성이 포함되어 있습니다.

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- cert_path 및 key_path 서버 인증서 변수입니다.
- ca_cert_path, ca_key_path, 및 ca_serial_path CA 인증서 변수입니다.

단계

1. 모든 `ca.*` 파일을 타사 인증서로 바꿉니다.
2. 및 인증서에서 인증서 체인을 `ca.crt` `ontap_mediator_server.crt` 생성합니다.

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

   , 및 의 값을 `mediator_cert` `mediator_key` `ca_certificate`업데이트합니다.

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
   - `mediator_key value`는 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
   - `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`
4. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.
   - Linux 그룹 소유자: `netapp:netapp`
   - Linux 권한: `600`
5. ONTAP Mediator를 다시 시작하세요:

   ```
   systemctl restart ontap_mediator
   ```

4단계**:** 타사 인증서에 다른 경로나 이름을 사용할 수도 있습니다

ONTAP Mediator 1.10 이상

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `intermediate.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `intermediate.crt` 개인 키를 해당 위치에 저장하면 `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

   > 인증서에 서명하는 데 사용한 경우 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 인증서 구조를 사용하는 경우 `root_ca.crt` 인증서는 다음을 제공합니다. `intermediate.crt` 서명하는 인증서 `ontap_mediator_server.crt` 인증서, 인증서 체인을 만듭니다. `intermediate.crt` 그리고 `ontap_mediator_server.crt` 인증서:

> ⓘ 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `intermediate.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. 업데이트 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` 파일.

값을 업데이트합니다 `ssl_keyfile` , `ssl_certfile` , 그리고 `ssl_ca_certs` :

```
ssl_keyfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

ssl_certfile:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

ssl_ca_certs:
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- 그만큼 `ssl_keyfile` 값은 키 경로입니다 `ontap_mediator_server.crt` 파일입니다 `ontap_mediator_server.key` .
- 그만큼 `ssl_certfile` 값은 경로입니다 `ontap_mediator_server_chain.crt` 파일.
- 그만큼 `ssl_ca_certs` 값은 경로입니다 `root_ca.crt` 파일.

> SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서. 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 및 1.9

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `intermediate.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `intermediate.crt` 개인 키를 해당 위치에 저장하면 `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

> 인증서에 서명하는 데 사용한 경우 `intermediate.crt` `ontap_mediator_server.crt` `intermediate.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 인증서 구조를 사용하는 경우 `root_ca.crt` 인증서는 다음을 제공합니다. `intermediate.crt` 서명하는 인증서 `ontap_mediator_server.crt` 인증서, 인증서 체인을 만듭니다. `intermediate.crt` 그리고 `ontap_mediator_server.crt` 인증서:

> ⓘ 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `intermediate.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 mediator_cert mediator_key `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
- `mediator_key`값은 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
- `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`

> SnapMirror Business Continuity(SM-BC) 클러스터의 경우 다음을 추가해야 합니다. `intermediate.crt` 그리고 `root_ca.crt` ONTAP 클러스터에 대한 인증서. 보다"SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성" .

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

ONTAP 중재자 **1.8** 이하

이 아닌 다른 이름을 가진 타사 인증서를 사용하거나 타사 인증서를 다른 위치에 저장할 수 `ca.*` 있습니다.

단계

1. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`파일의 기본 변수 값을 재정의하도록 파일을 `ontap_mediator.config.yaml` 구성합니다.

   PKI 권한으로부터 얻은 `ca.crt` 개인 키를 해당 위치에 저장하면 `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 파일은 다음 예제와 같이 표시됩니다.

> 인증서에 서명하는 데 사용한 경우 `ca.crt` `ontap_mediator_server.crt` `ca.srl` 파일이 생성됩니다. 자세한 내용은 을 2단계: 타사 CA 인증서로 서명하여 서버 인증서를 생성합니다 참조하십시오.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. 인증서가 인증서를 서명하는 인증서를 제공하는 인증서 구조를 사용하는 경우 `root_ca.crt` `ca.crt` `ontap_mediator_server.crt` 및 인증서에서 인증서 체인을 만듭니다 `ca.crt` `ontap_mediator_server.crt` .

> ⓘ 절차의 앞부분에 있는 PKI 기관으로부터 및 인증서를 받아야 `ca.crt` `ontap_mediator_server.crt` 합니다.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`파일을 업데이트합니다.

, 및 의 값을 `mediator_cert` `mediator_key` `ca_certificate`업데이트합니다.

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
```

```
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`값은 파일의 경로입니다. `ontap_mediator_server_chain.crt`
- `mediator_key`값은 파일의 키 경로입니다. `ontap_mediator_server.crt` `ontap_mediator_server.key`
- `ca_certificate`값은 파일의 경로입니다. `root_ca.crt`

> SM-BC(SnapMirror Business Continuity) 클러스터의 경우 및 인증서를 ONTAP 클러스터에 추가해야 `ca.crt` `root_ca.crt` 합니다. 을 "SnapMirror Active Sync를 위한 ONTAP Mediator 및 클러스터 구성"참조하십시오.

c. 새로 생성된 인증서의 다음 특성이 올바르게 설정되었는지 확인합니다.

- Linux 그룹 소유자: `netapp:netapp`
- Linux 권한: `600`

2. 구성 파일에서 인증서가 업데이트되면 ONTAP Mediator를 다시 시작합니다.

```
systemctl restart ontap_mediator
```

인증서 관련 문제 해결

인증서의 특정 속성을 확인할 수 있습니다.

인증서 만료 여부를 확인합니다

다음 명령을 사용하여 인증서 유효 범위를 식별합니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

CA 인증에서 **X509v3** 확장을 확인합니다

다음 명령을 사용하여 CA 인증에서 X509v3 확장을 확인합니다.

ONTAP 중재자 **1.9** 이상

에 `openssl_ca.cnf` 정의된 속성이 **v3_ca** 에서와 같이 `X509v3 extensions` `intermediate.crt` 표시됩니다.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP 중재자 **1.8** 이하

에 `openssl_ca.cnf` 정의된 속성이 **v3_ca** 에서와 같이 `X509v3 extensions` `ca.crt` 표시됩니다.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

서버 인증서 및 주체 대체 이름에서 **X509v3** 확장을 확인합니다

를 클릭합니다 `v3_req` 에 정의된 속성 `openssl_server.cnf` 구성 파일은 로 표시됩니다 `X509v3 extensions` 인증서에 입력합니다.

다음 예에서는 변수를 얻을 수 있습니다. `alt_names` 명령을 실행하여 섹션을 만듭니다. `hostname -A` 그리고 `hostname -I` ONTAP Mediator가 설치된 Linux VM에서.

변수의 올바른 값은 네트워크 관리자에게 문의하십시오.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

개인 키가 인증서와 일치하는지 확인합니다

특정 개인 키가 인증서와 일치하는지 확인할 수 있습니다.

키와 인증서에 각각 다음 OpenSSL 명령을 사용합니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

를 누릅니다 `-modulus` 특성 일치 모두에 대해 개인 키와 인증서 쌍이 호환되며 서로 작동할 수 있음을 나타냅니다.

서버 인증서가 특정 **CA** 인증서에서 생성되었는지 확인합니다

다음 명령을 사용하여 서버 인증서가 특정 CA 인증서에서 생성되었는지 확인할 수 있습니다.

ONTAP 중재자 **1.9** 이상

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP 중재자 **1.8** 이하

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

OCSP(Online Certificate Status Protocol) 유효성 검사가 사용 중인 경우 명령을 "OpenSSL - 확인"사용합니다.

ONTAP 중재자를 위한 호스트 OS를 유지 관리합니다

최적의 성능을 얻으려면 ONTAP Mediator의 호스트 OS를 정기적으로 유지 관리하세요.

호스트를 재부팅합니다

클러스터가 정상일 때만 호스트를 재부팅하세요. ONTAP Mediator가 오프라인인 동안에는 클러스터가 장애에 대응할 수 없습니다. 재부팅하기 전에 유지관리 시간을 설정하세요.

ONTAP Mediator는 재부팅 중에 자동으로 다시 시작되고 ONTAP 클러스터와 이전에 구성된 관계를 다시 입력합니다.

호스트 패키지 업데이트

커널을 제외한 모든 라이브러리나 yum 패키지를 업데이트합니다. 변경 사항을 적용하려면 필요한 경우 호스트를 재부팅하세요. 호스트를 재부팅하기 전에 서비스 창을 예약하세요.

를 설치하는 경우 `yum-utils` 패키지를 사용하려면 를 사용합니다 `needs-restarting` 명령을 사용하여 패키지 변경 사항을 탐지하려면 재부팅해야 합니다.

변경 사항이 즉시 적용되지 않으므로 ONTAP Mediator 종속성을 업데이트한 후 재부팅하세요.

호스트 **OS** 커널 업그레이드

SCST는 사용 중인 커널에 맞게 컴파일해야 합니다. OS를 업데이트하려면 유지관리 시간을 예약해야 합니다.

단계

호스트 OS 커널을 업그레이드하려면 다음 단계를 따르세요.

> ⓘ 커널을 업그레이드하기 전에 OS와 ONTAP Mediator 버전이 호환되는지 확인하세요. 지원되는 버전은 다음을 참조하세요."OS 지원 매트릭스" .

1. ONTAP 중재자를 중단하세요.
2. SCST 패키지를 제거하려면 다음을 참조하세요.호스트 유지관리 수행 . (SCST는 업그레이드 메커니즘을 제공하지 않습니다.)
3. OS를 업그레이드하고 재부팅합니다.
4. SCST 패키지를 다시 설치합니다.
5. ONTAP Mediator를 다시 활성화합니다.

호스트 유지관리 수행

VM 커널을 업그레이드하면 SCST 모듈과의 호환성 문제가 발생할 수 있습니다. SCST를 수동으로 제거했다가 다시 설치합니다.

1단계: SCST 제거

SCST를 제거하려면 ONTAP Mediator 버전용 tar 번들을 사용하세요.

단계

1. 다음 표에 표시된 대로 적절한 SCST 번들을 다운로드하고 압축을 풉니다.

이 버전의 경우…	이 tar 번들을 사용합니다…
ONTAP 중재자 1.11	scst-3.9.tar.gz
ONTAP 중재자 1.10	scst-3.9.tar.gz
ONTAP 중재자 1.9.1	scst-3.8.0.tar.bz2
ONTAP 중재자 1.9	scst-3.8.0.tar.bz2
ONTAP 중재자 1.8	scst-3.8.0.tar.bz2
ONTAP 중재자 1.7	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.6	scst - 3.7.0.tar.bz2
ONTAP 중재자 1.5	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.4	scst - 3.6.0.tar.bz2
ONTAP 중재자 1.3	scst - 3.5.0.tar.bz2
ONTAP 중재자 1.1	scst - 3.4.0.tar.bz2
ONTAP 중재자 1.0	scst - 3.3.0.tar.bz2

   a. 오픈 소스 패키지에 액세스하세요"SCST 소스포지 다운로드" .
   b. *출시된 버전 다운로드*를 선택하세요.
   c. 번들을 VM으로 추출합니다.
2. 다음 제거 명령을 실행하세요. `scst` 예배 규칙서:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

2단계**: SCST** 설치

SCST를 수동으로 설치하려면 ONTAP Mediator의 설치된 버전에 사용되는 SCST tar 번들이 필요합니다(참조).SCST 테이블).

ONTAP Mediator를 설치하기 전에 이 단계를 수행하세요. 사용 중인 SCST 버전이 ONTAP Mediator 설치 프로그램과 함께 제공되는 버전보다 최신인 경우 설치 프로그램은 이 단계를 건너뜁니다.

1. 다음 설치 명령을 실행하세요. `scst` 예배 규칙서:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      처음으로 설치를 수행하고 ONTAP Mediator를 미리 설치하려면 다음 단계로 넘어가기 전에 다음 명령을 실행하세요.

      ```
      mkdir -p
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
      ```

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      처음 설치할 때 ONTAP Mediator보다 SCST를 먼저 설치한 경우 이 단계를 건너뜁니다. 설치 프로그램은 관련 SCST 패치를 적용합니다.

2. 선택적으로 Secure Boot가 활성화되어 있는 경우 재부팅하기 전에 다음 단계를 수행하십시오.
   a. 각 파일 이름을 결정하세요 `scst_vdisk` , `scst` , 그리고 `iscsi_scst` 모듈:

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. 커널 릴리스를 확인합니다.

      ```
      [root@localhost ~]# uname -r
      ```

   c. 각 모듈 파일에 커널을 서명합니다.

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. 펌웨어와 함께 UEFI 키를 설치합니다.

UEFI 키 설치 지침은 다음 웹 사이트에서 확인할 수 있습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

생성된 UEFI 키는 다음 위치에 있습니다.

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. 시스템을 재부팅하세요:

