Dell EMC Data Domain® Operating System

6.2 버전

관리 가이드

302-005-407
REV. 01

DELL EMC

발행: 2018년 12월

한국이엠씨컴퓨터시스템즈(주)
서울특별시 강남구 테헤란로 152 강남파이낸스센터 18층 (우)06236
대표 전화: (02)2125-7000 구입/상담 문의: 080-775-7000 팩스: (02)2125-7280
www.DellEMC.com/ko-kr/index.htm

목차

머리말

Data Domain은 제품군을 향상시키기 위한 노력의 일환으로 소프트웨어와 하드웨어의 개정 버전을 정기적으로 릴리즈하고 있습니다. 따라서 이 문서에서 설명하는 일부 기능은 현재 사용 중인 소프트웨어 또는 하드웨어의 일부 버전에서 지원되지 않을 수 있습니다. 제품 릴리즈 노트는 제품 기능, 소프트웨어 업데이트, 소프트웨어 호환성 가이드 및 Data Domain 제품, 라이센스 등록 및 서비스에 대한 최신 정보를 제공합니다.

제품이 올바르게 작동하지 않거나 이 문서에 설명된 대로 작동하지 않는 경우 기술 지원 전문가에게 문의하십시오.

참고

이 문서는 발행일 현재 정확한 것으로 간주됩니다. 온라인 지원(https://support.emc.com)으로 이동하여 이 문서의 최신 버전을 사용하고 있는지 확인하십시오.

목적

이 가이드에서는 브라우저 기반 GUI(Graphical User Interface)인 DD System Manager(Data Domain System Manager)를 사용하는 절차에 중점을 두고 Data Domain® 시스템을 관리하는 방법에 대해 설명합니다. DD System Manager에서 중요 관리 작업이 지원되지 않을 경우 CLI(Command Line Interface) 명령에 대해 설명합니다.

참고

- DD System Manager의 이전 명칭은 Enterprise Manager입니다.
- 경우에 따라서 CLI 명령은 해당 DD System Manager 기능에서 제공하는 것보다 많은 옵션을 제공할 수 있습니다. 명령 및 해당 옵션에 대한 전체 설명은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

대상

이 가이드는 표준 백업 소프트웨어 패키지 및 일반 백업 관리에 익숙한 시스템 관리자를 위한 내용을 담고 있습니다.

관련 설명서

다음 Data Domain 시스템 문서는 추가 정보를 제공합니다.

- 시스템의 설치 및 설정 가이드(예: *Data Domain DD9300 System Installation Guide*)
- *Data Domain 하드웨어 기능 및 사양 가이드*
- *Data Domain Operating System USB Installation Guide*
- *Data Domain Operating System DVD Installation Guide*
- *Data Domain Operating System Release Notes*
- *Data Domain Operating System 초기 구성 가이드*
- *Data Domain 보안 구성 가이드*
- *Data Domain Operating System HA(High Availability) 백서*
- *Data Domain Operating System 명령 참조 가이드*
- *Data Domain Operating System MIB Quick Reference*

- *Data Domain Operating System Offline Diagnostics Suite User's Guide*
- 시스템 구성 요소에 대한 현장 교체 가이드(예: *Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade*)
- *Data Domain, System Controller Upgrade Guide*
- *Data Domain Expansion Shelf, Hardware Guide*(셸프 모델 ES30/FS15 또는 DS60의 경우)
- *Data Domain Boost for Partner Integration Administration Guide*
- *OpenStorage용 Data Domain Boost 관리 가이드*
- *Data Domain Boost for Oracle Recovery Manager 관리 가이드*
- *Statement of Volatility for the Data Domain DD2500 System*
- *Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System*
- *Statement of Volatility for the Data Domain DD6300, DD6800, or DD9300 System*
- *Statement of Volatility for the Data Domain DD9500 or DD9800 System*

선택 사항인 RSA Data Protection (DPM) Key Manager가 있는 경우 RSA Key Manager 제품과 함께 사용할 수 있는 *RSA Data Protection Manager Server Administrator's Guide*의 최신 버전을 참조하십시오.

본 문서에 사용된 중요 알림 표기법

특별히 고지해야 할 사항이 있을 경우 다음과 같은 표기법을 사용했습니다.

알림

알림은 비즈니스 또는 데이터 손실의 가능성을 경고하는 내용을 나타냅니다.

참고

참고는 해당 항목에 부수적이지만 필수적인 사항은 아닌 정보를 나타냅니다. 참고를 통해 설명, 주석, 본문 내용에서 강조할 사항을 제시하거나 단순히 관련 사항을 설명합니다.

입력 표기법

이 문서에서는 다음과 같은 글꼴을 사용했습니다.

표 1 인쇄용 서체

굵은 글꼴	인터페이스 요소 이름(예: 창, 대화 상자, 버튼, 필드, 탭, 키, 메뉴 경로 등 특히 사용자가 선택하거나 클릭할 수 있는 요소의 이름)을 나타냅니다.
기울임꼴	텍스트에 나열된 문서 제목을 강조 표시합니다.
`Monospace`	다음과 같은 시스템 정보를 나타냅니다. • 시스템 코드 • 시스템 출력(예: 오류 메시지 또는 스크립트) • 경로 이름, 파일 이름, 프롬프트 및 구문 • 명령 및 옵션
`Monospace 기울임꼴`	변수 값으로 바꿔야 하는 변수 이름을 강조 표시합니다.

표 1 인쇄용 서체 (계속)

Monospace 굵은 글꼴	사용자 입력을 위한 텍스트를 나타냅니다.
[ ]	선택적 값은 대괄호로 표시합니다.
|	세로 막대는 대체 선택 항목을 나타냅니다(막대는 “또는”을 의미함).
{ }	중괄호는 사용자가 지정해야 하는 내용(예: x, y 또는 z)을 의미합니다.
...	줄임표는 예에서 생략된 중요하지 않은 정보를 나타냅니다.

지원 정보

Data Domain 지원, 제품 및 라이센스 등록 정보는 다음과 같이 확인할 수 있습니다.

제품 정보

설명서, 릴리즈 노트, 소프트웨어 업데이트 또는 Data Domain 제품에 대한 자세한 정보는 온라인 지원(https://support.emc.com)에서 확인하십시오.

기술 지원

온라인 지원으로 이동한 후 서비스 센터를 클릭합니다. 기술 지원을 요청할 수 있는 몇 가지 옵션이 나타납니다. 서비스 요청을 개설하려면 유효한 지원 계약이 있어야 합니다. 유효한 지원 계약 체결에 대한 자세한 내용 또는 계정 관련 질문은 영업 담당자에게 문의하십시오.

사용자 의견

여러분이 보내주시는 의견은 EMC 사용 설명서의 체계적인 구성과 정확성, 전반적인 품질 향상을 위해 유용하게 사용됩니다. 다음 주소로 이 문서에 대한 여러분의 의견을 보내주십시오. DPAD.Doc.Feedback@emc.com.

1장

Data Domain 시스템 기능 및 통합

이 장에서 다루는 내용은 다음과 같습니다.

개정 내역

개정 내역에는 DD OS 릴리스 6.2에 관한 내용을 반영하기 위해 본 문서에서 변경된 주요 내용이 정리되어 있습니다.

표 2 문서 개정 내역

개정 버전	날짜	설명
01 (6.2.0)	2018년 12월	이 개정 버전에는 다음과 같은 새로운 기능에 대한 정보가 포함됩니다. • 메일 서버 자격 증명을 DD SM 구성 마법사의 일부로 구성합니다. • DD300 8TB~16TB 용량 확장 • 보안 LDAP 인증 • Active Directory 연결 진단 툴 • USB 드라이브에 코어 덤프 파일 저장 • SMB 변경 알림 • 트러스트된 도메인 오프라인 액세스 • Alibaba 및 Google Cloud Platform 클라우드 공급업체에 대한 DD Cloud Tier 지원

Data Domain 시스템 개요

Data Domain 시스템은 엔터프라이즈 환경에 데이터 보호 및 DR(Disaster Recovery)을 제공하는 디스크 기반 인라인 중복 제거 어플라이언스입니다.

모든 시스템은 DD OS(Data Domain Operating System)를 실행합니다. 이 DD OS는 모든 시스템 작업을 수행할 수 있는 CLI와 구성, 관리, 모니터링을 위한 Data DD System Manager(Data Domain System Manager) GUI를 제공합니다.

참고

DD System Manager의 이전 명칭은 Enterprise Manager입니다.

시스템은 스토리지 용량과 데이터 처리량이 서로 다른 어플라이언스로 구성됩니다. 시스템은 일반적으로 스토리지 공간을 추가하는 확장 엔클로저로 구성됩니다.

Data Domain 시스템 기능

Data Domain 시스템 기능은 데이터 무결성, 안정적인 복원, 효율적인 리소스 사용 및 관리 편의성을 보장합니다. 라이센스가 있는 기능을 사용하면 요구 사항 및 예산에 맞게 시스템 기능 집합을 확장할 수 있습니다.

데이터 무결성

DD OS Data Invulnerability Architecture™는 하드웨어 및 소프트웨어 장애로 인한 데이터 손실로부터 보호합니다.

