Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성

ONTAP 9

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/smb-hyper-v-sql/index.html on January 09, 2026. Always check docs.netapp.com for the latest.

목차

Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 . . . 1
Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요 . . . 1
SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다 . . . 1
SMB를 통한 Microsoft Hyper-V . . . 1
SMB를 통한 Microsoft SQL Server . . . 2
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영 . . . 2
Hyper-V 및 SQL Server over SMB의 무중단 운영은 무엇을 의미하는지 . . . 2
프로토콜을 지원하여 SMB를 통해 무중단 운영을 실현합니다 . . . 2
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영에 대한 주요 개념입니다 . . . 3
SMB 3.0 기능이 SMB 공유에서 무중단 운영을 지원하는 방법 . . . 4
Witness 프로토콜이 투명한 장애 조치를 강화하기 위해 수행하는 조치 . . . 5
Witness 프로토콜 작동 방식 . . . 5
원격 VSS와 공유 기반 백업 . . . 6
원격 VSS를 사용한 공유 기반 백업 개요 . . . 6
원격 VSS 개념 . . . 6
원격 VSS에서 사용하는 디렉토리 구조의 예 . . . 7
SnapManager for Hyper-V가 SMB를 통해 Hyper-V에 대한 원격 VSS 기반 백업을 관리하는 방법 . . . 8
SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법 . . . 9
구성 요구 사항 및 고려 사항 . . . 11
ONTAP 및 라이센스 요구 사항 . . . 11
네트워크 및 데이터 LIF 요구사항 . . . 11
SMB를 통한 Hyper-V의 SMB 서버 및 볼륨 요구 사항 . . . 12
SMB를 통한 SQL Server의 SMB 서버 및 볼륨 요구 사항 . . . 13
SMB를 통한 Hyper-V의 지속적인 가용성 공유 요구 사항 및 고려 사항 . . . 14
SMB를 통한 SQL Server의 지속적인 가용성 공유 요구 사항 및 고려 사항 . . . 15
SMB 구성을 통한 Hyper-V에 대한 원격 VSS 고려 사항 . . . 16
ODX SMB를 통한 SQL Server 및 Hyper-V의 복사 오프로드 요구 사항 . . . 17
SMB 구성을 통한 SQL Server 및 Hyper-V 권장 사항 . . . 18
일반 권장 사항 . . . 18
SMB를 통한 Hyper-V 또는 SQL Server 구성 계획 . . . 18
볼륨 구성 워크시트를 작성합니다 . . . 18
SMB 공유 구성 워크시트를 작성합니다 . . . 20
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성 . . . 22
SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 개요를 제공합니다 . . . 22
Kerberos 및 NTLMv2 인증이 모두 허용되는지 확인(SMB 공유를 통한 Hyper-V) . . . 22
도메인 계정이 ONTAP의 기본 UNIX 사용자에게 매핑되는지 확인합니다 . . . 24
SVM 루트 볼륨의 보안 스타일이 NTFS로 설정되어 있는지 확인합니다 . . . 26
필요한 CIFS 서버 옵션이 구성되었는지 확인합니다 . . . 27
성능 및 이중화를 위해 SMB 멀티 채널을 구성합니다 . . . 29

NTFS 데이터 볼륨을 생성합니다 . . . 31
지속적으로 사용 가능한 SMB 공유를 생성합니다 . . . 32
sSecurityPrivilege 권한을 사용자 계정에 추가합니다(SMB 공유의 SQL Server에 해당). . . . 34
VSS 섀도우 복제본 디렉토리 깊이 구성(SMB 공유를 통한 Hyper-V의 경우) . . . 35
SMB 구성을 통해 Hyper-V 및 SQL Server 관리 . . . 36
지속적인 가용성을 위해 기존 공유를 구성합니다 . . . 36
SMB 백업을 통해 Hyper-V에 대한 VSS 섀도우 복제본을 설정하거나 해제합니다 . . . 39
통계를 사용하여 SMB 작업을 통해 Hyper-V 및 SQL Server를 모니터링합니다 . . . 40
ONTAP에서 사용할 수 있는 통계 개체 및 카운터를 확인합니다 . . . 40
ONTAP에서 SMB 통계를 표시합니다 . . . 43
구성이 무중단 운영이 가능한지 확인합니다 . . . 43
상태 모니터링을 사용하여 무중단 운영 상태가 정상인지 확인하십시오 . . . 43
시스템 상태 모니터링을 사용하여 무중단 운영 상태를 표시합니다 . . . 44
지속적으로 사용 가능한 SMB 공유 구성을 확인합니다 . . . 46
LIF 상태를 확인합니다 . . . 48
SMB 세션을 지속적으로 사용할 수 있는지 확인합니다 . . . 50

Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성

Microsoft Hyper-V 및 SQL Server를 위한 SMB 구성 개요

ONTAP 기능을 사용하면 Microsoft Hyper-V와 Microsoft SQL Server라는 SMB 프로토콜을 통해 두 Microsoft 애플리케이션의 무중단 운영을 실현할 수 있습니다.

다음과 같은 상황에서 SMB 무중단 운영을 구현하려는 경우 다음 절차를 따라야 합니다.

- 기본 SMB 프로토콜 파일 액세스가 구성되었습니다.
- SVM에 상주하는 SMB 3.0 이상 파일 공유를 활성화하여 다음 오브젝트를 저장하려고 합니다.
  - Hyper-V 가상 머신 파일
  - SQL Server 시스템 데이터베이스

관련 정보

ONTAP 기술 및 외부 서비스와의 상호 작용에 대한 자세한 내용은 다음 기술 보고서(TR)를 참조하십시오 "NetApp 기술 보고서 4172: ONTAP 모범 사례를 사용한 SMB 3.0 기반 Microsoft Hyper-V".** "NetApp 기술 보고서 4369: clustered Data ONTAP을 사용한 Microsoft SQL Server의 모범 사례 및 SQL Server의 SnapManager 7.2"

SMB 솔루션을 통해 Microsoft Hyper-V 및 SQL Server용 ONTAP를 구성합니다

지속적으로 사용 가능한 SMB 3.0 이상 파일 공유를 사용하여 Hyper-V 가상 머신 파일 또는 SQL Server 시스템 데이터베이스와 사용자 데이터베이스를 SVM에 상주하는 볼륨에 저장하는 동시에 계획된 이벤트와 계획되지 않은 이벤트 모두에 무중단 운영(NDO)을 제공할 수 있습니다.

SMB를 통한 Microsoft Hyper-V

SMB를 통한 Hyper-V 솔루션을 생성하려면 먼저 ONTAP를 구성하여 Microsoft Hyper-V 서버에 스토리지 서비스를 제공해야 합니다. 또한 Microsoft 클러스터(클러스터 구성을 사용하는 경우), Hyper-V 서버, CIFS 서버에서 호스팅하는 공유에 대한 지속적인 SMB 3.0 연결, SVM 볼륨에 저장된 가상 시스템 파일을 보호하기 위한 백업 서비스도 구성해야 합니다.

> Hyper-V 서버는 Windows 2012 Server 이상에서 구성해야 합니다. 독립 실행형 및 클러스터링된 Hyper-V 서버 구성이 모두 지원됩니다.

- Microsoft 클러스터 및 Hyper-V 서버 생성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- SnapManager for Hyper-V는 SMB 구성을 통한 Hyper-V와 통합되도록 설계된 신속한 스냅샷 기반 백업 서비스를 지원하는 호스트 기반 애플리케이션입니다.

  SMB 구성을 통한 Hyper-V에서 SnapManager를 사용하는 방법에 대한 자세한 내용은 _SnapManager for Hyper-V 설치 및 관리 가이드 _ 를 참조하십시오.

SMB를 통한 Microsoft SQL Server

SMB를 통한 SQL Server 솔루션을 생성하려면 먼저 Microsoft SQL Server 애플리케이션에 스토리지 서비스를 제공하도록 ONTAP를 구성해야 합니다. 또한 클러스터된 구성을 사용하는 경우 Microsoft 클러스터도 구성해야 합니다. 그런 다음 Windows 서버에 SQL Server를 설치 및 구성하고 CIFS 서버에서 호스팅하는 공유에 대해 지속적으로 사용 가능한 SMB 3.0 연결을 생성합니다. 필요에 따라 SVM 볼륨에 저장된 데이터베이스 파일을 보호하도록 백업 서비스를 구성할 수 있습니다.

> SQL Server는 Windows 2012 Server 이상에서 설치 및 구성해야 합니다. 독립 실행형 구성과 클러스터 구성이 모두 지원됩니다.

- Microsoft 클러스터 만들기 및 SQL Server 설치 및 구성에 대한 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.
- Microsoft SQL Server용 SnapCenter 플러그인은 SMB 구성을 통해 SQL Server와 통합하도록 설계된 호스트 기반 애플리케이션으로, 신속한 스냅샷 기반 백업 서비스를 지원합니다.

  Microsoft SQL Server용 SnapCenter 플러그인 사용에 대한 자세한 내용은 를 참조하십시오 "Microsoft SQL Server용 SnapCenter 플러그인" 문서화:

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영

Hyper-V 및 SQL Server over SMB의 무중단 운영은 무엇을 의미하는지

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영은 애플리케이션 서버와 포함된 가상 머신 또는 데이터베이스를 온라인 상태로 유지하고 다양한 관리 작업 중에 지속적인 가용성을 제공할 수 있는 기능의 조합을 의미합니다. 여기에는 스토리지 인프라의 계획된 다운타임과 계획되지 않은 다운타임이 모두 포함됩니다.

SMB를 통해 애플리케이션 서버에서 지원되는 무중단 운영은 다음과 같습니다.

- 계획된 테이크오버 및 반환
- 계획되지 않은 테이크오버
- 업그레이드
- 계획된 애그리게이트 재배치(ARL)
- LIF 마이그레이션 및 페일오버
- 계획된 볼륨 이동

프로토콜을 지원하여 SMB를 통해 무중단 운영을 실현합니다

Microsoft는 SMB 3.0 릴리스와 함께 SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 데 필요한 기능을 제공하는 새로운 프로토콜을 출시했습니다.

ONTAP은 SMB를 통해 애플리케이션 서버에 무중단 운영을 제공할 때 다음과 같은 프로토콜을 사용합니다.

- SMB 3.0

- 증인

SMB를 통한 **Hyper-V** 및 **SQL Server**의 무중단 운영에 대한 주요 개념입니다

SMB 솔루션을 통해 Hyper-V 또는 SQL Server를 구성하기 전에 알아야 하는 무중단 운영(NDO)에 대한 몇 가지 개념이 있습니다.

- * 지속적으로 사용 가능한 공유 *

  지속적으로 사용 가능한 공유 속성이 설정된 SMB 3.0 공유입니다. 지속적으로 사용 가능한 공유를 통해 연결하는 클라이언트는 테이크오버, 반환 및 애그리게이트 재배치와 같은 운영 중단 이벤트를 견딜 수 있습니다.

- * 노드 *

  클러스터의 구성원인 단일 컨트롤러입니다. SFO 쌍의 두 노드를 구별하기 위해 한 노드는 _ local node _ 라고도 하며 다른 노드는 _ partner node _ 또는 _ remote node _ 라고도 합니다. 스토리지의 기본 소유자는 로컬 노드입니다. 기본 소유자가 실패하는 경우 스토리지를 제어하는 보조 소유자가 파트너 노드입니다. 각 노드는 해당 스토리지의 기본 소유자이며 파트너의 스토리지를 위한 2차 소유자입니다.

- * 무중단 애그리게이트 재배치 *

  클라이언트 애플리케이션을 중단하지 않고 클러스터에서 SFO 쌍 내의 파트너 노드 간에 애그리게이트를 이동할 수 있습니다.

- 무중단 페일오버 * 를 지원합니다

  테이크오버를 참조하십시오.

- * 무중단 LIF 마이그레이션 *

  LIF를 통해 클러스터에 연결된 클라이언트 애플리케이션을 중단하지 않고 LIF 마이그레이션을 수행할 수 있습니다. SMB 연결의 경우 SMB 2.0 이상을 사용하여 연결하는 클라이언트에만 가능합니다.

- 무중단 운영 *

  주요 ONTAP 관리 및 업그레이드 작업을 수행할 뿐만 아니라 클라이언트 애플리케이션을 중단하지 않고 노드 장애를 견딜 수 있는 기능 이때 무중단 테이크오버, 무중단 업그레이드, 무중단 마이그레이션 기능이 전반적으로 사용됩니다.

- 무중단 업그레이드 *

  애플리케이션 중단 없이 노드 하드웨어 또는 소프트웨어를 업그레이드할 수 있는 기능

- * 무중단 볼륨 이동 *

  볼륨을 사용하는 애플리케이션을 중단하지 않고 클러스터 전체에서 볼륨을 자유롭게 이동할 수 있습니다. SMB 연결의 경우, 모든 버전의 SMB가 무중단 볼륨 이동을 지원합니다.

- * 영구 핸들 *

  연결이 끊길 경우 지속적으로 사용 가능한 연결을 통해 CIFS 서버에 투명하게 다시 연결할 수 있도록 하는 SMB 3.0의 속성입니다. 내구성이 뛰어난 핸들과 마찬가지로 연결 클라이언트와의 통신이 끊긴 후 CIFS 서버가 일정 시간

동안 영구 핸들을 유지합니다. 그러나 지속적인 핸들은 내구성 있는 핸들보다 뛰어난 복원력을 제공합니다. 다시 연결한 후 60초 이내에 클라이언트에서 핸들을 다시 확보할 수 있는 기회를 제공할 뿐 아니라 CIFS 서버는 60초 동안 파일에 대한 액세스를 요청하는 다른 클라이언트에 대한 액세스를 거부합니다.