```
reboot
```

호스트가 호스트 이름 또는 **IP**로 변경됩니다

이 작업에 대해

- ONTAP Mediator를 설치한 Linux 호스트에서 이 작업을 수행합니다.
- ONTAP Mediator를 설치한 후 호스트 이름이나 IP 주소가 변경되어 자체 서명 인증서가 더 이상 유효하지 않은 경우에만 이 작업을 수행하세요.
- 임시 자체 서명 인증서가 신뢰할 수 있는 타사 인증서로 대체된 후에는 이 작업을 사용하여 인증서를 다시 생성할 수 없습니다. 자체 서명된 인증서가 없으면 이 절차를 사용할 수 없습니다.

단계

현재 호스트에 대한 임시 자체 서명 인증서를 만듭니다.

1. ONTAP Mediator를 다시 시작하세요:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

ONTAP System Manager를 사용한 MetroCluster IP 사이트 관리에 대해 알아보세요

MetroCluster 구성은 별도의 위치에 있는 두 ONTAP 클러스터 간에 데이터와 구성을 동기식으로 미러링합니다. ONTAP 9.8부터 System Manager를 사용하여 MetroCluster IP 구성을 간편하게 관리할 수 있습니다.

MetroCluster IP 구성에서 System Manager를 통해서만 MetroCluster 작업을 수행할 수 있습니다. MetroCluster FC 구성에서는 System Manager를 사용하여 MetroCluster 구성의 각 노드를 관리할 수 있지만 MetroCluster 관련 작업은 수행할 수 없습니다.

일반적으로, 별도의 두 지리적 사이트에서 MetroCluster 구성으로 클러스터를 설정하고 구성합니다. 그런 다음 클러스터 간에 피어링을 설정하여 데이터가 동기화되고 공유되도록 합니다. 피어링된 네트워크에 있는 두 클러스터는 양방향 DR(재해 복구)을 제공하며, 각 클러스터가 다른 클러스터의 소스와 백업될 수 있습니다. 8노드 또는 4노드 MetroCluster IP 구성에서 각 사이트는 하나 또는 두 개의 고가용성(HA) 쌍으로 구성된 스토리지 컨트롤러로

구성됩니다.

세 번째 위치에서 노드와 해당 DR 파트너의 상태를 모니터링할 수 "ONTAP Mediator 설치"있습니다. ONTAP Mediator는 재해 발생 시 Mediator 지원 비계획 전환(MAUSO)을 구현할 수 있습니다.

협상된 스위치오버를 수행하여 계획된 유지 관리를 위해 클러스터 중 하나를 가져올 수도 있습니다. 파트너 클러스터는 유지보수 작업을 수행한 클러스터를 불러와서 스위치백 작업을 수행할 때까지 두 클러스터에 대한 모든 데이터 I/O 작업을 처리합니다.

에서 System Manager를 사용하여 MetroCluster IP 구성을 설정 및 관리하는 절차를 찾을 수 "MetroCluster 설명서 "있습니다.

테이프 백업을 사용한 데이터 보호

ONTAP FlexVol 볼륨의 테이프 백업에 대해 알아보세요

ONTAP는 NDMP(네트워크 데이터 관리 프로토콜)를 통해 테이프 백업 및 복원을 지원합니다. NDMP를 사용하면 스토리지 시스템의 데이터를 테이프에 직접 백업할 수 있으므로 네트워크 대역폭을 효율적으로 사용할 수 있습니다. ONTAP는 테이프 백업을 위해 덤프 및 SMTape 엔진을 모두 지원합니다.

NDMP 호환 백업 애플리케이션을 사용하여 덤프 또는 SMTape 백업 또는 복구를 수행할 수 있습니다. NDMP 버전 4만 지원됩니다.

덤프를 사용한 테이프 백업

덤프는 파일 시스템 데이터가 테이프에 백업되는 스냅샷 기반 백업입니다. ONTAP 덤프 엔진은 파일, 디렉토리 및 해당 ACL(액세스 제어 목록) 정보를 테이프에 백업합니다. 전체 볼륨, 전체 qtree 또는 전체 볼륨 또는 전체 qtree가 아닌 하위 트리를 백업할 수 있습니다. 덤프는 기본, 차등 및 증분 백업을 지원합니다.

SMTape를 사용한 테이프 백업

SMTape는 데이터 블록을 테이프에 백업하는 ONTAP의 스냅샷 기반 재해 복구 솔루션입니다. SMTape를 사용하여 테이프에 볼륨 백업을 수행할 수 있습니다. 그러나 qtree 또는 하위 트리 레벨에서 백업을 수행할 수 없습니다. SMTape는 기본 백업, 차등 백업 및 증분 백업을 지원합니다.

ONTAP 9.13.1부터 SMTape를 사용한 테이프 백업이 와 함께 SnapMirror 활성 동기화지원됩니다.

ONTAP 테이프 백업 및 복원 워크플로

NDMP 지원 백업 애플리케이션을 사용하여 테이프 백업 및 복구 작업을 수행할 수 있습니다.

이 작업에 대해

테이프 백업 및 복원 워크플로우는 테이프 백업 및 복원 작업 수행과 관련된 작업에 대한 개요를 제공합니다. 백업 및 복원 작업 수행에 대한 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

단계

1. NDMP 지원 테이프 토폴로지를 선택하여 테이프 라이브러리 구성을 설정합니다.
2. 스토리지 시스템에서 NDMP 서비스를 설정합니다.

NDMP 서비스는 노드 레벨 또는 SVM(스토리지 가상 시스템) 레벨에서 설정할 수 있습니다. 테이프 백업 및 복구 작업을 수행하도록 선택한 NDMP 모드에 따라 다릅니다.

3. NDMP 옵션을 사용하여 스토리지 시스템의 NDMP를 관리합니다.

   노드 레벨 또는 SVM 레벨에서 NDMP 옵션을 사용할 수 있습니다. 테이프 백업 및 복구 작업을 수행하도록 선택한 NDMP 모드에 따라 다릅니다.

   명령을 사용하여 노드 레벨에서 및 SVM 레벨에서 명령을 `vserver services ndmp modify` 사용하여 NDMP 옵션을 수정할 수 `system services ndmp modify` 있습니다. 및 `vserver services ndmp modify` 에 대한 자세한 `system services ndmp modify` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

4. NDMP 지원 백업 애플리케이션을 사용하여 테이프 백업 또는 복구 작업을 수행합니다.

   ONTAP는 테이프 백업 및 복구를 위해 덤프 엔진과 SMTape 엔진을 모두 지원합니다.

   백업 애플리케이션(_Data Management Applications_or_DMA_라고도 함)을 사용하여 백업 또는 복구 작업을 수행하는 방법에 대한 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

관련 정보

일반적인 NDMP 테이프 백업 토폴로지

FlexVol 볼륨에 대한 덤프 엔진 이해

ONTAP SMTape 및 덤프 백업 엔진의 사용 사례

ONTAP는 SMTape와 dump의 두 가지 백업 엔진을 지원합니다. 테이프 백업 및 복원 작업을 수행할 백업 엔진을 선택하는 데 도움이 되는 SMTape 및 덤프 백업 엔진의 사용 사례를 알고 있어야 합니다.

덤프는 다음과 같은 경우에 사용할 수 있습니다.

- 파일 및 디렉토리의 DAR(Direct Access Recovery
- 특정 경로에 있는 하위 디렉터리 또는 파일의 하위 집합 백업
- 백업 중에 특정 파일 및 디렉토리를 제외합니다
- 장기간 백업 보존

SMTape는 다음과 같은 경우에 사용할 수 있습니다.

- 재해 복구 솔루션
- 복원 작업 중에 백업된 데이터의 중복 제거 절약 및 중복 제거 설정을 유지합니다
- 대용량 볼륨 백업

테이프 드라이브 관리

ONTAP 테이프 드라이브 관리에 대해 알아보세요

테이프 백업 또는 복구 작업을 수행하기 전에 테이프 라이브러리 연결을 확인하고 테이프 드라이브 정보를 볼 수 있습니다. 자격 없는 테이프 드라이브를 자격 있는 테이프 드라이브에 에뮬레이트하여 사용할 수 있습니다. 기존 별칭을 보는 것 외에도 테이프 별칭을 할당 및 제거할 수도 있습니다.

데이터를 테이프에 백업할 때 데이터는 테이프 파일에 저장됩니다. 파일 표시는 테이프 파일을 구분하며 파일에 이름이 없습니다. 테이프 파일의 위치를 사용하여 테이프 파일을 지정합니다. 테이프 디바이스를 사용하여 테이프 파일을 씁니다. 테이프 파일을 읽을 때 해당 테이프 파일을 쓰는 데 사용한 압축 유형이 동일한 디바이스를 지정해야 합니다.

테이프 드라이브, 미디어 체인저 및 테이프 드라이브 작업을 관리하기 위한 **ONTAP** 명령

클러스터의 테이프 드라이브 및 미디어 체인저에 대한 정보를 보고, 테이프 드라이브를 온라인 상태로 전환하고, 오프라인 상태로 만들고, 테이프 드라이브 카트리지 위치를 수정하고, 테이프 드라이브 별칭 이름을 설정 및 지우고, 테이프 드라이브를 재설정하는 데 사용되는 명령이 있습니다. 또한 테이프 드라이브 통계를 보거나 재설정할 수 있습니다.

원하는 작업	이 명령 사용...
테이프 드라이브를 온라인 상태로 전환합니다	'테이프 온라인 보관'
테이프 드라이브 또는 미디어 체인저의 별칭 이름을 지웁니다	'테이프 별칭 지우기'
테이프 드라이브에 대한 테이프 추적 작업을 활성화하거나 비활성화합니다	"테이프 추적 보관"
테이프 드라이브 카트리지 위치를 수정합니다	'테이프 보관 위치'
테이프 드라이브를 재설정합니다	'테이프 재설정'을 선택합니다 이 명령은 고급 권한 수준에서만 사용할 수 있습니다.
테이프 드라이브 또는 미디어 체인저의 별칭 이름을 설정합니다	'스토리지 테이프 별칭 세트'
테이프 드라이브를 오프라인 상태로 전환합니다	'테이프 오프라인 보관'
모든 테이프 드라이브 및 미디어 체인저에 대한 정보를 봅니다	'스토리지 테이프 쇼'
클러스터에 연결된 테이프 드라이브에 대한 정보를 봅니다	• '테이프 쇼테이프 드라이브 보관' • '시스템 노드 하드웨어 테이프 드라이브 표시

원하는 작업	이 명령 사용...
클러스터에 연결된 미디어 체인저에 대한 정보를 봅니다	'스토리지 테이프 쇼 미디어 체인저'
클러스터에 연결된 테이프 드라이브에 대한 오류 정보를 봅니다	'테이프 저장 표시 오류'입니다
클러스터의 각 노드에 연결된 모든 ONTAP 인증 및 지원 테이프 드라이브를 봅니다	'Storage tape show-supported-status'를 선택합니다
클러스터의 각 노드에 연결된 모든 테이프 드라이브 및 미디어 체인저의 별칭을 봅니다	'Storage tape alias show'
테이프 드라이브의 통계 판독값을 0으로 재설정합니다	'Storage stats tape zero' tape_name 이 명령은 노드 쉘에서 사용해야 합니다.
ONTAP에서 지원하는 테이프 드라이브를 봅니다	"torage show tape supported[-v]" 이 명령은 노드 쉘에서 사용해야 합니다. 각 테이프 드라이브에 대한 자세한 내용을 보려면 '-v' 옵션을 사용할 수 있습니다.
테이프 디바이스 통계를 보고 테이프 성능을 이해하고 사용 패턴을 확인합니다	'STORAGE STATS TAPE'TAPE_NAME'입니다 이 명령은 노드 쉘에서 사용해야 합니다.

관련 정보

- "저장 테이프"
- "저장 테이프 쇼"
- "저장 테이프 show-supported-status"
- "저장 테이프 쇼-테이프-드라이브"
- "저장 테이프 별칭 지우기"
- "저장 테이프 별칭 세트"
- "저장 테이프 별칭 표시"
- "저장 테이프 추적"

ONTAP 테이프 백업에 비적격 테이프 드라이브 사용

검증된 테이프 드라이브를 에뮬레이트할 수 있는 경우 스토리지 시스템에서 검증되지 않은 테이프 드라이브를 사용할 수 있습니다. 그런 다음 자격 있는 테이프 드라이브처럼 취급됩니다. 검증되지 않은 테이프 드라이브를 사용하려면 먼저 정규화된 테이프 드라이브를 에뮬레이트하는지 여부를 확인해야 합니다.

이 작업에 대해

검증되지 않은 테이프 드라이브는 스토리지 시스템에 연결되어 있지만 ONTAP에서 지원되거나 인식되지 않는 드라이브입니다.

단계

1. Storage tape show-supported-status 명령을 사용하여 스토리지 시스템에 연결된 검증되지 않은 테이프 드라이브를 확인합니다.

   다음 명령을 실행하면 스토리지 시스템에 연결된 테이프 드라이브와 각 테이프 드라이브의 지원 및 검증 상태가 표시됩니다. 검증되지 않은 테이프 드라이브도 나열됩니다. "tape_drive_vendor_name"은(는) 스토리지 시스템에 연결된 검증되지 않은 테이프 드라이브이지만 ONTAP에서 지원하지 않습니다.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. 검증된 테이프 드라이브를 에뮬레이트합니다.

   "NetApp 다운로드: 테이프 장치 구성 파일"

관련 정보

- 검증된 테이프 드라이브가 무엇입니까
- "저장 테이프 show-supported-status"

ONTAP 테이프 백업을 위해 테이프 드라이브 또는 미디어 체인저에 테이프 별칭을 할당합니다**.**

장치를 쉽게 식별할 수 있도록 테이프 드라이브 또는 미디어 체인저에 테이프 별칭을 할당할 수 있습니다. 별칭은 백업 디바이스의 논리적 이름과 테이프 드라이브 또는 미디어 체인저에 영구적으로 할당된 이름 간의 통신을 제공합니다.

단계

1. 'Storage tape alias set' 명령을 사용하여 테이프 드라이브 또는 미디어 체인저에 별칭을 할당합니다.

   에 대한 자세한 내용은 `storage tape alias set` "ONTAP 명령 참조입니다"을 참조하십시오.

'system node hardware tape drive show' 명령을 사용하여 테이프 드라이브에 대한 SN(일련 번호) 정보와 'system node hardware tape library show' 명령을 사용하여 테이프 라이브러리에 대한 정보를 볼 수 있습니다.

다음 명령은 일련 번호 SN[123456] L4가 노드 cluster1-01에 연결된 테이프 드라이브로 별칭 이름을 설정합니다.

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

다음 명령은 일련 번호 SN[65432]이 노드 cluster1-01에 연결된 미디어 체인저로 별칭 이름을 설정합니다.

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

관련 정보

- 테이프 앨리어싱이란 무엇입니까
- 테이프 별칭을 제거하는 중입니다
- "저장 테이프 별칭 세트"

ONTAP 테이프 백업을 위해 테이프 드라이브 또는 미디어 체인저에 대한 테이프 별칭 제거

테이프 드라이브 또는 미디어 체인저에 영구 별칭이 더 이상 필요하지 않은 경우 'Storage tape alias clear' 명령을 사용하여 별칭을 제거할 수 있습니다.

단계

1. 'Storage tape alias clear' 명령어를 사용해 테이프 드라이브 또는 미디어 체인저에서 별칭을 삭제한다.

   에 대한 자세한 내용은 `storage tape alias clear` "ONTAP 명령 참조입니다"을 참조하십시오.

   다음 명령을 실행하면 별칭 지우기 작업의 범위를 "테이프"로 지정하여 모든 테이프 드라이브의 별칭이 제거됩니다.

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

작업을 마친 후

NDMP를 사용하여 테이프 백업 또는 복구 작업을 수행하는 경우 테이프 드라이브 또는 미디어 체인저에서 별칭을 제거한 후 테이프 디바이스에 계속 액세스하려면 테이프 드라이브 또는 미디어 체인저에 새 별칭 이름을 할당해야 합니다.

관련 정보

- 테이프 앨리어싱이란 무엇입니까
- 테이프 별칭 할당
- "저장 테이프 별칭 지우기"

ONTAP 테이프 예약 활성화 또는 비활성화

Tape.예약 옵션을 사용하여 ONTAP에서 테이프 디바이스 예약을 관리하는 방법을 제어할 수 있습니다. 기본적으로 테이프 예약이 해제되어 있습니다.

이 작업에 대해

테이프 예약 옵션을 활성화하면 테이프 드라이브, 미디어 체인저, 브리지 또는 라이브러리가 제대로 작동하지 않을 경우 문제가 발생할 수 있습니다. 테이프 명령이 디바이스를 사용하는 다른 스토리지 시스템이 없을 때 디바이스가 예약된다는 것을 보고하는 경우 이 옵션을 해제해야 합니다.

단계

1. SCSI 예약/해제 메커니즘 또는 SCSI 영구 보존 명령을 사용하여 테이프 예약을 비활성화하려면 다음 명령을 클러스터 쉘에 입력합니다.

   "* 옵션 -옵션 -이름 테이프.예약 -옵션 -값{scsi|persistent|off} *"

   SCSI Reserve/Release mechanism을 선택한다.

   '영구'는 SCSI 영구 예약을 선택합니다.

   OFF는 테이프 예약을 비활성화합니다.

관련 정보

테이프 예약이란

테이프 라이브러리 연결을 확인하기 위한 ONTAP 명령

스토리지 시스템과 스토리지 시스템에 연결된 테이프 라이브러리 구성 사이의 접속 경로에 대한 정보를 볼 수 있습니다. 이 정보를 사용하여 테이프 라이브러리 구성에 대한 연결 경로를 확인하거나 연결 경로와 관련된 문제를 해결할 수 있습니다.

새 테이프 라이브러리를 추가하거나 생성한 후 또는 테이프 라이브러리에 대한 단일 경로 또는 다중 경로 액세스에서 장애가 발생한 경로를 복원한 후 테이프 라이브러리 연결을 확인하기 위해 다음 테이프 라이브러리 세부 정보를 볼 수 있습니다. 또한 경로 관련 오류를 해결하거나 테이프 라이브러리에 대한 액세스가 실패하는 경우에도 이 정보를 사용할 수 있습니다.

- 테이프 라이브러리가 연결된 노드입니다
- 장치 ID입니다
- NDMP 경로
- 테이프 라이브러리 이름입니다
- 타겟 포트 및 이니시에이터 포트 ID
- 모든 타겟 또는 FC 이니시에이터 포트를 위한 테이프 라이브러리에 단일 경로 또는 다중 경로 액세스
- ""경로 오류"" 및 ""경로 Qual""와 같은 경로 관련 데이터 무결성 세부 정보
- LUN 그룹 및 LUN 수

원하는 작업	이 명령 사용...
클러스터의 테이프 라이브러리에 대한 정보를 봅니다	'system node hardware tape library show'
테이프 라이브러리의 경로 정보를 봅니다	'storage tape library path show'
모든 이니시에이터 포트에 대한 테이프 라이브러리의 경로 정보를 봅니다	'storage tape library path show-by-initiator'를 선택합니다
스토리지 테이프 라이브러리와 클러스터 간의 접속 정보를 봅니다	'storage tape library config show'를 선택합니다

관련 정보

- "스토리지 테이프 라이브러리 구성 표시"
- "시스템 노드 하드웨어 테이프 라이브러리 표시"
- "스토리지 테이프 라이브러리 경로 표시"
- "스토리지 테이프 라이브러리 경로 표시-이니시에이터별"

테이프 드라이브 정보

적격 **ONTAP** 테이프 드라이브에 대해 알아보세요

스토리지 시스템에서 제대로 작동하는 것으로 테스트 및 확인된 인증된 테이프 드라이브를 사용해야 합니다. 테이프 에일리어싱을 따르고 테이프 예약을 활성화하여 특정 시간에 한 스토리지 시스템만 테이프 드라이브에 액세스할 수 있습니다.

검증된 테이프 드라이브는 테스트를 거쳐 스토리지 시스템에서 올바르게 작동하는 것으로 확인된 테이프 드라이브입니다. 테이프 구성 파일을 사용하여 기존 ONTAP 릴리스에 대해 테이프 드라이브를 검증할 수 있습니다.

ONTAP 테이프 구성 파일의 형식

테이프 구성 파일 형식은 공급업체 ID, 제품 ID 등의 필드와 테이프 드라이브의 압축 유형에 대한 세부 정보로 구성됩니다. 또한 이 파일은 테이프 드라이브의 자동 로드 기능을 활성화하고 테이프 드라이브의 명령 시간 초과 값을 변경하기 위한 선택적 필드로 구성되어 있습니다.

다음 표에는 테이프 구성 파일의 형식이 나와 있습니다.

항목	크기	설명
(string) ndor_id	최대 8바이트	CSI Inquiry 명령으로 조회한 Vendor ID
'product_id'(문자열)	최대 16바이트	CSI Inquiry 명령으로 조회한 제품 ID

항목	크기	설명
"id_match_size"(숫자)		식별 대상 테이프 드라이브를 감지하기 위해 일치시키는 데 사용할 제품 ID의 바이트 수(Inquiry data에서 제품 ID의 첫 번째 문자로 시작).
거미줄(string)	최대 16바이트	이 매개 변수가 있으면 'storage tape show -device-names' 명령으로 출력되는 문자열로 지정되고, 그렇지 않으면 INQ_vendor_ID로 출력된다.
'PRODUCT_PRETY'(문자열)	최대 16바이트	이 파라미터가 있으면 'STORAGE TAPE SHOW-DEVICE-Names' 명령으로 출력되는 문자열로 지정되고, 그렇지 않으면 INQ_PRODUCT_ID가 출력된다.

신도 예쁘고 제품예쁘다 필드는 선택 사항이지만 값이 있으면 다른 필드에도 값이 있어야 합니다.

다음 표에서는 l, mh, h, a 등 다양한 압축 유형에 대한 설명, 밀도 코드 및 압축 알고리즘을 설명합니다.

항목	크기	설명
'{l	m	h
a}_description = (string)'	최대 24바이트	특정 밀도 설정의 특성을 설명하는 notes지옥의 명령어 sysconfig -t를 위해 인쇄할 문자열입니다.
`{l	m	h
a}_density=(16진수 코드)'		l, m, h 또는 a에 대해 원하는 밀도 코드에 해당하는 SCSI 모드 페이지 블록 설명자에서 설정할 밀도 코드입니다
`{l	m	h
a}_algorithm=(16진수 코드)'		밀도 코드와 원하는 밀도 특성에 해당하는 SCSI 압축 모드 페이지에서 설정할 압축 알고리즘입니다.

다음 표에는 테이프 구성 파일에서 사용할 수 있는 옵션 필드가 설명되어 있습니다.

필드에 입력합니다	설명
'자동 로드 = (부울 예/아니요)	테이프 드라이브에 자동 로드 기능이 있는 경우 이 필드는 '예'로 설정됩니다. 즉, 테이프 카트리지를 삽입한 후 'scsi load(start/stop unit)' 명령을 실행하지 않아도 테이프 드라이브가 준비됩니다. 이 필드의 기본값은 no입니다.
'cmd_timeout_0x'입니다	개별 제한 시간 값입니다. 테이프 드라이버에서 기본값으로 사용 중인 값과 다른 시간 제한 값을 지정하려면 이 필드만 사용해야 합니다. 샘플 파일에는 테이프 드라이브에서 사용되는 기본 SCSI 명령 시간 초과 값이 나열되어 있습니다. 시간 초과 값은 분(m), 초(s) 또는 밀리초(ms) 단위로 나타낼 수 있습니다. 이 필드는 변경할 수 없습니다.

NetApp Support 사이트에서 테이프 구성 파일을 다운로드하고 볼 수 있습니다.

테이프 구성 파일 형식의 예

HP LTO5 Ultrium 테이프 드라이브의 테이프 구성 파일 형식은 다음과 같습니다.

전성자(ndor_id) = "HP"

'PRODUCT_id'="Ultrium 5-SCSI"

id_match_size=9

거미장군=HP 휴렛팩커드

"PRODUCT_PRETY" = "LTO-5"

"l_description" = "LTO-3(ro)/4/800GB"

'l_density' = 0x00

'l_algorithm' = 0x00

Ms_description"="LTO-3(ro)/4 8/1600GB CMP"

mdensity' = 0x00

m_algorithm'=0x01

"h_description" = "LTO-5 1600GB"

"h_density" = 0x58

'h_algorithm' = 0x00

"A_DESCRIPTION"="LTO-5 3200GB CMP"

'A_Density' = 0x58

"A_알고리즘" = 0x01

"자동 로드" = "예"

관련 정보

- "NetApp 툴: 테이프 장치 구성 파일"
- "저장 테이프 쇼"

ONTAP 스토리지 시스템이 테이프 드라이브를 동적으로 적격화하는 방법

스토리지 시스템은 공급업체 ID 및 제품 ID를 테이프 검증 표에 포함된 정보와 일치시켜 테이프 드라이브를 동적으로 자격을 평가합니다.

테이프 드라이브를 스토리지 시스템에 연결할 때 테이프 검색 중에 얻은 정보와 내부 테이프 검증 표의 정보 간에 공급업체 ID와 제품 ID가 일치하는지 확인합니다. 스토리지 시스템이 일치 항목을 검색하면 테이프 드라이브가 검증된 것으로 표시되고 테이프 드라이브에 액세스할 수 있습니다. 스토리지 시스템에서 일치하는 항목을 찾을 수 없는 경우 테이프 드라이브는 비정규화된 상태로 유지되며 액세스할 수 없습니다.

테이프 장치 개요

ONTAP 테이프 장치에 대해 알아보세요

테이프 디바이스는 테이프 드라이브를 나타냅니다. 테이프 드라이브의 되감기 유형과 압축 기능의 특정 조합입니다.

테이프 디바이스는 되감기 유형과 압축 기능의 각 조합에 대해 생성됩니다. 따라서 테이프 드라이브 또는 테이프 라이브러리에는 여러 개의 테이프 디바이스가 연결될 수 있습니다. 테이프를 이동, 쓰기 또는 읽을 테이프 디바이스를 지정해야 합니다.

스토리지 시스템에 테이프 드라이브 또는 테이프 라이브러리를 설치할 때 ONTAP는 테이프 드라이브 또는 테이프 라이브러리와 연결된 테이프 디바이스를 생성합니다.

ONTAP는 테이프 드라이브 및 테이프 라이브러리를 감지하고 논리적 번호 및 테이프 디바이스를 할당합니다. ONTAP는 파이버 채널, SAS 및 병렬 SCSI 테이프 드라이브와 라이브러리가 인터페이스 포트에 연결될 때 이를 감지합니다. ONTAP는 인터페이스가 활성화되어 있을 때 이러한 드라이브를 감지합니다.

ONTAP 테이프 장치 이름의 형식

각 테이프 디바이스에는 정의된 형식으로 표시되는 관련 이름이 있습니다. 형식은 장치 유형, 되감기 유형, 별칭 및 압축 유형에 대한 정보를 포함합니다.

테이프 디바이스 이름의 형식은 다음과 같습니다.

Rwind_type의 'st'alias_number'compression_type입니다

rewind_type은 되감기 유형입니다.

다음 목록에서는 다양한 되감기 유형 값을 설명합니다.

- * r *

ONTAP는 테이프 파일 쓰기를 완료한 후 테이프를 되감습니다.

- * nr *

  ONTAP는 테이프 파일 쓰기를 완료한 후 테이프를 되감지 않습니다. 동일한 테이프에 여러 개의 테이프 파일을 쓰려면 이 되감기 유형을 사용해야 합니다.

- * ur *

  이것은 언로드/다시 로드 되감기 유형입니다. 이 되감기 유형을 사용하면 테이프 라이브러리가 테이프 파일의 끝에 도달하면 테이프를 언로드한 다음 다음 다음 테이프가 있으면 로드합니다.

  다음과 같은 경우에만 이 되감기 유형을 사용해야 합니다.

  - 이 장치와 연결된 테이프 드라이브가 테이프 라이브러리에 있거나 라이브러리 모드에 있는 미디어 체인저에 있습니다.
  - 이 장치와 연결된 테이프 드라이브가 스토리지 시스템에 연결되어 있습니다.
  - 수행 중인 작업에 충분한 테이프를 이 테이프 드라이브에 대해 정의된 라이브러리 테이프 시퀀스에서 사용할 수 있습니다.

되감기 안 함 장치를 사용하여 테이프를 녹음하는 경우 테이프를 읽기 전에 테이프를 되감아야 합니다.

't'는 테이프 드라이브의 표준 지정입니다.

alias_number는 ONTAP가 테이프 드라이브에 할당하는 별칭입니다. ONTAP가 새 테이프 드라이브를 감지하면 ONTAP가 테이프 드라이브에 별칭을 할당합니다.

compression_type은 테이프의 데이터 밀도와 압축 유형을 나타내는 드라이브별 코드입니다.

다음 목록에는 압축 유형 의 다양한 값이 설명되어 있습니다.

- * A *

  최고의 압축

- * 시간 *

  높은 압축

- m *

  중간 압축

- * l * 를 선택합니다

  낮은 압축

예

nrst0a는 가장 높은 압축을 사용하여 테이프 드라이브 0에 되감기 안 함 장치를 지정합니다.

테이프 디바이스 목록의 예

다음 예는 HP Ultrium 2-SCSI와 연결된 테이프 장치를 보여줍니다.

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,         format is: HP (200GB)
nrst0l -  no rewind device,      format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,         format is: HP (200GB)
nrst0m -  no rewind device,      format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,         format is: HP (200GB)
nrst0h -  no rewind device,      format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,         format is: HP (400GB w/comp)
nrst0a -  no rewind device,      format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

다음 목록에서는 위의 예제에서 약어를 설명합니다.

- GB — 기가바이트. 테이프의 용량입니다.
- w/comp — 압축을 사용하면 테이프 용량이 압축 상태로 표시됩니다.

동시에 지원되는 **ONTAP** 테이프 장치 수

ONTAP는 Fibre Channel, SCSI 또는 SAS 접속 장치를 혼합하여 각 스토리지 시스템(노드당)에 대해 최대 64개의 동시 테이프 드라이브 접속, 16개의 미디어 체인저 및 16개의 브리지 또는 라우터 디바이스를 지원합니다.

테이프 드라이브 또는 미디어 체인저는 물리적 또는 가상 테이프 라이브러리 또는 독립 실행형 디바이스의 디바이스일 수 있습니다.

> 스토리지 시스템에서 64개의 테이프 드라이브 연결을 감지할 수 있지만 동시에 수행할 수 있는 최대 백업 및 복구 세션 수는 백업 엔진의 확장성 제한에 따라 달라집니다.

관련 정보

덤프 백업 및 복원 세션에 대한 확장성 제한

테이프 에일리어싱

테이프 앨리어싱 개요

에일리어싱은 장치 식별 과정을 간소화합니다. 앨리어싱은 테이프 또는 미디어 체인저의 물리적 경로 이름(PPN) 또는 일련 번호(SN)를 영구적이지만 수정할 수 있는 별칭 이름에 바인딩합니다.

다음 표에서는 테이프 드라이브(또는 테이프 라이브러리 또는 미디어 체인저)가 항상 단일 별칭 이름과 연결되도록 하는 테이프 앨리어싱을 사용하는 방법을 설명합니다.

시나리오	별칭을 다시 할당합니다
시스템이 재부팅될 때	테이프 드라이브는 이전 별칭을 자동으로 재할당합니다.
테이프 디바이스가 다른 포트로 이동할 때	새 주소를 가리키도록 별칭을 조정할 수 있습니다.
둘 이상의 시스템에서 특정 테이프 디바이스를 사용하는 경우	사용자는 모든 시스템에 대해 별칭을 동일하게 설정할 수 있습니다.

Data ONTAP 8.1.x에서 Data ONTAP 8.2.x로 업그레이드하면 Data ONTAP 8.2.x의 테이프 별칭 기능이 기존 테이프 별칭 이름을 수정합니다. 이러한 경우 백업 애플리케이션에서 테이프 별칭 이름을 업데이트해야 할 수 있습니다.

테이프 별칭을 할당하면 백업 디바이스의 논리적 이름(예: st0 또는 MC1)과 포트, 테이프 드라이브 또는 미디어 체인저에 영구적으로 할당되는 이름이 일치하게 됩니다.

st0과 st00은 서로 다른 논리적 이름입니다.

논리 이름 및 일련 번호는 장치에 액세스하는 경우에만 사용됩니다. 디바이스에 액세스한 후에는 물리적 경로 이름을 사용하여 모든 오류 메시지를 반환합니다.

앨리어싱에는 물리적 경로 이름과 일련 번호라는 두 가지 유형의 이름을 사용할 수 있습니다.

물리적 경로 이름에 대해 알아보세요

물리적 경로 이름(PPN)은 ONTAP가 스토리지 시스템에 접속된 SCSI-2/3 어댑터 또는 스위치(특정 위치)를 기반으로 테이프 드라이브 및 테이프 라이브러리에 할당하는 숫자 주소 시퀀스입니다. PPN은 전기 이름이라고도 합니다.

직접 연결된 장치의 PPN은 'host_adapter' 형식을 사용한다. device_id_lun

LUN 값이 0이 아닌 테이프 및 미디어 체인저 디바이스에 대해서만 LUN 값이 표시됩니다. 즉, LUN 값이 0이면 PPN의 'LUN' 부분이 표시되지 않습니다.

예를 들어, PPN 8.6은 호스트 어댑터 번호가 8이고, 장치 ID는 6이며, 논리 장치 번호(LUN)는 0임을 나타냅니다.

SAS 테이프 장치도 직접 연결 장치입니다. 예를 들어, PPN 5c.4는 스토리지 시스템에서 SAS HBA가 슬롯 5에 연결되어 있고 SAS 테이프가 SAS HBA의 포트 C에 연결되어 있고 장치 ID가 4임을 나타냅니다.

Fibre Channel 스위치 접속 디바이스의 PPN은 'switch:port_id' 형식을 사용합니다. device_id_lun

예를 들어, PPN my_switch:5.3L2는 my_switch라는 스위치의 포트 5에 연결된 테이프 드라이브가 장치 ID 3으로 설정되어 있고 LUN 2를 가지고 있음을 나타냅니다.

LUN(논리 유닛 번호)은 드라이브에 의해 결정됩니다. Fibre Channel, SCSI 테이프 드라이브 및 라이브러리 및 디스크에는 PPN이 있습니다.

테이프 드라이브 및 라이브러리의 PPN은 스위치의 이름이 변경되거나, 테이프 드라이브 또는 라이브러리가 이동하거나, 테이프 드라이브 또는 라이브러리를 다시 구성하지 않는 한 변경되지 않습니다. 재부팅 후 PPN은 변경되지 않습니다. 예를 들어 my_switch:5.3L2라는 테이프 드라이브가 제거되고 디바이스 ID와 LUN이 동일한 새 테이프

드라이브가 스위치 my_switch의 포트 5에 연결된 경우 my_switch:5.3L2를 사용하여 새 테이프 드라이브에 액세스할 수 있습니다.

일련 번호에 대해 알아보세요

일련 번호(SN)는 테이프 드라이브 또는 미디어 체인저의 고유 식별자입니다. ONTAP는 WWN 대신 SN을 기반으로 별칭을 생성합니다.

SN은 테이프 드라이브 또는 미디어 체인저의 고유 식별자이므로 테이프 드라이브 또는 미디어 체인저에 대한 여러 연결 경로에 관계없이 별칭은 동일하게 유지됩니다. 이를 통해 스토리지 시스템은 테이프 라이브러리 구성에서 동일한 테이프 드라이브 또는 미디어 체인저를 추적할 수 있습니다.

테이프 드라이브 또는 미디어 체인저가 연결된 Fibre Channel 스위치의 이름을 바꾸어도 테이프 드라이브 또는 미디어 체인저의 SN은 변경되지 않습니다. 그러나 테이프 라이브러리에서 기존 테이프 드라이브를 새 테이프 드라이브로 교체할 경우 ONTAP는 테이프 드라이브의 SN이 변경되므로 새 별칭을 생성합니다. 또한 기존 테이프 드라이브를 테이프 라이브러리의 새 슬롯으로 이동하거나 테이프 드라이브의 LUN을 다시 매핑할 경우 ONTAP는 해당 테이프 드라이브에 대한 새 별칭을 생성합니다.

백업 애플리케이션을 새로 생성된 별칭으로 업데이트해야 합니다.

테이프 장치의 SN은 S N[xxxxxxxxxx]L[X] 형식을 사용합니다

X는 영숫자 문자이고 L은 테이프 디바이스의 LUN입니다. LUN이 0이면 문자열 L의 X 부분이 표시되지 않습니다.

각 SN은 최대 32자로 구성되며, SN의 형식은 대/소문자를 구분하지 않습니다.

ONTAP 다중 경로 테이프 액세스 구성 시 고려 사항

테이프 라이브러리의 테이프 드라이브를 액세스할 수 있도록 스토리지 시스템에서 두 개의 경로를 구성할 수 있습니다. 한 경로에 장애가 발생할 경우 스토리지 시스템은 다른 경로를 사용하여 장애가 발생한 경로를 즉시 복구하지 않고도 테이프 드라이브를 액세스할 수 있습니다. 이렇게 하면 테이프 작업을 다시 시작할 수 있습니다.

스토리지 시스템에서 다중 경로 테이프 액세스를 구성할 때는 다음 사항을 고려해야 합니다.

- LUN 매핑을 지원하는 테이프 라이브러리에서 LUN 그룹에 대한 다중 경로 액세스를 위해 LUN 매핑은 각 경로에서 대칭적이어야 합니다.

  테이프 드라이브와 미디어 체인저는 테이프 라이브러리의 LUN 그룹(동일한 이니시에이터 경로 세트를 공유하는 LUN 세트)에 할당됩니다. LUN 그룹의 모든 테이프 드라이브를 여러 경로에 대한 백업 및 복원 작업에 사용할 수 있어야 합니다.

- 스토리지 시스템에서 테이프 라이브러리의 테이프 드라이브를 액세스하도록 최대 2개의 경로를 구성할 수 있습니다.
- 다중 경로 테이프 액세스는 로드 밸런싱을 지원합니다. 로드 밸런싱은 기본적으로 비활성화되어 있습니다.

다음 예제에서 스토리지 시스템은 두 개의 이니시에이터 경로 0b 및 0d를 통해 LUN 그룹 0에 액세스합니다. 두 경로 모두에서 LUN 그룹은 LUN 번호, 0 및 LUN 수, 5를 동일하게 갖습니다. 스토리지 시스템은 이니시에이터 경로 1개만을 통해 LUN 그룹 1을 3D로 액세스합니다.

```
STSW-3070-2_cluster::> storage tape library config show

Node                      LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
------------------------ ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0       5          IBM 3573-TL_1
510a09800000412d     0b

0d
                              1       2          IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

관련 정보

- "스토리지 테이프 라이브러리 구성 표시"

ONTAP 스토리지 시스템에 테이프 드라이브와 라이브러리를 추가하는 방법을 알아보세요.

스토리지 시스템을 오프라인으로 전환하지 않고도 테이프 드라이브와 라이브러리를 스토리지 시스템에 동적으로 추가할 수 있습니다.

새 미디어 체인저를 추가하면 스토리지 시스템이 미디어 체인저를 감지하여 구성에 추가합니다. 미디어 체인저가 별칭 정보에서 이미 참조되면 새 논리 이름이 생성되지 않습니다. 라이브러리가 참조되지 않으면 스토리지 시스템이 미디어 체인저에 대한 새 별칭을 생성합니다.

테이프 라이브러리 구성에서 ONTAP용 타겟 포트의 LUN 0에 테이프 드라이브 또는 미디어 체인저를 구성하여 해당 타겟 포트의 모든 미디어 체인저와 테이프 드라이브를 검색해야 합니다.

ONTAP 테이프 예약에 대해 알아보세요

여러 스토리지 시스템이 테이프 드라이브, 미디어 체인저, 브리지 또는 테이프 라이브러리에 대한 액세스를 공유할 수 있습니다. 테이프 예약은 SCSI 예약/해제 메커니즘 또는 모든 테이프 드라이브, 미디어 체인저, 브리지 및 테이프 라이브러리에 대한 SCSI 영구 예약을 활성화하여 특정 시간에 한 스토리지 시스템만 디바이스에 액세스할 수 있도록 합니다.

스위치가 포함되었는지 여부에 관계없이 라이브러리에서 디바이스를 공유하는 모든 시스템은 동일한 예약 방법을 사용해야 합니다.

디바이스 예약을 위한 SCSI 예약/해제 메커니즘은 정상 조건에서 잘 작동합니다. 그러나 인터페이스 오류 복구 절차 중에 예약을 유실할 수 있습니다. 이 경우 예약된 소유자 이외의 이니시에이터가 디바이스에 액세스할 수 있습니다.

SCSI 영구 예약으로 이루어진 예약은 루프 재설정 또는 대상 재설정과 같은 오류 복구 메커니즘의 영향을 받지 않지만 모든 장치에서 SCSI 영구 예약을 올바르게 구현하는 것은 아닙니다.

스토리지 시스템 간 데이터 전송

ndmpcopy를 사용하여 **ONTAP** 데이터 전송

ndmpcopy nodeswell 명령은 NDMP v4를 지원하는 스토리지 시스템 간에 데이터를 전송합니다. 전체 및 증분 데이터 전송을 모두 수행할 수 있습니다. 전체 또는 부분 볼륨, Qtree, 디렉토리 또는 개별 파일을 전송할 수 있습니다.

이 작업에 대해

ONTAP 8.x 및 이전 릴리즈를 사용하면 증분 전송은 최대 2개의 레벨(전체 백업 1개 및 최대 2개의 증분 백업)으로 제한됩니다.

ONTAP 9.0 이상 릴리즈부터 증분 전송은 최대 9개 레벨(전체 백업 1개 및 증분 백업 9개)으로 제한됩니다.

소스 및 대상 스토리지 시스템의 nodeswell 명령줄에서 ndmpcopy를 실행하거나 데이터 전송 소스 또는 대상이 아닌 스토리지 시스템을 실행할 수 있습니다. 또한 데이터 전송의 소스와 대상 모두에 대해 단일 스토리지 시스템에서 ndmpcopy를 실행할 수 있습니다.

ndmpcopy 명령에서 소스 및 대상 스토리지 시스템의 IPv4 또는 IPv6 주소를 사용할 수 있습니다. 경로 형식은 "/vserver_name/volume_name\[path\]"입니다.

단계

1. 소스 및 대상 스토리지 시스템에서 NDMP 서비스를 설정합니다.