- 디스크에 기록할 때 DD OS는 수신한 모든 데이터에 대해 체크섬과 자체로 설명이 되는 메타데이터를 생성하고 저장합니다. 디스크에 데이터를 기록한 후에 DD OS가 체크섬 및 메타데이터를 다시 계산하고 확인합니다.
- 추가 전용 쓰기 정책은 유효한 데이터를 덮어쓰지 못하도록 보호합니다.
- 백업이 완료되면 검증 프로세스가 디스크에 기록된 내용을 검토하고 파일 시스템 내에서 모든 파일 세그먼트가 논리적으로 올바르고 디스크에 쓰기 전후에 데이터가 동일한지 확인합니다.
- 백그라운드에서 실행되는 온라인 확인 작업은 디스크의 데이터가 올바르고 이전 검증 프로세스 이후에 변경되지 않았는지 지속적으로 확인합니다.
- 대부분의 Data Domain 시스템에 있는 스토리지는 이중 패리티 RAID 6 구성(2개의 패리티 드라이브)에서 설정됩니다. 또한 대부분의 구성에는 디스크 8개를 사용하는 DD1xx 시리즈 시스템을 제외하고 엔클로저마다 핫 스페어가 하나씩 포함됩니다. 각 패리티 스트라이프에서는 데이터가 올바른지 확인하기 위해 블록 체크섬을 사용합니다. 체크섬은 온라인 확인 작업과 Data Domain 시스템에서 데이터를 읽는 중에 계속해서 사용됩니다. 이중 패리티를 통해 시스템은 최대 2개의 디스크에서 동시 오류를 수정할 수 있습니다.
- 하드웨어 또는 전원 장애 중에 데이터를 동기화된 상태로 유지하기 위해 Data Domain 시스템은 NVRAM(Non-Volatile RAM)을 사용해 미해결 입출력 작업을 추적합니다. 배터리가 100% 충전된 NVRAM(일반 상태) 카드는 몇 시간 동안 데이터를 보존할 수 있습니다. 이 시간은 사용 중인 하드웨어에 의해 결정됩니다.
- 복구 작업에서 데이터를 다시 읽을 때 DD OS는 여러 계층의 정합성 검사를 사용해 복구된 데이터가 올바른지 확인합니다.
- SSD 캐시에 쓰는 경우 DD OS의 동작:
  - 캐시에 저장된 모든 레코드에 대해 SL 체크섬을 생성하여 캐시 데이터의 손상을 감지합니다. 모든 캐시 읽기에 대해 이 체크섬의 유효성을 검사합니다.
  - 캐시 데이터의 손상을 캐시 비적중으로 취급하므로 데이터 손실이 발생하지 않습니다. 따라서 캐시 클라이언트는 NVRAM, HDD 등과 같은 다른 백업 메커니즘 없이 최신 데이터 복제본을 저장할 수 없습니다.
  - 캐시 클라이언트가 잘못 지시되거나 손실된 쓰기를 감지하고 처리할 수 있으므로 캐시 쓰기에 대한 인라인 검증이 필요하지 않습니다. 따라서 입출력 대역폭도 절감됩니다.
  - 캐시의 데이터가 자주 변경되고 SAS BMS(Background Media Scan)에 의해 이미 스크러빙되기 때문에 파일 시스템의 SSD 스크러빙이 필요하지 않습니다.

데이터 중복 제거

DD OS 중복 제거는 각 백업 작업 중에 중복 데이터를 식별하고 고유한 데이터를 한 번만 저장합니다.

고유한 데이터의 저장은 백업 소프트웨어에 표시되지 않으며 데이터 형식과 독립적입니다. 데이터는 데이터베이스처럼 정형이거나, 텍스트 파일처럼 비정형일 수 있습니다. 데이터는 파일 시스템이나 원시 볼륨에서 파생될 수 있습니다.

일반적인 중복 제거 비율은 여러 주에 걸쳐 평균 20:1입니다. 이 비율은 매주 전체 백업 및 매일 증분 백업이 수행된다는 가정을 전제로 합니다. 다수의 중복 또는 유사 파일(일부 변경 사항과 함께 여러 차례 복제된 파일)을 포함하는 백업은 중복 제거의 혜택을 가장 많이 받습니다.

백업 볼륨, 크기, 보존 기간 및 변경률에 따라 중복 제거 용량이 달라질 수 있습니다. 중복 제거는 백업 볼륨 크기가 최소 10MiB(MiB는 MB의 2진 표기법에 해당) 이상일 때 가장 효과적입니다.

여러 Data Domain 시스템을 충분히 활용하기 위해서는 둘 이상의 Data Domain 시스템이 있는 사이트에서 동일한 클라이언트 시스템 또는 데이터 세트를 동일한 Data Domain 시스템에 일관적으로 백업해야 합니다. 예를 들어, 모든 판매 데이터의 전체 백업이 Data Domain 시스템 A로 이동할 경우 판매 데이터의 증분 백업 및 향후 전체 백업 또한 Data Domain 시스템 A로 이동하면 최대 중복 제거율이 달성됩니다.

복구 작업

파일 복구 작업 시 백업 또는 다른 복구 작업과 경합이 거의 또는 전혀 발생하지 않습니다.

Data Domain 시스템의 디스크에 백업하는 경우 증분 백업이 항상 안정적이며 손쉽게 액세스할 수 있습니다. 테이프 백업을 사용할 경우 복원 작업이 증분 백업을 보유한 여러 테이프에 의존할 수 있습니다. 또한 여러 테이프에 증분 백업이 많이 저장된 사이트일수록 복구 프로세스의 시간이 오래 걸리고 위험이 커집니다. 잘못된 테이프가 하나만 있어도 복원이 종료될 수 있습니다.

Data Domain 시스템을 사용하면 중복 데이터를 저장하는 낭비 없이 보다 자주 전체 백업을 수행할 수 있습니다. 테이프 드라이브 백업과 달리 여러 프로세스가 동시에 Data Domain 시스템에 액세스할 수 있습니다. Data Domain 시스템을 사용하면 사이트에서 안전한 사용자 중심의 단일 파일 복원 작업이 가능합니다.

Data Domain Replicator

Data Domain Replicator는 두 Data Domain 시스템 간 백업 데이터의 복제를 설정하고 관리합니다.

DD Replicator 페어는 소스 시스템과 대상 시스템으로 구성되며 소스 시스템의 전체 데이터 세트 또는 디렉토리를 대상 시스템에 복제합니다. 개별 Data Domain 시스템이 여러 복제 페어의 일부가 될 수 있으며 하나 이상 페어의 소스 및 하나 이상 페어의 대상 역할을 할 수 있습니다. 복제가 시작되면 소스 시스템이 대상 시스템에 새 백업 데이터를 자동으로 보냅니다.

다중 경로 및 로드 밸런싱

Fibre Channel 다중 경로 구성에서는 Data Domain 시스템과 백업 서버 또는 백업 대상 스토리지 간에 둘 이상의 경로가 설정됩니다. 여러 경로가 존재하는 경우 사용 가능한 경로 간에 자동으로 백업 로드가 분산됩니다.

다중 경로 구성을 생성하려면 둘 이상의 HBA 포트가 필요합니다. 백업 서버에 연결할 경우 다중 경로의 각 HBA 포트가 백업 서버의 개별 포트에 연결됩니다.

High Availability

HA(High Availability) 기능을 사용하면 두 Data Domain 시스템을 액티브-대기 쌍으로 구성하여 시스템 장애가 발생할 경우에 이중화 보호 기능을 제공할 수 있습니다. HA는 액티브 시스템과 대기 시스템을 동기화된 상태로 유지하므로, 하드웨어 또는 소프트웨어 문제로 인해 액티브 노드에 장애가 발생하면 대기 노드가 서비스를 인계받아 장애가 발생한 노드에서 수행하던 작업을 계속 진행할 수 있습니다.

HA 기능의 특징은 다음과 같습니다.

- 2노드 시스템에서 백업, 복구, 복제 및 관리 서비스의 페일오버를 지원합니다. 사용자가 별도의 작업을 수행할 필요 없이 자동으로 페일오버합니다.

- 권장하는 대로 구성된 경우 시스템 내에 단일 장애 지점 없이 완벽하게 이중화된 설계를 제공합니다.
- 페일오버 시 성능 저하 없이 Active-Standby 시스템을 제공합니다.
- 대부분의 작업을 10분 이내에 페일오버하는 기능을 제공합니다. CIFS, DD VTL 및 NDMP는 수동으로 재시작해야 합니다.

  참고

  Boost 애플리케이션 복구 작업은 DD 서버 페일오버가 완료되어야 시작할 수 있기 때문에 DD Boost 애플리케이션을 복구하는 데 10분보다 오래 걸릴 수 있습니다. 또한 애플리케이션에서 Boost 라이브러리를 호출할 때까지 Boost 애플리케이션 복구를 시작할 수 없습니다. 마찬가지로, NFS를 복구하는 데에도 추가 시간이 필요할 수 있습니다.

- DD OS CLI를 통해 손쉽게 관리 및 구성할 수 있도록 지원합니다.
- 제대로 작동하지 않는 하드웨어에 대한 알림을 제공합니다.
- 정상 모드와 성능이 저하된 모드 모두에서 HA 구성에 포함된 단일 노드의 성능과 확장성을 유지합니다.
- 독립 실행형 DD 시스템과 동일한 기능 세트를 지원합니다.

  참고

  DD Extended Retention과 vDisk는 지원되지 않습니다.

- SAS 드라이브로만 구성된 시스템을 지원합니다. 기존 시스템을 SAS 드라이브로만 구성된 시스템으로 업그레이드할 수도 있습니다.

  참고

  HA를 지원하는 Data Domain 시스템의 하드웨어 개요 및 설치 가이드에 새 HA 시스템을 설치하는 방법이 설명되어 있습니다. *Data Domain Single Node to HA Upgrade* 에서는 기존 시스템을 HA 쌍으로 업그레이드 방법에 대해 설명합니다.

- 제품을 확장하는 기능에 영향을 주지 않습니다.
- 운영 중단 없는 소프트웨어 업데이트를 지원합니다.

HA는 다음과 같은 Data Domain 시스템에서 지원됩니다.