영구 핸들에 대한 정보는 SFO 파트너의 영구 스토리지에 미러링되므로, 영구 핸들이 분리된 클라이언트는 SFO 파트너가 노드 스토리지에 대한 소유권을 갖게 된 후 내구성 있는 핸들을 다시 확보할 수 있습니다. 지속적인 핸들은 LIF 이동 시 무중단 운영(내구성이 뛰어난 핸들 지원)을 제공할 뿐만 아니라 테이크오버, 반환 및 애그리게이트 재배치를 위한 무중단 운영을 제공합니다.

- SFO 반환 *

  테이크오버 이벤트에서 복구할 때 애그리게이트를 홈 위치로 반환

- SFO 쌍 *

  두 노드 중 하나가 작동을 중지할 경우 컨트롤러가 상호 데이터를 제공하도록 구성된 노드 쌍입니다. 시스템 모델에 따라 두 컨트롤러 모두 단일 섀시 내에 있거나 컨트롤러가 별도 섀시에 있을 수 있습니다. 2노드 클러스터에서 HA 쌍이라고 합니다.

- * 테이크오버 *

  해당 스토리지의 기본 소유자가 실패한 경우 파트너가 스토리지를 제어하는 프로세스입니다. SFO 맥락에서 페일오버 및 테이크오버는 동의어입니다.

SMB 3.0 기능이 **SMB** 공유에서 무중단 운영을 지원하는 방법

SMB 3.0은 SMB 공유를 통해 Hyper-V 및 SQL Server의 무중단 운영을 지원하는 중요한 기능을 제공합니다. 여기에는 SMB 클라이언트가 파일 열기 상태를 재확보하고 SMB 연결을 투명하게 다시 설정할 수 있도록 하는 '연속 사용 가능' 공유 속성과 '영구 핸들'이라는 파일 핸들 유형이 포함됩니다.

지속적으로 사용 가능한 공유 속성 집합을 사용하여 공유에 연결하는 SMB 3.0 지원 클라이언트에 영구 핸들을 부여할 수 있습니다. SMB 세션의 연결이 끊기면 CIFS 서버는 영구 처리 상태에 대한 정보를 유지합니다. CIFS 서버는 클라이언트가 다시 연결될 수 있는 60초 동안 다른 클라이언트 요청을 차단하여, 영구 핸들이 있는 클라이언트가 네트워크 연결 해제 후 핸들을 다시 확보할 수 있도록 합니다. 핸들을 지속적으로 사용하는 클라이언트는 SVM(스토리지 가상 머신)의 데이터 LIF 중 하나를 사용하여 다시 연결할 수 있습니다. 즉, 동일한 LIF를 통해 다시 연결하거나 다른 LIF를 통해 다시 연결할 수 있습니다.

애그리게이트 재배치, 테이크오버 및 반환은 모두 SFO 쌍 간에 발생합니다. 영구 핸들이 있는 파일을 사용하여 세션의 분리 및 재연결을 원활하게 관리하기 위해 파트너 노드는 모든 영구 핸들 잠금 정보의 복사본을 유지 관리합니다. SFO 파트너는 이벤트의 계획인지 계획되지 않는지에 관계없이 영구 핸들 연결을 중단 없이 관리할 수 있습니다. 이 새로운 기능을 통해 CIFS 서버에 대한 SMB 3.0 연결이 예전부터 운영 중단 없이 할당된 SVM에 할당된 다른 데이터 LIF로 투명하게 페일오버할 수 있습니다.

영구 핸들을 사용하면 CIFS 서버가 SMB 3.0 연결을 투명하게 페일오버할 수 있지만 장애가 발생하여 Hyper-V 애플리케이션이 Windows Server 클러스터의 다른 노드로 페일오버될 경우 클라이언트는 연결이 끊어진 핸들의 파일 핸들을 다시 확보할 수 없습니다. 이 시나리오에서는 연결이 끊긴 상태의 파일 핸들이 다른 노드에서 다시 시작될 경우 Hyper-V 응용 프로그램의 액세스를 차단할 수 있습니다. ""장애 조치 클러스터링""은 SMB 3.0의 일부이며, 이러한 시나리오를 해결하기 위해 오래되고 충돌하는 핸들을 무효화하는 메커니즘을 제공합니다. 이 메커니즘을 사용하면 Hyper-V 클러스터 노드에 장애가 발생할 경우 Hyper-V 클러스터가 신속하게 복구될 수 있습니다.

Witness 프로토콜이 투명한 장애 조치를 강화하기 위해 수행하는 조치

Witness 프로토콜은 SMB 3.0에서 지속적으로 사용 가능한 공유(CA 공유)를 위한 향상된 클라이언트 페일오버 기능을 제공합니다. 입회자는 LIF 페일오버 복구 기간을 거치지 않으므로 더 빠른 페일오버를 촉진합니다. SMB 3.0 연결이 시간 초과될 때까지 기다리지 않고 노드를 사용할 수 없을 때 애플리케이션 서버에 알립니다.

클라이언트에서 실행 중인 애플리케이션이 페일오버가 발생했는지 알지 못하면서 페일오버가 원활하게 이루어집니다. Witness를 사용할 수 없는 경우에도 페일오버 작업은 성공적으로 수행되지만 Witness를 사용하지 않는 페일오버는 효율성이 떨어집니다.

다음 요구 사항이 충족되면 감시 강화 장애 조치가 가능합니다.

- SMB 3.0이 활성화된 SMB 3.0 지원 CIFS 서버에서만 사용할 수 있습니다.
- 공유는 지속적인 가용성 공유 속성 세트와 함께 SMB 3.0을 사용해야 합니다.
- 애플리케이션 서버가 연결되는 노드의 SFO 파트너는 애플리케이션 서버의 데이터를 호스팅하는 SVM(스토리지 가상 머신)에 적어도 하나의 운영 데이터 LIF가 할당되어 있어야 합니다.

> Witness 프로토콜은 SFO 쌍 사이에서 작동합니다. LIF가 클러스터 내의 노드로 마이그레이션할 수 있으므로 모든 노드가 SFO 파트너의 증인이 될 수 있습니다. 애플리케이션 서버용 데이터를 호스팅하는 SVM이 파트너 노드에 활성 데이터 LIF가 없는 경우 Witness 프로토콜은 특정 노드에서 SMB 연결을 빠르게 페일오버할 수 없습니다. 따라서 클러스터의 모든 노드는 이러한 구성 중 하나를 호스팅하는 각 SVM에 대해 적어도 하나의 데이터 LIF를 가져야 합니다.

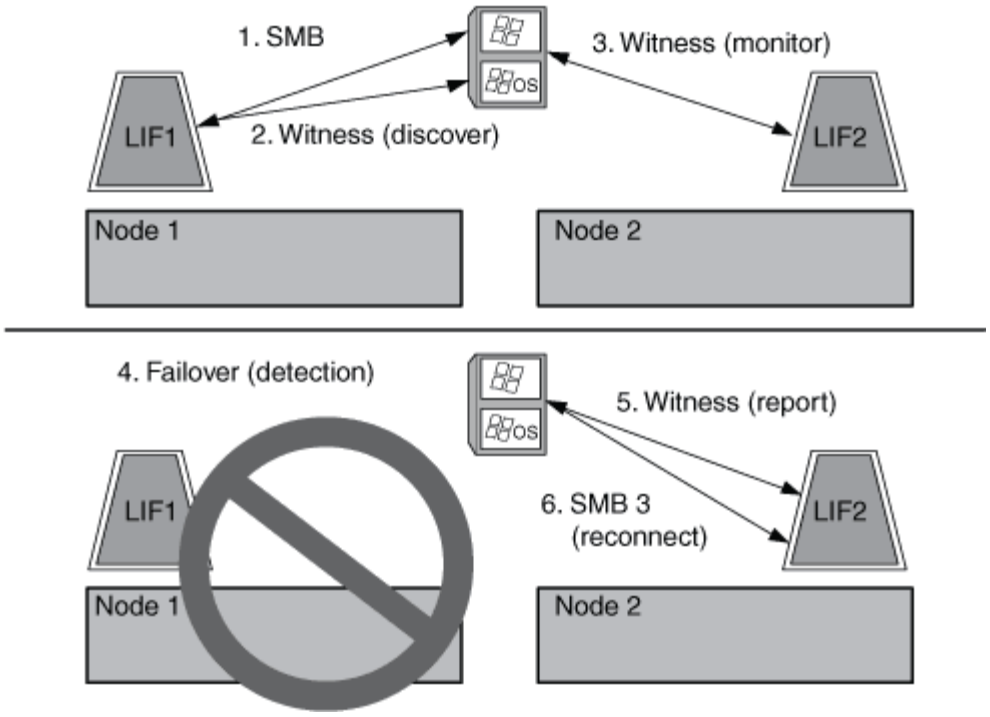
- 애플리케이션 서버는 개별 LIF IP 주소를 사용하는 대신 DNS에 저장된 CIFS 서버 이름을 사용하여 CIFS 서버에 연결해야 합니다.

Witness 프로토콜 작동 방식

ONTAP는 노드의 SFO 파트너를 증인으로 사용하여 Witness 프로토콜을 구현합니다. 장애가 발생할 경우 파트너는 빠르게 장애를 감지하고 SMB 클라이언트에 알립니다.

Witness 프로토콜은 다음 프로세스를 사용하여 향상된 장애 조치를 제공합니다.

1. 애플리케이션 서버가 Node1에 대한 지속적으로 사용 가능한 SMB 연결을 설정하면 CIFS 서버가 애플리케이션 서버에 Witness를 사용할 수 있음을 알립니다.
2. 애플리케이션 서버는 Node1에서 Witness 서버의 IP 주소를 요청하고, 스토리지 가상 시스템(SVM)에 할당된 Node2(SFO 파트너) 데이터 LIF IP 주소 목록을 수신합니다.
3. 애플리케이션 서버는 IP 주소 중 하나를 선택하고 Node2에 대한 Witness 연결을 생성하며, Node1에서 계속 사용 가능한 연결이 이동해야 하는 경우 알림을 받을 레지스터를 생성합니다.
4. Node1에서 페일오버 이벤트가 발생할 경우 Witness는 페일오버 이벤트를 발생하지만 반환과 관련이 없습니다.
5. 감시 기능은 장애 조치 이벤트를 감지하고 Witness 연결을 통해 애플리케이션 서버에 SMB 연결이 Node2로 이동해야 함을 알립니다.
6. 애플리케이션 서버는 SMB 세션을 Node2로 이동하고 클라이언트 액세스를 중단하지 않고 연결을 복구합니다.



원격 **VSS**와 공유 기반 백업

원격 **VSS**를 사용한 공유 기반 백업 개요

원격 VSS를 사용하여 CIFS 서버에 저장된 Hyper-V 가상 머신 파일의 공유 기반 백업을 수행할 수 있습니다.

Microsoft 원격 VSS(Volume Shadow Copy Services)는 기존 Microsoft VSS 인프라의 확장입니다. Microsoft는 원격 VSS를 통해 VSS 인프라스트럭처를 확장하여 SMB 공유의 섀도우 복제를 지원하고 있습니다. 또한 Hyper-V와 같은 서버 애플리케이션에서 SMB 파일 공유에 VHD 파일을 저장할 수 있습니다. 이러한 확장을 사용하면 데이터 및 구성 파일을 공유에 저장하는 가상 시스템에 대해 애플리케이션 정합성이 보장되는 섀도우 복제본을 가져올 수 있습니다.

원격 **VSS** 개념

SMB를 통한 Hyper-V 구성의 백업 서비스에서 원격 VSS(Volume Shadow Copy Service)를 사용하는 방법을 이해하는 데 필요한 특정 개념을 이해해야 합니다.

- * VSS(Volume Shadow Copy Service) *

  특정 시점에 특정 볼륨에 있는 데이터의 백업 복사본 또는 스냅샷을 생성하는 데 사용되는 Microsoft 기술입니다. VSS는 데이터 서버, 백업 애플리케이션 및 스토리지 관리 소프트웨어 사이에서 조정을 수행하여 일관된 백업의 생성 및 관리를 지원합니다.

- * 원격 VSS(원격 볼륨 섀도 복사본 서비스) *

  SMB 3.0 공유를 통해 데이터에 액세스할 수 있는 특정 시점의 데이터 정합성 보장 상태에 있는 데이터의 공유 기반 백업 복사본을 생성하는 데 사용되는 Microsoft 기술입니다. 볼륨 섀도 복사본 서비스 _ 라고도 합니다.

- * 섀도 복사본 *

  공유에 포함된 중복 데이터 집합을 적절하게 정의된 즉시 사용합니다. 섀도우 복제본은 데이터의 일관된 시점 백업을 생성하는 데 사용되므로 시스템이나 애플리케이션에서 원래 볼륨의 데이터를 계속 업데이트할 수 있습니다.

- * 섀도 복사본 세트 *

  한 공유에 해당하는 각 섀도 복사본을 포함하는 하나 이상의 섀도 복사본 모음입니다. 섀도우 복제본 세트 내의 섀도우 복제본은 동일한 작업에서 백업해야 하는 모든 공유를 나타냅니다. VSS 지원 애플리케이션의 VSS 클라이언트는 세트에 포함할 섀도우 복제본을 식별합니다.

- * 섀도우 복제본 세트 자동 복구 *

  섀도우 복제본이 포함된 복제본 디렉토리가 시점 정합성이 보장되는 원격 VSS 지원 백업 애플리케이션에 대한 백업 프로세스의 일부입니다. 백업을 시작할 때 애플리케이션의 VSS 클라이언트는 백업 예약된 데이터(Hyper-V의 경우 가상 머신 파일)에서 소프트웨어 체크포인트를 생성하도록 애플리케이션을 트리거합니다. 그러면 VSS 클라이언트가 응용 프로그램을 계속할 수 있습니다. 섀도우 복제본 세트가 생성된 후 원격 VSS는 섀도우 복제본 세트를 쓰기 가능하게 만들고 쓰기 가능한 복제본을 애플리케이션에 노출합니다. 애플리케이션은 앞서 생성한 소프트웨어 체크포인트를 사용하여 자동 복구를 수행하여 섀도우 복제본 세트를 백업할 준비를 합니다. 자동 복구는 체크포인트가 생성된 이후 파일 및 디렉토리의 변경 사항을 언롤링함으로써 섀도우 복제본을 정합성 보장 상태로 만듭니다. 자동 복구는 VSS 지원 백업을 위한 선택적 단계입니다.