의 소스 또는 대상에서 데이터 전송을 수행하는 경우…	다음 명령을 사용합니다…
SVM 범위의 NDMP 모드입니다	'vserver services ndmp on' admin SVM에서 NDMP 인증의 경우 사용자 계정은 admin이고 사용자 역할은 admin 또는 backup입니다. 데이터 SVM에서 사용자 계정은 vsadmin이고 사용자 역할은 vsadmin 또는 vsadmin-backup입니다.
노드 범위의 NDMP 모드입니다	'System services NDMP on'(시스템 서비스 NDMP 켜기)

2. 노드 쉘에서 'ndmpcopy' 명령을 사용하여 스토리지 시스템 내부 또는 스토리지 시스템 간에 데이터 전송:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

DNS 이름은 ndmpcopy에서 지원되지 않습니다. 소스 및 대상의 IP 주소를 제공해야 합니다. 루프백 주소(127.0.0.1)는 소스 IP 주소 또는 대상 IP 주소에 대해 지원되지 않습니다.

◦ "ndmpcopy" 명령은 다음과 같이 제어 연결의 주소 모드를 결정합니다.

- 제어 연결의 주소 모드는 제공된 IP 주소에 해당합니다.
- '-mcs' 및 '-mcd' 옵션을 사용하여 이러한 규칙을 재정의할 수 있습니다.

◦ 소스 또는 타겟이 ONTAP 시스템인 경우 NDMP 모드(노드 범위 또는 SVM 범위)에 따라 타겟 볼륨에 액세스할 수 있는 IP 주소를 사용하십시오.

◦ 'source_path'와 'destination_path'는 볼륨, qtree, 디렉토리 또는 파일의 세밀한 수준까지 가는 절대 경로 이름입니다.

◦ '-mcs'는 소스 스토리지 시스템에 대한 제어 접속의 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

◦ '-MCD'는 대상 저장소 시스템에 대한 제어 연결에 대해 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

◦ '-MD'는 소스와 대상 스토리지 시스템 간의 데이터 전송을 위한 기본 주소 지정 모드를 지정합니다.

inet은 IPv4 주소 모드를 나타내며 inet6은 IPv6 주소 모드를 나타냅니다.

ndmpcopy 명령에서 '-md' 옵션을 사용하지 않으면 데이터 연결의 주소 지정 모드가 다음과 같이 결정됩니다.

- 제어 연결에 지정된 주소 중 하나가 IPv6 주소이면 데이터 연결의 주소 모드는 IPv6입니다.
- 제어 연결에 지정된 두 주소가 모두 IPv4 주소이면 ndmpcopy 명령이 먼저 데이터 연결에 대한 IPv6 주소 모드를 시도합니다.

이 명령이 실패하면 IPv4 주소 모드를 사용합니다.

IPv6 주소가 지정된 경우 대괄호로 묶어야 합니다.

이 샘플 명령은 소스 경로('source_path')에서 대상 경로('Destination_path')로 데이터를 마이그레이션합니다.

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
이 샘플 명령은 IPv6 주소 모드를 사용할 제어 연결과 데이터 연결을 명시적으로 설정합니다.

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

ndmpcopy 명령에 대한 옵션입니다

nodeshell 명령에 사용할 수 있는 옵션을 `ndmpcopy` 이해해야 "데이터를 전송합니다"합니다.

다음 표에는 사용 가능한 옵션이 나와 있습니다.

옵션을 선택합니다	설명
'-sa"사용자 이름:['암호']	이 옵션은 소스 스토리지 시스템에 접속할 소스 인증 사용자 이름과 암호를 설정합니다. 필수 옵션입니다. admin 권한이 없는 사용자의 경우 시스템에서 생성한 NDMP 관련 암호를 지정해야 합니다. admin 및 non-admin 사용자 모두 시스템에서 생성한 암호는 필수입니다.
'-da"사용자 이름':['암호']	이 옵션은 대상 스토리지 시스템에 접속하기 위한 대상 인증 사용자 이름 및 암호를 설정합니다. 필수 옵션입니다.
'-st'{'md5'	'text'}
이 옵션은 소스 스토리지 시스템에 접속할 때 사용할 소스 인증 유형을 설정합니다. 이 옵션은 필수 옵션이므로 사용자는 "text" 또는 "md5" 옵션을 제공해야 합니다.	``dt'{'md5'
'text'}	이 옵션은 대상 스토리지 시스템에 접속할 때 사용할 대상 인증 유형을 설정합니다.
'-l'	이 옵션은 지정된 레벨 값으로 전송에 사용되는 덤프 레벨을 설정합니다. 유효한 값은 0, 1, 9, 0은 전체 전송을 나타내고 1은 9, 0은 증분 전송을 지정합니다. 기본값은 0입니다.
'-d'	이 옵션을 사용하면 ndmpcopy 디버그 로그 메시지를 생성할 수 있습니다. ndmpcopy 디버그 로그 파일은 '/mroot/etc/log' 루트 볼륨에 있습니다. ndmpcopy 디버그 로그 파일 이름은 ndmpcopy.yyyymmdd 형식으로 되어 있습니다.
"-f"	이 옵션은 강제 모드를 활성화합니다. 이 모드에서는 7-Mode 볼륨의 루트에 있는 '/etc' 디렉토리에서 시스템 파일을 덮어쓸 수 있습니다.
'-h'	이 옵션은 도움말 메시지를 인쇄합니다.

옵션을 선택합니다	설명
'-p'	이 옵션은 소스 및 대상 인증에 대한 암호를 입력하라는 메시지를 표시합니다. 이 암호는 '-sa' 및 '-da' 옵션에 지정된 암호보다 우선합니다. 이 옵션은 명령이 대화형 콘솔에서 실행 중인 경우에만 사용할 수 있습니다.
'-exclude'	이 옵션은 데이터 전송에 지정된 경로에서 지정된 파일 또는 디렉토리를 제외합니다. 값은 또는 과 `.txt` 같은 파일 이름 또는 디렉터리의 쉼표로 구분된 목록일 수 `.pst` 있습니다. 지원되는 제외 패턴의 최대 개수는 32개이고 지원되는 최대 문자 수는 255개입니다.

FlexVol 볼륨용 NDMP

ONTAP FlexVol 볼륨에 대한 NDMP에 대해 알아보세요

NDMP(Network Data Management Protocol)는 스토리지 시스템 및 테이프 라이브러리와 같은 운영 스토리지 디바이스와 보조 스토리지 디바이스 간의 백업, 복구 및 기타 데이터 전송 유형을 제어하는 표준화된 프로토콜입니다.

스토리지 시스템에서 NDMP 지원을 설정하면 해당 스토리지 시스템이 백업 또는 복구 작업에 참여하는 NDMP 지원 네트워크 연결 백업 애플리케이션(_Data Management Applications_or_DMA_라고도 함), 데이터 서버 및 테이프 서버와 통신할 수 있습니다. 모든 네트워크 통신은 TCPIP 또는 TCP/IPv6 네트워크를 통해 이루어집니다. NDMP는 또한 테이프 드라이브와 미디어 체인저에 대한 낮은 수준의 제어를 제공합니다.

노드 범위의 NDMP 모드 또는 SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서 테이프 백업 및 복구 작업을 수행할 수 있습니다.

NDMP, 환경 변수 목록 및 지원되는 NDMP 테이프 백업 토폴로지를 사용하는 동안 고려해야 할 사항에 대해 알고 있어야 합니다. 향상된 DAR 기능을 사용하거나 사용하지 않도록 설정할 수도 있습니다. ONTAP에서 스토리지 시스템에 대한 NDMP 액세스를 인증하는 데 지원하는 두 가지 인증 방법은 일반 텍스트 및 본인 확인 방법입니다.

관련 정보

ONTAP에서 지원하는 환경 변수입니다

NDMP 작업 모드에 대해 설명합니다

ONTAP NDMP 작동 모드에 대해 알아보세요

노드 레벨 또는 스토리지 가상 머신(SVM) 레벨에서 테이프 백업 및 복원 작업을 수행하도록 선택할 수 있습니다. SVM 레벨에서 이러한 작업을 성공적으로 수행하려면 SVM에서 NDMP 서비스를 사용하도록 설정해야 합니다.

Data ONTAP 8.2에서 Data ONTAP 8.3으로 업그레이드할 경우 8.2에서 사용되는 NDMP 작업 모드는 업그레이드 후에도 8.2에서 8.3으로 유지됩니다.

Data ONTAP 8.2 이상을 사용하여 새 클러스터를 설치하는 경우 NDMP는 기본적으로 SVM 범위의 NDMP 모드에 있습니다. 노드 범위 NDMP 모드에서 테이프 백업 및 복구 작업을 수행하려면 노드 범위 NDMP 모드를 명시적으로 설정해야 합니다.

노드 범위 **ONTAP NDMP** 모드에 대해 알아보세요

노드 범위의 NDMP 모드에서는 노드 수준에서 테이프 백업 및 복구 작업을 수행할 수 있습니다. Data ONTAP 8.2에서 사용되는 NDMP 작업 모드는 업그레이드 후에도 8.2에서 8.3으로 유지됩니다.

노드 범위의 NDMP 모드에서는 볼륨을 소유하는 노드에서 테이프 백업 및 복구 작업을 수행할 수 있습니다. 이러한 작업을 수행하려면 볼륨 또는 테이프 디바이스를 소유한 노드에서 호스팅되는 LIF에 NDMP 제어 연결을 설정해야 합니다.

이 모드는 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

SVM 범위 **ONTAP NDMP** 모드에 대해 알아보세요

SVM에서 NDMP 서비스가 활성화되어 있는 경우 SVM(스토리지 가상 시스템) 레벨에서 테이프 백업 및 복원 작업을 성공적으로 수행할 수 있습니다. 백업 애플리케이션이 CAB 확장을 지원하는 경우 클러스터 SVM의 여러 노드에서 호스팅되는 모든 볼륨을 백업 및 복원할 수 있습니다.

NDMP 제어 연결은 다른 LIF 유형에 설정할 수 있습니다. SVM 범위의 NDMP 모드에서 이러한 LIF는 데이터 SVM 또는 관리 SVM에 속합니다. 이 LIF를 소유한 SVM에서 NDMP 서비스를 사용하도록 설정한 경우에만 LIF에서 연결을 설정할 수 있습니다.

데이터 LIF는 데이터 SVM에 속하며 인터클러스터 LIF, 노드 관리 LIF 및 클러스터 관리 LIF는 관리 SVM에 속합니다.

SVM 범위의 NDMP 모드에서 백업 및 복원 작업에 대한 볼륨 및 테이프 장치의 가용성은 NDMP 제어 연결이 설정된 LIF 유형과 CAB 확장의 상태에 따라 다릅니다. 백업 애플리케이션이 CAB 확장 및 볼륨을 지원하고 테이프 디바이스가 동일한 선호도를 공유하는 경우 백업 애플리케이션은 3방향 백업 또는 복구 작업 대신 로컬 백업 또는 복구 작업을 수행할 수 있습니다.

관련 정보

노드 범위의 NDMP 모드를 관리하는 명령입니다

ONTAP NDMP 서비스 사용 시 고려 사항

스토리지 시스템에서 NDMP 서비스를 시작할 때는 여러 가지 고려 사항을 고려해야 합니다.

- 각 노드는 연결된 테이프 드라이브를 사용하여 최대 16개의 동시 백업, 복원 또는 2개의 조합을 지원합니다.
- NDMP 서비스는 NDMP 백업 애플리케이션의 요청에 따라 파일 기록 데이터를 생성할 수 있습니다.

  파일 기록은 백업 응용 프로그램에서 백업 이미지에서 선택한 데이터 하위 집합을 최적의 상태로 복구하는 데 사용됩니다. 파일 기록 생성 및 처리는 스토리지 시스템과 백업 애플리케이션 모두에 시간이 많이 걸리고 CPU가 많이 사용될 수 있습니다.

  SMTape는 파일 기록을 지원하지 않습니다.

  전체 백업 이미지가 복구될 재해 복구에 대해 데이터 보호가 구성된 경우 파일 기록 생성을 비활성화하여 백업 시간을 줄일 수 있습니다. NDMP 파일 기록 생성을 해제할 수 있는지 확인하려면 백업 애플리케이션 설명서를 참조하십시오.

- NDMP에 대한 방화벽 정책은 모든 LIF 유형에서 기본적으로 사용하도록 설정됩니다.
- 노드 범위의 NDMP 모드에서 FlexVol 볼륨을 백업하려면 백업 애플리케이션을 사용하여 볼륨을 소유하는 노드에서 백업을 시작해야 합니다.

  그러나 노드 루트 볼륨은 백업할 수 없습니다.

- 방화벽 정책에서 허용하는 한 모든 LIF에서 NDMP 백업을 수행할 수 있습니다.

  데이터 LIF를 사용하는 경우 페일오버에 대해 구성되지 않은 LIF를 선택해야 합니다. NDMP 작업 중에 데이터 LIF가 페일오버되면 NDMP 작업이 실패하고 다시 실행해야 합니다.

- NDMP 모드 및 SVM(Storage Virtual Machine) 범위의 NDMP 모드(CAB 확장 지원 안 함)에서는 NDMP 데이터 연결이 NDMP 제어 연결과 동일한 LIF를 사용합니다.
- LIF 마이그레이션 중에는 지속적인 백업 및 복원 작업이 중단됩니다.

  LIF 마이그레이션 후에 백업 및 복원 작업을 시작해야 합니다.

- NDMP 백업 경로는 '*/vserver_name/volume_name/path_name*' 형식입니다.

  path_name 는 선택 사항이며 디렉토리, 파일 또는 스냅샷의 경로를 지정합니다.

- 덤프 엔진을 사용하여 SnapMirror 대상을 테이프에 백업하는 경우 볼륨의 데이터만 백업됩니다.

  그러나 SMTape를 사용하여 SnapMirror 대상을 테이프에 백업하는 경우 메타데이터도 백업됩니다. SnapMirror 관계 및 관련 메타데이터는 테이프에 백업되지 않습니다. 따라서 복원 중에는 해당 볼륨의 데이터만 복원되지만 연결된 SnapMirror 관계는 복원되지 않습니다.

관련 정보

Cluster Aware Backup 확장의 기능

"시스템 관리"

환경 변수

ONTAP NDMP에 지원되는 환경 변수 알아보기

환경 변수는 NDMP 지원 백업 애플리케이션과 스토리지 시스템 간의 백업 또는 복구 작업에 대한 정보를 전달하는 데 사용됩니다.

예를 들어, 사용자가 백업 애플리케이션이 '/vserver1/vol1/dir1'을 백업하도록 지정하면 백업 애플리케이션이 파일 시스템 환경 변수를 '/vserver1/vol1/dir1'로 설정합니다. 마찬가지로 사용자가 백업을 레벨 1 백업으로 지정하면 백업 애플리케이션이 레벨 환경 변수를 1(1)로 설정합니다.

일반적으로 환경 변수의 설정 및 검사는 백업 관리자에게 영향을 미치지 않습니다. 즉, 백업 애플리케이션에서 자동으로 설정합니다.

백업 관리자는 환경 변수를 거의 지정하지 않지만, 기능 또는 성능 문제를 특성화하거나 해결할 수 있도록 백업 응용 프로그램에서 설정한 환경 변수의 값을 변경할 수 있습니다. 예를 들어, 관리자는 파일 기록 생성을 일시적으로 비활성화하여 백업 응용 프로그램의 파일 기록 정보 처리가 성능 문제 또는 기능 문제에 기여하는지 여부를 확인할 수 있습니다.

많은 백업 애플리케이션은 환경 변수를 재정의하거나 수정하거나 추가 환경 변수를 지정할 수 있는 수단을 제공합니다. 자세한 내용은 백업 애플리케이션 설명서를 참조하십시오.

ONTAP에서 지원하는 환경 변수입니다

ONTAP 연관된 기본값이 있는 환경 변수를 지원합니다. 하지만 이러한 기본값을 수동으로 수정할 수 있습니다.

백업 애플리케이션에서 설정한 값을 수동으로 수정하면 애플리케이션이 예상치 않게 작동할 수 있습니다. 이는 백업 또는 복원 작업에서 백업 애플리케이션이 예상한 작업을 수행하지 못할 수 있기 때문입니다. 그러나 경우에 따라 신중하게 수정하면 문제를 식별하거나 해결하는 데 도움이 될 수 있습니다.

다음 표에는 덤프 및 SMTape에 공통으로 사용되는 환경 변수와 덤프 및 SMTape에만 지원되는 변수가 나와 있습니다. 다음 표에는 ONTAP에서 지원하는 환경 변수가 사용되는 경우 해당 변수가 작동하는 방식이 설명되어 있습니다.

대부분의 경우 Y는 T, N도 F를 받아들입니다.

덤프 및 **SMTape**에 대해 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
디버그	Y, N	N	디버깅 정보가 인쇄되도록 지정합니다.
파일 시스템	'트링'	"없음"	백업할 데이터의 루트 경로 이름을 지정합니다.
NDMP_version	RETURN_OVERY'를 선택합니다	"없음"	NDMP_VERSION 변수를 수정하면 안 됩니다. 백업 작업에 의해 생성된 NDMP_VERSION 변수는 NDMP 버전을 반환합니다. ONTAP는 내부 사용을 위해 백업 중에 NDMP_VERSION 변수를 설정하고 정보 제공을 위해 백업 애플리케이션에 전달합니다. NDMP 세션의 NDMP 버전이 이 변수로 설정되지 않았습니다.

환경 변수	유효한 값	기본값	설명
경로 이름_구분 기호입니다	RETURN_VALUE’입니다	"없음"	경로 이름 구분 문자를 지정합니다. 이 문자는 백업되는 파일 시스템에 따라 다릅니다. ONTAP의 경우 문자 ""/"가 이 변수에 할당됩니다. NDMP 서버는 테이프 백업 작업을 시작하기 전에 이 변수를 설정합니다.
유형	'둔부' 또는 '스머테이프'	둔부	테이프 백업 및 복원 작업을 수행하는 데 지원되는 백업 유형을 지정합니다.
자세한 정보	Y, N	N	테이프 백업 또는 복구 작업을 수행하는 동안 로그 메시지를 늘립니다.

덤프에 대해 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
acl_start 를 선택합니다	RETURN_OVERY’를 선택합니다	"없음"	백업 작업에 의해 생성된 ACL_START 변수는 직접 액세스 복구 또는 재시작 가능한 NDMP 백업 작업에 사용되는 오프셋 값입니다. 오프셋 값은 덤프 파일에서 ACL 데이터(Pass V)가 시작되고 백업 끝에서 반환되는 바이트 오프셋입니다. 백업된 데이터를 올바르게 복원하기 위한 직접 액세스 복원 작업의 경우 ACL_START 값을 복구 작업이 시작될 때 복구 작업으로 전달해야 합니다. NDMP 재시작 가능 백업 작업에서는 acl_start 값을 사용하여 백업 스트림의 다시 시작 가능한 부분이 시작되는 백업 애플리케이션과 통신합니다.

환경 변수	유효한 값	기본값	설명
base_date 를 선택합니다	0, -1, dump_date 값	'-1'	증분 백업의 시작 날짜를 지정합니다. '-1'로 설정하면 base_date 증분 지정자가 비활성화됩니다. 레벨 0 백업에서 '0'으로 설정하면 증분 백업이 활성화됩니다. 초기 백업 후 이전 증분 백업의 dump_date 변수 값이 base_date 변수에 할당됩니다. 이러한 변수는 레벨 /업데이트 기반 증분 백업에 대한 대안입니다.
직접	Y, N	N	전체 테이프를 스캔하는 대신 복구가 파일 데이터가 상주하는 테이프 위치로 직접 빠르게 전달되도록 지정합니다. 직접 액세스 복구가 작동하려면 백업 애플리케이션이 위치 정보를 제공해야 합니다. 이 변수가 Y로 설정되어 있으면 백업 응용 프로그램에서 파일 또는 디렉터리 이름과 위치 지정 정보를 지정합니다.
dmp_name입니다	'트링'	"없음"	여러 하위 트리 백업의 이름을 지정합니다. 여러 하위 트리 백업에는 이 변수가 필수입니다.

환경 변수	유효한 값	기본값	설명
dump_date 를 참조하십시오	RETURN_VALUE’입니다	"없음"	이 변수를 직접 변경하지 않습니다. base_date 변수가 '-1’이 아닌 값으로 설정된 경우 백업에 의해 생성됩니다. dump_date 변수는 32비트 레벨 값을 덤프 소프트웨어에서 계산된 32비트 시간 값에 미리 추가하여 파생됩니다. 수준은 base_date 변수에 전달된 마지막 수준 값에서 증가합니다. 결과 값은 후속 증분 백업에서 base_date 값으로 사용됩니다.
Enhanced_DAR_ENABLED입니다	Y, N	N	향상된 DAR 기능의 사용 여부를 지정합니다. 향상된 DAR 기능은 NT 스트림이 있는 파일의 DAR 및 DAR 디렉토리를 지원합니다. 향상된 성능을 제공합니다. 복원 중 향상된 DAR는 다음 조건이 충족되는 경우에만 가능합니다. • ONTAP는 향상된 DAR를 지원합니다. • 백업 중에 파일 기록이 활성화됩니다(HIST=Y). • ndmpd.offset_map.enable 옵션이 on으로 설정되어 있습니다. • Enhanced_DAR_ENABLED 변수가 복원 중에 'Y’로 설정됩니다.

환경 변수	유효한 값	기본값	설명
제외	pattern_string	"없음"	데이터를 백업할 때 제외되는 파일 또는 디렉토리를 지정합니다. 제외 목록은 쉼표로 구분된 파일 또는 디렉토리 이름 목록입니다. 파일 또는 디렉토리의 이름이 목록의 이름 중 하나와 일치하면 백업에서 제외됩니다. 제외 목록에서 이름을 지정할 때 다음 규칙이 적용됩니다. • 파일 또는 디렉토리의 정확한 이름을 사용해야 합니다. • 와일드카드 문자인 별표(*)는 문자열의 첫 번째 문자 또는 마지막 문자여야 합니다. 각 문자열은 최대 2개의 별표를 포함할 수 있습니다. • 파일 또는 디렉터리 이름의 쉼표 앞에는 백슬래시가 있어야 합니다. • 제외 목록에는 최대 32개의 이름이 포함될 수 있습니다.  non_quota_tree를 동시에 Y로 설정하면 백업 대상에서 제외되도록 지정된 파일 또는 디렉토리가 제외되지 않습니다.

환경 변수	유효한 값	기본값	설명
압축 풀기	Y, N, E	N	백업된 데이터 집합의 하위 트리를 복원하도록 지정합니다. 백업 응용 프로그램은 추출할 하위 트리의 이름을 지정합니다. 지정된 파일이 콘텐츠가 백업된 디렉토리와 일치하면 디렉토리의 압축이 재귀적으로 풀립니다. DAR를 사용하지 않고 복원 중에 파일, 디렉토리 또는 qtree의 이름을 바꾸려면 추출 환경 변수를 "E"로 설정해야 합니다.
extract_acl 을 선택합니다	Y, N	Y를 누릅니다	백업 파일의 ACL이 복구 작업에서 복원되도록 지정합니다. 기본값은 데이터를 복원할 때 ACLS를 복원하는 것입니다. 단, DARs(direct=Y)는 예외입니다.
하중	Y, N	N	복구 작업에서 대상 볼륨의 볼륨 공간 및 inode 가용성을 확인해야 하는지 여부를 결정합니다. 이 변수를 'Y'로 설정하면 복원 작업에서 대상 경로의 볼륨 공간 및 inode 가용성 검사를 건너뜁니다. 대상 볼륨에 충분한 볼륨 공간 또는 inode를 사용할 수 없는 경우 복구 작업은 대상 볼륨 공간과 inode 가용성에 의해 허용되는 많은 데이터를 복구합니다. 볼륨 공간 또는 inode를 사용할 수 없는 경우 복구 작업이 중지됩니다.

환경 변수	유효한 값	기본값	설명
하이스트	Y, N	N	파일 기록 정보가 백업 응용 프로그램으로 전송되도록 지정합니다. 대부분의 상용 백업 애플리케이션은 HIST 변수를 Y로 설정합니다. 백업 작업의 속도를 증가시키거나 파일 기록 수집 문제를 해결하려는 경우 이 변수를 "N"으로 설정할 수 있습니다. 백업 응용 프로그램이 파일 기록을 지원하지 않는 경우 HIST 변수를 'Y'로 설정하지 않아야 합니다.

환경 변수	유효한 값	기본값	설명
ctime 무시	Y, N	N	이전 증분 백업 이후에 ctime 값만 변경된 경우 파일이 증분 백업되지 않도록 지정합니다. 바이러스 검사 소프트웨어와 같은 일부 응용 프로그램은 파일 또는 해당 속성이 변경되지 않았더라도 inode 내의 파일의 ctime 값을 변경합니다. 따라서 증분 백업은 변경되지 않은 파일을 백업할 수 있습니다. ctime 값이 수정되었기 때문에 증분 백업에 허용 가능한 시간 또는 공간이 필요한 경우에만 ignore_ctime 변수를 지정해야 합니다.  NDMP dump 명령은 기본적으로 ignore_ctime을 false로 설정합니다. "참"으로 설정하면 다음과 같은 데이터 손실이 발생할 수 있습니다. 1. 볼륨 레벨 증분 ndmpcopy를 사용하여 ignore_ctime을 true로 설정하면 소스의 qtree에서 이동된 파일이 삭제됩니다. 볼륨

환경 변수	유효한 값	기본값	설명
ignore_cQtree	Y, N	N	복구 작업이 백업된 qtree에서 qtree 정보를 복원하지 않음을 지정합니다.
레벨	0-31입니다	0	백업 레벨을 지정합니다. 레벨 0은 전체 데이터 세트를 복사합니다. 0보다 높은 값으로 지정된 증분 백업 레벨은 마지막 증분 백업 이후 모든 파일(새 파일 또는 수정된 파일)을 복사합니다. 예를 들어 레벨 1은 레벨 0 백업 이후에 새 파일이나 수정된 파일을 백업하며, 레벨 2는 레벨 1 백업 이후에 새 파일이나 수정된 파일을 백업합니다.
목록	Y, N	N	에는 실제로 데이터를 복원하지 않고 백업된 파일 이름 및 inode 번호가 나와 있습니다.
list_qtree 를 참조하십시오	Y, N	N	에는 실제로 데이터를 복원하지 않는 백업 qtree가 나와 있습니다.
multi_subtree_names를 선택합니다	'트링'	"없음"	백업이 여러 하위 트리 백업임을 지정합니다. 하위 트리 이름의 줄 바꿈, null 종료 목록인 문자열에 여러 개의 하위 트리가 지정됩니다. 하위 트리는 목록의 마지막 요소로 지정해야 하는 공통 루트 디렉터리를 기준으로 경로 이름으로 지정됩니다. 이 변수를 사용하는 경우 dmp_name 변수도 사용해야 합니다.

환경 변수	유효한 값	기본값	설명
NDMP_Unicode_FH	Y, N	N	파일 기록 정보에 있는 파일의 NFS 이름 외에 유니코드 이름이 포함되도록 지정합니다. 이 옵션은 대부분의 백업 응용 프로그램에서 사용되지 않으며, 이러한 추가 파일 이름을 받도록 백업 응용 프로그램을 설계하지 않는 한 설정해서는 안 됩니다. HIST 변수도 설정해야 합니다.
no_acls입니다	Y, N	N	데이터를 백업할 때 ACL을 복제하지 않도록 지정합니다.
non_quota_tree	Y, N	N	데이터를 백업할 때 Qtree의 파일 및 디렉토리를 무시하도록 지정합니다. 'Y'로 설정하면 파일 시스템 변수에 의해 지정된 데이터 세트의 qtree에 있는 항목이 백업되지 않습니다. 이 변수는 파일 시스템 변수가 전체 볼륨을 지정하는 경우에만 적용됩니다. non_quota_tree 변수는 레벨 0 백업에서만 작동하며 multi_subtree_names 변수가 지정된 경우에는 작동하지 않습니다. non_quota_tree를 동시에 Y로 설정하면 백업 대상에서 제외되도록 지정된 파일 또는 디렉토리가 제외되지 않습니다.