- DD6800
- DD9300
- DD9500
- DD9800

HA 아키텍처

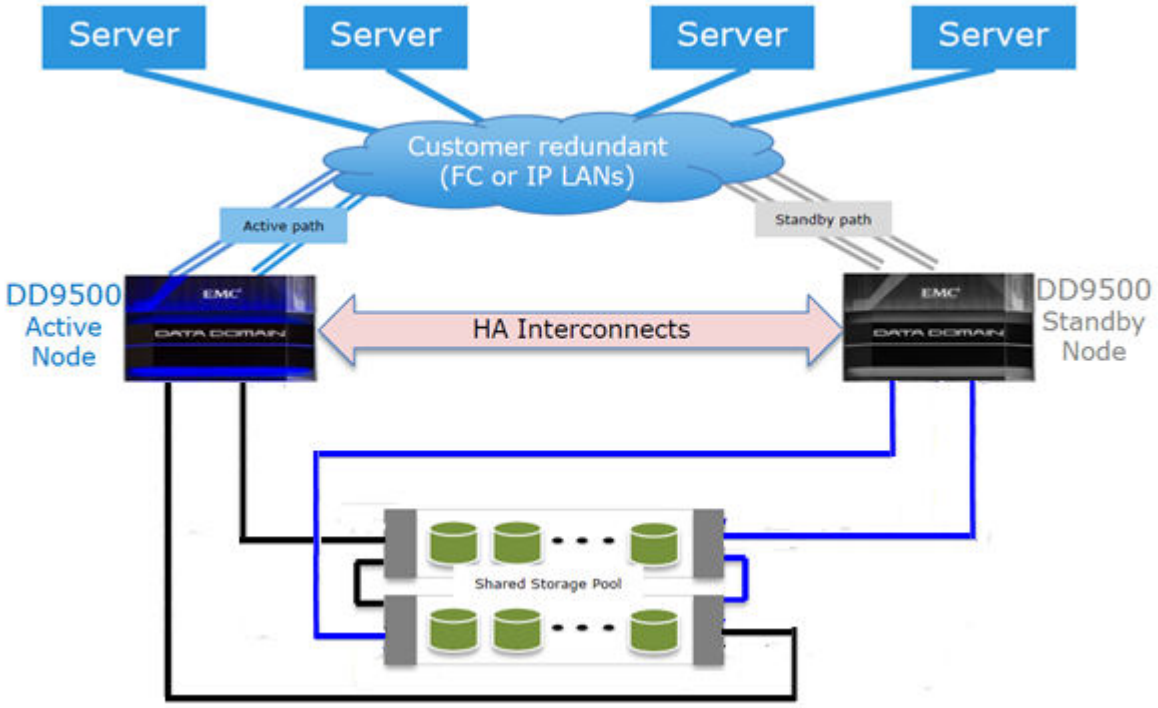
HA 기능은 IP 접속과 FC 접속에 사용할 수 있습니다. 환경에서 고가용성을 실현하려면 두 노드가 동일한 IP 주소, FC SAN 및 호스트에 액세스할 수 있어야 합니다.

HA는 어느 물리적 노드가 액티브 노드인지에 관계없이 유동 IP 주소를 사용하여 IP 네트워크를 통해 Data Domain HA 쌍에 대한 데이터 액세스를 제공합니다.

HA는 NPIV를 사용하여 FC SAN을 통해 노드 간에 FC WWN을 이동함으로써 페일오버 후에 FC 이니시에이터가 접속을 다시 설정할 수 있게 합니다.

그림 1(24페이지)에는 HA 아키텍처가 나와 있습니다.

그림 1 HA 아키텍처



랜덤 입출력 처리

DD OS에 포함된 랜덤 입출력 최적화 기능은 순차적 읽기 및 쓰기 작업보다 훨씬 많은 양의 랜덤 읽기 및 쓰기 작업을 생성하는 애플리케이션 및 활용 사례의 성능을 향상시킵니다.

DD OS는 가상 머신의 즉각적인 액세스 및 즉각적인 복구와 같은 랜덤 읽기 및 쓰기 작업과 Avamar와 같은 애플리케이션에서 생성되는 영구적으로 계속되는 증분 백업으로 구성된 워크로드를 처리하도록 최적화되었으며, 다음과 같은 최적화 기능을 제공합니다.

- 랜덤 읽기 및 랜덤 쓰기 지연 시간을 개선합니다.
- 더 작은 읽기 크기를 사용하여 IOPS를 향상시킵니다.
- 단일 스트림 내에서 동시 입출력 작업을 지원합니다.
- 훨씬 작은 스트림을 사용하여 최대 읽기 및 쓰기 처리량을 제공합니다.

> 참고
>
> 최대 랜덤 입출력 스트림 수는 Data Domain 시스템의 최대 복구 스트림 수로 제한됩니다.

랜덤 입출력이 개선되어 Data Domain 시스템이 Avamar 및 Networker 같은 백업 애플리케이션에 대한 즉각적인 액세스/즉각적인 복구 기능을 지원할 수 있습니다.

시스템 관리자 액세스

시스템 관리자는 CLI 또는 GUI를 사용해 시스템에 액세스하여 구성 및 관리 작업을 수행할 수 있습니다.

- DD OS CLI—직렬 콘솔이나 SSH 또는 Telnet을 사용하는 이더넷 접속을 통해 사용할 수 있는 명령줄 인터페이스입니다. CLI 명령을 사용해 초기 시스템 구성을 수행

하고 개별 시스템 설정을 변경하는 것은 물론 시스템 작동 상태를 표시할 수 있습니다.

- DD System Manager - 이더넷 접속을 통해 사용할 수 있는 브라우저 기반 GUI입니다. DD System Manager를 사용하여 초기 시스템 구성을 수행하고, 초기 구성 후 구성을 변경하고, 시스템 및 구성 요소 상태를 표시하고, 보고서와 차트를 생성할 수 있습니다.

참고

일부 시스템은 시스템에 직접 연결된 키보드와 모니터를 사용해 액세스할 수 있습니다.

라이센스를 통해 제공되는 기능

기능 라이센스를 사용하면 사용하려는 기능만 구매할 수 있습니다. 라이센스가 필요한 일부 기능의 예로는 DD Extended Retention, DD Boost 및 스토리지 용량 증가가 있습니다.

라이센스가 있는 기능의 구매에 대한 자세한 내용은 영업 담당자에게 문의하십시오.

표 3 라이센스가 필요한 기능

기능 이름	소프트웨어의 라이센스 이름	설명
Data Domain ArchiveStore	ARCHIVESTORE	파일 및 이메일 아카이빙, 파일 계층화 및 컨텐츠와 데이터베이스 아카이빙 같은 아카이브 사용을 위해 Data Domain 시스템에 라이센스를 등록합니다.
Data Domain Boost	DDBOOST	다음 애플리케이션에서 Data Domain 시스템 사용을 활성화합니다. Avamar, NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NBU(NetBackup) 및 Backup Exec DD Boost의 MFR(Managed File Replication) 기능을 사용하는 경우에도 DD Replicator 라이센스가 필요합니다.
Data Domain Capacity on Demand	CONTROLLER-COD	4TB DD2200 시스템의 용량을 필요에 따라 7.5TB 또는 13.18TB로 확장할 수 있습니다. 13.18TB로 증가하려면 EXPANDED-STORAGE 라이센스도 필요합니다.
Data Domain Cloud Tier	CLOUDTIER-CAPACITY	Data Domain 시스템이 데이터를 활성 계층에서 장기간 보존을 위해 퍼블릭, 프라이빗 또는 하이브리드 클라우드의 대용량 저가 오브젝트 스토리지로 이동할 수 있습니다.
Data Domain Encryption	ENCRYPTION	시스템을 다른 위치로 이동할 때 시스템 드라이브 또는 외부 스토리지의 데이터를 저장하고 잠그는 동안 데이터를 암호화할 수 있습니다.
Data Domain Expansion Storage	EXPANDED-STORAGE	Data Domain 시스템을 기본 시스템에 제공된 수준 이상으로 확장할 수 있습니다.
Data Domain Extended Retention(이전 명칭 DD Archiver)	EXTENDED-RETENTION	DD Extended Retention 스토리지 기능에 라이센스를 등록합니다.

표 3 라이센스가 필요한 기능 (계속)

기능 이름	소프트웨어의 라이센스 이름	설명
Data Domain I/OS(IBM i 운영 환경용)	I/OS	IBM i 운영 환경에서 시스템을 백업하는 데 DD VTL이 사용될 경우 I/OS 라이센스가 필요합니다. 라이브러리에 가상 테이프 드라이브를 추가하기 전에 이 라이센스를 적용합니다.
Data Domain Replicator	REPLICATION	Data Domain 시스템에서 다른 Data Domain 시스템에 데이터 복제를 위해 DD Replicator 기능을 추가합니다. 각 시스템에는 라이센스가 필요합니다.
Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	SEC17a-4 같은 규정 표준에서 가장 엄격한 데이터 보존 요구 사항을 충족합니다.
Data Domain Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	지정된 보존 기간이 만료되기 전에 선택한 파일이 수정 및 삭제되지 않도록 보호합니다.
Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Data Domain 시스템의 활성 계층 스토리지 용량을 추가 엔클로저 또는 엔클로저 내 디스크 팩으로 확장할 수 있습니다.
Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Data Domain 시스템의 아카이브 계층 스토리지 용량을 추가 엔클로저 또는 엔클로저 내 디스크 팩으로 확장할 수 있습니다.
Data Domain Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	한 엔클로저의 데이터를 다른 엔클로저로 마이그레이션하여 오래되고 용량이 적은 엔클로저를 교체할 수 있습니다.
DD VTL(Data Domain Virtual Tape Library)	VTL	Fibre Channel 네트워크를 통해 Data Domain 시스템을 VTL(Virtual Tape Library)로 사용할 수 있습니다. 이전에 개별 라이센스가 필요했던 NDMP Tape Server 기능도 이 라이센스로 활성화할 수 있습니다.
High Availability	HA-ACTIVE-PASSIVE	Active-Standby 구성으로 고가용성 기능을 지원합니다. HA 라이센스를 하나만 구매하면 됩니다. 라이센스가 액티브 노드에서 실행되고 대기 노드로 미러링됩니다.

스토리지 환경 통합

Data Domain 시스템은 기존 데이터 센터에 손쉽게 통합됩니다.

- 모든 Data Domain 시스템은 NFS, CIFS, DD Boost 또는 DD VTL 프로토콜을 사용하는 유수의 백업 및 아카이브 애플리케이션에 대해 스토리지 대상으로 구성될 수 있습니다.
- 여러 구성과 함께 사용할 수 있는 애플리케이션에 대한 정보는 *호환성 문서* (https://support.emc.com)를 검색하십시오.
- 여러 백업 서버가 하나의 Data Domain 시스템을 공유할 수 있습니다.
- 하나의 Data Domain 시스템이 여러 백업 및 복구 작업을 동시에 처리할 수 있습니다.

- 여러 Data Domain 시스템을 하나 이상의 백업 서버에 연결할 수 있습니다.