- * 섀도 복사본 ID *

  섀도우 복제본을 고유하게 식별하는 GUID입니다.

- * 섀도 복사본 세트 ID *

  동일한 서버에 대한 섀도우 복제본 ID의 컬렉션을 고유하게 식별하는 GUID입니다.

- * Hyper-V * 용 SnapManager

  Microsoft Windows Server 2012 Hyper-V의 백업 및 복원 작업을 자동화하고 단순화하는 소프트웨어입니다 SnapManager for Hyper-V는 원격 VSS와 자동 복구를 사용하여 SMB 공유를 통해 Hyper-V 파일을 백업합니다.

관련 정보

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영에 대한 주요 개념입니다

원격 VSS와 공유 기반 백업

원격 **VSS**에서 사용하는 디렉토리 구조의 예

원격 VSS는 섀도우 복제본을 생성할 때 Hyper-V 가상 머신 파일을 저장하는 디렉토리 구조를 통과합니다. 가상 머신 파일의 백업을 성공적으로 생성할 수 있도록 적절한 디렉토리 구조가 무엇인지 이해하는 것이 중요합니다.

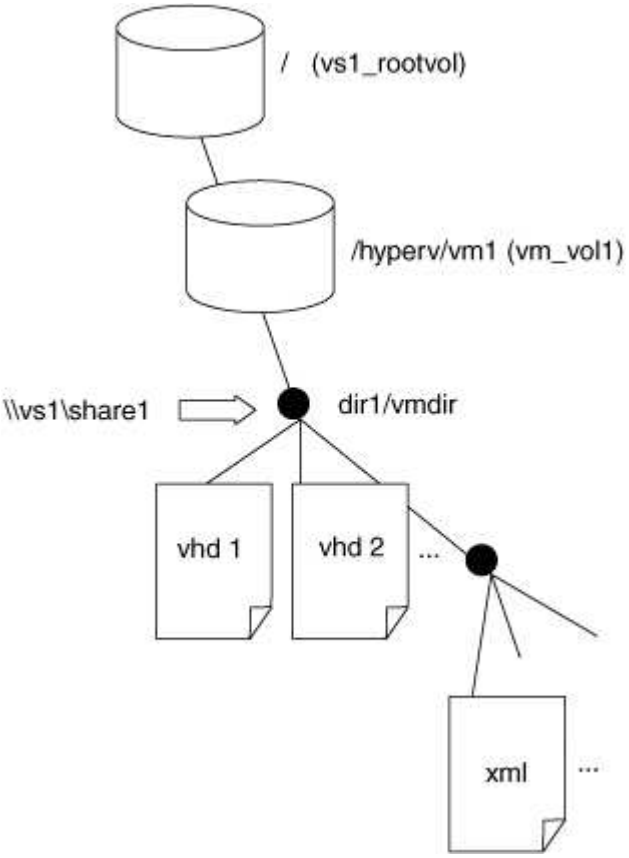
섀도우 복제본을 성공적으로 생성하기 위해 지원되는 디렉토리 구조는 다음 요구 사항을 따릅니다.

- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조 내에는 디렉토리와 일반 파일만 있습니다.

  디렉터리 구조에는 연결 지점, 링크 또는 비정규 파일이 포함되어 있지 않습니다.

- 가상 머신의 모든 파일은 단일 공유 내에 있습니다.
- 가상 머신 파일을 저장하는 데 사용되는 디렉토리 구조가 섀도 복사본 디렉토리의 구성된 깊이를 초과하지 않습니다.
- 공유의 루트 디렉토리에는 가상 머신 파일 또는 디렉토리만 포함됩니다.

다음 그림에서는 vm_vol1이라는 이름의 볼륨이 SVM(Storage Virtual Machine) VS1 의 '/hyperv/vm1'에 있는 접합 지점으로 생성됩니다. 가상 머신 파일을 포함하는 하위 디렉토리는 교차점 아래에 생성됩니다. Hyper-V 서버의 가상 머신 파일은 "/hyperv/vm1/dir1/vmdir" 경로가 있는 share1을 통해 액세스합니다. 섀도 복사본 서비스는 share1 아래의 디렉토리 구조 내에 포함된 모든 가상 머신 파일의 섀도 복사본을 만듭니다(섀도우 복제본 디렉토리의 구성된 깊이까지).



SnapManager for Hyper-V가 SMB를 통해 Hyper-V에 대한 원격 VSS 기반 백업을 관리하는 방법

SnapManager for Hyper-V를 사용하여 원격 VSS 기반 백업 서비스를 관리할 수 있습니다. SnapManager for Hyper-V 관리 백업 서비스를 사용하면 공간 효율적인 백업 세트를 생성할 수 있다는 이점이 있습니다.

Hyper-V 관리 백업을 위한 SnapManager 최적화 기능은 다음과 같습니다.

- ONTAP와 SnapDrive의 통합은 SMB 공유 위치를 검색할 때 성능을 최적화합니다.

  ONTAP는 공유가 상주하는 볼륨의 이름을 SnapDrive에 제공합니다.

- SnapManager for Hyper-V는 섀도우 복제본 서비스를 복제해야 하는 SMB 공유의 가상 머신 파일 목록을 지정합니다.

가상 머신 파일의 타겟 목록을 제공함으로써 섀도우 복제본 서비스는 공유에 있는 모든 파일의 섀도우 복제본을 생성할 필요가 없습니다.

- 스토리지 가상 머신(SVM)에 복원에 사용할 SnapManager for Hyper-V의 스냅샷이 보존됩니다.

  백업 단계가 없습니다. 백업은 공간 효율성이 뛰어난 스냅샷입니다.

SnapManager for Hyper-V는 다음 프로세스를 사용하여 SMB를 통한 Hyper-V의 백업 및 복원 기능을 제공합니다.

1. 섀도 복사본 작업을 준비하는 중입니다

   SnapManager for Hyper-V 애플리케이션의 VSS 클라이언트는 섀도우 복제본 세트를 설정합니다. VSS 클라이언트는 섀도 복사본 세트에 포함할 공유에 대한 정보를 수집하고 이 정보를 ONTAP에 제공합니다. 세트에는 하나 이상의 섀도 복사본이 포함될 수 있으며 하나의 섀도 복사본은 하나의 공유에 해당합니다.

2. 섀도 복사본 세트 생성(자동 복구가 사용되는 경우)

   섀도 복사본 세트에 포함된 모든 공유에서 ONTAP는 섀도 복사본을 만들고 섀도 복사본을 쓰기 가능하게 만듭니다.

3. 섀도우 복제본 세트를 노출합니다

   ONTAP에서 섀도우 복제본을 생성한 후 SnapManager for Hyper-V에 노출되므로 애플리케이션의 VSS 작성기가 자동 복구를 수행할 수 있습니다.

4. 섀도우 복제본 세트를 자동으로 복구합니다

   섀도우 복제본 세트를 생성하는 동안 백업 세트에 포함된 파일에 대한 활성 변경이 발생하는 기간이 있습니다. 애플리케이션의 VSS 작성자는 섀도우 복제본을 업데이트하여 백업 전에 정합성이 완벽하게 보장되는 상태인지 확인해야 합니다.

   ⓘ 자동 복구를 수행하는 방법은 애플리케이션에 따라 다릅니다. 원격 VSS가 이 단계에 없습니다.

5. 섀도 복사본 세트 완료 및 정리

   VSS 클라이언트는 자동 복구를 완료한 후 ONTAP에 알립니다. 섀도 복사본 세트는 읽기 전용으로 만들어져 백업할 준비가 된 상태입니다. 백업에 SnapManager for Hyper-V를 사용하면 스냅샷의 파일이 백업이 되므로 백업 단계의 경우 백업 세트의 공유를 포함하는 모든 볼륨에 대해 스냅샷이 생성됩니다. 백업이 완료되면 CIFS 서버에서 섀도우 복제본 세트가 제거됩니다.

SMB 공유를 통해 Hyper-V 및 SQL Server에서 ODX 복사 오프로드를 사용하는 방법

ODX(Offloaded Data Transfer)는 _copy offload_라고도 하며 호스트 컴퓨터를 통해 데이터를 전송하지 않고도 호환되는 스토리지 장치 내부 또는 간에 직접 데이터를 전송할 수 있습니다. ONTAP ODX 복사 오프로드를 사용하면 SMB 설치를 통해 애플리케이션 서버에서 복사 작업을 수행할 때 성능 이점을 얻을 수 있습니다.

ODX가 아닌 파일 전송에서는 소스 CIFS 서버에서 데이터를 읽고 네트워크를 통해 클라이언트 컴퓨터로 전송합니다. 클라이언트 컴퓨터는 네트워크를 통해 대상 CIFS 서버로 데이터를 다시 전송합니다. 요약하면 클라이언트 컴퓨터는 소스에서 데이터를 읽고 대상에 씁니다. ODX 파일 전송을 사용하면 데이터가 소스에서 타겟으로 직접 복사됩니다.