환경 변수	유효한 값	기본값	설명
노와이ITE	Y, N	N	복구 작업이 디스크에 데이터를 쓰지 않도록 지정합니다. 이 변수는 디버깅에 사용됩니다.

환경 변수	유효한 값	기본값	설명
반복	Y, N	Y를 누릅니다	DAR 복원 중에 디렉토리 항목을 확장하도록 지정합니다. DIRECT 및 Enhanced_DAR_ENABLED 환경 변수('Y'로 설정)도 활성화해야 합니다. 반복 변수가 비활성화된 경우('N'으로 설정), 원본 소스 경로의 모든 디렉토리에 대한 사용 권한과 ACL만 테이프에서 복원되며 디렉토리의 내용은 복구되지 않습니다. recursive 변수가 N으로 설정되어 있거나 recover_full_paths 변수가 Y로 설정되어 있으면 복구 경로가 원래 경로로 끝나야 합니다. 재귀 변수를 사용하지 않도록 설정하고 복구 경로가 둘 이상인 경우 모든 복구 경로가 복구 경로의 가장 긴 경로에 포함되어야 합니다. 그렇지 않으면 오류 메시지가 표시됩니다. 예를 들어 모든 복구 경로가 "foo/dir1/딥디르/myfile" 내에 있으므로 다음과 같은 복구 경로가 유효합니다. • '/foo' • "/foo/dir" • '/foo/dir1/딥디더' • '/foo/dir1/딥디르/myfile' 다음은 잘못된 복구 경로입니다. '/foo'

환경 변수	유효한 값	기본값	설명
RECOVER_FULL_경로	Y, N	N	전체 복구 경로에 DAR 이후에 복구된 해당 권한과 ACL이 포함되도록 지정합니다. Direct 및 Enhanced_DAR_ENABLED도 활성화('Y'로 설정)해야 합니다. recover_full_paths가 Y로 설정된 경우 복구 경로는 원래 경로로 끝나야 합니다. 대상 볼륨에 디렉토리가 이미 있으면 해당 사용 권한 및 ACL이 테이프에서 복원되지 않습니다.
업데이트	Y, N	Y를 누릅니다	레벨 기반 증분 백업을 사용하도록 메타데이터 정보를 업데이트합니다.

SMTape에 지원되는 환경 변수입니다

환경 변수	유효한 값	기본값	설명
base_date 를 선택합니다	dump_date를 선택합니다	'-1'	증분 백업의 시작 날짜를 지정합니다. `BASE_DATE` 은 참조 스냅샷 식별자의 문자열 표현입니다. SMTape는 문자열을 사용하여 `BASE_DATE` 참조 스냅샷을 찾습니다. 기본 백업에는 base_date가 필요하지 않습니다. 증분 백업의 경우 이전 기준 또는 증분 백업의 DUMP_DATE 변수 값이 기본_DATE 변수에 할당됩니다. 백업 애플리케이션은 이전 SMTape 기준 또는 증분 백업에서 DUMP_DATE 값을 할당합니다.
dump_date 를 참조하십시오	RETURN_VALUE’입니다	"없음"	SMTape 백업이 끝날 때 dump_date에는 해당 백업에 사용된 스냅샷을 식별하는 문자열 식별자가 포함됩니다. 이 스냅샷은 후속 증분 백업을 위한 참조 스냅샷으로 사용할 수 있습니다. dump_date의 결과 값은 후속 증분 백업의 base_date 값으로 사용됩니다.

환경 변수	유효한 값	기본값	설명
SMTape_backup_set_ID 입니다	'트링'	"없음"	기본 백업과 관련된 증분 백업의 시퀀스를 식별합니다. 백업 세트 ID는 기본 백업 중에 생성되는 128비트 고유 ID입니다. 백업 애플리케이션은 증분 백업 중에 이 ID를 'MTAPE_BACKUP_SET_ID' 변수에 대한 입력으로 할당합니다.
SMTape_snapshot_name 입니다	볼륨에서 사용 가능한 모든 유효한 스냅샷입니다	유효하지 않습니다	SMTAPE_snapshot_name 변수가 스냅샷으로 설정되면 해당 스냅샷과 이전 스냅샷이 테이프에 백업됩니다. 증분 백업의 경우 이 변수는 증분 스냅샷을 지정합니다. base_date 변수는 기준 스냅샷을 제공합니다.
SMTape_delete_snapshot	Y, N	N	SMTape에 의해 자동으로 생성된 스냅샷의 경우 SMTAPE_DELETE_SNAPSHOT 변수가 로 설정된 경우 ɣ 백업 작업이 완료된 후 SMTape가 이 스냅샷을 삭제합니다. 그러나 백업 애플리케이션에서 생성된 스냅샷은 삭제되지 않습니다.
SMTape_break_mirror입니다	Y, N	N	SMTAPE_break_mirror 변수가 Y로 설정되면 성공한 복구 후 dP 유형의 볼륨이 RW 볼륨으로 변경됩니다.

일반적인 **ONTAP NDMP** 테이프 백업 토폴로지에 대해 알아보세요**.**

NDMP는 백업 애플리케이션과 스토리지 시스템 또는 데이터(파일 시스템)와 테이프 서비스를 제공하는 다른 NDMP 서버 간의 다양한 토폴로지 및 구성을 지원합니다.

스토리지 시스템-로컬-테이프

가장 간단한 구성에서는 백업 애플리케이션이 스토리지 시스템의 데이터를 스토리지 시스템에 연결된 테이프 서브시스템으로 백업합니다. NDMP 제어 접속은 네트워크 경계를 넘어 존재합니다. 데이터와 테이프 서비스 간에

스토리지 시스템 내에 존재하는 NDMP 데이터 접속을 NDMP 로컬 구성이라고 합니다.

다른 스토리지 시스템에 연결된 스토리지 시스템-테이프

또한 백업 애플리케이션은 스토리지 시스템의 데이터를 다른 스토리지 시스템에 연결된 테이프 라이브러리(하나 이상의 테이프 드라이브가 있는 미디어 체인저)로 백업할 수도 있습니다. 이 경우 데이터와 테이프 서비스 간의 NDMP 데이터 연결은 TCP 또는 TCP/IPv6 네트워크 연결을 통해 제공됩니다. 이를 NDMP 3-way 스토리지 시스템-스토리지 시스템 구성이라고 합니다.

스토리지 시스템-네트워크 연결 테이프 라이브러리

NDMP 지원 테이프 라이브러리는 3방향 구성의 변형을 제공합니다. 이 경우 테이프 라이브러리는 TCP/IP 네트워크에 직접 연결되며 내부 NDMP 서버를 통해 백업 애플리케이션 및 스토리지 시스템과 통신합니다.

스토리지 시스템-데이터 서버-테이프 또는 데이터 서버-스토리지 시스템-테이프

NDMP는 스토리지 시스템-데이터-서버 및 데이터-서버-스토리지 시스템 3방향 구성도 지원합니다. 스토리지 시스템 대 서버 를 사용하면 스토리지 시스템 데이터를 백업 애플리케이션 호스트 또는 다른 데이터 서버 시스템에 연결된 테이프 라이브러리에 백업할 수 있습니다. 서버-스토리지 시스템 구성을 사용하면 서버 데이터를 스토리지 시스템에 연결된 테이프 라이브러리에 백업할 수 있습니다.

ONTAP 지원 **NDMP** 인증 방법

NDMP 연결 요청을 허용하는 인증 방법을 지정할 수 있습니다. ONTAP는 스토리지 시스템에 대한 NDMP 액세스를 인증하는 두 가지 방법인 일반 텍스트 및 본인 확인 방법을 지원합니다.

노드 범위 NDMP 모드에서는 기본적으로 본인 확인 및 일반 텍스트가 모두 설정됩니다. 그러나 챌린지를 비활성화할 수는 없습니다. 일반 텍스트를 사용하거나 사용하지 않도록 설정할 수 있습니다. 일반 텍스트 인증 방법에서는 로그인 암호가 일반 텍스트로 전송됩니다.

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 기본적으로 인증 방법이 본인 확인 방법입니다. 노드 범위 NDMP 모드와 달리 이 모드에서는 일반 텍스트 및 본인 확인 인증 방법을 모두 사용하거나 사용하지 않도록 설정할 수 있습니다.

관련 정보

노드 범위 NDMP 모드의 사용자 인증

SVM 범위의 NDMP 모드에서 사용자 인증

ONTAP에서 지원되는 **NDMP** 확장

NDMP v4는 핵심 NDMP v4 프로토콜을 수정하지 않고 NDMP v4 프로토콜 확장을 생성하는 메커니즘을 제공합니다. ONTAP에서 지원하는 NDMP v4 확장에 대해 알고 있어야 합니다.

ONTAP에서 지원되는 NDMP v4 확장은 다음과 같습니다.

- 운전실(Cluster Aware Backup)

  이러한 확장은 SVM 범위의 NDMP 모드에서만 지원됩니다.

- IPv6 지원을 위한 CAE(Connection Address Extension)

- 확장 클래스 0x2050

  이 확장은 재시작 가능한 백업 작업 및 Snapshot Management Extensions를 지원합니다.

  > Snapshot Management Extensions의 일부인 이 `NDMP_SNAP_RECOVER` 메시지는 복구 작업을 시작하고 로컬 스냅샷에서 로컬 파일 시스템 위치로 복구된 데이터를 전송하는 데 사용됩니다. ONTAP에서 이 메시지를 통해 볼륨 및 일반 파일만 복구할 수 있습니다.
  >
  > 이 `NDMP_SNAP_DIR_LIST` 메시지를 통해 볼륨의 스냅샷을 탐색할 수 있습니다. 탐색 작업이 진행 중인 동안 무중단 작업이 발생하면 백업 애플리케이션이 탐색 작업을 다시 시작해야 합니다.

- NDMP 재시작 가능 백업 확장

  NDMP RBE(재시작 가능한 백업 확장) 기능을 사용하여 장애가 발생하기 전에 데이터 스트림의 알려진 체크포인트에서 백업을 재시작할 수 있습니다.

ONTAP NDMP의 향상된 **DAR** 기능에 대해 알아보세요**.**

디렉토리 DAR 및 파일 및 NT 스트림의 DAR에 향상된 직접 액세스 복구(DAR) 기능을 사용할 수 있습니다. 기본적으로 향상된 DAR 기능은 활성화되어 있습니다.

향상된 DAR 기능을 사용하도록 설정하면 오프셋 맵을 생성하여 테이프에 기록해야 하기 때문에 백업 성능에 영향을 줄 수 있습니다. 노드 범위 및 SVM(스토리지 가상 머신) 범위 NDMP 모드 모두에서 향상된 DAR를 설정하거나 해제할 수 있습니다.

NDMP 세션에 대한 **ONTAP** 확장성 제한

서로 다른 시스템 메모리 용량의 스토리지 시스템에서 동시에 설정할 수 있는 NDMP 세션의 최대 수를 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

다음 표에 설명된 제한은 NDMP 서버에 대한 것입니다. '덤프 백업 및 복원 세션에 대한 계산 제한' 섹션에 언급된 제한은 덤프 및 복원 세션에 대한 것입니다.

덤프 백업 및 복원 세션에 대한 확장성 제한

스토리지 시스템의 시스템 메모리입니다	최대 **NDMP** 세션 수입니다
16GB 미만	8
16GB보다 크거나 같지만 24GB보다 작습니다	20
24GB보다 크거나 같습니다	36

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP FlexGroup 볼륨을 통한 NDMP 지원에 대해 알아보세요.

ONTAP 9.7부터는 FlexGroup 볼륨에서 NDMP가 지원됩니다.

ONTAP 9.7부터는 ndmpcopy 명령이 FlexVol 볼륨과 FlexGroup 볼륨 간의 데이터 전송에 지원됩니다.

ONTAP 9.7에서 이전 버전으로 되돌릴 경우 이전 전송의 증분 전송 정보가 유지되지 않으므로 되돌리기 후 기본 복사를 수행해야 합니다.

ONTAP 9.8부터는 FlexGroup 볼륨에서 다음 NDMP 기능이 지원됩니다.

- 확장자 클래스 0x2050의 ndmp_snap_recover 메시지는 FlexGroup 볼륨에서 개별 파일을 복구하는 데 사용할 수 있습니다.
- FlexGroup 볼륨에 대해 NDMP RBE(재시작 가능한 백업 확장)가 지원됩니다.
- FlexGroup 볼륨에 대해 환경 변수 exclude 및 multi_subtree_names가 지원됩니다.

ONTAP SnapLock 볼륨을 사용한 NDMP에 대해 알아보세요

규제가 적용되는 데이터의 여러 복제본을 생성하면 중복 복구 시나리오를 사용할 수 있으며, NDMP 덤프 및 복구를 사용하면 SnapLock 볼륨에서 소스 파일의 WORM(Write Once, Read Many) 특성을 보존할 수 있습니다.

SnapLock 볼륨의 파일에 있는 WORM 속성은 데이터를 백업, 복원 및 복사할 때 유지되지만 WORM 속성은 SnapLock 볼륨으로 복원할 때만 적용됩니다. SnapLock 볼륨의 백업이 SnapLock 볼륨 이외의 볼륨으로 복원되는 경우 WORM 속성은 유지되지만 무시되며 ONTAP에서 적용되지 않습니다.

FlexVol 볼륨에 대한 노드 범위 NDMP 모드를 관리합니다

FlexVol 볼륨에 대한 ONTAP 노드 범위 NDMP 모드 관리에 대해 알아보세요.

NDMP 옵션과 명령을 사용하여 노드 레벨에서 NDMP를 관리할 수 있습니다. 'options' 명령을 사용하여 NDMP 옵션을 수정할 수 있습니다. 테이프 백업 및 복구 작업을 수행하려면 NDMP 관련 자격 증명을 사용하여 스토리지 시스템을 액세스해야 합니다.

에 대한 자세한 내용은 `options` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP 노드 범위 NDMP 모드를 관리하기 위한 명령

'system services ndmp' 명령을 사용하여 노드 레벨에서 NDMP를 관리할 수 있습니다. 이러한 명령 중 일부는 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

다음 NDMP 명령은 고급 권한 수준에서만 사용할 수 있습니다.

- '시스템 서비스 NDMP 서비스 종료
- '시스템 서비스 NDMP 서비스 시작'
- '시스템 서비스 NDMP 서비스 중지'
- '시스템 서비스 NDMP 로그 시작'

- 'System services ndmp log stop'(시스템 서비스 NDMP 로그 중지)

원하는 작업	이 명령 사용...
NDMP 서비스를 설정합니다	'System services NDMP on' *
NDMP 서비스를 해제합니다	'시스템 서비스 NDMP 꺼짐' *
NDMP 구성을 표시합니다	'system services ndmp show' * 를 참조하십시오
NDMP 구성을 수정합니다	'시스템 서비스 NDMP 수정' *
기본 NDMP 버전을 표시합니다	'시스템 서비스 NDMP 버전' *
NDMP 서비스 구성을 표시합니다	'시스템 서비스 NDMP 서비스 쇼'
NDMP 서비스 구성을 수정합니다	'시스템 서비스 NDMP 서비스 수정'
모든 NDMP 세션을 표시합니다	'시스템 서비스 NDMP 상태'
모든 NDMP 세션에 대한 자세한 정보를 표시합니다	'System services ndmp probe
지정된 NDMP 세션을 종료합니다	'시스템 서비스 NDMP kill'
모든 NDMP 세션을 종료합니다	'시스템 서비스 NDMP kill-all'
NDMP 암호를 변경합니다	'시스템 서비스 NDMP 암호' *
노드 범위 NDMP 모드를 설정합니다	'System services NDMP node-scope-mode on' *
노드 범위 NDMP 모드를 해제합니다	'System services NDMP node-scope-mode off' *
노드 범위의 NDMP 모드 상태를 표시합니다	'System services NDMP node-scope-mode status' *
모든 NDMP 세션을 강제로 종료합니다	'시스템 서비스 NDMP 서비스 종료
NDMP 서비스 데몬을 시작합니다	'시스템 서비스 NDMP 서비스 시작'
NDMP 서비스 데몬을 중지합니다	'시스템 서비스 NDMP 서비스 중지'
지정된 NDMP 세션에 대해 로깅을 시작합니다	'시스템 서비스 NDMP 로그 시작' *
지정된 NDMP 세션에 대한 로깅을 중지합니다	'System services ndmp log stop' *

- 이러한 명령은 더 이상 사용되지 않으며 향후 주요 릴리즈에서 제거될 예정입니다.

에 대한 자세한 내용은 `system services ndmp` "ONTAP 명령 참조입니다"을 참조하십시오.

노드 범위 **NDMP** 모드의 사용자 인증

노드 범위 NDMP 모드에서는 NDMP 관련 자격 증명을 사용하여 스토리지 시스템에 액세스해야 테이프 백업 및 복구 작업을 수행할 수 있습니다.

기본 사용자 ID는 ""root""입니다. 노드에서 NDMP를 사용하기 전에 NDMP 사용자와 연결된 기본 NDMP 암호를 변경해야 합니다. 기본 NDMP 사용자 ID를 변경할 수도 있습니다.

관련 정보

노드 범위의 NDMP 모드를 관리하는 명령입니다

노드 범위의 NDMP 모드는 무엇입니까

FlexVol 볼륨에 대한 SVM 범위의 NDMP 모드를 관리합니다

FlexVol 볼륨에 대한 **ONTAP SVM** 범위 **NDMP** 모드 관리에 대해 알아보세요.

NDMP 옵션 및 명령을 사용하여 SVM별로 NDMP를 관리할 수 있습니다. 'vserver services ndmp modify' 명령을 사용하여 NDMP 옵션을 수정할 수 있습니다. SVM 범위의 NDMP 모드에서는 사용자 인증이 역할 기반 액세스 제어 메커니즘과 통합됩니다.

"vserver modify" 명령을 사용하여 허용 또는 허용되지 않는 프로토콜 목록에 NDMP를 추가할 수 있습니다. 기본적으로 NDMP는 허용되는 프로토콜 목록에 있습니다. NDMP가 허용되지 않는 프로토콜 목록에 추가되면 NDMP 세션을 설정할 수 없습니다.

옵션을 사용하여 NDMP 데이터 연결이 설정되는 LIF 유형을 제어할 수 `-preferred-interface-role` 있습니다. NDMP 데이터 연결을 설정하는 동안 NDMP는 이 옵션에 지정된 LIF 유형에 속하는 IP 주소를 선택합니다. IP 주소가 이러한 LIF 유형 중 하나에 속하지 않으면 NDMP 데이터 연결을 설정할 수 없습니다. 에 대한 자세한 내용은 `vserver services ndmp modify` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP SVM 범위 **NDMP** 모드를 관리하기 위한 명령

'vserver services NDMP' 명령을 사용하여 각 스토리지 가상 머신(SVM, 이전 명칭 Vserver)에서 NDMP를 관리할 수 있습니다.

원하는 작업	이 명령 사용...
NDMP 서비스를 설정합니다	'vserver services ndmp on' NDMP 서비스는 항상 클러스터의 모든 노드에서 설정해야 합니다. 'system services ndmp on' 명령을 사용하여 노드에서 NDMP 서비스를 설정할 수 있습니다. 기본적으로 NDMP 서비스는 노드에 대해 항상 설정됩니다.

원하는 작업	이 명령 사용...
NDMP 서비스를 해제합니다	'vserver services ndmp off'
NDMP 구성을 표시합니다	'vserver services ndmp show'
NDMP 구성을 수정합니다	'vserver services ndmp modify
기본 NDMP 버전을 표시합니다	'vserver services ndmp version
모든 NDMP 세션을 표시합니다	'vserver services ndmp status'
모든 NDMP 세션에 대한 자세한 정보를 표시합니다	'vserver services ndmp probe'
지정된 NDMP 세션을 종료합니다	'vserver services ndmp kill'
모든 NDMP 세션을 종료합니다	'vserver services ndmp kill-all'
NDMP 암호를 생성합니다	'vserver services ndmp generate-password
NDMP 확장 상태를 표시합니다	'vserver services ndmp extensions show' 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
NDMP 확장 상태를 수정(설정 또는 해제)합니다	'vserver services ndmp extensions modify(SVM 서비스 NDMP 확장 수정 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
지정된 NDMP 세션에 대해 로깅을 시작합니다	'vserver services ndmp log start'를 선택합니다 이 명령은 고급 권한 수준에서 사용할 수 있습니다.
지정된 NDMP 세션에 대한 로깅을 중지합니다	'vserver services ndmp log stop' 이 명령은 고급 권한 수준에서 사용할 수 있습니다.

에 대한 자세한 내용은 `vserver services ndmp` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

SVM 범위의 NDMP 모드를 관리하는 명령입니다

Cluster Aware Backup 확장의 기능

SVM 범위의 NDMP 모드는 무엇입니까

"시스템 관리"

ONTAP NDMP용 클러스터 인식 백업 확장에 대해 알아보세요

CAB(클러스터 인식 백업)은 NDMP v4 프로토콜 확장입니다. 이 확장을 통해 NDMP 서버는 볼륨을 소유하는 노드에서 데이터 연결을 설정할 수 있습니다. 또한 백업 애플리케이션에서 볼륨 및 테이프 디바이스가 클러스터의 동일한 노드에 있는지 확인할 수 있습니다.

NDMP 서버가 볼륨을 소유하는 노드를 식별하고 이러한 노드에서 데이터 연결을 설정하도록 하려면 백업 애플리케이션이 CAB 확장을 지원해야 합니다. CAB 확장을 사용하려면 백업 애플리케이션에서 데이터 연결을 설정하기 전에 백업 또는 복구할 볼륨에 대해 NDMP 서버에 알려야 합니다. 이를 통해 NDMP 서버가 볼륨을 호스팅하는 노드를 확인하고 데이터 연결을 적절하게 설정할 수 있습니다.

백업 애플리케이션에서 지원되는 CAB 확장을 통해 NDMP 서버는 볼륨 및 테이프 디바이스에 대한 선호도 정보를 제공합니다. 볼륨 및 테이프 디바이스가 클러스터의 동일한 노드에 있는 경우 이러한 선호도 정보를 사용하여 백업 애플리케이션이 3방향 백업 대신 로컬 백업을 수행할 수 있습니다.

다양한 **LIF** 유형의 백업 및 복원을 위한 **ONTAP** 볼륨 및 테이프 장치의 가용성

클러스터의 모든 LIF 유형에서 NDMP 제어 연결을 설정하도록 백업 애플리케이션을 구성할 수 있습니다. SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 이러한 LIF 유형과 CAB 확장 상태에 따라 백업 및 복원 작업에 대한 볼륨 및 테이프 장치의 가용성을 결정할 수 있습니다.

다음 표에는 NDMP 제어 연결 LIF 유형에 대한 볼륨 및 테이프 디바이스의 가용성과 CAB 확장의 상태가 나와 있습니다.

백업 애플리케이션에서 운전실 확장이 지원되지 않는 경우 볼륨 및 테이프 장치의 가용성을 유지할 수 있습니다

NDMP 제어 연결 **LIF** 유형입니다	백업 또는 복원에 사용할 수 있는 볼륨입니다	백업 또는 복원에 사용할 수 있는 테이프 디바이스입니다
노드 관리 LIF	노드에서 호스팅하는 모든 볼륨	노드 관리 LIF를 호스팅하는 노드에 연결된 테이프 디바이스입니다
데이터 LIF	데이터 LIF를 호스팅하는 노드에서 호스팅되는 SVM에 속하는 볼륨만	없음
클러스터 관리 LIF	클러스터 관리 LIF를 호스팅하는 노드에서 호스팅하는 모든 볼륨입니다	없음
인터클러스터 LIF	인터클러스터 LIF를 호스팅하는 노드에 의해 호스팅되는 모든 볼륨입니다	인터클러스터 LIF를 호스팅하는 노드에 연결된 테이프 장치

백업 애플리케이션에서 **CAB** 확장을 지원하는 경우 볼륨 및 테이프 장치의 가용성

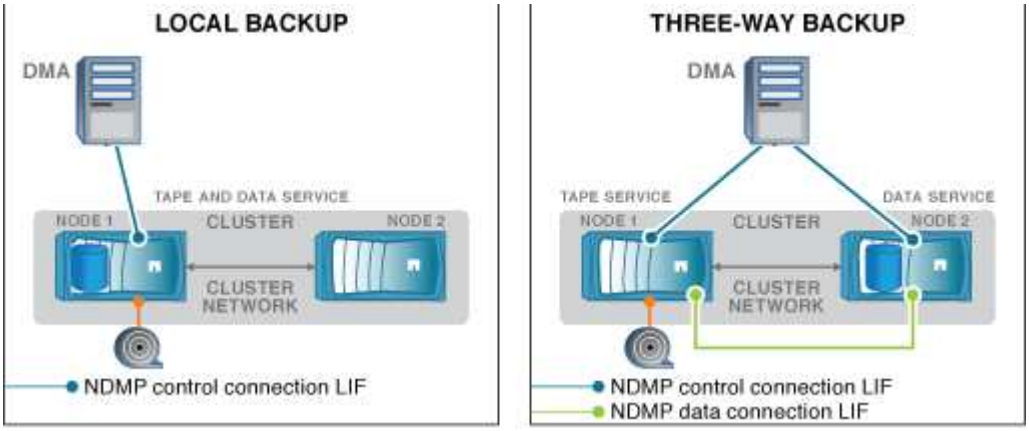
NDMP 제어 연결 **LIF** 유형입니다	백업 또는 복원에 사용할 수 있는 볼륨입니다	백업 또는 복원에 사용할 수 있는 테이프 디바이스입니다
노드 관리 LIF	노드에서 호스팅하는 모든 볼륨	노드 관리 LIF를 호스팅하는 노드에 연결된 테이프 디바이스입니다
데이터 LIF	데이터 LIF를 호스팅하는 SVM에 속한 모든 볼륨	없음
클러스터 관리 LIF	클러스터의 모든 볼륨	클러스터의 모든 테이프 디바이스
인터클러스터 LIF	클러스터의 모든 볼륨	클러스터의 모든 테이프 디바이스

ONTAP NDMP에 대한 친화성 정보에 대해 알아보세요

백업 애플리케이션이 CAB을 인식하면 NDMP 서버가 볼륨 및 테이프 디바이스에 대한 고유한 위치 정보를 제공합니다. 볼륨과 테이프 디바이스가 동일한 선호도를 공유하는 경우 이러한 선호도 정보를 사용하여 백업 애플리케이션이 3방향 백업 대신 로컬 백업을 수행할 수 있습니다.

노드 관리 LIF, 클러스터 관리 LIF에서 NDMP 제어 연결을 설정할 경우 또는 인터클러스터 LIF에서 백업 애플리케이션에서는 선호도 정보를 사용하여 볼륨 및 테이프 장치가 동일한 노드에 있는지 확인한 다음 로컬 또는 3방향 백업 또는 복원 작업을 수행할 수 있습니다. 데이터 LIF에서 NDMP 제어 연결이 설정되면 백업 애플리케이션이 항상 3방향 백업을 수행합니다.

로컬 **NDMP** 백업 및 **3**방향 **NDMP** 백업



DMA(백업 애플리케이션)는 볼륨 및 테이프 디바이스에 대한 선호도 정보를 사용하여 클러스터의 노드 1에 있는 볼륨 및 테이프 디바이스에 대해 로컬 NDMP 백업을 수행합니다. 볼륨이 노드 1에서 노드 2로 이동하는 경우 볼륨 및 테이프 디바이스에 대한 선호도 정보가 변경됩니다. 따라서 후속 백업을 위해 DMA는 3방향 NDMP 백업 작업을 수행합니다. 이렇게 하면 볼륨이 이동되는 노드에 관계없이 볼륨에 대한 백업 정책의 연속성을 보장할 수 있습니다.