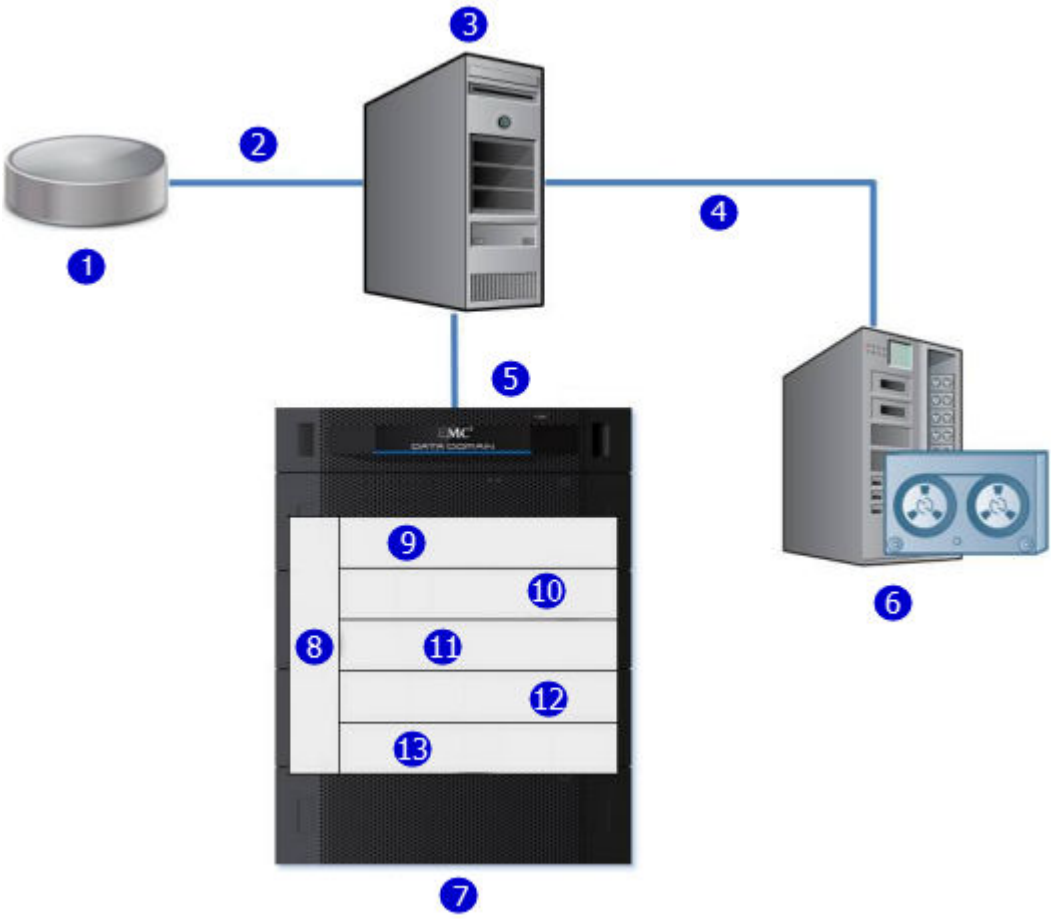
백업 대상으로 사용하기 위해서는 Data Domain 시스템을 이더넷 접속을 통해 액세스한 파일 시스템이 있는 디스크 스토리지 유닛 또는 Fibre Channel 연결을 통해 액세스한 VTL로 구성할 수 있습니다. DD VTL 기능은 테이프 백업을 위해 백업 소프트웨어가 이미 구성되어 있는 환경으로 Data Domain 시스템을 통합해 중단을 최소화할 수 있도록 활성화합니다.

구성은 이 가이드의 관련 섹션에 설명되어 있는 DD OS와 백업 애플리케이션의 관리자 가이드 및 Data Domain 애플리케이션 관련 가이드와 기술 노트에 설명되어 있는 백업 애플리케이션에서 수행할 수 있습니다.

모든 백업 애플리케이션은 Data Domain 디스크 디바이스의 NFS 또는 CIFS 파일 시스템으로 Data Domain 시스템에 액세스할 수 있습니다.

다음 그림은 기존 기본의 기본 백업 구성에 통합된 Data Domain 시스템을 보여 줍니다.

그림 2 스토리지 환경에 통합된 Data Domain 시스템



1. 운영 스토리지
2. 이더넷
3. 백업 서버
4. SCSI/Fibre Channel
5. 기가비트 이더넷 또는 Fibre Channel
6. 테이프 시스템
7. Data Domain 시스템
8. 관리

그림 2 스토리지 환경에 통합된 Data Domain 시스템 (계속)

9. NFS/CIFS/DD VTL/DD Boost
10. 데이터 검증
11. 파일 시스템
12. 글로벌 중복 제거 및 압축
13. RAID

그림 2(27페이지)에서 보듯이 데이터는 이더넷 또는 Fibre Channel 접속을 통해 Data Domain 시스템으로 이동합니다. 그 즉시 데이터 검증 프로세스가 시작되고 데이터가 Data Domain 시스템에 상주하는 동안에 계속됩니다. 파일 시스템에서 DD OS Global Compression™ 알고리즘이 스토리지를 위해 데이터를 중복 제거하고 압축합니다. 그리고 나서 데이터가 디스크 RAID 서브시스템으로 전송됩니다. 복구 작업이 필요할 경우 데이터가 Data Domain 스토리지에서 검색되거나, 압축 해제되거나, 정합성 보장을 위한 검증을 거치고 이더넷(NFS, CIFS, DD Boost의 경우) 또는 Fibre Channel(DD VTL 및 DD Boost의 경우)을 사용해 백업 서버로 전송됩니다.

DD OS는 백업 소프트웨어에서 비교적 큰 순차적 데이터 스트림을 수용하고 높은 처리량, 지속적인 데이터 검증 및 높은 압축을 위해 최적화됩니다. 또한 니어라인 스토리지(DD ArchiveStore)에서 다수의 크기가 작은 파일을 수용합니다.

Data Domain 시스템의 성능은 다음과 같은 경우에 특정 백업 소프트웨어가 아닌 애플리케이션의 데이터를 저장할 때 가장 우수합니다.

- 데이터가 순차적 쓰기(덮어쓰기 없음)로 Data Domain 시스템에 전송됩니다.
- 데이터가 Data Domain 시스템에 전송되기 전에 압축되거나 암호화되지 않습니다.

2장

시작

이 장에는 다음과 같은 내용이 포함됩니다.

Dell EMC Data Domain System Manager 개요

DD System Manager는 이더넷 연결을 통해 사용할 수 있는 브라우저 기반 사용자 인터페이스로서, 위치에 관계없이 단일 시스템을 관리할 수 있습니다. 통합된 단일 관리 인터페이스를 제공하는 DD System Manager를 사용하여 여러 시스템 기능과 시스템 설정을 구성 및 모니터링할 수 있습니다.

참고

Data Domain Management Center에서는 단일의 브라우저 창에서 여러 시스템을 관리할 수 있습니다.

DD System Manager를 사용하면 실시간 그래프와 표를 통해 시스템 하드웨어 구성 요소와 구성된 기능의 상태를 모니터링할 수 있습니다.

또한 CLI에서 모든 시스템 기능을 수행하는 명령 집합을 사용할 수도 있습니다. 이러한 명령을 사용하여 시스템 설정을 구성하고 시스템 상태, 기능 구성 및 작업을 표시할 수 있습니다.

명령줄 인터페이스는 직렬 콘솔이나 SSH 또는 Telnet을 사용하는 이더넷 접속을 통해 사용할 수 있습니다.

참고

일부 시스템은 시스템에 직접 연결된 키보드와 모니터를 사용해 액세스할 수 있습니다.

DD OS 소프트웨어 버전

DD OS 소프트웨어 릴리스는 해당 버전을 실행하는 설치된 시스템의 수를 나타내는 세 가지 공개 상태로 사용됩니다.

- **GA(General Availability)** 릴리스는 Data Domain 내부 QA 테스트를 완료했으며 프로덕션 환경에서 설치할 수 있습니다.
- **DA(Directed Availability) - 제어(Directed Availability)** 릴리스는 신중하게 제어되는 액세스 릴리스로, 소수의 설치로 전달됩니다. 고객은 이러한 릴리스에 액세스할 수 있는 자격을 요청할 수 있습니다.
- **대상 코드** - 가능한 경우 모든 시스템을 릴리스 제품군 내의 Data Domain OS 대상 코드로 업그레이드 하는 것이 좋습니다.

  참고

  지정된 제품군에는 대상 코드 릴리스가 하나만 있습니다. 대상 코드 릴리스는 설치 및 런타임 시간과 품질 메트릭을 충족하여 안정적이며 대부분의 고객에게 영향을 미치는 문제가 없음을 나타냅니다. 일부 제품군의 경우 제한된 고객 사용, 품질 문제 또는 기타 고려 사항으로 인해 대상 코드가 식별되지 않을 수 있습니다.

제품군 간에 업그레이드하는 경우 제품 호환성을 고려해야 할 수 있으며, 제품 호환성을 신중히 검토한 후에 새 릴리스 제품군으로 업그레이드해야 합니다.

DD System Manager 로그인 및 로그아웃

브라우저를 사용해 DD System Manager에 로그인합니다.

웹 브라우저에서 DD System Manager에 연결하는 경우 모든 HTTP 연결이 자동으로 HTTPS로 리디렉션됩니다.

절차

1. 다음과 같이 웹 브라우저를 열고 IP 주소 또는 호스트 이름을 입력해 DD System Manager에 접속합니다.
   - 정규화된 도메인 이름(예: `http://dd01.emc.com`)
   - 호스트 이름(`http://dd01`)
   - IP 주소(`http://10.5.50.5`)

   참고

   DD System Manager는 HTTP 포트 80 및 HTTPS 포트 443을 사용합니다. Data Domain 시스템에서 방화벽을 사용하는 경우 HTTP는 포트 80, HTTPS는 포트 443을 사용해서 시스템에 연결해야 할 수 있습니다. 포트 번호는 보안 요구 사항에 따라 손쉽게 변경할 수 있습니다.

   참고

   Data Domain System Manager를 웹 브라우저에서 시작할 수 없는 경우 "GUI 서비스를 일시적으로 사용할 수 없습니다. 브라우저를 새로 고치십시오. 문제가 계속되면 Data Domain 지원 부서에 문의하십시오." 오류 메시지가 표시됩니다. SSH는 Data Domain 시스템에 로그인하는 데 사용할 수 있으며 모든 명령을 실행할 수 있습니다.
   DD OS를 업그레이드하지 않았지만 여전히 이 GUI 오류가 발생하는 경우 다음 절차를 따르십시오.

   a. 해당 오류가 보고된 Data Domain 시스템에서 웹 브라우저 세션을 닫습니다.
   b. 다음 명령을 순서대로 실행합니다.
      - `adminaccess disable http`
      - `adminaccess disable https`
      - `adminaccess enable http`
      - `adminaccess enable https`
   c. http 및 https 서비스가 완전히 시작될 때까지 5분 정도 기다립니다.
   d. 웹 브라우저를 열고 Data Domain System Manager에 연결합니다.