오프로드 복사본은 소스 및 타겟 스토리지 간에 직접 수행되므로 성능이 크게 향상됩니다. 소스 및 대상 간의 복제 시간 단축, 클라이언트의 리소스 활용률(CPU, 메모리) 감소, 네트워크 I/O 대역폭 사용률 감소 등의 성능 이점을 얻을 수 있습니다.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
ODX 복사 및 이동 사용을 지원하는 사용 사례는 다음과 같습니다.
```

- 체내

  소스 및 대상 파일 또는 LUN이 동일한 볼륨 내에 있습니다.

- 볼륨 간, 동일한 노드, 동일한 SVM(스토리지 가상 머신)

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- 볼륨 간, 다른 노드, 동일한 SVM

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 동일한 SVM이 소유합니다.

- SVM 간, 동일한 노드

  소스 및 대상 파일 또는 LUN이 동일한 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

- SVM 간, 다른 노드

  소스 및 대상 파일 또는 LUN이 서로 다른 노드에 있는 서로 다른 볼륨에 있습니다. 데이터는 서로 다른 SVM에서 소유합니다.

Hyper-V 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- Hyper-V에서 ODX 복사 오프로드 패스스스루 를 사용하여 VHD(가상 하드 디스크) 파일 내부 또는 VHD 파일 간에 데이터를 복사하거나, 매핑된 SMB 공유와 동일한 클러스터 내에서 연결된 iSCSI LUN 간에 데이터를 복사할 수 있습니다.

  이렇게 하면 게스트 운영 체제에서 복제본을 기본 스토리지로 전달할 수 있습니다.

- 고정 크기의 VHD를 생성할 때 ODX는 잘 알려진 제로화 토큰을 사용하여 0으로 디스크를 초기화하는 데 사용됩니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드가 가상 머신 스토리지 마이그레이션에 사용됩니다.

> Hyper-V를 사용한 ODX 복사 오프로드 패스쓰루 사용 사례를 활용하려면 게스트 운영 체제가 ODX를 지원하고, 게스트 운영 체제 디스크는 ODX를 지원하는 스토리지(SMB 또는 SAN)를 통해 지원되는 SCSI 디스크여야 합니다. 게스트 운영 체제의 IDE 디스크는 ODX 패스스스루 를 지원하지 않습니다.

SQL Server 솔루션을 사용한 ODX 복사 오프로드의 구체적인 사용 사례는 다음과 같습니다.

- ODX 복사 오프로드 를 사용하여 매핑된 SMB 공유 간에 또는 동일한 클러스터 내에서 SMB 공유와 연결된 iSCSI LUN 간에 SQL Server 데이터베이스를 내보내고 가져올 수 있습니다.
- 소스 및 타겟 스토리지가 동일한 클러스터에 있는 경우 ODX 복사 오프로드를 사용하여 데이터베이스를 내보내고 가져올 수 있습니다.

구성 요구 사항 및 고려 사항

ONTAP 및 라이센스 요구 사항

SVM에서 무중단 운영을 위해 SQL Server 또는 Hyper-V over SMB 솔루션을 생성할 때 특정 ONTAP 및 라이센스 요구사항을 알아야 합니다.

ONTAP 버전 요구 사항

- SMB를 통한 Hyper-V

  ONTAP는 Windows 2012 이상에서 실행되는 Hyper-V에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

- SMB를 통한 SQL Server

  ONTAP는 Windows 2012 이상에서 실행되는 SQL Server 2012 이상에 대해 SMB 공유를 통한 무중단 운영을 지원합니다.

SMB 공유에서 무중단 운영을 지원하는 ONTAP, Windows Server 및 SQL Server의 지원되는 버전에 대한 최신 정보는 상호 운용성 매트릭스 를 참조하십시오.

"NetApp 상호 운용성 매트릭스 툴"

라이센스 요구 사항

다음 라이센스가 필요합니다.

- CIFS를 선택합니다
- FlexClone(SMB를 통한 Hyper-V만 해당)

  원격 VSS를 백업에 사용하는 경우 이 라이센스가 필요합니다. 섀도 복사본 서비스는 FlexClone을 사용하여 백업을 만들 때 사용되는 파일의 시점 복사본을 만듭니다.

  FlexClone 라이센스는 원격 VSS를 사용하지 않는 백업 방법을 사용하는 경우 선택 사항입니다.

FlexClone 라이센스는 에 포함되어 "ONTAP 1 을 참조하십시오"있습니다. ONTAP One이 없는 경우, "필요한 라이센스가 설치되어 있는지 확인합니다"그리고 필요한 경우, 를 수행해야 "설치합니다"합니다.

네트워크 및 데이터 **LIF** 요구사항

무중단 운영을 위해 SQL Server 또는 SMB를 통한 Hyper-V 구성을 생성할 때 특정 네트워크 및 데이터 LIF 요구사항을 알고 있어야 합니다.

네트워크 프로토콜 요구 사항

- IPv4 및 IPv6 네트워크가 지원됩니다.
- SMB 3.0 이상이 필요합니다.

  SMB 3.0은 무중단 운영을 제공하는 데 필요한 지속적으로 사용 가능한 SMB 연결을 생성하는 데 필요한 기능을 제공합니다.

- DNS 서버에는 SVM(Storage Virtual Machine)의 데이터 LIF에 할당된 IP 주소에 CIFS 서버 이름을 매핑하는 항목이 포함되어 있어야 합니다.

  Hyper-V 또는 SQL Server 애플리케이션 서버는 일반적으로 가상 머신 또는 데이터베이스 파일에 액세스할 때 여러 데이터 LIF를 통해 여러 개의 연결을 생성합니다. 적절한 기능을 위해 애플리케이션 서버는 여러 고유 IP 주소에 여러 번 연결하는 대신 CIFS 서버 이름을 사용하여 이러한 여러 SMB 연결을 설정해야 합니다.

  또한 감시 기능을 사용하려면 개별 LIF IP 주소 대신 CIFS 서버의 DNS 이름을 사용해야 합니다.

  ONTAP 9.4부터 SMB 멀티 채널을 활성화하여 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다. 이렇게 하려면 클러스터 및 클라이언트에 1G, 10G 또는 더 큰 NIC가 여러 개 설치되어 있어야 합니다.

데이터 **LIF** 요구사항

- SMB 솔루션을 통해 애플리케이션 서버를 호스팅하는 SVM은 클러스터의 모든 노드에 운영 데이터 LIF가 하나 이상 있어야 합니다.

  SVM 데이터 LIF는 애플리케이션 서버에서 액세스하는 데이터를 현재 호스팅하지 않는 노드를 비롯하여 클러스터 내의 다른 데이터 포트로 페일오버할 수 있습니다. 또한 Witness 노드는 항상 애플리케이션 서버가 접속된 노드의 SFO 파트너이므로 클러스터의 모든 노드가 잠재적인 Witness 노드입니다.

- 데이터 LIF가 자동으로 복구되도록 구성하지 않아야 합니다.

  테이크오버 또는 반환 이벤트가 발생한 후에는 데이터 LIF를 홈 포트로 수동으로 되돌려야 합니다.

- 모든 데이터 LIF IP 주소에는 DNS에 항목이 있어야 하며 모든 항목이 CIFS 서버 이름으로 확인되어야 합니다.

  애플리케이션 서버는 CIFS 서버 이름을 사용하여 SMB 공유에 접속해야 합니다. LIF IP 주소를 사용하여 연결되도록 애플리케이션 서버를 구성하지 마십시오.

- CIFS 서버 이름이 SVM 이름과 다른 경우 DNS 항목이 CIFS 서버 이름으로 확인되어야 합니다.

SMB를 통한 **Hyper-V**의 **SMB** 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 Hyper-V 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

  애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

  Hyper-V 시스템 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- Kerberos 및 NTLM 인증은 SMB 서버가 속한 도메인에서 모두 허용되어야 합니다.

  ONTAP는 원격 VSS에 대한 Kerberos 서비스를 광고하지 않으므로 NTLM을 허용하도록 도메인을 설정해야 합니다.

- 섀도 복사본 기능이 활성화되어 있어야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 섀도 복사본을 만들 때 섀도 복사본 서비스가 사용하는 Windows 도메인 계정은 SMB 서버 로컬 BUILTIN\Administrators 또는 BUILTIN\Backup Operators 그룹의 구성원이어야 합니다.

볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 섀도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

  사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

SMB를 통한 **SQL Server**의 **SMB** 서버 및 볼륨 요구 사항

무중단 운영을 위해 SMB를 통한 SQL Server 구성을 생성할 때 특정 SMB 서버 및 볼륨 요구사항을 알고 있어야 합니다.

SMB 서버 요구 사항

- SMB 3.0을 활성화해야 합니다.

  이 기능은 기본적으로 활성화되어 있습니다.

- 기본 UNIX 사용자 CIFS 서버 옵션은 유효한 UNIX 사용자 계정으로 구성해야 합니다.

  애플리케이션 서버는 SMB 연결을 생성할 때 컴퓨터 계정을 사용합니다. 모든 SMB 액세스를 위해서는 Windows 사용자가 UNIX 사용자 계정 또는 기본 UNIX 사용자 계정에 성공적으로 매핑되어야 하므로 ONTAP는 애플리케이션 서버의 컴퓨터 계정을 기본 UNIX 사용자 계정에 매핑할 수 있어야 합니다.

  또한 SQL Server에서는 도메인 사용자를 SQL Server 서비스 계정으로 사용합니다. 서비스 계정도 기본 UNIX 사용자에게 매핑되어야 합니다.

- 자동 노드 조회를 비활성화해야 합니다(이 기능은 기본적으로 비활성화되어 있습니다).

  SQL Server 데이터베이스 파일 이외의 데이터에 액세스하기 위해 자동 노드 조회를 사용하려면 해당 데이터에 대해 별도의 SVM을 생성해야 합니다.

- ONTAP에 SQL Server를 설치하는 데 사용되는 Windows 사용자 계정에 SeSecurityPrivilege 권한이 할당되어야 합니다.

  이 권한은 SMB 서버 로컬 BUILTIN\Administrators 그룹에 할당됩니다.

볼륨 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 사용하여 애플리케이션 서버에 NDO를 제공하려면 공유가 포함된 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통해 NDO에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인 백업 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다.

  SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

관련 정보

"Microsoft TechNet 라이브러리: technet.microsoft.com/en-us/library/"

SMB를 통한 **Hyper-V**의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 Hyper-V에서 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

공유 요구 사항

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

  지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배치와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 원격 VSS 지원 백업 서비스를 사용하려는 경우 접합을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.

  자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 섀도우 복제본 생성이 실패합니다. 자동 복구가 아닌 경우 섀도우 복제본 생성이 실패하지는 않지만 교차점은 아무 것도 가리키지 않습니다.

- 자동 복구와 함께 원격 VSS 지원 백업 서비스를 사용하려는 경우 다음을 포함하는 공유에 Hyper-V 파일을 넣을 수 없습니다.
  - symlinks, hardlinks 또는 wdelink
  - 일반 파일이 아닙니다

    공유에 섀도우 복제본으로 연결되는 링크나 비정규 파일이 있는 경우 섀도우 복제본 생성이 실패합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

  - 섀도 복사본 작업이 성공하려면 볼륨에 충분한 공간이 있어야 합니다(SMB를 통한 Hyper-V만 해당).

    사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다. 이 요구 사항은 자동 복구를 사용하는 섀도우 복제본에만 적용됩니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.
  - 더 높여 줍니다
  - 특성 캐싱
  - BranchCache입니다

고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 Hyper-V 구성에서는 다음 기능이 지원되지 않습니다.
  - 감사
  - FPolicy를 참조하십시오
- '연속 가용성' 매개변수가 '예'로 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

SMB를 통한 **SQL Server**의 지속적인 가용성 공유 요구 사항 및 고려 사항

무중단 운영을 지원하는 SMB 구성을 통해 SQL Server에 대해 지속적으로 사용 가능한 공유를 구성할 때 특정 요구사항과 고려 사항을 알고 있어야 합니다.

공유 요구 사항

- 가상 머신 파일을 저장하는 데 사용되는 볼륨은 NTFS 보안 스타일 볼륨으로 만들어야 합니다.

  지속적으로 사용 가능한 SMB 연결을 통해 애플리케이션 서버에 무중단 운영을 제공하려면 공유를 포함하는 볼륨이 NTFS 볼륨이어야 합니다. 또한 항상 NTFS 볼륨이어야 합니다. 혼합 보안 스타일 볼륨 또는 UNIX 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 운영에 직접 사용할 수는 없습니다. 혼합 보안 스타일 볼륨을 NTFS 보안 스타일 볼륨으로 변경하고 SMB 공유를 통한 무중단 작업에 사용하려면 ACL을 볼륨 상단에 수동으로 배치하고 해당 ACL을 포함된 모든 파일 및 폴더에 전파해야 합니다. 그렇지 않으면 소스 또는 대상 볼륨이 처음에 혼합 또는 UNIX 보안 스타일 볼륨으로 생성된 후 나중에 NTFS 보안 스타일로 변경된 경우 가상 머신 마이그레이션 또는 데이터베이스 파일 내보내기 및 가져오기가 다른 볼륨으로 이동될 수 있습니다.

- 응용 프로그램 서버에서 사용하는 공유는 지속적으로 사용 가능한 속성 집합을 사용하여 구성해야 합니다.

  지속적으로 사용 가능한 공유에 연결되는 애플리케이션 서버에는 SMB 공유에 중단 없이 다시 연결할 수 있는 영구 핸들이 제공되며, 테이크오버, 반환, 애그리게이트 재배치와 같은 운영 중단 이벤트가 발생한 후 파일 잠금을 재확보할 수 있습니다.

- 데이터베이스 파일이 포함된 볼륨에는 접합부가 포함될 수 있지만 SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 접합을 교차하지 않습니다.
- Microsoft SQL Server용 SnapCenter 플러그인을 성공적으로 사용하려면 볼륨에 충분한 공간이 있어야 합니다.

  SQL Server 데이터베이스 파일이 있는 볼륨은 데이터베이스 디렉토리 구조와 공유 내에 있는 모든 포함된 파일을 저장할 수 있을 만큼 커야 합니다.

- 애플리케이션 서버에서 계속 사용 가능한 공유에 대해 다음 공유 속성을 설정하지 않아야 합니다.
  - 더 높여 줍니다
  - 특성 캐싱
  - BranchCache입니다

공유 고려 사항

- 할당량은 지속적으로 사용 가능한 공유에서 지원됩니다.
- SMB를 통한 SQL Server 구성에서는 다음 기능이 지원되지 않습니다.
  - 감사
  - FPolicy를 참조하십시오
- 지속적으로 사용 가능한 공유 자산이 설정된 SMB 공유에서는 바이러스 검사가 수행되지 않습니다.

SMB 구성을 통한 **Hyper-V**에 대한 원격 **VSS** 고려 사항

SMB를 통한 Hyper-V 구성에 대해 원격 VSS 지원 백업 솔루션을 사용할 때는 특정 고려 사항을 염두에 두어야 합니다.

일반 원격 **VSS** 고려 사항

- Microsoft 애플리케이션 서버당 최대 64개의 공유를 구성할 수 있습니다.

  섀도우 복제본 세트에 64개 이상의 공유가 있는 경우 섀도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구

사항입니다.

- CIFS 서버당 하나의 활성 섀도 복사본 세트만 허용됩니다.

  동일한 CIFS 서버에 섀도우 복제본 작업이 진행 중인 경우 섀도우 복제본 작업이 실패합니다. 이는 Microsoft의 요구 사항입니다.

- 원격 VSS가 섀도우 복제본을 생성하는 디렉토리 구조 내에서는 접합을 수행할 수 없습니다.
  - 자동 복구 사례에서는 공유를 이동하는 동안 분기점이 발생하면 섀도우 복제본 생성이 실패합니다.
  - 비자동 복구 사례에서는 섀도우 복제본 생성이 실패하지 않지만 접합은 아무 것도 가리키지 않습니다.

자동 복구를 사용하는 섀도우 복제본에만 적용되는 원격 **VSS** 고려 사항

자동 복구를 사용하는 섀도 복사본에만 특정 제한사항이 적용됩니다.

- 섀도우 복제본 생성에는 하위 디렉토리 5개의 최대 디렉토리 수준이 허용됩니다.

  섀도우 복제본 서비스가 섀도우 복제본 백업 세트를 생성하는 디렉토리 깊이입니다. 가상 머신 파일이 포함된 디렉토리가 5개 수준 이상 중첩되면 섀도우 복제본 생성이 실패합니다. 이는 공유를 복제할 때 디렉토리 트래버설을 제한하기 위한 것입니다. 최대 디렉토리 깊이는 CIFS 서버 옵션을 사용하여 변경할 수 있습니다.

- 볼륨의 사용 가능한 공간이 적절해야 합니다.

  사용 가능한 공간은 섀도 복사본 백업 세트에 포함된 공유 내에 포함된 모든 파일, 디렉토리 및 하위 디렉토리에 사용되는 결합된 공간보다 최소한 크거나 같아야 합니다.

- 원격 VSS가 섀도우 복제본을 생성하는 디렉토리 구조 내에서 링크나 일반 파일이 허용되지 않습니다.

  공유에 섀도 복사본에 대한 링크 또는 비정규 파일이 있는 경우 섀도 복사본 생성이 실패합니다. 클론 프로세스에서 이를 지원하지 않습니다.

- 디렉토리에는 NFSv4 ACL이 허용되지 않습니다.

  섀도우 복제본 생성이 파일에 NFSv4 ACL을 유지하지만 디렉토리의 NFSv4 ACL이 손실됩니다.

- 섀도 복사본 세트를 생성할 수 있는 시간은 최대 60초입니다.

  Microsoft 사양은 섀도 복사본 세트를 생성하는 데 최대 60초를 허용합니다. VSS 클라이언트가 이 시간 내에 섀도우 복제본 세트를 생성할 수 없는 경우 섀도우 복제본 작업이 실패하므로 섀도우 복제본 세트의 파일 수가 제한됩니다. 백업 세트에 포함될 수 있는 실제 파일 또는 가상 머신 수는 서로 다르며, 이 수는 여러 요인에 따라 달라지며 각 고객 환경에 따라 결정되어야 합니다.

ODX SMB를 통한 **SQL Server** 및 **Hyper-V**의 복사 오프로드 요구 사항

가상 머신 파일을 마이그레이션하거나 애플리케이션 서버를 통해 데이터를 전송하지 않고 데이터베이스 파일을 소스에서 대상 스토리지 위치로 직접 내보내고 가져오려면 ODX 복사 오프로드를 활성화해야 합니다. SQL Server에서 ODX 복사 오프로드를 사용하고 SMB 솔루션을 통해 Hyper-V를 사용하는 것에 대해 이해해야 하는 특정 요구사항이 있습니다.

ODX 복사 오프로드를 사용하면 성능을 대폭 향상할 수 있습니다. 이 CIFS 서버 옵션은 기본적으로 설정되어 있습니다.

- ODX 복사 오프로드를 사용하려면 SMB 3.0을 설정해야 합니다.
- 소스 볼륨은 최소 1.25GB여야 합니다.
- 복사본 오프로드와 함께 사용되는 볼륨에 대해 중복제거를 활성화해야 합니다.
- 압축 볼륨을 사용하는 경우 압축 유형은 적응 가능해야 하며 압축 그룹 크기 8K만 지원됩니다.

  보조 압축 유형은 지원되지 않습니다

- ODX 복사 오프로드를 사용하여 디스크 내부 및 디스크 간에 Hyper-V 게스트를 마이그레이션하려면 SCSI 디스크를 사용하도록 Hyper-V 서버를 구성해야 합니다.

  기본값은 IDE 디스크를 구성하는 것이지만, 디스크가 IDE 디스크를 사용하여 생성된 경우 게스트가 마이그레이션될 때 ODX 복사 오프로드가 작동하지 않습니다.

SMB 구성을 통한 SQL Server 및 Hyper-V 권장 사항

SQL Server 및 Hyper-V over SMB 구성이 강력하고 작동 가능한지 확인하려면 솔루션 구성 시 권장 모범 사례를 숙지해야 합니다.

일반 권장 사항

- 일반 사용자 데이터와 애플리케이션 서버 파일을 분리합니다.

  가능하면 전체 SVM(스토리지 가상 시스템)과 해당 스토리지를 애플리케이션 서버의 데이터에 사용합니다.

- 최상의 성능을 위해 SVM에서 애플리케이션 서버의 데이터를 저장하는 데 사용되는 SMB 서명을 활성화하지 마십시오.
- 최상의 성능과 향상된 내결함성을 위해 SMB 멀티 채널을 통해 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 개의 연결을 제공할 수 있습니다.
- Hyper-V 또는 SQL Server over SMB 구성에서 사용되는 공유 이외의 공유에 대해 지속적으로 사용 가능한 공유를 생성하지 마십시오.
- 지속적인 가용성에 사용되는 공유에 대한 변경 알림을 해제합니다.
- ARL에는 일부 작업을 일시 중지하는 단계가 있으므로 ARL(Aggregate relocation)과 동시에 볼륨 이동을 수행하지 마십시오.
- SMB를 통한 Hyper-V 솔루션의 경우 클러스터 가상 머신을 생성할 때 게스트 내 iSCSI 드라이브를 사용합니다. 공유 '.vHDX' 파일은 ONTAP SMB 공유에서 SMB를 통한 Hyper-V에 지원되지 않습니다.

SMB를 통한 Hyper-V 또는 SQL Server 구성 계획

볼륨 구성 워크시트를 작성합니다

이 워크시트는 SMB 구성을 통해 SQL Server 및 Hyper-V용 볼륨을 생성할 때 필요한 값을 쉽게 기록할 수 있는 방법을 제공합니다.

각 볼륨에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

  SVM 이름은 모든 볼륨에서 동일합니다.

- 볼륨 이름입니다
- 애그리게이트 이름입니다

  클러스터의 노드에 있는 애그리게이트에 볼륨을 생성할 수 있습니다.

- 크기
- 접합 경로

애플리케이션 서버 데이터를 저장하는 데 사용되는 볼륨을 생성할 때 다음 사항을 염두에 두어야 합니다.

- 루트 볼륨에 NTFS 보안 스타일이 없는 경우 볼륨을 생성할 때 보안 스타일을 NTFS로 지정해야 합니다.

  기본적으로 볼륨은 SVM 루트 볼륨의 보안 스타일을 상속합니다.

- 볼륨은 기본 볼륨 공간 보장으로 구성해야 합니다.
- 필요에 따라 공간 자동 크기 조정 관리 설정을 구성할 수 있습니다.
- 스냅숏 공간 예비 공간을 결정하는 옵션을 로 `0`설정해야 합니다.
- 볼륨에 적용된 스냅샷 정책을 해제해야 합니다.

  SVM 스냅샷 정책이 해제되어 있으면 볼륨에 대한 스냅샷 정책을 지정할 필요가 없습니다. 볼륨은 SVM에 대한 스냅샷 정책을 상속합니다. SVM에 대한 스냅샷 정책이 해제되지 않고 스냅샷을 생성하도록 구성된 경우 볼륨 레벨에서 스냅샷 정책을 지정해야 하며 해당 정책을 비활성화해야 합니다. 섀도 복사본 서비스 가능 백업 및 SQL Server 백업은 스냅샷 생성 및 삭제를 관리합니다.

- 볼륨에 대한 로드 공유 미러는 구성할 수 없습니다.

공유 진입점 아래에 접합된 볼륨이 없도록 애플리케이션 서버가 사용하는 공유를 생성하려는 연결 경로를 선택해야 합니다.

예를 들어, 가상 시스템 파일을 ""vol1"", ""vol2", ""vol3"" 및 ""vol4""라는 네 개의 볼륨에 저장하려면 예제에 표시된 네임스페이스를 생성할 수 있습니다. 그런 다음 '/data1/vol1', '/data1/vol2', '/data2/vol3', '/data2/vol4' 경로에서 애플리케이션 서버에 대한 공유를 생성할 수 있습니다.