관련 정보

Cluster Aware Backup 확장의 기능

NDMP 서버는 **SVM** 범위 모드에서 보안 **ONTAP** 제어 연결을 지원합니다**.**

보안 소켓(SSL/TLS)을 통신 메커니즘으로 사용하여 DMA(Data Management Application)와 NDMP 서버 간에 보안 제어 연결을 설정할 수 있습니다. 이 SSL 통신은 서버 인증서를 기반으로 합니다. NDMP 서버는 포트 30000에서 수신 대기합니다(IANA에서 ""ndmps"" 서비스에 할당).

이 포트에서 클라이언트와의 연결을 설정한 후 서버가 클라이언트에 인증서를 제공하는 표준 SSL 핸드셰이크가 발생합니다. 클라이언트가 인증서를 수락하면 SSL 핸드셰이크가 완료됩니다. 이 프로세스가 완료되면 클라이언트와 서버 간의 모든 통신이 암호화됩니다. NDMP 프로토콜 워크플로우는 이전과 동일하게 유지됩니다. 보안 NDMP 접속에는 서버 측 인증서 인증만 필요합니다. DMA는 보안 NDMP 서비스 또는 표준 NDMP 서비스에 연결하여 연결을 설정할 수 있습니다.

기본적으로 SVM(스토리지 가상 머신)에는 보안 NDMP 서비스가 사용되지 않습니다. 'vserver services ndmp modify -vserver vserver -is -secure-control -connection -enabled [true|false]' 명령을 사용하여 지정된 SVM에서 보안 NDMP 서비스를 설정하거나 해제할 수 있습니다.

NDMP ONTAP 데이터 연결 유형

SVM(스토리지 가상 머신) 범위의 NDMP 모드에서 지원되는 NDMP 데이터 연결 유형은 NDMP 제어 연결 LIF 유형과 CAB 확장 상태에 따라 다릅니다. 이 NDMP 데이터 연결 유형은 로컬 또는 3방향 NDMP 백업 또는 복구 작업을 수행할 수 있는지 여부를 나타냅니다.

TCP 또는 TCP/IPv6 네트워크를 통해 3방향 NDMP 백업 또는 복구 작업을 수행할 수 있습니다. 다음 표에서는 NDMP 제어 연결 LIF 유형과 CAB 확장의 상태를 기반으로 하는 NDMP 데이터 연결 유형을 보여 줍니다.

백업 애플리케이션에서 **CAB** 확장을 지원하는 경우의 **NDMP** 데이터 연결 유형입니다

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
노드 관리 LIF	로컬, TCP, TCP/IPv6
데이터 LIF	TCP, TCP/IPv6
클러스터 관리 LIF	로컬, TCP, TCP/IPv6
인터클러스터 LIF	로컬, TCP, TCP/IPv6

백업 애플리케이션에서 **CAB** 확장을 지원하지 않는 경우 **NDMP** 데이터 연결 유형입니다

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
노드 관리 LIF	로컬, TCP, TCP/IPv6
데이터 LIF	TCP, TCP/IPv6
클러스터 관리 LIF	TCP, TCP/IPv6

NDMP 제어 연결 **LIF** 유형입니다	**NDMP** 데이터 연결 유형입니다
인터클러스터 LIF	로컬, TCP, TCP/IPv6

관련 정보

Cluster Aware Backup 확장의 기능

"네트워크 관리"

SVM 범위 **NDMP** 모드에서 **ONTAP** 사용자 인증

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 NDMP 사용자 인증이 역할 기반 액세스 제어와 통합됩니다. SVM 맥락에서 NDMP 사용자는 ""vsadmin" 또는 ""vsadmin-backup" 역할을 가져야 합니다. 클러스터 컨텍스트에서 NDMP 사용자는 ""admin" 또는 ""backup" 역할이 있어야 합니다.

이러한 사전 정의된 역할을 제외하고, 사용자 지정 역할과 연결된 사용자 계정은 명령 디렉토리에 ""vserver services ndmp"" 폴더가 있고 폴더의 액세스 수준이 ""none""이 아닌 경우 NDMP 인증에 사용할 수 있습니다. 이 모드에서는 역할 기반 액세스 제어를 통해 생성된 특정 사용자 계정에 대해 NDMP 암호를 생성해야 합니다. admin 또는 백업 역할의 클러스터 사용자는 노드 관리 LIF, 클러스터 관리 LIF 또는 인터클러스터 LIF에 액세스할 수 있습니다. vsadmin-backup 또는 vsadmin 역할의 사용자는 해당 SVM의 데이터 LIF에만 액세스할 수 있습니다. 따라서 사용자의 역할에 따라 백업 및 복원 작업에 사용할 수 있는 볼륨 및 테이프 디바이스의 가용성이 달라집니다.

이 모드는 NIS 및 LDAP 사용자에 대한 사용자 인증도 지원합니다. 따라서 NIS 및 LDAP 사용자는 공통 사용자 ID 및 암호를 사용하여 여러 SVM에 액세스할 수 있습니다. 그러나 NDMP 인증은 Active Directory 사용자를 지원하지 않습니다.

이 모드에서는 사용자 계정이 SSH 애플리케이션 및 ""사용자 암호" 인증 방법과 연결되어 있어야 합니다.

관련 정보

SVM 범위의 NDMP 모드를 관리하는 명령입니다

"시스템 관리"

ONTAP NDMP 사용자를 위한 **NDMP** 특정 암호 생성

SVM(스토리지 가상 시스템) 범위의 NDMP 모드에서는 특정 사용자 ID에 대한 암호를 생성해야 합니다. 생성된 암호는 NDMP 사용자의 실제 로그인 암호를 기반으로 합니다. 실제 로그인 암호가 변경되면 NDMP 관련 암호를 다시 생성해야 합니다.

단계

1. NDMP 관련 암호를 생성하려면 'vserver services ndmp generate-password' 명령을 사용하십시오.

   현재 또는 미래의 모든 NDMP 작업에서 암호 입력이 필요한 경우 이 암호를 사용할 수 있습니다.

   스토리지 가상 시스템(SVM, 이전의 Vserver)에서 해당 SVM에 속하는 사용자에 대해서만 NDMP 암호를 생성할 수 있습니다.

   다음 예에서는 사용자 ID user1에 대한 NDMP 관련 암호를 생성하는 방법을 보여 줍니다.

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

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

2. 암호를 일반 스토리지 시스템 계정으로 변경하는 경우 이 절차를 반복하여 새 NDMP 관련 암호를 가져옵니다.

ONTAP MetroCluster 구성에서 재해 복구 중에 테이프 백업 및 복원 작업이 어떻게 영향을 받는가

MetroCluster 구성에서 재해 복구 중에 테이프 백업 및 복원 작업을 동시에 수행할 수 있습니다. 재해 복구 중에 이러한 작업이 어떻게 영향을 받는지 알아야 합니다.

재해 복구 관계에서 anSVM 볼륨에서 테이프 백업 및 복원 작업을 수행하는 경우, 전환 및 스위치백 후 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.

FlexVol 볼륨의 덤프 엔진 정보

FlexVol 볼륨을 위한 **ONTAP** 덤프 엔진에 대해 알아보세요

덤프는 ONTAP의 스냅샷 기반 백업 및 복구 솔루션으로, 스냅샷에서 테이프 디바이스로 파일 및 디렉토리를 백업하고 백업된 데이터를 스토리지 시스템에 복구할 수 있도록 지원합니다.

덤프 백업을 사용하여 디렉토리, 파일 및 관련 보안 설정과 같은 파일 시스템 데이터를 테이프 디바이스에 백업할 수 있습니다. 전체 볼륨, 전체 qtree 또는 전체 볼륨 또는 전체 qtree가 아닌 하위 트리를 백업할 수 있습니다.

NDMP 호환 백업 애플리케이션을 사용하여 덤프 백업 또는 복구를 수행할 수 있습니다.

덤프 백업을 수행할 때 백업에 사용할 스냅샷을 지정할 수 있습니다. 백업에 대한 스냅샷을 지정하지 않으면 덤프 엔진이 백업에 대한 스냅샷을 생성합니다. 백업 작업이 완료되면 덤프 엔진이 이 스냅샷을 삭제합니다.

덤프 엔진을 사용하여 레벨 0, 증분 또는 차등 백업을 테이프에 수행할 수 있습니다.

Data ONTAP 8.3 이전의 릴리즈로 되돌린 후에는 증분 백업 작업을 수행하기 전에 기본 백업 작업을 수행해야 합니다.

관련 정보

"업그레이드, 되돌리기 또는 다운그레이드를 수행할 수 있습니다"

ONTAP NDMP를 사용한 덤프 백업 작동 방식

덤프 백업은 미리 정의된 프로세스를 사용하여 파일 시스템 데이터를 디스크에서 테이프로 씁니다. 볼륨, qtree 또는 전체 볼륨이나 qtree가 아닌 하위 트리를 백업할 수 있습니다.

다음 표에서는 ONTAP에서 덤프 경로로 표시된 개체를 백업하는 데 사용하는 프로세스를 설명합니다.

단계	조치
1	전체 볼륨 또는 전체 qtree 백업보다 작은 경우 ONTAP에서는 백업할 파일을 식별하기 위해 디렉토리를 통과합니다. 전체 볼륨 또는 qtree를 백업하는 경우 ONTAP는 이 단계를 2단계와 결합합니다.
2	전체 볼륨 또는 전체 qtree 백업의 경우 ONTAP는 백업할 볼륨 또는 qtree의 디렉토리를 식별합니다.
3	ONTAP는 디렉토리를 테이프에 기록합니다.
4	ONTAP는 파일을 테이프에 씁니다.
5	ONTAP는 ACL 정보(해당되는 경우)를 테이프에 기록합니다.

덤프 백업에서는 백업에 데이터 스냅샷을 사용합니다. 따라서 백업을 시작하기 전에 볼륨을 오프라인으로 전환할 필요가 없습니다.

덤프 백업은 생성하는 각 스냅샷의 이름을 `snapshot_for_backup.n` 지정합니다. 여기서 는 0부터 시작하는 정수입니다. `n` 덤프 백업이 스냅샷을 생성할 때마다 정수를 1씩 증가시킵니다. 스토리지 시스템이 재부팅되면 정수가 0으로 재설정됩니다. 백업 작업이 완료되면 덤프 엔진이 이 스냅샷을 삭제합니다.

ONTAP에서 동시에 여러 덤프 백업을 수행하면 덤프 엔진이 여러 개의 스냅샷을 생성합니다. 예를 들어 ONTAP에서 두 개의 덤프 백업을 동시에 실행하는 경우 데이터가 백업되는 볼륨에서 다음 스냅샷을 찾을 수 있습니다. `snapshot_for_backup.0` `snapshot_for_backup.1`

스냅샷에서 백업하는 경우 덤프 엔진은 추가 스냅샷을 생성하지 않습니다.

덤프 엔진이 백업하는 데이터 유형입니다

덤프 엔진을 사용하여 데이터를 테이프에 백업함으로써 재해 또는 컨트롤러 중단을 방지할 수 있습니다. 덤프 엔진은 파일, 디렉토리, qtree 또는 전체 볼륨과 같은 데이터 오브젝트를 백업할 뿐 아니라 각 파일에 대한 여러 유형의 정보를 백업할 수 있습니다. 덤프 엔진이 백업할 수 있는 데이터의 유형과 고려해야 할 제한 사항을 알면 재해 복구에 대한 접근 방식을 계획하는 데 도움이 됩니다.

덤프 엔진은 파일의 데이터 백업 외에도 각 파일에 대한 다음 정보를 필요에 따라 백업할 수 있습니다.

- UNIX GID, 소유자 UID 및 파일 권한
- UNIX 액세스, 생성 및 수정 시간
- 파일 형식
- 파일 크기
- DOS 이름, DOS 속성 및 생성 시간입니다
- 1,024개의 ACE(액세스 제어 항목)가 있는 ACL(액세스 제어 목록)
- Qtree 정보
- 접합 경로

연결 경로는 심볼 링크로 백업됩니다.

- LUN 및 LUN 복제

  전체 LUN 개체를 백업할 수 있지만 LUN 개체 내에서 단일 파일을 백업할 수는 없습니다. 마찬가지로, LUN 내에 단일 파일이 아니라 전체 LUN 개체를 복원할 수 있습니다.

  덤프 엔진은 LUN 클론을 독립 LUN으로 백업합니다.

- VM 정렬 파일

  Data ONTAP 8.1.2 이전 릴리즈에서는 VM 정렬 파일의 백업이 지원되지 않습니다.

스냅샷 지원 LUN 클론이 7-Mode에서 작동하는 Data ONTAP에서 ONTAP로 전환되면 일관성 없는 LUN이 됩니다. 덤프 엔진이 일관성 없는 LUN을 백업하지 않습니다.

볼륨에 데이터를 복구할 때는 복구 중인 LUN에서 클라이언트 입출력이 제한됩니다. LUN 제한은 덤프 복원 작업이 완료된 경우에만 제거됩니다. 마찬가지로, SnapMirror 단일 파일 또는 LUN 복원 작업 중에 클라이언트 I/O는 복원 중인 파일 및 LUN 모두에서 제한됩니다. 이 제한은 단일 파일 또는 LUN 복원 작업이 완료된 경우에만 제거됩니다. 덤프 복원 또는 SnapMirror 단일 파일 또는 LUN 복원 작업이 수행되고 있는 볼륨에서 덤프 백업을 수행하는 경우 클라이언트 I/O 제한이 있는 파일 또는 LUN은 백업에 포함되지 않습니다. 이러한 파일 또는 LUN은 클라이언트 입출력 제한이 제거된 경우 이후의 백업 작업에 포함됩니다.

Data ONTAP 8.3에서 실행 중이며 테이프에 백업된 LUN은 이전 릴리즈가 아닌 8.3 이상 릴리즈로만 복원할 수 있습니다. LUN이 이전 릴리즈로 복원되면 LUN이 파일로 복원됩니다.

SnapVault 보조 볼륨 또는 볼륨 SnapMirror 대상을 테이프에 백업하는 경우 볼륨의 데이터만 백업됩니다. 연결된 메타데이터는 백업되지 않습니다. 따라서 볼륨을 복원하려고 하면 해당 볼륨의 데이터만 복원됩니다. volume SnapMirror 관계에 대한 정보는 백업에서 제공되지 않으므로 복원되지 않습니다.

Windows NT 권한만 있는 파일을 덤프하고 UNIX 스타일 qtree 또는 볼륨으로 복원하면 해당 qtree 또는 볼륨에 대한 기본 UNIX 권한이 파일에 부여됩니다.

UNIX 사용 권한만 있는 파일을 덤프하고 NTFS 스타일 qtree 또는 볼륨으로 복원하면 해당 qtree 또는 볼륨에 대한 기본 Windows 사용 권한이 파일에 부여됩니다.

다른 덤프 및 복원으로 사용 권한이 보존됩니다.

VM 정렬 파일과 'VM 정렬 섹터' 옵션을 백업할 수 있습니다. VM 정렬 파일에 대한 자세한 내용은 을 참조하십시오 "논리적 스토리지 관리".

증가 체인과 **ONTAP NDMP**에 대해 알아보세요

증분 체인은 동일한 경로의 일련의 증분 백업입니다. 언제든지 백업 레벨을 지정할 수 있으므로 백업 및 복원을 효과적으로 수행할 수 있도록 증분 체인을 이해해야 합니다. 31가지 레벨의 증분 백업 작업을 수행할 수 있습니다.

증분 체인에는 두 가지 유형이 있습니다.

- 연속 증분 체인으로, 레벨 0부터 시작하여 각 후속 백업에서 1씩 상승하는 증분 백업의 시퀀스입니다.

- 증분 백업이 레벨을 건너뛰거나 0, 2, 3, 1, 2, 3, 1 등의 레벨이 시퀀스를 벗어난 경우 연속되지 않은 증분 체인입니다. 4 또는 0, 1, 1, 1 또는 0, 1, 2, 1, 2.

증분 백업은 가장 최근의 하위 레벨 백업을 기반으로 합니다. 예를 들어 백업 레벨 0, 2, 3, 1, 4의 시퀀스는 0, 2, 3 및 0, 1, 4의 두 증분 체인을 제공합니다. 다음 표에는 증분 백업의 기반이 정리되어 있습니다.

백업 순서	증분 수준	체인 증분	베이스	파일이 백업되었습니다
1	0	둘 다 해당되며	스토리지 시스템의 파일입니다	백업 경로에 있는 모든 파일
2	2	0, 2, 3	레벨 0 백업	레벨 0 백업 이후에 생성된 백업 경로의 파일입니다
3	3	0, 2, 3	레벨 2 백업	레벨 2 백업 이후에 생성된 백업 경로의 파일입니다
4	1	0, 1, 4	레벨 0 백업입니다. 레벨 1 백업보다 낮은 최신 레벨이기 때문입니다	레벨 0 백업 이후에 생성된 백업 경로의 파일(레벨 2 및 레벨 3 백업에 있는 파일 포함)입니다
5	4	0, 1, 4	레벨 1 백업은 하위 레벨이고 레벨 0, 레벨 2 또는 레벨 3 백업보다 최신이므로 레벨 1 백업입니다	레벨 1 백업 이후에 생성된 파일

차단 요소와 **ONTAP NDMP**에 대해 알아보세요

테이프 블록은 1,024바이트의 데이터입니다. 테이프 백업 또는 복원 중에 각 읽기/쓰기 작업에서 전송되는 테이프 블록 수를 지정할 수 있습니다. 이 수를 _blocking factor_라고 합니다.

4 ~ 256의 차단 계수를 사용할 수 있습니다. 백업을 수행하는 시스템 이외의 시스템에 백업을 복원하려는 경우 복원 시스템은 백업에 사용한 차단 계수를 지원해야 합니다. 예를 들어, 차단 계수 128을 사용하는 경우 해당 백업을 복원하는 시스템은 차단 계수 128을 지원해야 합니다.

NDMP 백업 중에 mover_record_size가 차단 계수를 결정합니다. ONTAP에서는 mover_record_size에 대해 최대 256KB의 값을 허용합니다.

ONTAP 덤프 백업을 다시 시작해야 하는 경우

테이프 쓰기 오류, 정전, 실수로 인한 사용자 중단 또는 스토리지 시스템의 내부 불일치 등과 같은 내부 또는 외부 오류로 인해 덤프 백업이 완료되지 않는 경우가 있습니다. 이러한 이유 중 하나로 인해 백업이 실패할 경우 백업을 다시 시작할 수 있습니다.

스토리지 시스템에서 트래픽이 많지 않은 기간을 피하거나 테이프 드라이브와 같은 스토리지 시스템의 다른 제한된 리소스에 대한 경쟁 방지를 위해 백업을 중단 및 재시작할 수 있습니다. 보다 긴급한 복원(또는 백업)에 동일한 테이프 드라이브가 필요한 경우 긴 백업을 중단하고 나중에 다시 시작할 수 있습니다. 재시작 가능한 백업은 재부팅 후에도 유지됩니다. 다음 조건이 참인 경우에만 중단된 테이프 백업을 다시 시작할 수 있습니다.

- 중단된 백업은 단계 IV에 있습니다
- dump 명령으로 잠긴 모든 관련 스냅샷을 사용할 수 있습니다.
- 파일 기록을 활성화해야 합니다.

이러한 덤프 작업이 중단되고 재시작 가능한 상태로 유지되면 연결된 스냅샷이 잠깁니다. 이러한 스냅샷은 백업 컨텍스트가 삭제된 후에 해제됩니다. 명령을 사용하여 백업 컨텍스트 목록을 볼 수 `vserver services ndmp restartable backup show` 있습니다.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                        Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Auto-created?: true
                   Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                   Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

ONTAP NDMP를 사용한 덤프 복원 작동 방식

덤프 복구는 미리 정의된 프로세스를 사용하여 파일 시스템 데이터를 테이프에서 디스크로 씁니다.

다음 표의 프로세스는 덤프 복구가 작동하는 방식을 보여 줍니다.

단계	조치
1	ONTAP는 테이프에서 추출해야 하는 파일을 카탈로그로 작성합니다.
2	ONTAP는 디렉토리와 빈 파일을 생성합니다.
3	ONTAP는 테이프에서 파일을 읽고 이를 디스크에 쓴 다음 해당 테이프에 대한 사용 권한(ACL 포함)을 설정합니다.
4	ONTAP는 지정된 모든 파일이 테이프에서 복사될 때까지 2단계와 3단계를 반복합니다.

덤프 엔진이 복원하는 데이터의 유형입니다

재해 또는 컨트롤러 중단이 발생할 경우 덤프 엔진은 단일 파일에서 파일 속성, 전체 디렉토리에 이르기까지 백업한 모든 데이터를 여러 가지 방법으로 복구할 수 있습니다. 덤프 엔진이 복구할 수 있는 데이터의 유형과 복구 방법을 언제 사용해야 다운타임을 최소화할 수 있는지 알고 있습니다.

데이터를 온라인 매핑된 LUN에 복원할 수 있습니다. 그러나 복구 작업이 완료될 때까지 호스트 애플리케이션이 이 LUN에 액세스할 수 없습니다. 복구 작업이 완료된 후 LUN 데이터의 호스트 캐시를 플러시하여 복구된 데이터에 대한 일관성을 제공해야 합니다.

덤프 엔진은 다음 데이터를 복구할 수 있습니다.

- 파일 및 디렉토리의 컨텐츠
- UNIX 파일 권한
- ACL

  NTFS qtree 또는 볼륨에 대한 UNIX 파일 권한만 있는 파일을 복원하는 경우 파일에 Windows NT ACL이 없습니다. 스토리지 시스템은 Windows NT ACL을 생성할 때까지 이 파일에 대한 UNIX 파일 권한만 사용합니다.

  Data ONTAP 8.2를 실행하는 스토리지 시스템에서 백업된 ACL을 ACE 제한이 1,024 이하인 Data ONTAP 8.1.x 및 이전 버전의 스토리지 시스템으로 복원하는 경우 기본 ACL이 복원됩니다.

- Qtree 정보

  qtree 정보는 qtree가 볼륨의 루트에 복원되는 경우에만 사용됩니다. Qtree 정보는 "/vs1/vol1/subdir/lowerdir" 같은 하위 디렉토리로 qtree가 복원되고 qtree가 아닌 경우 사용되지 않습니다.

- 다른 모든 파일 및 디렉토리 속성
- Windows NT 스트림
- LUN을 클릭합니다

◦ LUN을 LUN으로 유지하려면 볼륨 레벨 또는 qtree 레벨로 복원해야 합니다.

디렉터리에 복원되면 유효한 메타데이터가 없기 때문에 파일로 복원됩니다.

◦ 7-Mode LUN은 ONTAP 볼륨에서 LUN으로 복구됩니다.

- 7-Mode 볼륨을 ONTAP 볼륨으로 복원할 수 있습니다.
- 대상 볼륨에 복원된 VM 정렬 파일은 대상 볼륨의 VM 정렬 속성을 상속합니다.
- 복구 작업의 대상 볼륨에 필수 잠금 또는 권장 잠금이 있는 파일이 있을 수 있습니다.

이러한 대상 볼륨에 대한 복구 작업을 수행하는 동안 덤프 엔진은 이러한 잠금을 무시합니다.

ONTAP NDMP로 데이터를 복원하기 전 고려 사항

백업된 데이터를 원래 경로 또는 다른 대상으로 복원할 수 있습니다. 백업된 데이터를 다른 대상으로 복원하는 경우 복원 작업을 위한 대상을 준비해야 합니다.

데이터를 원래 경로 또는 다른 대상으로 복원하기 전에 다음 정보가 있어야 하며 다음 요구 사항을 충족해야 합니다.

- 복구 수준입니다
- 데이터를 복원할 경로입니다
- 백업 중에 사용되는 차단 요소입니다
- 증분 복원을 수행하는 경우 모든 테이프가 백업 체인에 있어야 합니다
- 복원할 테이프와 호환 및 사용 가능한 테이프 드라이브

데이터를 다른 대상으로 복원하기 전에 다음 작업을 수행해야 합니다.

- 볼륨을 복원하는 경우 새 볼륨을 만들어야 합니다.
- qtree 또는 디렉토리를 복원하는 경우, 복원 중인 파일과 이름이 같은 파일을 이동하거나 이름을 변경해야 합니다.

ONTAP 9에서는 qtree 이름이 유니코드 형식을 지원합니다. 이전 버전의 ONTAP에서는 이 형식을 지원하지 않습니다. ONTAP 9의 유니코드 이름이 있는 qtree가 'ndmpcopy' 명령을 사용하여 ONTAP의 이전 릴리즈로 복제되거나 테이프의 백업 이미지에서 복원을 통해 복사되면 qtree가 유니코드 형식이 있는 qtree가 아닌 일반 디렉토리로 복원됩니다.

복구된 파일의 이름이 기존 파일과 같으면 복구된 파일이 기존 파일을 덮어씁니다. 그러나 디렉토리는 덮어쓰지 않습니다.

DAR를 사용하지 않고 복원 중에 파일, 디렉토리 또는 qtree의 이름을 바꾸려면 추출 환경 변수를 "E"로 설정해야 합니다.

대상 스토리지 시스템의 필수 공간입니다

대상 스토리지 시스템에 복원할 데이터 양보다 약 100MB의 공간이 필요합니다.

복구 작업은 복구 작업이 시작될 때 대상 볼륨의 볼륨 공간 및 inode 가용성을 확인합니다. 강제 환경 변수를 'Y'로 설정하면 복원 작업에서 대상 경로의 볼륨 공간 및 inode 가용성 검사를 건너뜁니다. 대상 볼륨에 사용 가능한 볼륨 공간 또는 inode가 충분하지 않은 경우 복구 작업은 대상 볼륨 공간과 inode 가용성에 의해 허용되는 데이터 양을 복구합니다. 볼륨 공간 또는 inode가 더 이상 남아 있지 않으면 복구 작업이 중지됩니다.

ONTAP 덤프 백업 및 복원 세션에 대한 확장성 제한

서로 다른 시스템 메모리 용량의 스토리지 시스템에서 동시에 수행할 수 있는 최대 덤프 백업 및 복원 세션 수에 대해 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

다음 표에 나와 있는 제한은 덤프 또는 복원 엔진에 대한 것입니다. NDMP 세션의 확장성 제한에서 언급한 제한은 엔진 제한값보다 높은 NDMP 서버에 대한 것입니다.

스토리지 시스템의 시스템 메모리입니다	총 덤프 백업 및 복원 세션 수입니다
16GB 미만	4
16GB보다 크거나 같지만 24GB보다 작습니다	16
24GB보다 크거나 같습니다	32

스토리지 시스템 내에서 데이터를 복제하기 위해 'ndmpcopy' 명령을 사용하는 경우 두 개의 NDMP 세션이 설정됩니다. 하나는 덤프 백업용이고 다른 하나는 덤프 복구용으로 설정됩니다.

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

NDMP 세션의 확장성 제한

ONTAP SVM 이름과 컨텍스트 **ID**를 제공하여 재시작 가능한 컨텍스트를 삭제합니다**.**

컨텍스트를 다시 시작하지 않고 백업을 시작하려면 컨텍스트를 삭제할 수 있습니다.

이 작업에 대해

SVM 이름과 컨텍스트 ID를 제공하여 "vserver services ndmp restable-backup delete" 명령을 사용하여 재시작 가능한 컨텍스트를 삭제할 수 있습니다.

단계

1. 재시작 가능한 컨텍스트 삭제:

   '* vserver services ndmp restarable-backup delete-vserver_vserver-name_-context-id_context_identifier_*'.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

ONTAP SnapVault 보조 볼륨에서 덤프가 작동하는 방식

SnapVault 보조 볼륨에 미러링되는 데이터에 대해 테이프 백업 작업을 수행할 수 있습니다. SnapVault 보조 볼륨에 미러링되는 데이터만 테이프에 백업할 수 있고 SnapVault 관계 메타데이터는 백업할 수 없습니다.

데이터 보호 미러 관계를 중단하거나 SnapMirror 재동기화가 발생하면 항상 기본 백업을 수행해야 합니다.