   DD OS 업그레이드 후에 이 GUI 문제가 발생하면 다음 절차를 따르십시오.

   a. 해당 오류가 보고된 Data Domain 시스템에서 웹 브라우저 세션을 닫습니다.
   b. 다음 명령을 순서대로 실행합니다.
      - `adminaccess disable http`
      - `adminaccess disable https`
      - `adminaccess certificate generate self-signed-cert`
      - `adminaccess enable http`
      - `adminaccess enable https`

   a. http 및 https 서비스가 완전히 시작될 때까지 5분 정도 기다립니다.
   b. 웹 브라우저를 열고 Data Domain System Manager에 연결합니다.

2. HTTPS 보안 로그인을 위해 **Secure Login**을 클릭합니다.

   HTTPS를 통한 보안 로그인을 위해서는 DD OS 시스템의 ID를 확인하고 DD System Manager와 브라우저 간의 양방향 암호화를 지원하기 위한 디지털 인증서가 필요합니다. DD OS에는 자체 서명된 인증서가 포함되어 있으며, DD OS에서 자신의 고유한 인증서를 가져올 수 있습니다.

3. 지정된 사용자 이름과 암호를 입력합니다.

   참고

   초기 사용자 이름은 *sysadmin*이고 초기 암호는 시스템 일련 번호입니다. 새 시스템 설정에 대한 자세한 내용은 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.

4. **Log In**을 클릭합니다.

   처음으로 로그인한 경우 정보 패널에 Home 보기가 표시됩니다.

   참고

   잘못된 암호를 4번 연속 입력할 경우 지정된 사용자 이름이 시스템에 의해 120초 동안 잠깁니다. 로그인 횟수 및 잠금 기간은 구성 가능하며 시스템에 따라 다를 수 있습니다.

   참고

   처음으로 로그인한 경우 암호를 변경해야 할 수 있습니다. 시스템 관리자가 암호를 변경하도록 사용자 이름을 구성한 경우 암호를 변경해야 DD System Manager에 액세스할 수 있습니다.

5. 로그아웃하려면 DD System Manager 배너에서 로그아웃 버튼을 클릭합니다.

   로그아웃하면 로그아웃이 완료되었다는 메시지와 함께 페이지에 로그가 표시됩니다.

인증서를 사용한 로그인

사용자 이름과 암호를 사용하여 로그인하는 대신 CA(Certificate Authority)에서 발급한 인증서를 사용하여 DD System Manager에 로그인할 수 있습니다.

인증서를 사용하여 로그인하려면 Data Domain 시스템에 인증 권한이 있고 Data Domain 시스템이 CA 인증서를 신뢰해야 합니다. 사용자 이름은 인증서의 일반 이름 필드에 지정되어야 합니다.

절차

1. Data Domain 시스템에 사용자 계정이 있는지 확인합니다.

   로컬 사용자 또는 이름 서비스 사용자(NIS/AD)가 될 수 있습니다. 이름 서비스 사용자의 경우 Data Domain 시스템에 그룹-역할 매핑을 구성해야 합니다.

2. 다음 CLI 명령을 사용하여 인증서를 발급한 CA에서 공개 키를 가져옵니다.
   `adminaccess certificate import ca application login-auth`.

3. 브라우저에서 PKCS12 형식의 인증서를 로드합니다.

   Data Domain 시스템에서 CA 인증서를 신뢰하면 HTTPS 로그인 화면에 **Log in with certificate** 링크가 표시됩니다.

4. **Log in with certificate**를 클릭하고 브라우저에 표시되는 인증서 목록에서 인증서를 선택합니다.

결과

Data Domain 시스템이 신뢰할 수 있는 저장소와 대조하여 사용자 인증서를 검증합니다. 계정에 연결된 인증 권한에 따라 System Manager 세션이 생성됩니다.

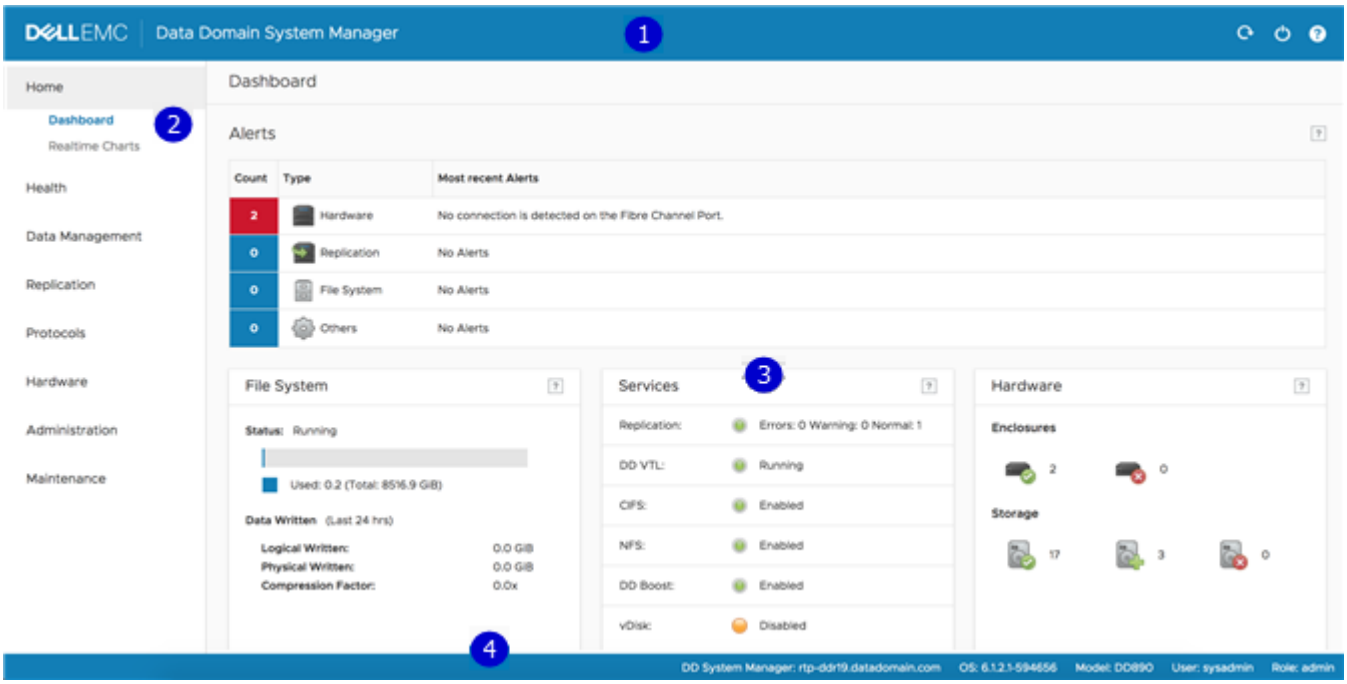
DD System Manager 인터페이스

DD System Manager 인터페이스는 구성 및 표시 옵션을 탐색하고 컨텍스트 기반 도움말을 표시할 수 있는 공통 요소를 대부분의 페이지에 제공합니다.

페이지 요소

기본적인 페이지 요소는 배너, 탐색 패널, 정보 패널 및 바닥글입니다.

그림 3 DD System Manager 페이지 구성 요소



1. 배너
2. 탐색 패널
3. 정보 패널
4. 바닥글

배너

DD System Manager 배너에는 프로그램 이름과 **Refresh**, **Log Out** 및 **Help** 버튼이 표시됩니다.

탐색 패널

탐색 패널에는 관리할 시스템 구성 요소 또는 작업을 식별하는 데 사용할 수 있는 최상위 메뉴 선택 항목이 표시됩니다.

탐색 패널에는 탐색 시스템의 맨 위 수준이 두 개까지 표시됩니다. 최상위 수준의 제목을 클릭하면 두 번째 수준의 제목이 표시됩니다. 추가로 탐색하려면 정보 패널의 탭과 메뉴를 사용합니다.

정보 패널

정보 패널에는 탐색 패널에서 선택한 항목과 관련된 정보 및 컨트롤이 표시됩니다. 정보 패널에서 시스템 상태 정보를 찾고 시스템을 구성할 수 있습니다.

탐색 패널에서 선택한 기능 또는 작업에 따라 탭 모음, 항목 영역, 테이블 보기 컨트롤 및 More Tasks 메뉴가 정보 패널에 표시될 수 있습니다.

탭 모음
탭에서는 탐색 패널에서 선택한 항목의 서로 다른 측면에 액세스할 수 있습니다.

항목 영역
항목 영역에는 탐색 패널 또는 상위 탭에서 선택한 항목의 서로 다른 측면을 나타내는 섹션으로 정보 패널이 분리되어 표시됩니다.

HA(High-Availability) 시스템의 경우 System Manager 대시보드의 HA Readiness 탭에 HA 시스템이 액티브 노드에서 대기 노드로 페일오버할 준비가 되었는지 여부가 나타납니다. **HA Readiness**를 클릭하여 **HEALTH**의 **High Availability** 섹션으로 이동할 수 있습니다.

테이블 보기 옵션 작업
항목 테이블이 있는 보기에는 대부분 테이블의 정보를 필터링, 탐색 및 정렬하기 위한 컨트롤이 포함되어 있습니다.

일반적인 테이블 컨트롤을 사용하는 방법:

- 열 머리글에 있는 다이아몬드 모양 아이콘을 클릭해 열의 항목 정렬 순서를 반대로 바꿉니다.
- 보기 오른쪽 맨 아래에서 **<** 및 **>** 화살표를 클릭해 페이지를 앞뒤로 이동합니다. 페이지의 시작 지점으로 건너뛰려면 **|<**를 클릭합니다. 마지막 지점으로 건너뛰려면 **>|**를 클릭합니다.
- 테이블의 모든 항목을 보려면 스크롤 막대를 사용합니다.
- 해당 항목을 검색하거나 항목 나열의 우선 순위를 지정하려면 **Filter By** 상자에 텍스트를 입력합니다.
- **Update**를 클릭해 목록을 새로 고칩니다.
- 기본 나열 방식으로 돌아가려면 **Reset**을 클릭합니다.