```
                      Junction                        Junction
Vserver Volume       Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     data1         true     /data1                RW_volume
vs1     vol1          true     /data1/vol1           RW_volume
vs1     vol2          true     /data1/vol2           RW_volume
vs1     data2         true     /data2                RW_volume
vs1     vol3          true     /data2/vol3           RW_volume
vs1     vol4          true     /data2/vol4           RW_volume
```

정보 유형	값
_Volume 1: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 2: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 3: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 4: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 5: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_Volume 6: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	
_추가 볼륨: 볼륨 이름, 애그리게이트, 크기, 접합 경로 _	

SMB 공유 구성 워크시트를 작성합니다

이 워크시트를 사용하여 SMB 구성에서 SQL Server 및 Hyper-V에 대해 지속적으로 사용 가능한 SMB 공유를 생성할 때 필요한 값을 기록하십시오.

SMB 공유 속성 및 구성 설정에 대한 정보입니다

각 공유에 대해 다음 정보를 지정해야 합니다.

- 스토리지 가상 시스템(SVM) 이름

  SVM 이름은 모든 공유에서 동일합니다

- 공유 이름
- 경로
- 공유 속성

  다음 두 공유 속성을 구성해야 합니다.

  - oplocks
  - "계속 사용할 수 있습니다.

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리 attributecache
- 브랜치캐시
- '액세스 기반 열거'
  - symlinks를 비활성화해야 합니다('-symlink-properties' 매개 변수의 값은 null ['] 이어야 함).

공유 경로에 대한 정보입니다

원격 VSS를 사용하여 Hyper-V 파일을 백업하는 경우 Hyper-V 서버에서 가상 머신 파일이 저장된 스토리지 위치로 SMB 연결을 설정할 때 사용할 공유 경로를 선택해야 합니다. 네임스페이스에서 어느 지점에서나 공유를 생성할 수 있지만 Hyper-V 서버가 사용하는 공유의 경로에 접합된 볼륨이 포함되어서는 안 됩니다. 교차점이 포함된 공유 경로에서는 섀도 복사본 작업을 수행할 수 없습니다.

SQL Server는 데이터베이스 디렉토리 구조를 생성할 때 교차점을 교차할 수 없습니다. 교차점이 포함된 SQL Server에 대한 공유 경로를 생성할 수 없습니다.

예를 들어, 표시된 네임스페이스를 사용할 경우 가상 머신 파일 또는 데이터베이스 파일을 볼륨 ""vol1"", ""vol2"", ""vol3"", ""vol4""에 저장하려면 "/data1/vol1", "/data1/vol2", "/data2/data4" 경로에 애플리케이션 서버의 공유를 생성해야 합니다.

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- --------------------    -----------
vs1     data1         true     /data1                 RW_volume
vs1     vol1          true     /data1/vol1            RW_volume
vs1     vol2          true     /data1/vol2            RW_volume
vs1     data2         true     /data2                 RW_volume
vs1     vol3          true     /data2/vol3            RW_volume
vs1     vol4          true     /data2/vol4            RW_volume
```

관리 관리를 위해 및 `/data2` 경로에 공유를 만들 수 있지만 `/data1`, 애플리케이션 서버가 이러한 공유를 사용하여 데이터를 저장하도록 구성하지 마십시오.

계획 워크시트

정보 유형	값
_볼륨 1: SMB 공유 이름 및 경로 _	
_Volume 2: SMB 공유 이름 및 경로 _	
_Volume 3: SMB 공유 이름 및 경로 _	
_Volume 4: SMB 공유 이름 및 경로 _	
_Volume 5: SMB 공유 이름 및 경로 _	
_Volume 6: SMB 공유 이름 및 경로 _	
_Volume 7: SMB 공유 이름 및 경로 _	

정보 유형	값
_추가 볼륨: SMB 공유 이름 및 경로 _	

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 생성

SMB를 통한 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성 개요를 제공합니다

SMB를 통한 무중단 운영을 제공하는 Hyper-V 및 SQL Server 설치를 준비하기 위해 수행해야 하는 몇 가지 ONTAP 구성 단계가 있습니다.

SMB를 통해 Hyper-V 및 SQL Server의 무중단 운영을 위한 ONTAP 구성을 생성하기 전에 다음 작업을 완료해야 합니다.

- 클러스터에서 시간 서비스를 설정해야 합니다.
- SVM에 대해 네트워킹을 설정해야 합니다.
- SVM을 생성해야 합니다.
- 데이터 LIF 인터페이스는 SVM에서 구성해야 합니다.
- SVM에서 DNS를 구성해야 합니다.
- SVM에 대해 원하는 이름 서비스를 설정해야 합니다.
- SMB 서버를 생성해야 합니다.

관련 정보

SMB를 통한 Hyper-V 또는 SQL Server 구성 계획

구성 요구 사항 및 고려 사항

Kerberos 및 NTLMv2 인증이 모두 허용되는지 확인(SMB 공유를 통한 Hyper-V)

SMB를 통한 Hyper-V의 무중단 운영에서는 데이터 SVM 및 Hyper-V 서버의 CIFS 서버가 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다. 허용되는 인증 방법을 제어하는 CIFS 서버와 Hyper-V 서버 모두에서 설정을 확인해야 합니다.

이 작업에 대해

지속적으로 사용 가능한 공유 연결을 만들 때는 Kerberos 인증이 필요합니다. 원격 VSS 프로세스의 일부는 NTLMv2 인증을 사용합니다. 따라서 SMB를 통한 Hyper-V 구성에서는 두 인증 방법을 모두 사용하는 연결이 지원되어야 합니다.

Kerberos 및 NTLMv2 인증을 모두 허용하도록 다음 설정을 구성해야 합니다.

- 스토리지 가상 시스템(SVM)에서 SMB를 위한 엑스포트 정책을 사용하지 않도록 설정해야 합니다.

Kerberos 및 NTLMv2 인증은 항상 SVM에서 활성화되지만, 엑스포트 정책을 사용하여 인증 방법에 따라 액세스를 제한할 수 있습니다.

SMB에 대한 엑스포트 정책은 선택 사항이며 기본적으로 비활성화되어 있습니다. 내보내기 정책을 사용하지 않도록 설정하면 기본적으로 CIFS 서버에서 Kerberos 및 NTLMv2 인증이 모두 허용됩니다.

- CIFS 서버 및 Hyper-V 서버가 속하는 도메인은 Kerberos 및 NTLMv2 인증을 모두 허용해야 합니다.

Kerberos 인증은 Active Directory 도메인에서 기본적으로 활성화됩니다. 그러나 보안 정책 설정 또는 그룹 정책을 사용하여 NTLMv2 인증을 허용하지 않을 수 있습니다.

단계

1. SVM에서 엑스포트 정책이 비활성화되어 있는지 확인하려면 다음을 수행하십시오.
   a. 권한 수준을 고급으로 설정합니다.

      ' * set-Privilege advanced * '

   b. '-is-exportpolicy-enabled' CIFS server 옵션이 'false'로 설정되어 있는지 확인합니다.

      '* vserver cifs options show -vserver_vserver_name_-fields vserver, is-exportpolicy-enabled *

   c. 관리자 권한 레벨로 돌아갑니다.

      ' * set-privilege admin * '

2. SMB에 대한 엑스포트 정책이 비활성화되어 있지 않으면 다음을 비활성화하십시오.

   '* vserver cifs options modify -vserver_vserver_name_-is-exportpolicy -enabled false *

3. 도메인에서 NTLMv2 및 Kerberos 인증이 모두 허용되는지 확인합니다.

   도메인에서 허용되는 인증 방법을 결정하는 방법에 대한 자세한 내용은 Microsoft TechNet 라이브러리를 참조하십시오.

4. 도메인이 NTMLv2 인증을 허용하지 않는 경우 Microsoft 설명서에 설명된 방법 중 하나를 사용하여 NTLMv2 인증을 사용하도록 설정합니다.