관련 정보

- "SnapMirror가 깨졌습니다"

ONTAP 스토리지 장애 조치 및 **ARL** 작업에서 덤프가 작동하는 방식

덤프 백업 또는 복원 작업을 수행하기 전에 이러한 작업이 스토리지 페일오버(테이크오버 및 반환) 또는 애그리게이트 재배치(ARL) 작업과 어떻게 연동되는지 이해해야 합니다. '-override-vetoes' 옵션은 스토리지 페일오버 또는 ARL 작업 중 덤프 엔진의 동작을 결정합니다.

덤프 백업 또는 복원 작업이 실행되고 '-override-vetoes' 옵션이 'false'로 설정되어 있으면 사용자 실행 스토리지 페일오버 또는 ARL 작업이 중지됩니다. 그러나 '–override-vetoes' 옵션이 true로 설정되어 있으면 스토리지 페일오버 또는 ARL 작업이 계속되고 덤프 백업 또는 복원 작업이 중단됩니다. 스토리지 시스템에 의해 스토리지 페일오버 또는 ARL 작업이 자동으로 시작되면 활성 덤프 백업 또는 복원 작업이 항상 중단됩니다. 스토리지 페일오버 또는 ARL 작업이 완료된 후에도 덤프 백업 및 복원 작업을 다시 시작할 수 없습니다.

운전실 확장이 지원되는 경우의 덤프 작업

백업 애플리케이션이 CAB 확장을 지원하는 경우 스토리지 페일오버 또는 ARL 작업 후 백업 정책을 재구성하지 않고 증분 덤프 백업 및 복원 작업을 계속 수행할 수 있습니다.

운전실 확장이 지원되지 않을 때 덤프 작업

백업 애플리케이션이 CAB 확장을 지원하지 않는 경우 백업 정책에 구성된 LIF를 대상 애그리게이트를 호스팅하는 노드로 마이그레이션할 경우 증분 덤프 백업 및 복원 작업을 계속 수행할 수 있습니다. 그렇지 않으면 스토리지 페일오버 및 ARL 작업 후에 증분 백업 작업을 수행하기 전에 기본 백업을 수행해야 합니다.

스토리지 페일오버 작업의 경우 백업 정책에 구성된 LIF를 파트너 노드로 마이그레이션해야 합니다.

관련 정보

"고가용성"

ONTAP 볼륨 이동 시 덤프 작동 방식

스토리지 시스템에서 최종 컷오버 단계를 시도할 때까지 테이프 백업 및 복원 작업과 볼륨 이동을 병렬로 실행할 수 있습니다. 이 단계 이후에는 이동 중인 볼륨에 대해 새 테이프 백업 및 복원 작업이 허용되지 않습니다. 그러나 현재 작업은 완료될 때까지 계속 실행됩니다.

다음 표에서는 볼륨 이동 작업 후 테이프 백업 및 복원 작업의 동작에 대해 설명합니다.

에서 테이프 백업 및 복원 작업을 수행하는 경우...	그러면...
백업 애플리케이션에서 CAB 확장이 지원되는 경우 SVM(스토리지 가상 머신) 범위가 NDMP 모드임	백업 정책을 재구성하지 않고도 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.
백업 애플리케이션에서 CAB 확장을 지원하지 않는 경우 SVM 범위의 NDMP 모드입니다	백업 정책에 구성된 LIF를 대상 애그리게이트를 호스팅하는 노드로 마이그레이션할 경우, 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다. 그렇지 않으면 볼륨 이동 후 증분 백업 작업을 수행하기 전에 기본 백업을 수행해야 합니다.

볼륨 이동이 발생하는 경우, 대상 노드의 다른 SVM에 속한 볼륨의 이름이 이동한 볼륨의 이름과 동일한 경우 이동한 볼륨의 증분 백업 작업을 수행할 수 없습니다.

ONTAP FlexVol volume 가득 찼을 때 덤프가 작동하는 방식

증분 덤프 백업 작업을 수행하기 전에 FlexVol 볼륨에 충분한 여유 공간이 있는지 확인해야 합니다.

작업이 실패하면 크기를 늘리거나 스냅샷을 삭제하여 Flex Vol 볼륨의 여유 공간을 늘려야 합니다. 그런 다음 증분 백업 작업을 다시 수행합니다.

ONTAP 볼륨 액세스 유형이 변경될 때 덤프가 작동하는 방식

SnapMirror 대상 볼륨 또는 SnapVault 보조 볼륨의 상태가 읽기/쓰기에서 읽기 전용으로 또는 읽기 전용에서 읽기/쓰기로 변경되면 기본 테이프 백업 또는 복원 작업을 수행해야 합니다.

SnapMirror 타겟 및 SnapVault 보조 볼륨은 읽기 전용 볼륨입니다. 이러한 볼륨에 대해 테이프 백업 및 복원 작업을 수행할 경우 볼륨이 읽기 전용에서 읽기/쓰기 또는 읽기/쓰기에서 읽기 전용으로 상태가 변경될 때마다 기본 백업 또는 복원 작업을 수행해야 합니다.

ONTAP SnapMirror 단일 파일 또는 **LUN** 복원을 통한 덤프 작동 방식

SnapMirror 기술을 사용하여 단일 파일 또는 LUN이 복원되는 볼륨에서 덤프 백업 또는 복원 작업을 수행하기 전에 단일 파일 또는 LUN 복원 작업에서 덤프 작업이 어떻게 작동하는지 이해해야 합니다.

SnapMirror 단일 파일 또는 LUN 복원 작업 중에 클라이언트 I/O는 복원 중인 파일 또는 LUN에서 제한됩니다. 단일 파일 또는 LUN 복원 작업이 완료되면 파일 또는 LUN에 대한 입출력 제한이 제거됩니다. 단일 파일 또는 LUN이 복구되는 볼륨에서 덤프 백업을 수행하는 경우 클라이언트 I/O 제한이 있는 파일 또는 LUN은 덤프 백업에 포함되지 않습니다. 이후의 백업 작업에서는 입출력 제한이 제거된 후 이 파일 또는 LUN이 테이프로 백업됩니다.

동일한 볼륨에서 덤프 복구와 SnapMirror 단일 파일 또는 LUN 복원 작업을 동시에 수행할 수 없습니다.

ONTAP MetroCluster 구성에서 덤프 백업 및 복원 작업이 어떻게 영향을 받는가

MetroCluster 구성에서 덤프 백업 및 복원 작업을 수행하기 전에 스위치오버 또는 스위치백 작업이 수행될 때 덤프 작업이 어떻게 영향을 받는지 이해해야 합니다.

백업 또는 복구 작업을 덤프한 후 전환

클러스터 1과 클러스터 2의 두 클러스터를 고려합니다. 클러스터 1에서 덤프 백업 또는 복원 작업 중에 클러스터 1에서 클러스터 2로 전환이 시작되면 다음이 발생합니다.

- 'override-vetoes' 옵션의 값이 'false'이면 절체가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 true이면 덤프 백업 또는 복원 작업이 중단되고 전환이 계속됩니다.

백업 또는 복원 작업을 덤프한 다음 스위치백을 수행합니다

클러스터 1에서 클러스터 2로 전환이 수행되고 클러스터 2에서 덤프 백업 또는 복원 작업이 시작됩니다. 덤프 작업은 클러스터 2에 있는 볼륨을 백업 또는 복구합니다. 이 시점에서는 클러스터 2에서 클러스터 1로 스위치백을 시작한 경우 다음이 발생합니다.

- 'override-vetoes' 옵션의 값이 'false'인 경우, 스위치백을 취소하고 백업 또는 복원 작업을 계속합니다.
- 옵션 값이 true이면 백업 또는 복원 작업이 중단되고 스위치백이 계속됩니다.

스위치오버 또는 스위치백 중에 덤프 백업 또는 복원 작업이 시작되었습니다

클러스터 1에서 클러스터 2로 전환하는 동안 클러스터 1에서 덤프 백업 또는 복원 작업이 시작되면 백업 또는 복원 작업이 실패하고 전환이 계속됩니다.

클러스터 2에서 클러스터 1로 스위치백을 진행하는 동안 클러스터 2에서 덤프 백업 또는 복원 작업이 시작되면 백업

또는 복원 작업이 실패하고 스위치백을 계속합니다.

FlexVol 볼륨용 SMTape 엔진 정보

FlexVol 볼륨을 위한 ONTAP SMTape 엔진에 대해 알아보세요

SMTape는 데이터 블록을 테이프로 백업하는 ONTAP의 재해 복구 솔루션입니다. SMTape를 사용하여 테이프에 볼륨 백업을 수행할 수 있습니다. 그러나 qtree 또는 하위 트리 레벨에서 백업을 수행할 수 없습니다. SMTape는 기본 백업, 차등 백업 및 증분 백업을 지원합니다. SMTape에는 라이센스가 필요하지 않습니다.

NDMP 호환 백업 애플리케이션을 사용하여 SMTape 백업 및 복구 작업을 수행할 수 있습니다. SMTape를 선택하면 스토리지 가상 시스템(SVM) 범위 NDMP 모드에서만 백업 및 복원 작업을 수행할 수 있습니다.

> SMTape 백업 또는 복구 세션이 진행 중일 때는 되돌리기 프로세스가 지원되지 않습니다. 세션이 완료될 때까지 기다리거나 NDMP 세션을 중단해야 합니다.

SMTape를 사용하여 255개의 스냅샷을 백업할 수 있습니다. 이후 기준, 증분 또는 차등 백업의 경우 이전에 백업된 스냅샷을 삭제해야 합니다.

기준 복원을 수행하기 전에 데이터가 복원되는 볼륨은 DP 유형이어야 하며 이 볼륨은 제한된 상태여야 합니다. 성공적으로 복구되면 이 볼륨이 자동으로 온라인 상태가 됩니다. 백업을 수행한 순서대로 이 볼륨에 대해 이후의 증분 또는 차등 복원을 수행할 수 있습니다.

SMTape 백업 중 ONTAP 스냅샷 사용에 대해 알아보세요

SMTape 기준 백업 및 증분 백업 중에 스냅샷이 사용되는 방식을 이해해야 합니다. 또한 SMTape를 사용하여 백업을 수행하는 동안 유의해야 할 고려 사항도 있습니다.

기본 백업

기준 백업을 수행하는 동안 테이프에 백업할 스냅샷의 이름을 지정할 수 있습니다. 스냅샷이 지정되지 않은 경우 볼륨의 액세스 유형(읽기/쓰기 또는 읽기 전용)에 따라 스냅샷이 자동으로 생성되거나 기존 스냅샷이 사용됩니다. 백업에 대한 스냅샷을 지정하면 지정된 스냅샷보다 오래된 모든 스냅샷도 테이프에 백업됩니다.

백업에 대한 스냅샷을 지정하지 않으면 다음과 같은 현상이 발생합니다.

- 읽기/쓰기 볼륨의 경우 스냅샷이 자동으로 생성됩니다.

  새로 생성된 스냅샷과 모든 이전 스냅샷이 테이프에 백업됩니다.

- 읽기 전용 볼륨의 경우 최신 스냅샷을 포함한 모든 스냅샷이 테이프에 백업됩니다.

  백업이 시작된 후에 생성된 새 스냅샷은 백업되지 않습니다.

증분 백업

SMTape 증분 또는 차등 백업 작업의 경우 NDMP 호환 백업 애플리케이션에서 스냅샷을 생성하고 관리합니다.

증분 백업 작업을 수행하는 동안 항상 스냅샷을 지정해야 합니다. 성공적인 증분 백업 작업의 경우 이전 백업 작업(기본

또는 증분) 중에 백업된 스냅샷이 백업이 수행되는 볼륨에 있어야 합니다. 이 백업된 스냅샷을 사용하려면 백업 정책을 구성할 때 이 볼륨에 할당된 스냅샷 정책을 고려해야 합니다.

SnapMirror 대상에 대한 **SMTape** 백업 고려 사항

- 데이터 보호 미러 관계는 복제를 위해 대상 볼륨에 임시 스냅샷을 생성합니다.

  SMTape 백업에 이러한 스냅샷을 사용해서는 안 됩니다.

- 동일한 볼륨에서 SMTape 백업 작업 중에 데이터 보호 미러 관계의 대상 볼륨에서 SnapMirror 업데이트가 발생하면 SMTape에서 백업한 스냅샷은 소스 볼륨에서 삭제되지 않아야 합니다.

  백업 작업 중에 SMTape는 대상 볼륨의 스냅샷을 잠급니다. 소스 볼륨에서 해당 스냅샷이 삭제되면 후속 SnapMirror 업데이트 작업이 실패합니다.

- 증분 백업 중에는 이러한 스냅샷을 사용하지 마십시오.

ONTAP 테이프 백업 및 복원 작업을 최적화하는 **SMTape** 기능

스냅샷 백업, 증분 및 차등 백업, 복원된 볼륨에 대한 중복 제거 및 압축 기능 보존, 테이프 시딩과 같은 SMTape 기능을 사용하여 테이프 백업 및 복원 작업을 최적화할 수 있습니다.

SMTape는 다음과 같은 기능을 제공합니다.

- 재해 복구 솔루션을 제공합니다
- 증분 및 차등 백업을 지원합니다
- 스냅샷을 백업합니다
- 중복 제거된 볼륨을 백업 및 복원하고 복원된 볼륨에서 중복 제거를 유지할 수 있습니다
- 압축된 볼륨을 백업하고 복원된 볼륨의 압축을 유지합니다
- 테이프 시딩을 활성화합니다

SMTape는 4KB에서 256KB 사이의 4KB의 배수로 차단 계수를 지원합니다.

ⓘ 최대 2개의 주요 연속 ONTAP 릴리즈에서만 생성된 볼륨에 데이터를 복원할 수 있습니다.

SMTape 백업 및 복원 세션에 대한 **ONTAP** 확장성 제한

NDMP 또는 CLI(테이프 시드)를 통해 SMTape 백업 및 복원 작업을 수행하는 동안 시스템 메모리 용량이 서로 다른 스토리지 시스템에서 동시에 수행할 수 있는 SMTape 백업 및 복원 세션의 최대 수를 알고 있어야 합니다. 이 최대 개수는 스토리지 시스템의 시스템 메모리에 따라 다릅니다.

ⓘ SMTape 백업 및 복구 세션 확장성 제한은 NDMP 세션 제한 및 덤프 세션 제한과 다릅니다.

스토리지 시스템의 시스템 메모리입니다	총 **SMTape** 백업 및 복구 세션 수입니다
16GB 미만	6

스토리지 시스템의 시스템 메모리입니다	총 **SMTape** 백업 및 복구 세션 수입니다
16GB보다 크거나 같지만 24GB보다 작습니다	16
24GB보다 크거나 같습니다	32

명령(노드 쉘을 통해 사용 가능)을 사용하여 스토리지 시스템의 시스템 메모리를 확보할 수 `sysconfig -a` 있습니다. 에 대한 자세한 내용은 `sysconfig -a` "ONTAP 명령 참조입니다"을 참조하십시오.

관련 정보

- NDMP 세션의 확장성 제한
- 덤프 백업 및 복원 세션에 대한 확장성 제한

ONTAP 테이프 시딩에 대해 알아보세요

테이프 시딩은 데이터 보호 미러 관계에서 대상 FlexVol 볼륨을 초기화하는 데 도움이 되는 SMTape 기능입니다.

테이프 시딩을 사용하면 낮은 대역폭 연결을 통해 소스 시스템과 대상 시스템 간에 데이터 보호 미러 관계를 설정할 수 있습니다.

낮은 대역폭 연결을 통해 소스에서 대상으로 스냅샷을 증분 미러링할 수 있습니다. 그러나 기본 스냅샷의 초기 미러링은 저대역폭 연결보다 시간이 오래 걸립니다. 이 경우 소스 볼륨의 SMTape 백업을 테이프에 수행하고 테이프를 사용하여 초기 기본 스냅샷을 대상으로 전송할 수 있습니다. 그런 다음 낮은 대역폭 연결을 사용하여 대상 시스템에 대한 증분 SnapMirror 업데이트를 설정할 수 있습니다.

SMTape가 **ONTAP** 스토리지 장애 조치 및 **ARL** 작업과 함께 작동하는 방식

SMTape 백업 또는 복원 작업을 수행하기 전에 이러한 작업이 스토리지 페일오버(테이크오버 및 반환) 또는 애그리게이트 재배치(ARL) 작업에서 어떻게 작동하는지 이해해야 합니다. '-override-vetoes' 옵션은 스토리지 페일오버 또는 ARL 작업 중 SMTape 엔진의 동작을 결정합니다.

SMTape 백업 또는 복원 작업이 실행 중이고 '-override-vetoes' 옵션이 'false'로 설정되어 있으면 사용자 시작 스토리지 페일오버 또는 ARL 작업이 중지되고 백업 또는 복원 작업이 완료됩니다. 백업 애플리케이션이 CAB 확장을 지원하는 경우 백업 정책을 재구성하지 않고 증분 SMTape 백업 및 복원 작업을 계속 수행할 수 있습니다. 그러나 '–override-vetoes' 옵션이 "true"로 설정되어 있으면 스토리지 페일오버 또는 ARL 작업이 계속되고 SMTape 백업 또는 복원 작업이 중단됩니다.

관련 정보

"네트워크 관리"

"고가용성"

SMTape가 **ONTAP** 볼륨 이동과 함께 작동하는 방식

SMTape 백업 작업 및 볼륨 이동 작업은 스토리지 시스템이 최종 컷오버 단계를 시도할 때까지 병렬로 실행될 수 있습니다. 이 단계 이후에는 이동 중인 볼륨에서 새 SMTape 백업 작업을 실행할 수 없습니다. 그러나 현재 작업은 완료될 때까지 계속 실행됩니다.

볼륨의 컷오버 단계를 시작하기 전에 볼륨 이동 작업은 동일한 볼륨에서 활성 SMTape 백업 작업을 확인합니다. 활성 SMTape 백업 작업이 있는 경우 볼륨 이동 작업이 컷오버 지연 상태로 이동하고 SMTape 백업 작업을 완료할 수 있습니다. 이러한 백업 작업이 완료되면 볼륨 이동 작업을 수동으로 다시 시작해야 합니다.

백업 애플리케이션이 CAB 확장을 지원하는 경우 백업 정책을 재구성하지 않고도 읽기/쓰기 및 읽기 전용 볼륨에서 증분 테이프 백업 및 복원 작업을 계속 수행할 수 있습니다.

기본 복원 및 볼륨 이동 작업은 동시에 수행할 수 없지만 볼륨 이동 작업과 병행하여 증분 복원을 실행할 수 있으며, 볼륨 이동 작업 중에 SMTape 백업 작업과 유사한 동작을 수행할 수 있습니다.

SMTape가 **ONTAP** 볼륨 재호스트 작업과 함께 작동하는 방식

볼륨에서 볼륨 재호스트 작업이 진행 중인 경우 SMTape 작업을 시작할 수 없습니다. 볼륨이 볼륨 재호스트 작업에 관련되어 있는 경우 해당 볼륨에서 SMTape 세션을 시작하지 않아야 합니다.

볼륨 재호스트 작업이 진행 중인 경우 SMTape 백업 또는 복구가 실패합니다. SMTape 백업 또는 복구가 진행 중인 경우 볼륨 재호스트 작업이 실패하고 적절한 오류 메시지가 표시됩니다. 이 조건은 NDMP 기반 백업 및 CLI 기반 백업 또는 복구 작업에 모두 적용됩니다.

ADB 동안 **ONTAP NDMP** 백업 정책이 어떻게 영향을 받는가

ADB(자동 데이터 밸런서)가 활성화되면 밸런서는 애그리게이트의 사용 통계를 분석하여 구성된 상위 임계값 사용 비율을 초과한 애그리게이트를 식별합니다.

임계값을 초과한 애그리게이트를 식별한 후, 밸런서는 클러스터의 다른 노드에 있는 애그리게이트로 이동할 수 있는 볼륨을 식별하고 해당 볼륨을 이동하려고 시도합니다. 이 상황은 DMA(Data Management Application)가 CAB을 인식하지 못하는 경우 사용자가 백업 정책을 다시 구성하고 기본 백업 작업을 실행해야 하기 때문에 이 볼륨에 대해 구성된 백업 정책에 영향을 줍니다.

DMA가 CAB을 인식하며 특정 인터페이스를 사용하여 백업 정책을 구성한 경우 ADB는 영향을 받지 않습니다.

ONTAP MetroCluster 구성에서 **SMTape** 백업 및 복원 작업이 어떻게 영향을 받는지

MetroCluster 구성에서 SMTape 백업 및 복원 작업을 수행하기 전에 전환 또는 스위치백 작업이 수행될 때 SMTape 작업이 어떤 영향을 받는지 알아야 합니다.

SMTape 백업 또는 복원 작업 후 전환

클러스터 1과 클러스터 2의 두 클러스터를 고려합니다. 클러스터 1에서 SMTape 백업 또는 복원 작업 중에 클러스터 1에서 클러스터 2로 전환을 시작하는 경우 다음이 발생합니다.

- '–override-vetoes' 옵션의 값이 false이면 전환 프로세스가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 "true"이면 SMTape 백업 또는 복구 작업이 중단되고 전환 프로세스가 계속됩니다.

SMTape 백업 또는 복원 작업 후 스위치백

클러스터 1에서 클러스터 2로 전환이 수행되고 클러스터 2에서 SMTape 백업 또는 복원 작업이 시작됩니다. SMTape 작업은 클러스터 2에 있는 볼륨을 백업 또는 복구합니다. 이 시점에서는 클러스터 2에서 클러스터 1로 스위치백을

시작한 경우 다음이 발생합니다.

- '–override-vetoes' 옵션의 값이 false이면 스위치백 프로세스가 중단되고 백업 또는 복원 작업이 계속됩니다.
- 옵션 값이 true이면 백업 또는 복원 작업이 중단되고 스위치백 프로세스가 계속됩니다.

전환 또는 스위치백 중에 **SMTape** 백업 또는 복원 작업이 시작되었습니다

클러스터 1에서 클러스터 2로 전환 프로세스 중에 클러스터 1에서 SMTape 백업 또는 복원 작업이 시작되면 백업 또는 복원 작업이 실패하고 전환이 계속됩니다.

클러스터 2에서 클러스터 1로 스위치백 프로세스 중에 클러스터 2에서 SMTape 백업 또는 복원 작업이 시작되는 경우 백업 또는 복원 작업이 실패하고 스위치백을 계속합니다.

FlexVol 볼륨에 대한 테이프 백업 및 복원 작업을 모니터링합니다

FlexVol 볼륨에 대한 **ONTAP** 테이프 백업 및 복원 작업 모니터링

이벤트 로그 파일을 보고 테이프 백업 및 복구 작업을 모니터링할 수 있습니다. ONTAP는 중요한 백업 및 복원 이벤트와 해당 이벤트가 발생한 시간을 컨트롤러의 '/etc/log/' 디렉토리에 있는 'backup'이라는 로그 파일에 자동으로 기록합니다. 기본적으로 이벤트 로깅은 "on"으로 설정됩니다.

다음과 같은 이유로 이벤트 로그 파일을 볼 수 있습니다.

- 야간 백업이 성공했는지 확인 중입니다
- 백업 작업에 대한 통계를 수집하는 중입니다
- 이전 이벤트 로그 파일의 정보를 사용하여 백업 및 복원 작업의 문제를 진단하는 데 사용됩니다

매주 한 번씩 이벤트 로그 파일이 회전합니다. '/etc/log/backup' 파일의 이름이 '/etc/log/backup.0'으로 바뀌고, '/etc/log/backup.0' 파일의 이름이 '/etc/log/backup.1'로 변경됩니다. 시스템은 로그 파일을 최대 6주 동안 저장하므로 최대 7개의 메시지 파일('/etc/log/backup.[0-5]' 및 현재 '/etc/log/backup' 파일)을 가질 수 있습니다.

테이프 백업 및 복원 작업을 위해 **ONTAP** 이벤트 로그 파일에 액세스합니다**.**

notes지옥의 'rdfile' 명령을 사용하여 '/etc/log/' 디렉토리에서 테이프 백업 및 복구 작업을 위한 이벤트 로그 파일에 액세스할 수 있습니다. 이러한 이벤트 로그 파일을 보고 테이프 백업 및 복원 작업을 모니터링할 수 있습니다.

이 작업에 대해

'pi' 웹 서비스를 이용할 수 있는 액세스 제어 역할 또는 'http' 액세스 방식으로 설정된 사용자 계정 등의 추가 구성을 통해 웹 브라우저를 사용하여 이러한 로그 파일에 액세스할 수도 있습니다.

단계

1. 노드 쉘에 액세스하려면 다음 명령을 입력합니다.

   ' * node run-node_node_name_ * '

   node_name은 노드의 이름입니다.

2. 테이프 백업 및 복원 작업을 위해 이벤트 로그 파일에 액세스하려면 다음 명령을 입력합니다.

   '* rdfile /etc/log/backup * '

관련 정보

"시스템 관리"

덤프 및 복원 이벤트 로그 메시지 형식은 무엇입니까

ONTAP 덤프 및 복원 이벤트 로그 메시지 형식

각 덤프 및 복원 이벤트에 대해 백업 로그 파일에 메시지가 기록됩니다.

덤프 및 복원 이벤트 로그 메시지의 형식은 다음과 같습니다.

'_TYPE TIMESTAMP IDENTIFIER EVENT (EVENT_INFO) _'

다음 목록에서는 이벤트 로그 메시지 형식의 필드를 설명합니다.

- 각 로그 메시지는 다음 표에 설명된 유형 표시기 중 하나로 시작됩니다.

유형	설명
로그	이벤트를 로깅하는 중입니다
DMP	덤프 이벤트
RST	복원 이벤트

- 타임 스탬프는 이벤트의 날짜와 시간을 표시합니다.
- 덤프 이벤트의 식별자 필드에는 덤프 경로와 덤프의 고유 ID가 포함됩니다. 복구 이벤트의 '식별자' 필드는 복구 대상 경로 이름만 고유 식별자로 사용합니다. 로깅 관련 이벤트 메시지에는 '식별자' 필드가 포함되지 않습니다.

ONTAP 로깅 이벤트에 대해 알아보세요

로그로 시작하는 메시지의 이벤트 필드는 로깅 시작 또는 로깅 종료를 지정합니다.

다음 표에 나와 있는 이벤트 중 하나가 포함되어 있습니다.

이벤트	설명
Start_Logging(로깅 시작)	로깅의 시작 또는 비활성화된 후 로깅이 다시 설정되었음을 나타냅니다.
Stop_Logging(로깅 중지)	로깅이 해제되었음을 나타냅니다.

ONTAP 덤프 이벤트에 대해 알아보세요

덤프 이벤트의 이벤트 필드에는 이벤트 유형 다음에 괄호 안에 이벤트 관련 정보가 표시됩니다.

다음 표에서는 덤프 작업에 대해 기록될 수 있는 이벤트, 설명 및 관련 이벤트 정보를 설명합니다.

이벤트	설명	이벤트 정보
시작	NDMP 덤프가 시작되었습니다	덤프 레벨과 덤프 유형입니다
끝	덤프가 성공적으로 완료되었습니다	처리된 데이터의 양입니다
중단	작업이 취소됩니다	처리된 데이터의 양입니다
옵션	지정된 옵션이 나열됩니다	NDMP 옵션을 포함한 모든 옵션과 관련 값
tape_open 을 참조하십시오	테이프가 읽기/쓰기를 위해 열려 있습니다	새 테이프 디바이스 이름입니다
테이프_닫기	읽기/쓰기를 위해 테이프가 닫혀 있습니다	테이프 디바이스 이름입니다
변경 단계	덤프가 새 처리 단계로 들어가고 있습니다	새 단계 이름입니다
오류	덤프에 예기치 않은 이벤트가 발생했습니다	오류 메시지
스냅샷	스냅샷이 생성되거나 배치됩니다	스냅샷의 이름과 시간입니다
base_dump입니다	내부 메타파일의 기본 덤프 항목이 있습니다	기본 덤프의 레벨 및 시간(증분 덤프에만 해당)

ONTAP 복원 이벤트에 대해 알아보세요

복원 이벤트의 이벤트 필드에는 이벤트 유형 다음에 이벤트 관련 정보가 괄호 안에 표시됩니다.