More Tasks 메뉴
일부 페이지에는 보기의 오른쪽 맨 위에 현재 보기와 관련된 명령이 포함된 More Tasks 메뉴가 제공됩니다.

바닥글

DD System Manager 바닥글에는 관리 세션에 대한 중요한 정보가 표시됩니다.

배너에는 다음 정보가 나열됩니다.

- 시스템 호스트 이름

- DD OS 버전
- 선택한 시스템 모델 번호
- 현재 로그인된 사용자의 사용자 이름 및 역할

도움말 버튼

?로 표시되는 도움말 버튼은 배너, 정보 패널에 있는 여러 영역의 제목 및 다수의 대화 상자에 나타납니다. 도움말 버튼을 클릭하면 사용 중인 현재 기능과 관련된 도움말 창이 표시됩니다.

도움말 창의 도움말 위에는 목차 버튼과 탐색 버튼이 있습니다. 가이드 목차와 도움말을 검색하는 데 사용할 수 있는 검색 버튼을 표시하려면 목차 버튼을 클릭하십시오. 도움말 항목을 페이지 순서대로 살펴보려면 방향 화살표 버튼을 사용하십시오.

End User License Agreement

EULA(End User License Agreement)를 보려면 **Maintenance** > **System** > **View EULA**를 선택합니다.

구성 마법사를 사용해 시스템 구성

구성 마법사에는 DD System Manager 구성 마법사와 CLI 구성 마법사가 있습니다. 구성 마법사는 시스템을 빠르게 작동하는 데 필요한 단순화된 시스템 구성을 안내합니다.

마법사로 기본 구성을 완료한 후에는 DD System Manager 및 CLI의 추가 구성 컨트롤을 사용해 시스템을 추가로 구성할 수 있습니다.

참고

다음 절차는 시스템의 초기 구성 이후에 DD System Manager 구성 마법사를 시작하고 실행하는 방법을 설명합니다. 시스템 시작 시 구성 마법사를 실행하는 방법에 대한 지침은 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.

참고

시스템을 HA(High Availability) 시스템으로 구성하려면 CLI 구성 마법사를 사용하여 이 작업을 수행해야 합니다. 자세한 내용은 *Data Domain DD9500/DD9800 하드웨어 개요 및 설치 가이드* 및 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.

절차

1. **Maintenance** > **System** > **Configure System**을 선택합니다.
2. Configuration Wizard 대화 상자 맨 아래에 있는 컨트롤을 사용해 어떤 기능을 구성할지 선택하고 마법사를 진행합니다. 기능에 대한 도움말을 표시하려면 대화 상자 왼쪽 하단 모서리에 있는 도움말 아이콘(물음표)을 클릭합니다.

License 페이지

License 페이지에는 설치된 모든 라이센스가 표시됩니다. **Yes**를 클릭해 라이센스를 추가, 수정 또는 삭제하거나 **No**를 클릭해 라이센스 설치를 건너뛰십시오.

라이센스 구성

Licenses Configuration 섹션을 사용하여 라이센스 파일의 라이센스를 추가, 수정 또는 삭제할 수 있습니다. Data Domain Operating System 6.0 이상은 단일 라이센스 파일

업로드에 여러 기능을 포함시킬 수 있도록 허용하는 ELMS 라이센스 등록을 지원합니다.

라이센스가 구성되어 있지 않은 시스템에서 Configuration Wizard를 사용할 경우 드롭다운에서 라이센스 유형을 선택한 다음 **...** 버튼을 클릭합니다. 라이센스 파일이 있는 디렉토리로 이동하고 시스템에 업로드할 라이센스 파일을 선택합니다.

표 4 License Configuration 페이지 값

항목	설명
Add Licenses	라이센스 파일에서 라이센스를 추가하려면 이 옵션을 선택합니다.
Replace Licenses	라이센스가 이미 구성되어 있는 경우 **Add Licenses** 선택 항목이 **Replace Licenses**로 변경됩니다. 이미 추가한 라이센스를 바꾸려면 이 옵션을 선택합니다.
Delete Licenses	시스템에 이미 구성된 라이센스를 삭제하려면 이 옵션을 선택합니다.

Network

Network 섹션을 사용하여 네트워크 설정을 구성할 수 있습니다. 네트워크 설정을 구성하려면 **Yes**를 클릭하고, 네트워크 구성을 건너뛰려면 **No**를 클릭합니다.

네트워크 General 페이지

General 페이지에서는 시스템이 IP 네트워크에 참여하는 방법을 정의하는 네트워크 설정을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 네트워크 설정을 구성하려면 **Hardware** > **Ethernet**을 선택하십시오.

표 5 General 페이지 설정

항목	설명
Obtain Settings using DHCP	시스템이 DHCP(Dynamic Host Control Protocol) 서버에서 네트워크 설정을 수집하도록 지정하려면 이 옵션을 선택합니다. 네트워크 인터페이스를 구성할 때 인터페이스 중 적어도 하나는 DHCP를 사용하도록 구성해야 합니다.
Manually Configure	이 페이지의 Settings 영역에서 정의된 네트워크 설정을 사용하도록 하려면 이 옵션을 선택합니다.
Host Name	이 시스템의 네트워크 호스트 이름을 지정합니다. 참고 DHCP를 통해 네트워크 설정을 가져오도록 선택한 경우 **Hardware** > **Ethernet** > **Settings**에서 또는 `net set hostname` 명령을 사용하여 수동으로 호스트 이름을 구성할 수 있습니다. IPv6에서 DHCP를 사용할 때에는 수동으로 호스트 이름을 구성해야 합니다.
Domain Name	이 시스템이 속한 네트워크 도메인을 지정합니다.

표 5 General 페이지 설정 (계속)

항목	설명
Default IPv4 Gateway	대상 시스템에 대한 라우트 항목이 없을 경우 시스템이 네트워크 요청을 전달할 게이트웨이의 IPv4 주소를 지정합니다.
Default IPv6 Gateway	대상 시스템에 대한 라우트 항목이 없을 경우 시스템이 네트워크 요청을 전달할 게이트웨이의 IPv6 주소를 지정합니다.

네트워크 Interfaces 페이지

Interfaces 페이지에서는 각 인터페이스가 IP 네트워크에 참여하는 방법을 정의하는 네트워크 설정을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 네트워크 설정을 구성하려면 **Hardware** > **Ethernet** > **Interfaces**를 선택하십시오.

표 6 Interfaces 페이지 설정

항목	설명
Interface	시스템에서 사용할 수 있는 인터페이스를 나열합니다.
Enabled	각 인터페이스가 설정(확인란이 선택됨) 또는 해제(선택되지 않음)되었는지 여부를 보여 줍니다. 인터페이스의 상태(설정 및 해제)를 전환하려면 확인란을 클릭합니다.
DHCP	각 인터페이스의 현재 DHCP(Dynamic Host Control Protocol) 구성을 보여 줍니다. IPv4 DHCP 접속의 경우 **v4**, IPv6 접속의 경우 **v6**, DHCP를 해제하려면 **no**를 선택합니다.
IP Address	이 시스템의 IPv4 또는 IPv6 주소를 지정합니다. IP 주소를 구성하려면 DHCP를 **No**로 설정해야 합니다. 참고 DD140, DD160, DD610, DD620 및 DD630 시스템은 인터페이스 eth0a(기존 포트 이름을 사용하는 시스템은 eth0) 또는 해당 인터페이스에서 생성된 VLAN에서 IPv6를 지원하지 않습니다.
Netmask	이 시스템의 네트워크 마스크를 지정합니다. 네트워크 마스크를 구성하려면 DHCP를 **No**로 설정해야 합니다.
Link	이더넷 링크의 활성 여부를 표시합니다(Yes/No).

네트워크 DNS 페이지

DNS 페이지에서는 시스템이 DNS(Domain Name System)에서 DNS 서버에 대한 IP 주소를 가져오는 방법을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 네트워크 설정을 구성하려면 **Hardware** > **Ethernet** > **Settings**를 선택하십시오.

표 7 DNS 페이지 설정

항목	설명
Obtain DNS using DHCP.	시스템이 DHCP(Dynamic Host Control Protocol) 서버에서 DNS IP 주소를 수집하도록 지정하려면 이 옵션을 선택합니다. 네트워크 인터페이스를 구성할 때 인터페이스 중 적어도 하나는 DHCP를 사용하도록 구성해야 합니다.
Manually configure DNS list.	DNS 서버 IP 주소를 수동으로 입력할 경우 이 옵션을 선택합니다.
추가(+) 버튼	DNS IP Address 목록에 DNS IP 주소를 추가할 수 있는 대화 상자를 표시하려면 이 버튼을 클릭합니다. 먼저 **Manually configure DNS list**를 선택해야만 DNS IP 주소를 추가하거나 삭제할 수 있습니다.
삭제(X) 버튼	DNS IP Address 목록에서 DNS IP 주소를 삭제하려면 이 버튼을 클릭합니다. 이 버튼이 설정되기 전에 삭제할 IP 주소를 선택해야 합니다. 또한 먼저 **Manually configure DNS list**를 선택해야만 DNS IP 주소를 추가하거나 삭제할 수 있습니다.
IP Address 확인란	삭제할 DNS IP 주소의 확인란을 선택합니다. 모든 IP 주소를 삭제하려는 경우 DNS IP Address 확인란을 선택합니다. 먼저 **Manually configure DNS list**를 선택해야만 DNS IP 주소를 추가하거나 삭제할 수 있습니다.

파일 시스템

File System 섹션을 사용하여 Active 및 Cloud Tier 스토리지를 구성할 수 있습니다. 각 계층에는 별도의 마법사 페이지가 있습니다. 또한 이 섹션에서 파일 시스템을 생성할 수도 있습니다. 파일 시스템이 이미 생성되어 있는 경우 구성 페이지에 액세스할 수 없습니다.

파일 시스템이 생성되지 않은 경우 **File System** 섹션을 표시할 때마다 오류 메시지가 표시됩니다. 파일 시스템을 생성하는 절차를 계속합니다.