예

다음 명령을 실행하면 SVM VS1 에서 SMB용 엑스포트 정책이 비활성화되어 있는지 확인할 수 있습니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

도메인 계정이 **ONTAP**의 기본 **UNIX** 사용자에게 매핑되는지 확인합니다

Hyper-V 및 SQL Server는 도메인 계정을 사용하여 지속적으로 사용 가능한 공유에 대한 SMB 연결을 생성합니다. 연결을 성공적으로 생성하려면 컴퓨터 계정이 UNIX 사용자에게 성공적으로 매핑되어야 합니다. 이 작업을 수행하는 가장 편리한 방법은 컴퓨터 계정을 기본 UNIX 사용자에게 매핑하는 것입니다.

이 작업에 대해

Hyper-V 및 SQL Server는 도메인 컴퓨터 계정을 사용하여 SMB 연결을 만듭니다. 또한 SQL Server는 도메인 사용자 계정을 서비스 계정으로 사용하여 SMB 연결을 만듭니다.

스토리지 가상 머신(SVM)을 생성하면 ONTAP에서 자동으로 기본 사용자 이름을 생성합니다. `pcuser` (UID가 있는 `65534`) 및 그룹 이름 `pcuser` (GID가 있는 `65534`), 그리고 기본 사용자를 추가합니다. `pcuser` 그룹. 클러스터를 Data ONTAP 8.2로 업그레이드하기 전에 존재했던 SVM에서 SMB를 통한 Hyper-V 솔루션을 구성하는 경우 기본 사용자 및 그룹이 없을 수 있습니다. 그렇지 않으면 CIFS 서버의 기본 UNIX 사용자를 구성하기 전에 생성해야 합니다.

단계

1. 기본 UNIX 사용자가 있는지 확인합니다.

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

2. 기본 사용자 옵션이 설정되지 않은 경우 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 있는지 확인합니다.

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

3. 기본 사용자 옵션이 설정되어 있지 않고 기본 UNIX 사용자로 지정할 수 있는 UNIX 사용자가 없는 경우, 기본 그룹과 기본 UNIX 사용자를 만들고, 기본 사용자를 그룹에 추가합니다.
4. 기본 그룹에는 일반적으로 "pcuser"라는 그룹 이름이 지정됩니다 그룹에 할당된 GID는 `65534` 이어야 합니다.
   a. 기본 그룹을 만듭니다.

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

b. 기본 사용자를 만들고 기본 그룹에 기본 사용자를 추가합니다.

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

c. 기본 사용자와 기본 그룹이 올바르게 구성되었는지 확인하세요.

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

5. CIFS 서버의 기본 사용자가 구성되지 않은 경우 다음을 수행합니다.

a. 기본 사용자를 구성합니다.

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

b. 기본 UNIX 사용자가 올바르게 구성되었는지 확인합니다.

```
vserver cifs options show -vserver <vserver_name>
```

6. 애플리케이션 서버의 컴퓨터 계정이 기본 사용자에게 올바르게 매핑되었는지 확인하려면 SVM에 상주하는 공유에 드라이브를 매핑하고 "vserver cifs session show" 명령을 사용하여 Windows 사용자를 UNIX 사용자 매핑으로 확인합니다.

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

예

존재합니다. `pcuser` 사용자는 SVM vs1에서 CIFS 서버의 기본 사용자로 지정됩니다.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
```

```
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

SVM 루트 볼륨의 보안 스타일이 **NTFS**로 설정되어 있는지 확인합니다

Hyper-V 및 SQL Server over SMB의 무중단 운영이 성공하려면 NTFS 보안 스타일로 볼륨을 만들어야 합니다. 루트 볼륨의 보안 스타일은 SVM(스토리지 가상 머신)에서 생성된 볼륨에

기본적으로 적용되므로 루트 볼륨의 보안 스타일을 NTFS로 설정해야 합니다.

이 작업에 대해

- SVM을 생성할 때 루트 볼륨 보안 스타일을 지정할 수 있습니다.
- 루트 볼륨이 NTFS 보안 스타일로 설정되어 있는 SVM이 생성되지 않으면 나중에 'volume modify' 명령을 사용하여 보안 스타일을 변경할 수 있습니다.

단계

1. SVM 루트 볼륨의 현재 보안 유형을 확인합니다.

   '* volume show -vserver_vserver_name_- 필드 vserver, 볼륨, 보안 스타일 *

2. 루트 볼륨이 NTFS 보안 스타일 볼륨이 아닌 경우 보안 스타일을 NTFS로 변경합니다.

   '* volume modify -vserver_vserver_name_-volume root_volume_name -security-style NTFS * '

3. SVM 루트 볼륨이 NTFS 보안 스타일로 설정되었는지 확인합니다.

   '* volume show -vserver_vserver_name_- 필드 vserver, 볼륨, 보안 스타일 *

예

다음 명령은 SVM VS1 에서 루트 볼륨 보안 스타일이 NTFS인지 확인합니다.

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

필요한 **CIFS** 서버 옵션이 구성되었는지 확인합니다

필요한 CIFS 서버 옵션이 Hyper-V 및 SQL Server over SMB의 무중단 운영 요구 사항에 따라 설정 및 구성되었는지 확인해야 합니다.

이 작업에 대해

- SMB 2.x 및 SMB 3.0을 활성화해야 합니다.
- ODX 복사 오프로드를 사용하여 성능을 향상시키려면 ODX 복사 오프로드를 활성화해야 합니다.
- Hyper-V over SMB 솔루션에서 원격 VSS 지원 백업 서비스를 사용하는 경우 VSS Shadow Copy 서비스를

활성화해야 합니다(Hyper-V만 해당).

단계

1. 필요한 CIFS 서버 옵션이 SVM(스토리지 가상 시스템)에서 설정되었는지 확인합니다.
   a. 권한 수준을 고급으로 설정합니다.

      ' * set-Privilege advanced * '

   b. 다음 명령을 입력합니다.

      '* vserver CIFS options show -vserver_vserver_name_ *'

      다음 옵션은 "참"으로 설정해야 합니다.

      - '-SMB2-ENABLED'입니다
      - '-SMB3-enabled'입니다
      - '-copy-offload-enabled'
      - '-shadowcopy -enabled'(Hyper-V만 해당)
2. "참"으로 설정되어 있지 않은 옵션이 있는 경우 다음을 수행하십시오.
   a. vserver cifs options modify 명령을 사용하여 "true"로 설정합니다.
   b. vserver cifs options show 명령을 사용하여 옵션이 "true"로 설정되어 있는지 확인합니다.
3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

예

다음 명령은 SVM VS1 기반 Hyper-V 구성에 필요한 옵션이 설정되어 있는지 확인합니다. 이 예에서는 옵션 요구 사항을 충족하도록 ODX 복사 오프로드를 활성화해야 합니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

성능 및 이중화를 위해 **SMB** 멀티 채널을 구성합니다

ONTAP 9.4부터 SMB 다중 채널을 구성하여 단일 SMB 세션에서 ONTAP와 클라이언트 간에 여러 연결을 제공할 수 있습니다. 이렇게 하면 SMB 구성에서 Hyper-V 및 SQL Server의 처리량과 내결함성을 향상시킬 수 있습니다.

시작하기 전에

SMB 3.0 이상 버전에서 클라이언트가 협상하는 경우에만 SMB 멀티 채널 기능을 사용할 수 있습니다. SMB 3.0 이상은 기본적으로 ONTAP SMB 서버에서 사용하도록 설정됩니다.

이 작업에 대해

ONTAP 클러스터에서 적절한 구성이 식별되는 경우 SMB 클라이언트가 자동으로 여러 네트워크 연결을 감지하고 사용합니다.

SMB 세션의 동시 연결 수는 구축한 NIC에 따라 달라집니다.

- * 클라이언트와 ONTAP 클러스터의 1G NIC *

  클라이언트는 NIC당 하나의 연결을 설정하고 모든 연결에 세션을 바인딩합니다.

- * 클라이언트 및 ONTAP 클러스터에 10G 이상의 대용량 NIC *

  클라이언트는 NIC당 최대 4개의 연결을 설정하고 모든 연결에 세션을 바인딩합니다. 클라이언트는 여러 개의 10G 및 대용량 NIC에 연결을 설정할 수 있습니다.

다음 매개 변수(고급 권한)도 수정할 수 있습니다.

- `-max-connections-per-session`

  다중 채널 세션당 허용되는 최대 연결 수입니다. 기본값은 32개 연결입니다.

  기본값보다 더 많은 연결을 설정하려면 기본값인 32개의 연결을 사용하는 클라이언트 구성을 동일하게 조정해야 합니다.

- `-max-lifs-per-session`

  Multichannel 세션당 공고되는 최대 네트워크 인터페이스 수입니다. 기본값은 256개의 네트워크 인터페이스입니다.

단계

1. 권한 수준을 고급으로 설정합니다.

```
set -privilege advanced
```

2. SMB 서버에서 SMB 멀티 채널 활성화:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. ONTAP가 SMB 멀티 채널 세션을 보고하는지 확인합니다.

```
vserver cifs session show
```

4. 관리자 권한 레벨로 돌아갑니다.

```
set -privilege admin
```

예

다음 예에서는 모든 SMB 세션에 대한 정보를 표시하며 단일 세션에 대해 여러 개의 연결을 표시합니다.