다음 표에서는 복구 작업을 위해 기록할 수 있는 이벤트, 설명 및 관련 이벤트 정보에 대한 정보를 제공합니다.

이벤트	설명	이벤트 정보
시작	NDMP 복구가 시작되었습니다	복구 레벨 및 복구 유형
끝	복원이 성공적으로 완료되었습니다	처리된 파일 수 및 데이터 양
중단	작업이 취소됩니다	처리된 파일 수 및 데이터 양

이벤트	설명	이벤트 정보
옵션	지정된 옵션이 나열됩니다	NDMP 옵션을 포함한 모든 옵션과 관련 값
tape_open 을 참조하십시오	테이프가 읽기/쓰기를 위해 열려 있습니다	새 테이프 디바이스 이름입니다
테이프_닫기	읽기/쓰기를 위해 테이프가 닫혀 있습니다	테이프 디바이스 이름입니다
변경 단계	복원이 새 처리 단계로 들어가고 있습니다	새 단계 이름입니다
오류	복원에서 예기치 않은 이벤트가 발생합니다	오류 메시지

ONTAP 테이프 백업 및 복원 작업에 대한 이벤트 로깅 활성화 또는 비활성화

이벤트 로깅을 설정하거나 해제할 수 있습니다.

단계

1. 이벤트 로깅을 사용하거나 사용하지 않도록 설정하려면 클러스터 쉘에서 다음 명령을 입력합니다.

   '* options_-option_name_backup.log.enable_-option-value_{on|off} *'

   On은 이벤트 로깅을 켭니다.

   OFF는 이벤트 로깅을 해제합니다.

   이벤트 로깅은 기본적으로 설정되어 있습니다.

FlexVol 볼륨의 테이프 백업 및 복원에 대한 오류 메시지입니다

백업 및 복원 오류 메시지

리소스 제한**:** 사용 가능한 스레드가 없습니다

- * 메시지 *

  자원 제한: 사용 가능한 스레드가 없습니다

- * 원인 *

  현재 사용 중인 최대 활성 로컬 테이프 입출력 스레드 수입니다. 최대 16개의 활성 로컬 테이프 드라이브를 사용할 수 있습니다.

- * 시정 조치 *

새 백업 또는 복원 작업을 시작하기 전에 일부 테이프 작업이 완료될 때까지 기다립니다.

테이프 예약이 사전 비어 있습니다

- * 메시지 *

  테이프 예약이 전제되었습니다

- * 원인 *

  테이프 드라이브가 다른 작업에서 사용 중이거나 테이프가 너무 일찍 닫혔습니다.

- * 시정 조치 *

  테이프 드라이브를 다른 작업에서 사용하고 있지 않은지, DMA 응용 프로그램이 작업을 중지하지 않았는지 확인한 다음 다시 시도하십시오.

미디어를 초기화할 수 없습니다

- * 메시지 *

  미디어를 초기화할 수 없습니다

- * 원인 *

  다음 이유 중 하나로 인해 이 오류가 발생할 수 있습니다.

  ◦ 백업에 사용된 테이프 드라이브가 손상되었거나 손상되었습니다.
  ◦ 테이프에 전체 백업이 포함되어 있지 않거나 손상되었습니다.
  ◦ 현재 사용 중인 최대 활성 로컬 테이프 입출력 스레드 수입니다.

  최대 16개의 활성 로컬 테이프 드라이브를 사용할 수 있습니다.

- * 시정 조치 *
  ◦ 테이프 드라이브가 손상되었거나 손상된 경우 유효한 테이프 드라이브로 작업을 재시도하십시오.
  ◦ 테이프에 전체 백업이 포함되어 있지 않거나 손상된 경우 복구 작업을 수행할 수 없습니다.
  ◦ 테이프 리소스를 사용할 수 없는 경우 일부 백업 또는 복구 작업이 완료될 때까지 기다린 다음 작업을 다시 시도하십시오.

진행 중인 최대 허용 덤프 또는 복원 수(최대 세션 제한)

- * 메시지 *

  허용되는 덤프 또는 복원 횟수 중 최대값 _ (최대 세션 제한) _ 이(가) 진행 중입니다

- * 원인 *

  최대 백업 또는 복원 작업 수가 이미 실행 중입니다.

- * 시정 조치 *

  현재 실행 중인 일부 작업이 완료된 후 작업을 재시도하십시오.

테이프 쓰기의 미디어 오류입니다

- * 메시지 *

  테이프 쓰기의 미디어 오류

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업 작업을 다시 시도하십시오.

테이프 쓰기에 실패했습니다

- * 메시지 *

  테이프 쓰기가 실패했습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업 작업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프에 미디어 오류가 발생했습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프에 미디어 오류가 발생했습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프가 파손되었거나 쓰기 보호되어 있습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프가 파손되었거나 쓰기 보호되어 있습니다

- * 원인 *

  백업에 사용된 테이프가 손상되었거나 쓰기 보호되어 있습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 실패 - 새 테이프가 이미 미디어 끝에 있습니다

- * 메시지 *

  테이프 쓰기 실패 - 새 테이프가 이미 미디어 끝에 있습니다

- * 원인 *

  테이프에 공간이 부족하여 백업을 완료할 수 없습니다.

- * 시정 조치 *

  테이프를 교체하고 백업을 다시 시도하십시오.

테이프 쓰기 오류입니다

- * 메시지 *

  테이프 쓰기 오류 - 이전 테이프의 최소 용량(MB)이 이 이 테이프 작업의 최소 용량(MB)보다 적었습니다. 작업을 처음부터 다시 시작해야 합니다

- * 원인 *

  테이프 용량이 부족하여 백업 데이터를 포함할 수 없습니다.

- * 시정 조치 *

  용량이 큰 테이프를 사용하고 백업 작업을 재시도하십시오.

테이프 읽기에서 미디어 오류가 발생했습니다

- * 메시지 *

  '테이프 읽기에 미디어 오류'

- * 원인 *

  데이터가 복구되는 테이프가 손상되어 전체 백업 데이터가 포함되어 있지 않을 수 있습니다.

- * 시정 조치 *

  테이프에 전체 백업이 있는지 확인하려면 복구 작업을 다시 시도하십시오. 테이프에 전체 백업이 포함되어 있지 않으면 복구 작업을 수행할 수 없습니다.

테이프 읽기 오류입니다

- * 메시지 *

  "테이프 읽기 오류"

- * 원인 *

  테이프 드라이브가 손상되었거나 테이프에 전체 백업이 포함되어 있지 않습니다.

- * 시정 조치 *

  테이프 드라이브가 손상된 경우 다른 테이프 드라이브를 사용하십시오. 테이프에 전체 백업이 포함되어 있지 않으면 데이터를 복원할 수 없습니다.

이미 테이프 끝에 있습니다

- * 메시지 *

  이미 테이프 끝에 있습니다

- * 원인 *

  테이프에 데이터가 포함되어 있지 않거나 되감아야 합니다.

- * 시정 조치 *

  테이프에 데이터가 포함되어 있지 않은 경우 백업이 포함된 테이프를 사용하고 복구 작업을 다시 시도하십시오. 그렇지 않으면 테이프를 되감고 복구 작업을 다시 시도하십시오.

테이프 레코드 크기가 너무 작습니다. 더 큰 크기로 시도하십시오.

- * 메시지 *

  테이프 레코드 크기가 너무 작습니다. 더 큰 사이즈를 시도해 보세요

- * 원인 *

  복구 작업에 지정된 차단 계수가 백업 중에 사용된 차단 요소보다 작습니다.

- * 시정 조치 *

  백업 중에 지정된 것과 동일한 차단 계수를 사용합니다.

테이프 레코드 크기는 **block_size1**이 아니라 **block_size2**여야 합니다

- * 메시지 *

  테이프 레코드 크기는 block_size1이 아니라 block_size2여야 합니다

- * 원인 *

로컬 복구에 대해 지정된 차단 계수가 잘못되었습니다.

- * 시정 조치 *

  블록 크기1을 차단 요소로 사용하여 복원 작업을 재시도하십시오.

테이프 레코드 크기는 **4KB**에서 **256KB** 사이여야 합니다

- * 메시지 *

  테이프 레코드 크기는 4KB에서 256KB 사이여야 합니다

- * 원인 *

  백업 또는 복원 작업에 대해 지정된 차단 계수가 허용 범위 내에 있지 않습니다.

- * 시정 조치 *

  4KB ~ 256KB 범위의 차단 계수를 지정합니다.

NDMP 오류 메시지입니다

네트워크 통신 오류입니다

- * 메시지 *

  네트워크 통신 오류

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에 대한 통신이 실패했습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

Read Socket 의 메시지**: error_string**

- * 메시지 *

  '읽기 소켓의 메시지: error_string'

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에서 통신 복구 시 오류가 발생했습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

Write Dirnet의 메시지**: error_string**

- * 메시지 *

  '쓰기 Dirnet의 메시지: error_string'

- * 원인 *

  NDMP 3-way 연결에서 원격 테이프에 대한 백업 통신에 오류가 있습니다.

- * 시정 조치 *

  원격 Mover에 대한 네트워크 연결을 확인하십시오.

소켓 수신 **EOF**를 판독합니다

- * 메시지 *

  Read Socket Received EOF(읽기 소켓 수신 EOF)

- * 원인 *

  NDMP 3방향 연결에서 원격 테이프와 파일 끝 표시에 도달하려고 했습니다. 블록 크기가 더 큰 백업 이미지에서 3방향 복원을 시도할 수 있습니다.

- * 시정 조치 *

  올바른 블록 크기를 지정하고 복구 작업을 재시도하십시오.

ndmpd 잘못된 버전 번호**: version_number '**

- * 메시지 *

  'ndmpd 잘못된 버전 번호: version_number'

- * 원인 *

  지정된 NDMP 버전은 스토리지 시스템에서 지원되지 않습니다.

- * 시정 조치 *

  NDMP 버전 4를 지정합니다.

ndmpd 세션 **session_ID**가 활성 상태가 아닙니다

- * 메시지 *

  ndmpd session session_ID not active

- * 원인 *

  NDMP 세션이 없을 수 있습니다.

- * 시정 조치 *

  활성 NDMP 세션을 보려면 'ndmpd status' 명령을 사용합니다.

volume volume_name에 대한 **vol ref**를 가져올 수 없습니다

- * 메시지 *

  'vol_name 볼륨에 대한 vol ref를 얻을 수 없습니다.

- * 원인 *

  볼륨이 다른 작업에서 사용 중이므로 볼륨 참조를 가져올 수 없습니다.

- * 시정 조치 *

  나중에 작업을 다시 시도하십시오.

["IPv6"|"IPv4"] 제어 연결에서는 데이터 연결 유형 **["NDMP4_ADDR_TCP_IPv6"]** 이(가) 지원되지 않습니다

- * 메시지 *

  ["IPv6"|"IPv4"] 제어 연결에 대해 Data 연결 유형 ["NDMP4_ADDR_TCP_IPv6"] 지원되지 않습니다

- * 원인 *

  노드 범위 NDMP 모드에서는 설정된 NDMP 데이터 연결이 NDMP 제어 연결과 동일한 네트워크 주소 유형(IPv4 또는 IPv6)이어야 합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

데이터 수신**: CAB** 데이터 연결 준비 전제 조건 오류

- * 메시지 *

  dATA Listen: cab data connection prepare pre전제 조건 오류

- * 원인 *

  백업 애플리케이션이 NDMP 서버와 CAB 확장을 협상하고 NDMP_CAB_DATA_CONN_Prepare 및 NDMP_DATA_LECEIVE 메시지 간에 지정된 NDMP 데이터 연결 주소 유형이 일치하지 않으면 NDMP 데이터 수신 작업이 실패합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

데이터 연결**:CAB** 데이터 연결 준비 전제 조건 오류

- * 메시지 *

  "cab data connection prepare pre전제 조건 오류"

- * 원인 *

  백업 애플리케이션이 NDMP 서버와 CAB 확장을 협상하고 NDMP_CAB_DATA_CONN_Prepare 및 NDMP_DATA_CONNECT 메시지 간에 지정된 NDMP 데이터 연결 주소 유형이 일치하지 않으면 NDMP 데이터 연결이 실패합니다.

- * 시정 조치 *

  백업 애플리케이션 공급업체에 문의하십시오.

오류**:** 표시 실패**: '<**사용자 이름**>'** 사용자의 암호를 가져올 수 없습니다**.**

- * 메시지 *

  '<오류: 표시 실패: '<사용자 이름>' 사용자의 암호를 가져올 수 없습니다

- * 원인 *

  NDMP에 대한 사용자 계정 구성이 불완전합니다

- * 시정 조치 *

  사용자 계정이 SSH 액세스 방법과 연결되어 있고 인증 방법이 사용자 암호인지 확인합니다.

덤프 오류 메시지

대상 볼륨이 읽기 전용입니다

- * 메시지 *

  대상 볼륨이 읽기 전용입니다

- * 원인 *

  복구 작업이 시도되는 경로는 읽기 전용입니다.

- * 시정 조치 *

  데이터를 다른 위치로 복원해 보십시오.

타겟 **qtree**는 읽기 전용입니다

- * 메시지 *

  "대상 qtree는 읽기 전용입니다.

- * 원인 *

  복원이 시도되는 qtree는 읽기 전용입니다.

- * 시정 조치 *

  데이터를 다른 위치로 복원해 보십시오.

볼륨에 대해 일시적으로 비활성화된 덤프를 다시 시도하십시오

- * 메시지 *

  볼거리가 일시적으로 부피를 사용할 수 없게 되었습니다. 다시 시도하십시오

- * 원인 *

  NDMP 덤프 백업은 '스냅샷 중단' 또는 '스냅샷 재동기화' 작업의 일부인 SnapMirror 대상 볼륨에서 시도됩니다.

- * 시정 조치 *

  '스냅샷 미러 중단' 또는 '스냅샷 미러 재동기화' 작업이 완료될 때까지 기다린 다음 덤프 작업을 수행합니다.

> SnapMirror 대상 볼륨의 상태가 읽기/쓰기에서 읽기 전용으로 또는 읽기 전용에서 읽기/쓰기로 변경될 때마다 기본 백업을 수행해야 합니다.

관련 정보

- "SnapMirror가 깨졌습니다"
- "스냅미러 재동기화"

NFS 레이블을 인식할 수 없습니다

- * 메시지 *

  "오류: 중단 중: 덤프가 파일 시스템에서 NFS 보안 레이블을 발견했습니다.

- * 원인 *

  NFS 보안 레이블은 NFSv4.2가 활성화된 경우 ONTAP 9.9.1부터 지원됩니다. 그러나 덤프 엔진에서 NFS 보안 레이블을 현재 인식하지 않습니다. 파일, 디렉토리 또는 덤프 형식의 특수 파일에 NFS 보안 레이블이 있으면 덤프가 실패합니다.

- * 시정 조치 *

  파일 또는 디렉토리에 NFS 보안 레이블이 없는지 확인합니다.

파일이 생성되지 않았습니다

- * 메시지 *

  파일이 생성되지 않았습니다

- * 원인 *

  향상된 DAR 기능을 사용하지 않고 DAR 디렉토리 DAR을 시도했습니다.

- * 시정 조치 *

  향상된 DAR 기능을 사용하도록 설정하고 DAR를 다시 시도합니다.

file name> 파일을 복원하지 못했습니다

- * 메시지 *

  파일 이름을 복원하지 못했습니다

- * 원인 *

  대상 볼륨에 있는 LUN의 파일 이름과 동일한 파일 이름의 DAR(Direct Access Recovery)이 수행된 경우 DAR가 실패합니다.

- * 시정 조치 *

  파일의 DAR를 다시 시도하십시오.

src inode <inode number>... 에 대한 잘라내기에 실패했습니다

- * 메시지 *

  "src inode <inode number>에 대한 잘림 실패. 오류 <오류 번호>. inode를 건너뜁니다

- * 원인 *

  파일 inode는 파일이 복원될 때 삭제됩니다.

- * 시정 조치 *

  해당 볼륨을 사용하기 전에 볼륨의 복원 작업이 완료될 때까지 기다립니다.

덤프에 필요한 스냅샷을 잠글 수 없습니다

- * 메시지 *

  "덤프에 필요한 스냅샷을 잠글 수 없습니다.

- * 원인 *

  백업에 지정된 스냅샷을 사용할 수 없습니다.

- * 시정 조치 *

  다른 스냅샷을 사용하여 백업을 재시도합니다.

명령을 사용하여 `snap list` 사용 가능한 스냅샷 목록을 봅니다.

에 대한 자세한 내용은 `snap list` "ONTAP 명령 참조입니다"을 참조하십시오.

비트맵 파일을 찾을 수 없습니다

- * 메시지 *

  비트맵 파일을 찾을 수 없습니다

- * 원인 *

  백업 작업에 필요한 비트맵 파일이 삭제되었을 수 있습니다. 이 경우 백업을 다시 시작할 수 없습니다.

- * 시정 조치 *

  백업을 다시 수행합니다.

볼륨이 일시적으로 전환 상태입니다

- * 메시지 *

  용적이 과도기 상태에 있습니다

- * 원인 *

  백업되는 볼륨이 일시적으로 마운트 해제 상태입니다.

- * 시정 조치 *

  잠시 기다린 후 백업을 다시 수행합니다.

SMTape 오류 메시지입니다

청크가 순서가 아닙니다

- * 메시지 *

  "덩어리가 오르지 않았습니다.

- * 원인 *

  백업 테이프가 올바른 순서로 복구되지 않습니다.

- * 시정 조치 *

  복구 작업을 재시도하고 올바른 순서로 테이프를 로드합니다.

청크 형식이 지원되지 않습니다

- * 메시지 *

청크 형식이 지원되지 않습니다

- * 원인 *

  백업 이미지가 SMTape가 아닙니다.

- * 시정 조치 *

  백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.

메모리를 할당하지 못했습니다

- * 메시지 *

  메모리를 할당하지 못했습니다

- * 원인 *

  시스템의 메모리가 부족합니다.

- * 시정 조치 *

  시스템 사용량이 너무 많으면 나중에 작업을 다시 시도하십시오.

데이터 버퍼를 가져오지 못했습니다

- * 메시지 *

  데이터 버퍼를 가져오지 못했습니다

- * 원인 *

  스토리지 시스템의 버퍼가 부족했습니다.

- * 시정 조치 *

  일부 스토리지 시스템 작업이 완료될 때까지 기다린 다음 작업을 재시도하십시오.

스냅샷을 찾지 못했습니다

- * 메시지 *

  스냅샷을 찾지 못했습니다

- * 원인 *

  백업에 지정된 스냅샷을 사용할 수 없습니다.

- * 시정 조치 *

  지정된 스냅샷을 사용할 수 있는지 확인합니다. 그렇지 않은 경우 올바른 스냅샷을 사용하여 재시도하십시오.

스냅샷을 생성하지 못했습니다

- * 메시지 *

  스냅샷을 만들지 못했습니다

- * 원인 *

  볼륨에 이미 최대 스냅샷 수가 포함되어 있습니다.

- * 시정 조치 *

  일부 스냅샷을 삭제한 다음 백업 작업을 다시 시도하십시오.

스냅샷을 잠그지 못했습니다

- * 메시지 *

  스냅샷을 잠그는 데 실패했습니다

- * 원인 *

  스냅샷이 사용 중이거나 삭제되었습니다.

- * 시정 조치 *

  다른 작업에서 스냅샷을 사용 중인 경우 해당 작업이 완료될 때까지 기다린 다음 백업을 다시 시도하십시오. 스냅샷이 삭제된 경우 백업을 수행할 수 없습니다.

스냅샷을 삭제하지 못했습니다

- * 메시지 *

  스냅샷을 삭제하지 못했습니다

- * 원인 *

  자동 스냅샷이 다른 작업에서 사용 중이므로 삭제할 수 없습니다.

- * 시정 조치 *

  명령을 사용하여 `snap` 스냅샷의 상태를 확인합니다. 스냅샷이 필요하지 않은 경우 수동으로 삭제합니다.

최신 스냅샷을 가져오지 못했습니다

- * 메시지 *

  최근 스냅샷을 가져오지 못했습니다

- * 원인 *

  SnapMirror에서 볼륨을 초기화하는 중이므로 최신 스냅샷이 없을 수 있습니다.

- * 시정 조치 *

  초기화가 완료된 후 다시 시도하십시오.

새 테이프를 로드하지 못했습니다

- * 메시지 *

  새 테이프를 로드하지 못했습니다

- * 원인 *

  테이프 드라이브 또는 미디어에 오류가 있습니다.

- * 시정 조치 *

  테이프를 교체하고 작업을 다시 시도하십시오.

테이프를 초기화하지 못했습니다

- * 메시지 *

  테이프 초기화 실패

- * 원인 *

  다음 이유 중 하나로 인해 이 오류 메시지가 나타날 수 있습니다.

  ◦ 백업 이미지가 SMTape가 아닙니다.
  ◦ 지정된 테이프 차단 계수가 올바르지 않습니다.
  ◦ 테이프가 손상되었거나 손상되었습니다.
  ◦ 복원을 위해 잘못된 테이프가 로드되었습니다.

- * 시정 조치 *
  ◦ 백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.
  ◦ 차단 계수가 올바르지 않은 경우 올바른 차단 계수를 지정하고 작업을 재시도하십시오.
  ◦ 테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.
  ◦ 잘못된 테이프가 로드된 경우 올바른 테이프를 사용하여 작업을 재시도하십시오.

복원 스트림을 초기화하지 못했습니다

- * 메시지 *

  복원 스트림을 초기화하지 못했습니다

- * 원인 *

  다음 이유 중 하나로 인해 이 오류 메시지가 나타날 수 있습니다.

◦ 백업 이미지가 SMTape가 아닙니다.
◦ 지정된 테이프 차단 계수가 올바르지 않습니다.
◦ 테이프가 손상되었거나 손상되었습니다.
◦ 복원을 위해 잘못된 테이프가 로드되었습니다.

- * 시정 조치 *
  ◦ 백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.
  ◦ 차단 계수가 올바르지 않은 경우 올바른 차단 계수를 지정하고 작업을 재시도하십시오.
  ◦ 테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.
  ◦ 잘못된 테이프가 로드된 경우 올바른 테이프를 사용하여 작업을 재시도하십시오.

백업 이미지를 읽지 못했습니다

- * 메시지 *

  백업 이미지를 읽지 못했습니다

- * 원인 *

  테이프가 손상되었습니다.

- * 시정 조치 *

  테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.

이미지 헤더가 없거나 손상되었습니다

- * 메시지 *

  '이미지 헤더 누락 또는 손상'

- * 원인 *

  테이프에 유효한 SMTape 백업이 없습니다.

- * 시정 조치 *

  유효한 백업이 포함된 테이프로 다시 시도하십시오.

내부 어설션

- * 메시지 *

  내부 어설션

- * 원인 *

  내부 SMTape 오류가 있습니다.

- * 시정 조치 *

  오류를 보고하고 기술 지원 부서에 'etc/log/backup' 파일을 보냅니다.

백업 이미지 매직 번호가 잘못되었습니다

- * 메시지 *

  백업 이미지 마술 번호가 잘못되었습니다

- * 원인 *

  백업 이미지가 SMTape가 아닙니다.

- * 시정 조치 *

  백업 이미지가 SMTape가 아닌 경우 SMTape 백업이 있는 테이프를 사용하여 작업을 재시도하십시오.

백업 이미지 체크섬이 잘못되었습니다

- * 메시지 *

  백업 이미지 체크섬이 잘못되었습니다

- * 원인 *

  테이프가 손상되었습니다.

- * 시정 조치 *

  테이프가 손상된 경우 복원 작업을 수행할 수 없습니다.

입력 테이프가 잘못되었습니다

- * 메시지 *

  잘못된 입력 테이프

- * 원인 *

  백업 이미지의 서명이 테이프 헤더에서 유효하지 않습니다. 테이프에 손상된 데이터가 있거나 유효한 백업 이미지가 없습니다.

- * 시정 조치 *

  유효한 백업 이미지로 복원 작업을 다시 시도하십시오.

볼륨 경로가 잘못되었습니다

- * 메시지 *

잘못된 볼륨 경로입니다

- * 원인 *

  백업 또는 복원 작업에 대해 지정된 볼륨을 찾을 수 없습니다.

- * 시정 조치 *

  유효한 볼륨 경로 및 볼륨 이름을 사용하여 작업을 재시도하십시오.

백업 세트 **ID**가 일치하지 않습니다

- * 메시지 *

  백업 세트 ID의 mismatch

- * 원인 *

  테이프 변경 중에 로드된 테이프는 백업 세트의 일부가 아닙니다.

- * 시정 조치 *

  올바른 테이프를 로드하고 작업을 재시도하십시오.

백업 타임 스탬프가 일치하지 않습니다

- * 메시지 *

  백업 타임 스탬프에 일치

- * 원인 *

  테이프 변경 중에 로드된 테이프는 백업 세트의 일부가 아닙니다.

- * 시정 조치 *

  'msape restore -h' 명령어를 사용하여 테이프의 헤더 정보를 확인한다.

종료로 인해 작업이 중단되었습니다

- * 메시지 *

  종료로 인해 작업이 중단되었습니다

- * 원인 *

  스토리지 시스템을 재부팅하는 중입니다.

- * 시정 조치 *

  스토리지 시스템이 재부팅된 후 작업을 재시도하십시오.

스냅샷 자동 삭제로 인해 작업이 중단되었습니다

- * 메시지 *

  `Job aborted due to snapshot autodelete`

- * 원인 *

  볼륨에 공간이 부족하여 스냅샷 자동 삭제를 트리거했습니다.

- * 시정 조치 *

  볼륨에서 공간을 확보하고 작업을 다시 시도하십시오.

현재 다른 작업에서 테이프를 사용하고 있습니다

- * 메시지 *

  테이프는 현재 다른 작업에서 사용 중입니다

- * 원인 *

  테이프 드라이브가 다른 작업에서 사용 중입니다.

- * 시정 조치 *

  현재 활성 작업이 완료된 후 백업을 다시 시도하십시오.

테이프 순서가 없습니다

- * 메시지 *

  테이프가 순서를 벗어났어

- * 원인 *

  복원 작업에 대한 테이프 시퀀스의 첫 번째 테이프에는 이미지 헤더가 없습니다.

- * 시정 조치 *

  이미지 헤더로 테이프를 로드하고 작업을 재시도하십시오.

전송 실패**(MetroCluster** 작업으로 인해 중단됨**)**

- * 메시지 *

  "전송 실패(MetroCluster 작업으로 인해 중단됨)

- * 원인 *

  전환 또는 스위치백 작업으로 인해 SMTape 작업이 중단됩니다.

- * 시정 조치 *

  스위치오버 또는 스위치백 작업이 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(ARL** 시작 중단**)**

- * 메시지 *

  "전송 실패(ARL 시작 중단)"

- * 원인 *

  SMTape 작업이 진행 중인 동안 집계 재배치를 시작하면 SMTape 작업이 중단됩니다.

- * 시정 조치 *

  집계 재배치 작업이 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(CFO**가 중단을 초기화함**)**

- * 메시지 *

  "전송 실패(CFO가 중단을 시작함)"

- * 원인 *

  SMTape 작업은 CFO 애그리게이트의 스토리지 페일오버(테이크오버 및 반환) 작업 때문에 중단됩니다.

- * 시정 조치 *

  CFO 애그리게이트의 스토리지 페일오버가 완료된 후 SMTape 작업을 수행합니다.