스토리지 계층 페이지 구성

스토리지 계층 구성 페이지를 사용하여 시스템의 라이센스가 부여된 각 계층(Active Tier, Archive Tier 및 DD Cloud Tier)에 대한 스토리지를 구성할 수 있습니다. 각 계층에는 별도의 마법사 페이지가 있습니다. 파일 시스템이 이미 생성되어 있는 경우 스토리지 계층 구성 페이지에 액세스할 수 없습니다.

Active Tier 구성

Configure Active Tier 섹션을 사용하여 Active Storage Tier 디바이스를 구성할 수 있습니다. Active Tier는 백업 데이터가 상주하는 장소입니다. Active Tier에 스토리지를 추가하려면 하나 이상의 디바이스를 선택하여 계층에 추가하십시오. 설치된 용량 라이센스까지 스토리지 디바이스를 추가할 수 있습니다.

DD3300 시스템에는 Active Tier에 4TB 디바이스가 필요합니다.

표 8 Addable Storage

항목	설명
ID(DD VE의 경우 Device)	디스크 식별자로 다음 중 하나일 수 있습니다.

표 8 Addable Storage (계속)

항목	설명
	• 엔클로저 및 디스크 번호(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식) • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Model	디스크 셸프의 유형입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
License Needed	계층에 스토리지를 추가하는 데 필요한 라이센스가 부여된 용량입니다.
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Type	SCSI입니다. DD VE 인스턴스에만 적용됩니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

표 9 Active Tier 값

항목	설명
ID(DD VE의 경우 Device)	디스크 식별자로 다음 중 하나일 수 있습니다. • 엔클로저 및 디스크 번호입니다(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식). DD VE 인스턴스에는 적용되지 않습니다. • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Model	디스크 셸프의 유형입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
License Used	스토리지에 의해 사용된 라이센스가 부여된 용량입니다.

표 9 Active Tier 값 (계속)

항목	설명
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Configured	새 스토리지 또는 기존 스토리지입니다. DD VE 인스턴스에는 적용되지 않습니다.
Type	SCSI입니다. DD VE 인스턴스에만 적용됩니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

Archive Tier 구성

Configure Archive Tier 섹션을 사용하여 Archive Storage Tier 디바이스를 구성할 수 있습니다. Archive Tier는 DD Extended Retention 기능으로 아카이빙된 데이터가 상주하는 장소입니다. Archive Tier에 스토리지를 추가하려면 하나 이상의 디바이스를 선택하여 계층에 추가하십시오. 설치된 용량 라이센스까지 스토리지 디바이스를 추가할 수 있습니다.

DD3300 시스템이나 DD VE 인스턴스에서는 Archive Tier 스토리지를 사용할 수 없습니다.

표 10 Addable Storage

항목	설명
ID	디스크 식별자로 다음 중 하나일 수 있습니다. • 엔클로저 및 디스크 번호(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식) • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다.
모델	디스크 셸프의 유형입니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
License Needed	계층에 스토리지를 추가하는 데 필요한 라이센스가 부여된 용량입니다.
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

표 11 Archive Tier 값

항목	설명
ID	디스크 식별자로 다음 중 하나일 수 있습니다.

표 11 Archive Tier 값 (계속)

항목	설명
	• 엔클로저 및 디스크 번호입니다(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식). DD VE 인스턴스에는 적용되지 않습니다. • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다.
모델	디스크 셸프의 유형입니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
License Used	스토리지에 의해 사용된 라이센스가 부여된 용량입니다.
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다.
Configured	새 스토리지 또는 기존 스토리지입니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

Cloud Tier 구성

Configure Cloud Tier 섹션을 사용하여 Cloud Storage Tier 디바이스를 구성할 수 있습니다. Cloud Tier에 스토리지를 추가하려면 하나 이상의 디바이스를 선택하여 계층에 추가하십시오. 설치된 용량 라이센스까지 스토리지 디바이스를 추가할 수 있습니다.

DD3300 시스템에는 DD Cloud Tier에 1TB 디바이스가 필요합니다.

표 12 Addable Storage

항목	설명
ID(DD VE의 경우 Device)	디스크 식별자로 다음 중 하나일 수 있습니다. • 엔클로저 및 디스크 번호(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식) • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Model	디스크 셸프의 유형입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]

표 12 Addable Storage (계속)

항목	설명
License Needed	계층에 스토리지를 추가하는 데 필요한 라이센스가 부여된 용량입니다.
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Type	SCSI입니다. DD VE 인스턴스에만 적용됩니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

표 13 Cloud Tier 값

항목	설명
ID(DD VE의 경우 Device)	디스크 식별자로 다음 중 하나일 수 있습니다. • 엔클로저 및 디스크 번호입니다(Enclosure Slot 형식, 또는 DS60 셸프의 경우 Enclosure Pack 형식). DD VE 인스턴스에는 적용되지 않습니다. • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Disks	디스크 팩 또는 LUN을 구성하는 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Model	디스크 셸프의 유형입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Count	디스크 팩 또는 LUN의 디스크 수입니다. DD VE 인스턴스에는 적용되지 않습니다.
Disk Size(DD VE의 경우 Size)	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
License Used	스토리지에 의해 사용된 라이센스가 부여된 용량입니다.
Failed Disks	디스크 팩 또는 LUN에서 장애가 발생한 디스크입니다. DD VE 인스턴스에는 적용되지 않습니다.
Configured	새 스토리지 또는 기존 스토리지입니다. DD VE 인스턴스에는 적용되지 않습니다.
Type	SCSI입니다. DD VE 인스턴스에만 적용됩니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

Create File System 페이지

Create File System 페이지에는 파일 시스템의 각 스토리지 계층에 허용되는 크기가 표시되며, 파일 시스템이 생성된 후 자동으로 활성화되도록 지정하는 기능도 있습니다.

System Settings

System Settings 섹션을 사용하여 시스템 암호 및 이메일 설정을 구성할 수 있습니다. 시스템 설정을 구성하려면 **Yes**를 클릭하고, 시스템 설정 구성을 건너뛰려면 **No**를 클릭합니다.

시스템 설정 Administrator 페이지

Administrator 페이지에서는 관리자 암호와 시스템이 관리자와 통신하는 방법을 구성할 수 있습니다.

표 14 Administrator 페이지 설정

항목	설명
User Name	기본 관리자 이름은 *sysadmin*입니다. Sysadmin 사용자는 이름을 바꾸거나 삭제할 수 없습니다.
Old Password	Sysadmin의 이전 암호를 입력합니다.
New Password	Sysadmin의 새 암호를 입력합니다.
Verify New Password	Sysadmin의 새 암호를 다시 입력합니다.
Admin Email	DD System Manager가 알림 및 자동 지원 이메일 메시지를 보낼 이메일 주소를 지정합니다.
Send Alert Notification Emails to this address	알림 이벤트가 발생하면 관리자 이메일 주소로 알림을 보내도록 DD System Manager를 구성하려면 선택합니다.
Send Daily Alert Summary Emails to this address	하루가 끝날 때 관리자 이메일 주소로 알림 요약을 보내도록 DD System Manager를 구성하려면 선택합니다.
Send Autosupport Emails to this address	문서 시스템 작업과 상태를 문서화하는 일일 보고서, 즉 관리자 사용자 자동 지원 이메일을 보내도록 DD System Manager를 구성하려면 선택합니다.

시스템 설정 Email/Location 페이지

Email/Location 페이지에서는 메일 서버 이름을 구성하고, Data Domain에 어떤 시스템 정보가 전송되는지 제어하고, 위치 이름을 지정해 시스템을 식별할 수 있습니다.

표 15 Email/Location 페이지 설정

항목	설명
Mail Server	시스템에서 보내고 받는 e-메일을 관리하는 메일 서버의 이름을 지정합니다.
자격 증명	메일 서버에 대한 자격 증명을 요구할지 여부를 선택합니다.
사용자 이름	자격 증명이 활성화된 경우 메일 서버 사용자 이름을 지정합니다.
암호	자격 증명이 활성화된 경우 메일 서버 암호를 지정합니다.
Send Alert Notification Emails to Data Domain	DD System Manager를 구성해 Data Domain에 경고 알림 e-메일을 보내도록 하려면 선택합니다.

표 15 Email/Location 페이지 설정 (계속)

항목	설명
Send Vendor Support Notification Emails to Data Domain	DD System Manager를 구성해 Data Domain에 공급업체 지원 알림 e-메일을 보내도록 하려면 선택합니다.
Location	필요에 따라 이 선택적 속성을 사용해 시스템의 위치를 기록합니다. 위치를 지정할 경우 이 정보가 SNMP 시스템 위치로 저장됩니다.

DD Boost 프로토콜

DD Boost 설정 섹션을 사용하여 DD Boost 프로토콜 설정을 구성할 수 있습니다. DD Boost 프로토콜 설정을 구성하려면 **Yes**를 클릭하고, DD Boost 구성을 건너뛰려면 **No**를 클릭합니다.

DD Boost 프로토콜 Storage Unit 페이지

Storage Unit 페이지에서는 DD Boost 스토리지 유닛을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **Protocols** > **DD Boost** > **Storage Units** > **+(더하기 기호)**를 선택해 스토리지 유닛을 추가하거나, **연필 모양**을 선택해 스토리지 유닛을 수정하거나, **X**를 선택해 스토리지 유닛을 삭제하십시오.

표 16 Storage Unit 페이지 설정

항목	설명
Storage Unit	DD Boost 스토리지 유닛의 이름입니다. 필요에 따라 이 이름을 변경할 수 있습니다.
User	기본 DD Boost 사용자의 경우 기존 사용자를 선택하거나 Create a new Local User를 선택하고 사용자 이름, 암호, 관리 역할을 입력합니다. 이 역할은 다음 중 하나에 해당될 수 있습니다. • *Admin 역할*: 전체 Data Domain 시스템을 구성하고 모니터링할 수 있습니다. • *User 역할*: Data Domain 시스템을 모니터링하고 자신의 암호를 변경할 수 있습니다. • *Security 역할*: user 역할 권한 외에도 보안 책임자 구성을 설정하고 다른 보안 책임자 운영자를 관리할 수 있습니다. • *Backup-operator 역할*: user 역할 권한 외에도 스냅샷을 생성하고, 테이프를 가져오거나 내보내고, DD VTL 내에서 테이프를 이동할 수 있습니다. • *None 역할*: DD Boost 인증만을 위한 역할이므로 Data Domain 시스템을 모니터링하거나 구성할 수 없습니다. 또한 None 역할은 SMT tenant-admin 및 tenant-user 역할의 상위 역할입니다. None 역할은 DD Boost 스토리지 소유자의 기본 설정 사용자 유형이기도 합니다. 여기서 새

표 16 Storage Unit 페이지 설정 (계속)

항목	설명
	로컬 사용자를 생성할 경우 해당 사용자는 "none" 역할만 가질 수 있습니다.