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

다음 예에서는 세션 ID 1이 있는 SMB 세션에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                   NetBIOS Name: -
```

NTFS 데이터 볼륨을 생성합니다

Hyper-V 또는 SQL Server over SMB 애플리케이션 서버에서 사용할 수 있도록 지속적으로 사용 가능한 공유를 구성하려면 먼저 SVM(스토리지 가상 머신)에 NTFS 데이터 볼륨을

생성해야 합니다. 볼륨 구성 워크시트를 사용하여 데이터 볼륨을 생성합니다.

이 작업에 대해

데이터 볼륨을 사용자 지정하는 데 사용할 수 있는 선택적 매개 변수가 있습니다. 볼륨 사용자 지정에 대한 자세한 내용은 를 참조하십시오 "논리적 스토리지 관리".

데이터 볼륨을 생성할 때 다음을 포함하는 볼륨 내에 교차점을 생성해서는 안 됩니다.

- ONTAP에서 섀도 복사본을 만드는 Hyper-V 파일입니다
- SQL Server를 사용하여 백업되는 SQL Server 데이터베이스 파일입니다

> 혼합 또는 UNIX 보안 스타일을 사용하는 볼륨을 실수로 만든 경우 볼륨을 NTFS 보안 스타일 볼륨으로 변경한 다음 이 볼륨을 직접 사용하여 무중단 운영을 위해 지속적으로 사용 가능한 공유를 생성할 수 없습니다. Hyper-V 및 SQL Server over SMB의 무중단 운영은 구성에 사용된 볼륨이 NTFS 보안 스타일 볼륨으로 만들어지지 않는 한 제대로 작동하지 않습니다. 볼륨을 삭제하고 NTFS 보안 스타일로 볼륨을 다시 생성해야 합니다. 또는 Windows 호스트에서 볼륨을 매핑하고 볼륨 상단에 ACL을 적용하고 볼륨의 모든 파일 및 폴더에 ACL을 전파할 수 있습니다.

단계

1. 적절한 명령을 입력하여 데이터 볼륨을 생성합니다.

SVM에서 루트 볼륨 보안 유형이 인 볼륨을 생성하려는 경우...	명령 입력...
NTFS입니다	'* volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size 정수 [KB|MB|GB|TB|PB]-junction-path_path_ *'
NTFS가 아닙니다	'* volume create-vserver_vserver_name_-volume_volume_name_-aggregate_aggregate_name_-size integer [KB|MB|GB|TB|PB]-security-style NTFS-junction-path *'

2. 볼륨 구성이 올바른지 확인합니다.

   '* volume show -vserver_vserver_name_-volume_volume_name_*'

지속적으로 사용 가능한 **SMB** 공유를 생성합니다

데이터 볼륨을 생성한 후 애플리케이션 서버가 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 액세스하는 데 사용하는 연속 사용 가능한 공유를 생성할 수 있습니다. SMB 공유를 생성할 때 공유 구성 워크시트를 사용해야 합니다.

단계

1. 기존 데이터 볼륨 및 연결 경로에 대한 정보를 표시합니다.

   '* volume show -vserver_vserver_name_-junction *'

2. 지속적으로 사용 가능한 SMB 공유 생성:

   '* vserver CIFS 공유 create-vserver_vserver_name_-share-name_share_name_-path_path_-share-properties oplocks, Continuously-available-symlink""[-comment text] *'

   - 필요에 따라 공유 구성에 주석을 추가할 수 있습니다.
   - 기본적으로 오프라인 파일 공유 속성은 공유에서 구성되며 '수동'으로 설정됩니다.
   - ONTAP는 Everyone/Full Control의 Windows 기본 공유 권한으로 공유를 생성합니다.
3. 공유 구성 워크시트의 모든 공유에 대해 이전 단계를 반복합니다.
4. 'vserver cifs share show' 명령을 사용하여 구성이 올바른지 확인하십시오.
5. 드라이브를 각 공유에 매핑하고 * Windows 속성 * 창을 사용하여 파일 권한을 구성하여 지속적으로 사용 가능한 공유에서 NTFS 파일 권한을 구성합니다.

예

다음 명령을 실행하면 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 에 "data2"라는 이름의 연속 사용 가능한 공유가 생성됩니다. '-symlink' 매개변수를 """로 설정하면 Symlink가 비활성화됩니다.

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

sSecurityPrivilege 권한을 사용자 계정에 추가합니다**(SMB** 공유의 **SQL Server**에 해당**).**

SQL Server 설치에 사용되는 도메인 사용자 계정에는 "'seSecurityPrivilege'" 권한이 할당되어 있어야 도메인 사용자에게 기본적으로 할당되지 않은 권한이 필요한 CIFS 서버에서 특정 작업을 수행할 수 있습니다.

시작하기 전에

SQL Server 설치에 사용되는 도메인 계정이 이미 있어야 합니다.

이 작업에 대해

SQL Server 설치 관리자의 계정에 권한을 추가할 때 ONTAP는 도메인 컨트롤러에 연락하여 계정의 유효성을 검사할 수 있습니다. ONTAP가 도메인 컨트롤러에 연결할 수 없으면 명령이 실패할 수 있습니다.

단계

1. "seSecurityPrivilege" 권한 추가:

'* vserver cifs users-and-groups 권한 add-privilege-vserver_vserver_name_-user-or-group-name_account_name_-Privileges SeSecurityPrivilege*'

'-user-or-group-name' 매개 변수의 값은 SQL Server 설치에 사용되는 도메인 사용자 계정의 이름입니다.

2. 계정에 권한이 적용되는지 확인합니다.

   '* vserver cifs users-and-groups 권한 show -vserver_vserver_name_-user-or-group -name_account_name_*'

예

다음 명령을 실행하면 SVM(Storage Virtual Machine) VS1 예제 도메인의 SQL Server 설치 관리자 계정에 "seSecurityPrivilege" 권한이 추가됩니다.

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

VSS 섀도우 복제본 디렉토리 깊이 구성(SMB 공유를 통한 Hyper-V의 경우)

필요에 따라 SMB 공유 내에서 섀도우 복제본을 생성할 디렉토리의 최대 깊이를 구성할 수 있습니다. 이 매개 변수는 ONTAP에서 섀도 복사본을 만들어야 하는 하위 디렉터리의 최대 수준을 수동으로 제어하려는 경우에 유용합니다.

시작하기 전에

VSS 섀도우 복제본 기능을 활성화해야 합니다.

이 작업에 대해

기본값은 최대 5개의 하위 디렉토리에 대한 섀도우 복제본을 생성하는 것입니다. 이 값이 '0'으로 설정되면 ONTAP는 모든 하위 디렉토리에 대한 섀도우 복제본을 만듭니다.

> 섀도우 복제본 세트 디렉토리 깊이에 5개 이상의 하위 디렉토리나 모든 하위 디렉토리가 포함되도록 지정할 수 있지만 섀도우 복제본 세트 생성이 60초 이내에 완료되어야 한다는 Microsoft 요구 사항이 있습니다. 이 시간 내에 완료할 수 없는 경우 섀도우 복제본 세트 생성이 실패합니다. 선택한 섀도 복사본 디렉토리 깊이로 인해 생성 시간이 시간 제한을 초과하지 않아야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ' * set-Privilege advanced * '

2. VSS 섀도우 복제본 디렉토리 깊이를 원하는 레벨로 설정합니다.

``vserver cifs options modify -vserver_vserver_name_-shadowcopy -dir -depth integer*'

``vserver cifs options modify -vserver vs1-shadowcopy -dir-depth 6 *'

3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

SMB 구성을 통해 Hyper-V 및 SQL Server 관리

지속적인 가용성을 위해 기존 공유를 구성합니다

Hyper-V 및 SQL Server 애플리케이션 서버에서 Hyper-V 가상 머신 및 구성 파일, SQL Server 데이터베이스 파일에 중단 없이 액세스하는 데 사용하는 공유를 계속 사용할 수 있도록 기존 공유를 수정할 수 있습니다.

이 작업에 대해

공유에 다음과 같은 특성이 있는 경우 SMB를 통해 애플리케이션 서버와 무중단 운영을 위해 기존 공유를 지속적으로 사용할 수 있는 공유로 사용할 수 없습니다.

- 이 공유에 homedory 공유 속성이 설정되어 있으면
- 공유에 활성화된 symlink 또는 widelink가 포함된 경우
- 공유에 공유의 루트 아래에 접합된 볼륨이 포함되어 있는 경우

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.
- Symlink를 비활성화해야 합니다.

다음 공유 속성을 구성해야 합니다.

- "계속 사용할 수 있습니다.
- oplocks

다음 공유 속성을 설정하지 않아야 합니다. 현재 공유 속성 목록에 있는 경우 지속적으로 사용 가능한 공유에서 제거해야 합니다.

- 'attributecache
- 브랜치캐시

단계

1. 현재 공유 매개 변수 설정 및 구성된 공유 속성의 현재 목록을 표시합니다.

   ```
   vserver cifs share show -vserver <vserver_name> -share-name <share_name>
   ```

2. 필요한 경우 명령을 사용하여 공유 매개 변수를 수정하여 symlink를 비활성화하고 오프라인 파일을 manual로

`vserver cifs share modify` 설정합니다.

- '-symlink' 매개 변수의 값을 ""로 설정하여 symlink를 비활성화할 수 있습니다.
- '-offline-files' 파라미터는 'Manual'을 지정하여 올바른 설정으로 설정할 수 있습니다.

3. 공유 속성을 추가하고 필요한 경우 공유 속성을 추가합니다 `continuously-available` `oplocks` .

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

oplocks 공유 속성이 아직 설정되지 않은 경우 계속 사용 가능한 공유 속성과 함께 추가해야 합니다.

4. 지속적으로 사용 가능한 공유에서 지원되지 않는 공유 속성을 제거합니다.

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

쉼표로 구분된 목록으로 공유 속성을 지정하여 하나 이상의 공유 속성을 제거할 수 있습니다.

5. '-symlink' 및 '-offline-files' 매개 변수가 올바르게 설정되었는지 확인합니다.

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. 구성된 공유 속성 목록이 올바른지 확인합니다.

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

예

다음 예에서는 SMB를 통해 애플리케이션 서버가 있는 NDOs에 대해 SVM(스토리지 가상 머신) "VS1"이라는 기존 공유를 구성하는 방법을 보여 줍니다.

- 매개 변수를 로 설정하면 공유에서 symlink가 `-symlink` `""`비활성화됩니다.
- '-offline-file' 파라미터가 수정되어 'manual'로 설정됩니다.
- 이 공유에 계속 이용 가능한 공유자산이 추가됩니다.
- oplocks 공유 속성은 이미 공유 속성 목록에 있으므로 추가할 필요가 없습니다.
- 이 지분에서는 attributecache 공유재산을 빼내기도 합니다.
- "탐색 가능" 공유 속성은 SMB를 통해 애플리케이션 서버와 NDO에 사용되는 지속적인 사용 가능 공유에 대한 선택 사항이며 공유 속성 중 하나로 유지됩니다.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

SMB 백업을 통해 Hyper-V에 대한 VSS 섀도우 복제본을 설정하거나 해제합니다

VSS 인식 백업 애플리케이션을 사용하여 SMB 공유에 저장된 Hyper-V 가상 머신 파일을 백업하는 경우 VSS 섀도우 복제본을 설정해야 합니다. VSS 인식 백업 애플리케이션을 사용하지 않는 경우 VSS 섀도우 복제본을 비활성화할 수 있습니다. 기본값은 VSS 섀도우 복제본을 설정하는 것입니다.

이 작업에 대해

언제든지 VSS 섀도우 복제본을 설정하거나 해제할 수 있습니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   ' * set-Privilege advanced * '

2. 다음 작업 중 하나를 수행합니다.

VSS 섀도우 복제본을 만들려는 경우...	명령 입력...
활성화됨	``vserver cifs options modify -vserver_vserver_name_-shadowcopy -enabled true *'
사용 안 함	'* vserver cifs options modify -vserver_vserver_name_-shadowcopy -enabled false *

3. 관리자 권한 레벨로 돌아갑니다.

   ' * set-privilege admin * '

예

다음 명령을 실행하면 SVM VS1 에서 VSS 섀도우 복제본이 활성화됩니다.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

통계를 사용하여 SMB 작업을 통해 Hyper-V 및 SQL Server를 모니터링합니다

ONTAP에서 사용할 수 있는 통계 개체 및 카운터를 확인합니다

CIFS, SMB, 감사 및 BranchCache 해시 통계에 대한 정보를 얻고 성능을 모니터링하려면 데이터를 가져올 수 있는 개체와 카운터를 알고 있어야 합니다.

단계

1. 권한 수준을 고급으로 설정합니다.

   세트 프리빌리지 고급

2. 다음 작업 중 하나를 수행합니다.

다음 사항을 확인하고자 하는 경우:	입력...
사용할 수 있는 개체	'통계 카탈로그 개체 쇼'
사용할 수 있는 특정 개체입니다	`statistics catalog object show -object` *`object_name`*
사용할 수 있는 카운터	`statistics catalog counter show -object` *`object_name`*

   자세히 알아보세요 `statistics catalog object show` 그리고 `statistics catalog counter show` 에서 "ONTAP 명령 참조입니다" .

3. 관리자 권한 레벨로 돌아갑니다.

   'Set-Privilege admin'입니다

예

다음 명령을 실행하면 고급 권한 수준에 표시된 대로 클러스터에서 CIFS 및 SMB 액세스와 관련된 선택한 통계 개체에 대한 설명이 표시됩니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

다음 명령을 실행하면 고급 권한 수준에서 표시되는 "CIFS" 개체의 일부 카운터에 대한 정보가 표시됩니다.

> 이 예제에서는 "CIFS" 객체에 대해 사용 가능한 카운터를 모두 표시하지 않고 출력이 잘립니다.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ---------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                             vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

에 대한 자세한 내용은 `statistics start` "ONTAP 명령 참조입니다"을 참조하십시오.

ONTAP에서 SMB 통계를 표시합니다

다양한 SMB 통계를 표시하여 성능을 모니터링하고 문제를 진단할 수 있습니다.

단계

1. '통계 시작' 및 '통계 중지' 옵션 명령을 사용하여 데이터 샘플을 수집합니다.
2. 다음 작업 중 하나를 수행합니다.

에 대한 통계를 표시하려면...	다음 명령을 입력합니다...
모든 SMB 버전	' * statistics show-object cifs *'
SMB 1.0	' * statistics show-object SMB1 * '
SMB 2.x 및 SMB 3.0	' * statistics show-object SMB2 * '
노드의 SMB 하위 시스템입니다	'* statistics show -object nblade_cifs * '

관련 정보

- "통계에 따르면"
- "통계 시작"
- "통계 중지"

구성이 무중단 운영이 가능한지 확인합니다

상태 모니터링을 사용하여 무중단 운영 상태가 정상인지 확인하십시오

상태 모니터링 에서는 클러스터 전체의 시스템 상태에 대한 정보를 제공합니다. 상태 모니터는 SMB 구성을 통해 Hyper-V 및 SQL Server를 모니터링하여 애플리케이션 서버에 대한 무중단 운영(NDO)을 보장합니다. 상태가 성능 저하인 경우 가능한 원인 및 권장 복구 조치를 포함하여 문제에 대한 세부 정보를 볼 수 있습니다.

여러 개의 상태 모니터가 있습니다. ONTAP는 개별 상태 모니터의 전체 시스템 상태와 상태를 모두 모니터링합니다. 노드 연결 상태 모니터에는 CIFS-NDO 서브시스템이 포함되어 있습니다. 모니터에는 특정 물리적 조건으로 인해 운영 중단이 발생할 수 있는 경우 알림을 트리거하는 상태 정책이 있으며, 중단 상태가 있을 경우 알림을 생성하고 수정 조치에 대한 정보를 제공합니다. SMB 구성을 통한 NDO의 경우 다음 두 가지 조건에 대한 경고가 생성됩니다.

경고 **ID**	심각도입니다	조건
``HaNotReadyCifsNdo_Alert*’	전공	노드에서 애그리게이트에서 볼륨에 호스팅되는 하나 이상의 파일이 장애 발생 시 지속성을 약속하는 지속적으로 사용 가능한 SMB 공유를 통해 열렸습니다. 파트너와의 HA 관계는 구성되지 않았거나 상태가 아닙니다.
'* NoStandbyLifcifsNdo_Alert * '	경미합니다	SVM(스토리지 가상 머신)은 노드를 통해 SMB를 통해 데이터를 능동적으로 제공하고, 지속적으로 사용 가능한 공유를 통해 지속적으로 열려 있는 SMB 파일이 있지만, 해당 파트너 노드가 SVM을 위한 활성 데이터 LIF를 노출하지 않습니다.

시스템 상태 모니터링을 사용하여 무중단 운영 상태를 표시합니다

'시스템 상태' 명령을 사용하면 클러스터의 전체 시스템 상태 및 CIFS-NDO 하위 시스템의 상태에 대한 정보를 표시하고, 알림에 응답하고, 향후 알림을 구성하고, 상태 모니터링 구성 방법에 대한 정보를 표시할 수 있습니다.

단계

1. 적절한 작업을 수행하여 상태 모니터링:

를 표시하려면...	명령 입력...
개별 상태 모니터의 전체 상태를 반영하는 시스템의 상태입니다	'* 시스템 상태 표시 *'
CIFS-NDO 서브시스템의 상태에 대한 정보입니다	'* 시스템 상태 하위 시스템 표시 - 하위 시스템 cifs-NDO-instance*'

2. 적절한 작업을 수행하여 CIFS-NDO 알림 모니터링을 구성하는 방법에 대한 정보를 표시합니다.

다음에 대한 정보를 표시하려면...	명령 입력...
모니터링되는 노드, 초기화 상태 및 상태와 같은 CIFS-NDO 서브시스템에 대한 상태 모니터의 구성 및 상태입니다	'* 시스템 상태 구성 show-subsystem cifs-NDO *'
상태 모니터에서 잠재적으로 생성할 수 있는 CIFS-NDO 알림을 나타냅니다	'* 시스템 상태 경고 정의 show-subsystem cifs-NDO *'
CIFS-NDO 상태 모니터링 정책으로 알림이 발생하는 시기를 결정합니다	'* 시스템 상태 정책 정의 표시 - 모니터 노드 연결 * '

자세한 정보를 표시하려면 '-instance' 매개 변수를 사용합니다.

예

다음 출력에는 클러스터 및 CIFS-NDO 서브시스템의 전체 상태에 대한 정보가 표시됩니다.

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

다음 출력에는 CIFS-NDO 서브시스템의 상태 모니터 구성 및 상태에 대한 자세한 정보가 나와 있습니다.

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

지속적으로 사용 가능한 **SMB** 공유 구성을 확인합니다

무중단 운영을 지원하려면 Hyper-V 및 SQL Server SMB 공유를 지속적으로 사용 가능한 공유로 구성해야 합니다. 또한 확인해야 할 다른 공유 설정도 있습니다. 계획된 또는 계획되지 않은 중단 이벤트가 있는 경우 공유가 애플리케이션 서버에 무중단 운영을 원활하게 제공하도록 올바르게 구성되었는지 확인해야 합니다.

이 작업에 대해

다음 두 공유 매개 변수가 올바르게 설정되었는지 확인해야 합니다.

- '-offline-files' 매개변수는 수동(기본값) 또는 없음(없음)으로 설정됩니다.

- Symlink를 비활성화해야 합니다.

적절한 무중단 운영을 위해서는 다음 공유 속성을 설정해야 합니다.

- "계속 사용할 수 있습니다.
- oplocks

다음 공유 속성을 설정하지 않아야 합니다.

- 홈디렉토리
- 'attributecache
- 브랜치캐시
- '액세스 기반 열거'

단계

1. 오프라인 파일이 '수동' 또는 '사용 안 함'으로 설정되어 있고 symlink가 비활성화되어 있는지 확인합니다.

   '* vserver CIFS 공유 show -vserver_vserver_name_*'

2. SMB 공유가 무중단 가용성을 위해 구성되었는지 확인합니다.

   '* vserver cifs 공유 속성 표시 - vserver_vserver_name_*'

예

다음 예에서는 스토리지 가상 머신(SVM, 이전 명칭 Vserver) VS1 의 "shay1"이라는 공유 설정을 표시합니다. 오프라인 파일은 '수동'으로 설정되고 symlink는 비활성화됩니다('대칭 링크 속성' 필드 출력에서 하이픈으로 지정됨).

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

다음 예에서는 SVM VS1 에서 "shay1"이라는 이름의 공유에 대한 공유 속성을 표시합니다.

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

LIF 상태를 확인합니다

Hyper-V와 SQL Server over SMB 구성을 통해 SVM(스토리지 가상 시스템)을 구성하여 클러스터의 각 노드에 LIF를 갖는 일상적인 작업을 수행하는 경우에도 일부 LIF는 다른 노드의 포트로 이동할 수 있습니다. LIF 상태를 확인하고 필요한 수정 조치를 취해야 합니다.

이 작업에 대해

원활한 무중단 운영 지원을 제공하려면 클러스터의 각 노드에 SVM을 위한 LIF가 하나 이상 있어야 하며 모든 LIF가 홈 포트와 연결되어야 합니다. 구성된 LIF 중 일부가 현재 홈 포트에 연결되어 있지 않으면 포트 문제를 해결한 다음 LIF를 홈 포트로 되돌려야 합니다.

단계

1. SVM을 위해 구성된 LIF 정보 표시:

   '* 네트워크 인터페이스 show -vserver_vserver_name_*'

   이 예에서 ""lif1"은 홈 포트에 없습니다.

   네트워크 인터페이스 show-vserver vs1

   ```
   