전송 실패**(SFO** 시작 중단**)**

- * 메시지 *

  전송 실패(SFO 시작 중단)

- * 원인 *

  SMTape 작업은 스토리지 페일오버(테이크오버 및 반환) 작업으로 인해 중단됩니다.

- * 시정 조치 *

  스토리지 페일오버(테이크오버 및 반환) 작업이 완료된 후 SMTape 작업을 수행합니다.

마이그레이션 중인 기본 애그리게이트

- * 메시지 *

  이주 중인 기본 골재

- * 원인 *

  마이그레이션 중인 Aggregate(스토리지 페일오버 또는 애그리게이트 재배치)에서 SMTape 작업이 시작되면 SMTape 작업이 실패합니다.

- * 시정 조치 *

  애그리게이트 마이그레이션이 완료된 후 SMTape 작업을 수행합니다.

볼륨이 현재 마이그레이션 중입니다

- * 메시지 *

  볼륨이 현재 마이그레이션 중입니다

- * 원인 *

  볼륨 마이그레이션 및 SMTape 백업을 동시에 실행할 수 없습니다.

- * 시정 조치 *

  볼륨 마이그레이션이 완료된 후 백업 작업을 다시 시도하십시오.

볼륨이 오프라인 상태입니다

- * 메시지 *

  볼륨 오프라인

- * 원인 *

  백업 중인 볼륨이 오프라인 상태입니다.

- * 시정 조치 *

  볼륨을 온라인으로 전환하고 백업을 다시 시도하십시오.

볼륨이 제한되지 않았습니다

- * 메시지 *

  볼륨이 제한되지 않음

- * 원인 *

  데이터가 복원되는 대상 볼륨은 제한되지 않습니다.

- * 시정 조치 *

  볼륨을 제한하고 복원 작업을 다시 시도하십시오.

NDMP 구성

ONTAP NDMP 구성에 대해 자세히 알아보십시오

타사 백업 애플리케이션을 사용하여 데이터를 테이프에 직접 백업하기 위해 NDMP(네트워크 데이터 관리 프로토콜)를 사용하도록 ONTAP 9 클러스터를 빠르게 구성할 수 있습니다.

백업 애플리케이션이 CAB(Cluster Aware Backup)를 지원하는 경우 NDMP를 _SVM-scope_or_node-scope_로 구성할 수 있습니다.

- 클러스터(admin SVM) 레벨에서 SVM 범위가 지정되므로 클러스터의 서로 다른 노드에 호스팅된 모든 볼륨을 백업할 수 있습니다. 가능한 경우 SVM 범위의 NDMP를 사용하는 것이 좋습니다.
- 노드 범위 NDMP에서는 해당 노드에서 호스팅되는 모든 볼륨을 백업할 수 있습니다.

백업 애플리케이션이 CAB를 지원하지 않는 경우 노드 범위 NDMP를 사용해야 합니다.

SVM 범위 및 노드 범위 NDMP는 상호 배타적이므로 동일한 클러스터에서 구성할 수 없습니다.

노드 범위 NDMP는 ONTAP 9에서 더 이상 사용되지 않습니다.

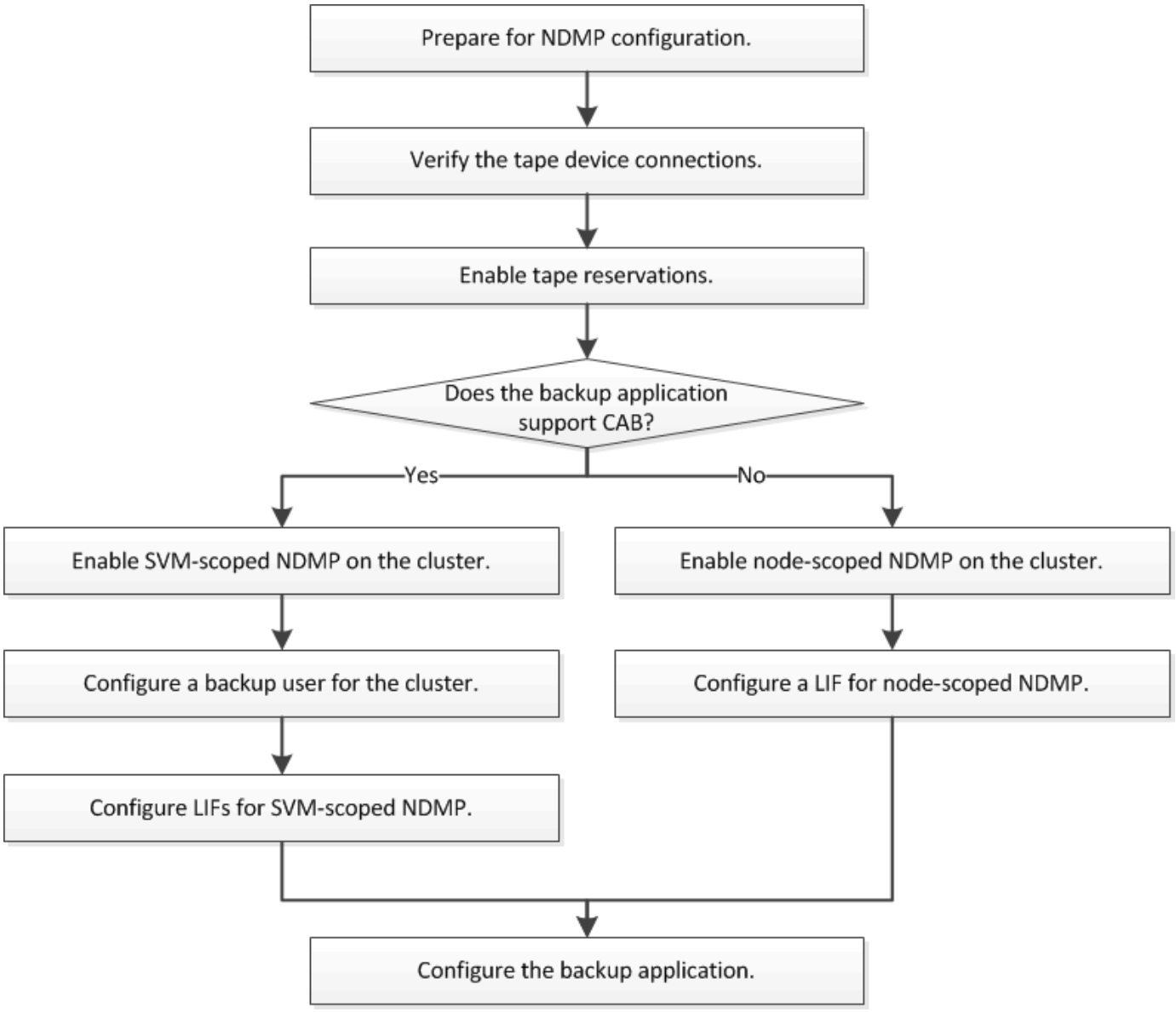
에 대해 자세히 "운전실(Cluster Aware Backup)"알아보십시오.

NDMP를 구성하기 전에 다음을 확인하십시오.

- 타사 백업 애플리케이션(DMA라고도 함)이 있습니다.
- 클러스터 관리자입니다.
- 테이프 장치 및 옵션 미디어 서버가 설치됩니다.
- 테이프 장치는 FC(파이버 채널) 스위치를 통해 또는 로컬로 연결된 상태로 클러스터에 연결됩니다.
- 하나 이상의 테이프 디바이스에 LUN(Logical Unit Number)이 0인 경우

ONTAP NDMP 구성 워크플로에 대해 알아보세요

NDMP를 통해 테이프 백업을 설정하려면 NDMP 구성 준비, 테이프 디바이스 연결 확인, 테이프 예약 활성화, SVM 또는 노드 레벨에서 NDMP 구성, 클러스터에서 NDMP 설정, 백업 사용자 구성, LIF 구성 및 백업 애플리케이션 구성이 필요합니다.



ONTAP NDMP 구성 준비

NDMP(Network Data Management Protocol)를 통해 테이프 백업 액세스를 구성하기 전에 계획된 구성이 지원되는지 확인하고, 테이프 드라이브가 각 노드의 적격 드라이브로 나열되는지 확인하고, 모든 노드에 인터클러스터 LIF가 있는지 확인해야 합니다. 백업 애플리케이션이 CAB(Cluster Aware Backup) 확장을 지원하는지 여부를 확인합니다.

단계

1. ONTAP 지원에 대한 자세한 내용은 백업 애플리케이션 공급자의 호환성 매트릭스를 참조하십시오(NetApp은 ONTAP 또는 NDMP를 통한 타사 백업 애플리케이션을 지원하지 않음).

   다음 NetApp 구성 요소가 호환되는지 확인해야 합니다.

   - 클러스터에서 실행 중인 ONTAP 9 버전입니다.
   - 백업 애플리케이션 공급업체 및 버전: 예: Veritas NetBackup 8.2 또는 CommVault.
   - 테이프 드라이브의 제조업체, 모델 및 인터페이스(예: IBM Ultrium 8 또는 HPE StoreEver Ultrium 30750

LTO-8)와 같은 테이프 장치 세부 정보

◦ 클러스터에 있는 노드 플랫폼: FAS8700 또는 A400.

에서 백업 애플리케이션에 대한 기존 ONTAP 호환성 지원 매트릭스를 확인할 수 있습니다 "NetApp 상호 운용성 매트릭스 툴".

2. 테이프 드라이브가 각 노드의 내장 테이프 구성 파일에 검증된 드라이브로 나열되어 있는지 확인합니다.

   a. CLI에서 Storage tape show-supported-status 명령을 사용하여 내장 테이프 구성 파일을 봅니다.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                  Is
Tape Drives                       Supported  Support Status
--------------------------------  ---------
--------------------------------
Certance Ultrium 2                true       Dynamically Qualified
Certance Ultrium 3                true       Dynamically Qualified
Digital DLT2000                   true       Qualified
```

   b. 테이프 드라이브를 출력의 적격 드라이브 목록과 비교합니다.

출력에 표시되는 테이프 디바이스의 이름은 디바이스 레이블 또는 상호 운용성 매트릭스의 이름과 약간 다를 수 있습니다. 예를 들어 디지털 DLT2000은 DLT2K라고도 합니다. 이러한 사소한 이름 차이는 무시할 수 있습니다.

   c. 장치가 상호 운용성 매트릭스에 따라 적격 장치임에도 불구하고 출력에 적격 장치로 표시되지 않는 경우, NetApp Support 사이트의 지침에 따라 장치에 대한 업데이트된 구성 파일을 다운로드하여 설치하십시오.

   "NetApp 다운로드: 테이프 장치 구성 파일"

노드를 제공한 후 테이프 장치가 검증된 경우, 내장 테이프 구성 파일에 검증된 장치가 나열되지 않을 수 있습니다.

3. 클러스터의 모든 노드에 인터클러스터 LIF가 있는지 확인합니다.

   a. 'network interface show-role 인터클러스터' 명령을 사용하여 노드의 인터클러스터 LIF를 봅니다.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

b. 인터클러스터 LIF가 노드에 없으면 '네트워크 인터페이스 만들기' 명령을 사용하여 인터클러스터 LIF를 만듭니다.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

에 대한 자세한 내용은 `network interface create` "ONTAP 명령 참조입니다"을 참조하십시오.

"네트워크 관리"

4. 백업 애플리케이션과 함께 제공된 설명서를 사용하여 백업 애플리케이션이 CAB(Cluster Aware Backup)를 지원하는지 여부를 확인합니다.

   CAB 지원은 수행할 수 있는 백업 유형을 결정하는 핵심 요소입니다.

관련 정보

- "저장 테이프 쇼"
- "저장 테이프 show-supported-status"

ONTAP NDMP 테이프 장치 연결 확인

모든 드라이브와 미디어 체인저가 ONTAP에 디바이스로 표시되는지 확인해야 합니다.

단계

1. 'storage tape show' 명령을 사용하여 모든 드라이브와 미디어 체인저에 대한 정보를 봅니다.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                 Device Type     Description
Status
------------------------  --------------  ------------------------------
--------
sw4:10.11                 tape drive      HP LTO-3
normal
0b.125L1                  media changer   HP MSL G3 Series
normal
0d.4                      tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                    media changer   IBM 3573-TL
normal
...
```

2. 테이프 드라이브가 표시되지 않으면 문제를 해결합니다.
3. 미디어 체인저가 표시되지 않는 경우 'storage tape show -media-changer' 명령을 사용하여 미디어 체인저에 대한 정보를 확인한 후 문제를 해결하십시오.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

관련 정보

- "저장 테이프 쇼 미디어 체인저"

ONTAP NDMP 백업 작업에 대한 테이프 예약 활성화

NDMP 백업 작업을 위해 테이프 드라이브가 백업 애플리케이션에서 사용하도록 예약되어 있는지 확인해야 합니다.

이 작업에 대해

예약 설정은 백업 애플리케이션에 따라 다르며, 이러한 설정은 동일한 드라이브를 사용하는 백업 애플리케이션과 노드 또는 서버와 일치해야 합니다. 올바른 예약 설정은 백업 애플리케이션의 공급업체 설명서를 참조하십시오.

단계

1. options -option -name tape.예약 -option -value persistent 명령을 사용하여 예약을 활성화합니다.

   다음 명령을 실행하면 '영구적' 값을 가진 예약이 활성화됩니다.

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. options tape.enervations 명령을 사용하여 모든 노드에서 예약이 활성화되었는지 확인한 다음 출력을 검토합니다.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                 persistent

cluster1-2
    tape.reservations                 persistent
2 entries were displayed.
```

SVM 범위 NDMP를 구성합니다

ONTAP 클러스터에서 SVM 범위 NDMP 활성화

DMA가 CAB(Cluster Aware Backup) 확장을 지원하는 경우 SVM 범위의 NDMP를 사용하도록 설정하고, 클러스터에서 NDMP 서비스를 설정하고(admin SVM), 데이터 및 제어 연결을 위해 LIF를 구성하여 클러스터의 여러 노드에서 호스팅되는 모든 볼륨을 백업할 수 있습니다.

시작하기 전에

CAB 확장은 DMA에서 지원해야 합니다.

이 작업에 대해

노드 범위의 NDMP 모드를 해제하면 클러스터에서 SVM 범위의 NDMP 모드가 설정됩니다.

단계

1. SVM 범위 NDMP 모드 활성화:

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   SVM 범위 NDMP 모드가 설정되었습니다.

2. 관리자 SVM에서 NDMP 서비스 활성화:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   기본적으로 인증 유형은 "challenge"로 설정되고 일반 텍스트 인증은 비활성화됩니다.

   보안 통신을 위해 일반 텍스트 인증을 사용하지 않도록 설정해야 합니다.

3. NDMP 서비스가 설정되었는지 확인합니다.

   ```
   cluster1::> vserver services ndmp show
   ```

```
Vserver        Enabled   Authentication type
-------------- --------- -------------------
cluster1       true      challenge
vs1            false     challenge
```

ONTAP NDMP 인증을 위한 백업 사용자 활성화

백업 애플리케이션에서 SVM 범위의 NDMP를 인증하려면 충분한 권한과 NDMP 암호를 가진 관리 사용자가 있어야 합니다.

이 작업에 대해

백업 관리자 사용자를 위해 NDMP 암호를 생성해야 합니다. 클러스터 또는 SVM 레벨에서 백업 관리자를 지원하고, 필요한 경우 새 사용자를 생성할 수 있습니다. 기본적으로 다음 역할을 가진 사용자는 NDMP 백업에 대해 인증할 수 있습니다.

- 클러스터 전체: `admin` 또는 `backup`
- 개별 SVM: `vsadmin` 또는 `vsadmin-backup`

NIS 또는 LDAP 사용자를 사용하는 경우 사용자는 해당 서버에 있어야 합니다. Active Directory 사용자는 사용할 수 없습니다.

단계

1. 현재 관리자 사용자 및 권한을 표시합니다.

   '보안 로그인 쇼'

   에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 필요한 경우 를 사용하여 새 NDMP 백업 사용자를 생성합니다 `security login create` 클러스터 전체 또는 개별 SVM 권한에 따라 명령을 수행하고 적절한 역할을 수행합니다.

   '-user-or-group-name' 매개 변수에 로컬 백업 사용자 이름 또는 NIS 또는 LDAP 사용자 이름을 지정할 수 있습니다.

   다음 명령을 실행하면 백업 사용자가 생성됩니다 `backup_admin1` 를 사용하여 `backup` 전체 클러스터의 역할:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   다음 명령을 실행하면 백업 사용자가 생성됩니다 `vsbackup_admin1` 를 사용하여 `vsadmin-backup` 개별 SVM의 역할:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   새 사용자의 암호를 입력하고 확인합니다.

   에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

3. 'vserver services ndmp generate password' 명령을 사용하여 admin SVM에 대한 암호를 생성합니다.

   생성된 암호를 사용하여 백업 애플리케이션에서 NDMP 접속을 인증해야 합니다.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

SVM 범위 **NDMP**에 대한 **ONTAP LIF** 구성

데이터와 테이프 리소스 간에 데이터 연결을 설정하고, 관리 SVM과 백업 애플리케이션 간의 연결을 제어하는 데 사용할 LIF를 식별해야 합니다. LIF를 식별한 후 서비스 및 페일오버 정책이 설정되었는지 확인해야 합니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 "지원되는 트래픽을 관리합니다"참조하십시오.

ONTAP 9.10.1 이상

단계

1. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 인터클러스터 LIF를 `network interface show` 식별합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

   에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 관리 LIF를 `network interface show` 식별합니다.

   ```
   network interface show -service-policy default-management
   ```

3. 인터클러스터 LIF에 서비스가 포함되는지 확인합니다. `backup-ndmp-control`

   네트워크 인터페이스 서비스 정책 쇼

   에 대한 자세한 내용은 `network interface service-policy show` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 모든 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 클러스터 관리 LIF의 페일오버 정책이 브로드캐스트 도메인 전체에 설정되어 있고, 인터클러스터 및 노드 관리 LIF에 대한 정책이 '네트워크 인터페이스 show-failover' 명령을 사용하여 '로컬 전용'으로 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 클러스터 관리, 인터클러스터 및 노드 관리 LIF에 대한 페일오버 정책이 표시됩니다.

```
cluster1::> network interface show -failover

           Logical          Home             Failover    Failover
Vserver    Interface        Node:Port        Policy      Group
-------    --------------   --------------   ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                         Failover
Targets:
                                                         .......
cluster1   cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                         Failover
Targets:
                                                         .......
           IC1              cluster1-1:e0a   local-only  Default
                                                         Failover
Targets:
           IC2              cluster1-1:e0b   local-only  Default
                                                         Failover
Targets:
                                                         .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
```

a. 페일오버 정책이 제대로 설정되지 않은 경우 -failover-policy 매개 변수와 함께 network interface modify 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

5. 데이터 연결에 필요한 LIF를 'preferred-interface-role' 매개 변수와 함께 'vserver services ndmp modify' 명령을 사용하여 지정합니다.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. 'vserver services ndmp show' 명령을 사용하여 클러스터에 대해 기본 인터페이스 역할이 설정되어 있는지 확인합니다.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 이하

단계

1. '-role' 매개 변수가 있는 'network interface show' 명령을 사용하여 인터클러스터, 클러스터 관리 및 노드 관리 LIF를 식별합니다.

   다음 명령을 실행하면 인터클러스터 LIF가 표시됩니다.

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   다음 명령을 실행하면 클러스터 관리 LIF가 표시됩니다.

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

다음 명령을 실행하면 노드 관리 LIF가 표시됩니다.

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 방화벽 정책이 인터클러스터, 클러스터 관리(`cluster-mgmt`) 및 노드 관리에 NDMP에 대해 사용하도록 설정되어 있는지 확인(`node-mgmt`) LIF:

   a. 'system services firewall policy show' 명령을 사용하여 NDMP에 대해 방화벽 정책이 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 클러스터 관리 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      다음 명령을 실행하면 인터클러스터 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

다음 명령을 실행하면 노드 관리 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. 방화벽 정책이 활성화되지 않은 경우 '-service' 매개 변수를 사용하여 'system services firewall policy modify' 명령을 사용하여 방화벽 정책을 활성화합니다.

   다음 명령을 실행하면 인터클러스터 LIF에 대한 방화벽 정책을 사용할 수 있습니다.

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 모든 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

a. 클러스터 관리 LIF의 페일오버 정책이 브로드캐스트 도메인 전체에 설정되어 있고, 인터클러스터 및 노드 관리 LIF에 대한 정책이 '네트워크 인터페이스 show-failover' 명령을 사용하여 '로컬 전용'으로 설정되어 있는지 확인합니다.

   다음 명령을 실행하면 클러스터 관리, 인터클러스터 및 노드 관리 LIF에 대한 페일오버 정책이 표시됩니다.

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ------------------ --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1   cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
           IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
           IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. 페일오버 정책이 제대로 설정되지 않은 경우 -failover-policy 매개 변수와 함께 network interface modify

명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 데이터 연결에 필요한 LIF를 'preferred-interface-role' 매개 변수와 함께 'vserver services ndmp modify' 명령을 사용하여 지정합니다.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. 'vserver services ndmp show' 명령을 사용하여 클러스터에 대해 기본 인터페이스 역할이 설정되어 있는지 확인합니다.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

노드 범위 **NDMP**를 구성합니다

ONTAP 클러스터에서 노드 범위 **NDMP** 활성화

노드 범위 NDMP를 설정하고, NDMP 서비스를 사용하도록 설정하고, 데이터 및 제어 연결을 위해 LIF를 구성하여 단일 노드에서 호스팅되는 볼륨을 백업할 수 있습니다. 이 작업은 클러스터의 모든 노드에 대해 수행할 수 있습니다.

노드 범위 NDMP는 ONTAP 9에서 더 이상 사용되지 않습니다.

이 작업에 대해

노드 범위 모드에서 NDMP를 사용하는 경우 노드 단위로 인증을 구성해야 합니다. 자세한 내용은 을 참조하십시오 "기술 자료 문서 "'노드 범위' 모드에서 NDMP 인증을 구성하는 방법"".

단계

1. 노드 범위 NDMP 모드 설정:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP 노드 범위 모드가 설정되었습니다.

2. 클러스터의 모든 노드에서 NDMP 서비스 설정:

   와일드카드 "" * ""를 사용하면 모든 노드에서 동시에 NDMP 서비스를 사용할 수 있습니다.

   백업 애플리케이션에서 NDMP 접속을 인증할 암호를 지정해야 합니다.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. 를 비활성화합니다 `-clear-text` NDMP 암호의 보안 통신을 위한 옵션:

   와일드카드 "" * "를 사용하면 모든 노드에서 "-clear-text" 옵션을 동시에 사용할 수 없습니다.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. NDMP 서비스가 설정되어 있고 이 설정되어 있는지 확인합니다 `-clear-text` 옵션이 비활성화됨:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

노드 범위 **NDMP**에 대한 **ONTAP LIF** 구성

노드와 백업 애플리케이션 간의 데이터 연결 및 제어 연결을 설정하는 데 사용할 LIF를 식별해야 합니다. LIF를 식별한 후 LIF에 대한 방화벽 및 페일오버 정책이 설정되어 있는지 확인해야 합니다.

ONTAP 9.10.1.1부터 방화벽 정책이 사용되지 않으며 LIF 서비스 정책으로 완전히 대체됩니다. 자세한 내용은 을 "지원되는 트래픽을 관리합니다"참조하십시오.

ONTAP 9.10.1 이상

단계

1. 매개 변수와 함께 명령을 `-service-policy` 사용하여 노드에 호스팅된 인터클러스터 LIF를 `network interface show` 식별합니다.

   네트워크 인터페이스 show-service-policy default-인터클러스터

2. 인터클러스터 LIF에 서비스가 포함되는지 확인합니다. `backup-ndmp-control`

   네트워크 인터페이스 서비스 정책 쇼

3. 인터클러스터 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 네트워크 인터페이스 show-failover 명령을 사용하여 인터클러스터 LIF의 페일오버 정책이 "로컬 전용 "으로 설정되었는지 확인합니다.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. 페일오버 정책이 적절하게 설정되지 않은 경우 '-failover-policy' 매개 변수와 함께 'network interface modify' 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

에 대한 자세한 `network interface show` `network interface service-policy show`

내용은, 및 `network interface modify`"ONTAP 명령 참조입니다" 을 참조하십시오.

ONTAP 9.9 이하

단계

1. '-role' 매개 변수가 있는 'network interface show' 명령을 사용하여 노드에 호스팅된 인터클러스터 LIF를 식별합니다.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. 인터클러스터 LIF에서 NDMP에 대해 방화벽 정책이 활성화되어 있는지 확인합니다.

   a. 'system services firewall policy show' 명령을 사용하여 NDMP에 대해 방화벽 정책이 설정되어 있는지 확인합니다.

      다음 명령을 실행하면 인터클러스터 LIF의 방화벽 정책이 표시됩니다.

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. 방화벽 정책이 활성화되지 않은 경우 '-service' 매개 변수를 사용하여 'system services firewall policy modify' 명령을 사용하여 방화벽 정책을 활성화합니다.

다음 명령을 실행하면 인터클러스터 LIF에 대한 방화벽 정책을 사용할 수 있습니다.

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 인터클러스터 LIF에 대해 페일오버 정책이 적절하게 설정되었는지 확인합니다.

   a. 네트워크 인터페이스 show-failover 명령을 사용하여 인터클러스터 LIF의 페일오버 정책이 "로컬 전용 "으로 설정되었는지 확인합니다.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. 페일오버 정책이 적절하게 설정되지 않은 경우 '-failover-policy' 매개 변수와 함께 'network interface modify' 명령을 사용하여 페일오버 정책을 수정합니다.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

및 `network interface modify` 에 대한 자세한 `network interface show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

ONTAP NDMP 구성을 위한 백업 애플리케이션 구성

NDMP 액세스용으로 클러스터를 구성한 후에는 클러스터 구성에서 정보를 수집한 다음 백업 애플리케이션에서 나머지 백업 프로세스를 구성해야 합니다.

단계

1. ONTAP에서 이전에 구성한 다음 정보를 수집합니다.
   - 백업 애플리케이션이 NDMP 접속을 생성하는 데 필요한 사용자 이름 및 암호입니다
   - 백업 애플리케이션이 클러스터에 연결하는 데 필요한 인터클러스터 LIF의 IP 주소입니다
2. ONTAP에서 'storage tape alias show' 명령어를 사용해 각 디바이스에 할당된 ONTAP의 별칭을 출력한다.

   별칭은 백업 애플리케이션을 구성하는 데 유용합니다.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- ------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. 백업 애플리케이션에서 백업 애플리케이션의 설명서를 사용하여 나머지 백업 프로세스를 구성합니다.

작업을 마친 후

볼륨 이동 또는 LIF 마이그레이션과 같은 데이터 이동성 이벤트가 발생할 경우 중단된 백업 작업을 다시 초기화할 준비를 해야 합니다.

관련 정보

- "저장 테이프 별칭 표시"

NetApp Element 소프트웨어와 ONTAP 간 복제 개요

SnapMirror를 사용하여 Element 볼륨의 스냅샷을 ONTAP 대상에 복제하면 Element 시스템에서 비즈니스 연속성을 보장할 수 있습니다. Element 사이트에서 재해가 발생할 경우 ONTAP 시스템에서 클라이언트로 데이터를 제공하고 서비스가 복원되면 Element 시스템을 다시 활성화할 수 있습니다.

ONTAP 9.4부터는 ONTAP 노드에 생성된 LUN의 스냅샷을 Element 시스템에 다시 복제할 수 있습니다. Element 사이트에서 운영 중단 중에 LUN을 생성했거나, LUN을 사용하여 ONTAP에서 Element 소프트웨어로 데이터를 마이그레이션할 수 있습니다.

"NetApp Element 소프트웨어 및 ONTAP의 복제를 구성합니다"..