   Vserver     Logical    Status     Network          Current     Current Is
   Home        Interface  Admin/Oper Address/Mask     Node        Port
   ----------- ---------- ---------- ---------------- ----------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2       e0d
   false
               lif2         up/up    10.0.0.129/24    node2       e0d
   true
   ```

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

2. 일부 LIF가 홈 포트에 없는 경우 다음 단계를 수행하십시오.

   a. 각 LIF에서 LIF의 홈 포트가 무엇인지 확인합니다.

      '* 네트워크 인터페이스 show -vserver_vserver_name_-lif_lif_name_-fields home-node, home-port *

'* network interface show -vserver vs1-lif lif lif1-fields home-node, home-port * '

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. 각 LIF에서 LIF의 홈 포트가 작동하는지 확인합니다.

'* 네트워크 포트 show-node_node_name_-port_port_- 필드 포트, 링크 *

'network port show-node node1-port e0d-fields port, link

```
node       port link
---------- ---- ----
node1      e0d  up
```

이 예에서는 "lif1"을 홈 포트인 node1:e0d로 다시 마이그레이션해야 합니다.

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

3. LIF와 연결되어야 하는 홈 포트 네트워크 인터페이스 중 하나가 상태에 있지 않은 경우 `up`, 이러한 인터페이스가 작동되도록 문제를 해결하십시오. 에 대한 자세한 내용은 `up` "ONTAP 명령 참조입니다"을 참조하십시오.
4. 필요한 경우 LIF를 홈 포트로 되돌립니다.

   '* 네트워크 인터페이스 되돌리기 - vserver_vserver_name_-lif_lif_name_*'

   '* 네트워크 인터페이스 되돌리기 - vserver vs1-lif lif liff li1*'

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

5. 클러스터의 각 노드에 SVM을 위한 액티브 LIF가 있는지 확인합니다.

   '* 네트워크 인터페이스 show -vserver_vserver_name_*'

   '* 네트워크 인터페이스 show-vserver vs1*'

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

SMB 세션을 지속적으로 사용할 수 있는지 확인합니다

SMB 세션 정보를 표시합니다

SMB 연결 및 세션 ID와 세션을 사용하는 워크스테이션의 IP 주소를 포함하여 설정된 SMB 세션에 대한 정보를 표시할 수 있습니다. 세션의 SMB 프로토콜 버전 및 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시하여 세션이 무중단 운영을 지원하는지 여부를 확인할 수 있습니다.

이 작업에 대해

SVM의 모든 세션에 대한 정보를 요약 형식으로 표시할 수 있습니다. 그러나 대부분의 경우 반환되는 출력량이 큽니다. 옵션 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 대한 출력을 표시할 수 있습니다.

  필드를 입력할 수 있습니다 사용할 수 있는 필드를 결정합니다.

- '-instance' 매개 변수를 사용하면 설정된 SMB 세션에 대한 자세한 정보를 표시할 수 있습니다.
- '-fields' 매개 변수 또는 '-instance' 매개 변수를 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
SVM의 모든 세션에 대해 요약 양식을 작성합니다	'* vserver cifs session show -vserver_vserver_name_*'
지정된 연결 ID에 있습니다	'* vserver cifs session show -vserver_vserver_name_-connection-id integer *'
지정된 워크스테이션 IP 주소에서	'* vserver cifs session show -vserver_vserver_name_ -address_workstation_ip_address_ *'

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
지정된 LIF IP 주소입니다	'* vserver cifs session show -vserver_vserver_name_-lif -address_LIF_ip_address_ *'
지정된 노드에서	'* vserver cifs session show -vserver_vserver_name_-node{node_name
local} *'	지정된 Windows 사용자로부터
'* vserver cifs session show -vserver_vserver_name_ -windows -user_user_name_*' user_name 형식은 '[domain]\user'입니다.	지정된 인증 메커니즘을 사용합니다
'* vserver cifs session show -vserver_vserver_name_ -auth-mechanism authentication_mechanism *' '-auth-mechanism'의 값은 다음 중 하나일 수 있습니다. • "NTLMv1"입니다 • NTLMv2 • Kerberos • '익명'	지정된 프로토콜 버전을 사용하여

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
'* vserver cifs session show -vserver_vserver_name_ -protocol-version protocol_version *' '-protocol-version'의 값은 다음 중 하나일 수 있습니다. • 'MB1'입니다 • MB2 • MB2_1 • MB3 • 'MB3_1' ⓘ 지속적으로 사용 가능한 보호 기능과 SMB 멀티 채널은 SMB 3.0 이상 세션에서만 사용할 수 있습니다. 모든 적격 세션에서 해당 상태를 보려면 이 매개변수를 'MB3' 이상으로 설정한 값으로 지정해야 합니다.	지속적으로 사용 가능한 보호 수준을 지정합니다

SMB 세션 정보를 표시하려면...	다음 명령을 입력합니다...
'* vserver cifs session show -vserver_vserver_name_ -Continuously -available_Continuously_available_protection_level_*' '-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다. • 아니 • 네 • 부분	지정된 SMB 서명 세션 상태

예

다음 명령을 실행하면 IP 주소가 10.1.1.1인 워크스테이션에서 설정된 SVM VS1 세션의 세션 정보가 표시됩니다.

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

다음 명령을 실행하면 SVM VS1 에서 지속적으로 사용 가능한 보호 기능을 지원하는 세션에 대한 자세한 세션 정보가 표시됩니다. 도메인 계정을 사용하여 연결을 만들었습니다.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

다음 명령을 실행하면 SVM VS1 기반 SMB 3.0 및 SMB 멀티 채널을 사용하는 세션에 대한 세션 정보가 표시됩니다. 이 예에서 사용자는 LIF IP 주소를 사용하여 SMB 3.0 지원 클라이언트에서 이 공유에 연결했습니다. 따라서 인증 메커니즘은 NTLMv2로 기본값입니다. 지속적으로 사용 가능한 보호 기능을 사용하여 연결하려면 Kerberos 인증을 사용하여 연결해야 합니다.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

ONTAP에서 열린 **SMB** 파일에 대한 정보를 표시합니다

SMB 연결 및 세션 ID, 호스팅 볼륨, 공유 이름 및 공유 경로를 포함하여 열려 있는 SMB 파일에 대한 정보를 표시할 수 있습니다. 또한 파일의 지속적으로 사용 가능한 보호 수준에 대한 정보를 표시할 수도 있습니다. 이 정보는 열려 있는 파일이 무중단 작업을 지원하는 상태에 있는지 여부를 확인하는 데 유용합니다.

이 작업에 대해

설정된 SMB 세션에서 열린 파일에 대한 정보를 표시할 수 있습니다. 표시된 정보는 SMB 세션 내의 특정 파일에 대한 SMB 세션 정보를 확인해야 할 때 유용합니다.

예를 들어, 열린 파일 중 일부가 지속적으로 사용 가능한 보호 기능을 통해 열려 있고 일부는 지속적으로 사용 가능한 보호 기능을 통해 열려 있지 않은 SMB 세션이 있는 경우(vserver cifs session show 명령의 출력 값이 부분(Partial)인 경우), 이 명령을 사용하여 계속 사용할 수 없는 파일을 확인할 수 있습니다.

선택적 매개 변수 없이 'vserver cifs session file show' 명령을 사용하면 SVM(스토리지 가상 시스템)에서 설정된 SMB 세션의 모든 열려 있는 파일에 대한 정보를 요약 형식으로 표시할 수 있습니다.

그러나 대부분의 경우 반환되는 출력량이 큽니다. 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 이 기능은 열려 있는 파일의 작은 하위 집합에 대한 정보만 보려는 경우에 유용합니다.

- 옵션 '-fields' 매개변수를 사용하여 선택한 필드에 출력을 표시할 수 있습니다.

이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

- '-instance' 매개 변수를 사용하여 열려 있는 SMB 파일에 대한 자세한 정보를 표시할 수 있습니다.

  이 매개 변수는 단독으로 사용하거나 다른 선택적 매개 변수와 함께 사용할 수 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

열려 있는 **SMB** 파일을 표시하려면...	다음 명령을 입력합니다...
SVM에 대해 요약 형식으로 표시됩니다	'* vserver cifs 세션 파일 표시 -vserver_vserver_name_*'
지정된 노드에서	'* vserver CIFS 세션 파일 show -vserver_vserver_name_-node{node_name
local} *	지정된 파일 ID에 있습니다
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-file-id integer*'	지정된 SMB 연결 ID에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-connection-id integer*'	지정된 SMB 세션 ID에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-session-id integer*'	지정된 호스팅 집계에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-hosting-aggregate_aggregate_name_*'	지정된 볼륨에서
'* vserver cifs 세션 파일 표시 -vserver_vserver_name_-hosting-volume_volume_name_*'	지정된 SMB 공유에서
'* vserver CIFS 세션 파일 표시 -vserver_vserver_name_-share_share_name_*'	지정된 SMB 경로에 있어야 합니다
'* vserver CIFS 세션 파일 표시 -vserver_vserver_name_-path_path_*'	지속적으로 사용 가능한 보호 수준을 지정합니다

열려 있는 **SMB** 파일을 표시하려면...	다음 명령을 입력합니다...
'* vserver cifs 세션 파일 표시 - vserver_vserver_name_-Continuously-available_Continuously_available_status_ * '-연속 사용 가능'의 값은 다음 중 하나일 수 있습니다. • 아니 • 네 계속 사용 가능한 상태가 '아니요'인 경우 열려 있는 파일은 Takeover와 Giveback에서 중단 없이 복구할 수 없습니다. 또한, 고가용성 관계에 있는 파트너 간의 일반 애그리게이트 재배치에서 복구할 수 없습니다.	지정된 다시 연결된 상태에서

출력 결과를 구체화하는 데 사용할 수 있는 추가 선택적 매개 변수가 있습니다. 이 절차에서 설명하는 명령에 대한 자세한 내용은 를 "ONTAP 명령 참조입니다"참조하십시오.

예

다음 예에서는 SVM VS1 에서 열린 파일에 대한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1
Node:        node1
Vserver:     vs1
Connection:  3151274158
Session:     1
File     File       Open Hosting                Continuously
ID       Type       Mode Volume     Share       Available
------- --------- ---- --------- ----------- ------------
41       Regular    r    data       data        Yes
Path: \mytest.rtf
```

다음 예에서는 SVM VS1에서 파일 ID 82가 있는 개방형 SMB 파일에 대한 자세한 정보를 표시합니다.

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.