DD Boost 프로토콜 Fibre Channel 페이지

Fibre Channel 페이지에서는 Fibre Channel을 통해 DD Boost 액세스 그룹을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **Protocols** > **DD Boost** > **Fibre Channel** > **+(더하기 기호)**를 선택해 액세스 그룹을 추가하거나, **연필 모양**을 선택해 액세스 그룹을 수정하거나, **X**를 선택해 액세스 그룹을 삭제하십시오.

표 17 Fibre Channel 페이지 설정

항목	설명
Configure DD Boost over Fibre Channel	Fibre Channel을 통해 DD Boost를 구성하려면 이 확인란을 선택합니다.
Group Name (1-128 Chars)	액세스 그룹을 생성합니다. 고유한 이름을 입력합니다. 중복 액세스 그룹은 지원되지 않습니다.
Initiators	하나 이상의 이니시에이터를 선택합니다. 필요에 따라 새 이름을 입력해 이니시에이터 이름을 바꿉니다. 이니시에이터는 FC(Fibre Channel) 프로토콜을 사용하여 데이터를 읽고 쓰기 위해 시스템에 접속하는 백업 클라이언트입니다. 특정 이니시에이터는 FC 기반 DD Boost 또는 DD VTL을 지원하지만 둘 모두를 지원하지는 않습니다.
Devices	사용할 수 있는 디바이스가 나열됩니다. 이러한 디바이스는 모든 엔드포인트에서 사용할 수 있습니다. 엔드포인트는 이니시에이터가 연결하는 Data Domain 시스템에 있는 논리 타겟입니다.

CIFS 프로토콜

CIFS Protocol 설정 섹션을 사용하여 CIFS 프로토콜 설정을 구성할 수 있습니다. CIFS 프로토콜 설정을 구성하려면 **Yes**를 클릭하고, CIFS 구성을 건너뛰려면 **No**를 클릭합니다.

Data Domain 시스템에서는 MTree라는 용어를 사용하여 디렉토리를 설명합니다. 디렉토리 경로를 구성할 경우 DD OS에서 데이터가 상주할 MTree를 생성합니다.

CIFS 프로토콜 Authentication 페이지

Authentication 페이지에서 시스템에 대한 Active Directory 및 워크그룹을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **Administration** > **Access** > **Authentication**을 선택합니다.

표 18 Authentication 페이지 설정

항목	설명
Active Directory/Kerberos Authentication	Active Directory Kerberos 인증을 활성화, 비활성화 및 구성하려면 이 패널을 확장합니다.
Workgroup Authentication	워크그룹 인증을 구성하려면 이 패널을 확장합니다.
LDAP 인증	LDAP 인증을 구성하려면 이 패널을 확장합니다.
NIS Authentication	NIS 인증을 구성하려면 이 패널을 확장합니다.

CIFS 프로토콜 Share 페이지

Share 페이지에서는 시스템의 CIFS 프로토콜 공유 이름과 디렉토리 경로를 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **Protocols** > **CIFS** > **Shares** > **Create**를 선택합니다.

표 19 Share 페이지 설정

항목	설명
Share Name	시스템의 공유 이름을 입력합니다.
Directory Path	시스템의 디렉토리 경로를 입력합니다.
추가(+) 버튼	시스템 클라이언트, 사용자 또는 그룹을 입력하려면 +를 클릭합니다.
연필 아이콘	클라이언트, 사용자 또는 그룹을 수정합니다.
삭제(X) 버튼	선택한 클라이언트, 사용자 또는 그룹을 삭제하려면 X를 클릭합니다.

NFS protocol

NFS Protocol 설정 섹션을 사용하여 NFS 프로토콜 설정을 구성할 수 있습니다. NFS 프로토콜 설정을 구성하려면 **Yes**를 클릭하고, NFS 구성을 건너뛰려면 **No**를 클릭합니다.

Data Domain 시스템에서는 MTree라는 용어를 사용하여 디렉토리를 설명합니다. 디렉토리 경로를 구성할 경우 DD OS에서 데이터가 상주할 MTree를 생성합니다.

NFS 프로토콜 Export 페이지

Export 페이지에서는 NFS Protocol 내보내기 디렉토리 경로, 네트워크 클라이언트 및 NFSv4 참조를 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **Protocols** > **NFS** > **Create**를 선택하십시오.

표 20 Export 페이지 설정

항목	설명
Directory Path	내보내기 경로 이름을 입력합니다.

표 20 Export 페이지 설정 (계속)

항목	설명
추가(+) 버튼	시스템 클라이언트 또는 NFSv4 참조를 입력하려면 +를 클릭합니다.
연필 아이콘	클라이언트 또는 NFSv4 참조를 수정합니다.
삭제(X) 버튼	선택한 클라이언트 또는 NFSv4 참조를 삭제하려면 X를 클릭합니다.

DD VTL 프로토콜

DD VTL Protocol 설정 섹션을 사용하여 Data Domain VTL(Virtual Tape Library) 설정을 구성할 수 있습니다. DD VTL 설정을 구성하려면 **Yes**를 클릭하고, DD VTL 구성을 건너뛰려면 **No**를 클릭합니다.

VTL 프로토콜 Library 페이지

Library 페이지에서는 라이브러리에 대한 DD VTL 프로토콜 설정을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **PROTOCOLS** > **VTL** > **Virtual Tape Libraries** > **VTL Service** > **Libraries** > **More Tasks** > **Library** > **Create**를 선택하십시오.

표 21 Library 페이지 설정

항목	설명
Library Name	1~32자의 영숫자로 이름을 입력합니다.
Number of Drives	지원되는 테이프 드라이브의 개수입니다.
Drive Model	드롭다운 목록에서 원하는 모델을 선택합니다. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5(기본값) • HP-LTO-3 • HP-LTO-4
Number of Slots	라이브러리당 슬롯의 개수를 입력합니다. • 라이브러리당 최대 32,000개의 슬롯 • 시스템당 최대 64,000개의 슬롯 • 드라이브 수보다 많거나 같아야 합니다.
Number of CAPs	(선택 사항) CAP(Cartridge Access Port)의 개수를 입력합니다. • 라이브러리당 최대 100개의 CAP • 시스템당 최대 1,000개의 CAP

표 21 Library 페이지 설정 (계속)

항목	설명
Changer Model Name	드롭다운 목록에서 원하는 모델을 선택합니다. • L180(기본값) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	A990000LA 형식으로 첫 번째 테이프에 대해 원하는 바코드를 입력합니다.
Tape Capacity	(선택 사항) 테이프 용량을 입력합니다. 지정되지 않은 경우 용량은 바코드의 마지막 문자에서 파생됩니다.

VTL 프로토콜 Access Group 페이지

Access Group 페이지에서는 액세스 그룹에 대한 DD VTL 프로토콜 설정을 구성할 수 있습니다.

구성 마법사를 사용하지 않고 이 설정을 구성하려면 **PROTOCOLS** > **VTL** > **Access Groups** > **Groups** > **More Tasks** > **Group** > **Create**를 선택하십시오.

표 22 Access Group 페이지 설정

항목	설명
Group Name	1~128자의 고유한 이름을 입력합니다. 중복 액세스 그룹은 지원되지 않습니다.
Initiators	하나 이상의 이니시에이터를 선택합니다. 필요에 따라 새 이름을 입력해 이니시에이터 이름을 바꿉니다. 이니시에이터는 FC(Fibre Channel) 프로토콜을 사용하여 데이터를 읽고 쓰기 위해 시스템에 접속하는 백업 클라이언트입니다. 특정 이니시에이터는 FC 기반 DD Boost 또는 DD VTL을 지원하지만 둘 모두를 지원하지는 않습니다.
Devices	사용할 수 있는 디바이스(드라이브 및 체인저)가 나열됩니다. 이러한 디바이스는 모든 엔드포인트에서 사용할 수 있습니다. 엔드포인트는 이니시에이터가 연결하는 Data Domain 시스템에 있는 논리 타겟입니다.

Data Domain CLI

CLI(Command Line Interface)는 DD System Manager 대신 사용하거나 DD System Manager와 함께 사용할 수 있는 텍스트 기반 인터페이스입니다. 대부분의 관리 작업은 DD System Manager 또는 CLI를 통해 수행할 수 있습니다. 일부 경우 DD System Manager에서 아직 지원되지 않는 구성 옵션 및 보고서를 CLI에서 사용할 수 있습니다.

IP 주소 목록과 같은 목록을 받는 모든 Data Domain 시스템 명령은 쉼표, 공백 또는 둘 다로 구분된 항목을 받습니다.

Tab 키는 다음을 수행하는 데 사용할 수 있습니다.

- 항목이 고유할 경우 명령 항목을 완성합니다. Tab 완료 기능이 모든 키워드에서 지원됩니다. 예를 들어 `syst` Tab `sh`Tab `st` Tab을 입력하면 명령 `system show stats`가 표시됩니다.
- Tab 키를 누르기 전에 문자를 입력하지 않을 경우 다음으로 사용할 수 있는 옵션을 표시합니다.
- Tab 키를 누르기 전에 문자를 입력할 경우 부분적으로 일치하는 토큰을 표시하거나 고유한 항목을 완성합니다.

각 CLI 명령에 대한 정보는 *Data Domain Operating System 명령 참조 가이드*에 제공됩니다. 온라인 도움말을 사용할 수 있으며 여기에서 각 명령의 전체 구문을 볼 수 있습니다.

CLI에 로그인

시스템에 대한 직접 연결 또는 SSH 또는 Telenet을 통한 이더넷 연결을 사용해 CLI에 액세스할 수 있습니다.

시작하기 전에

CLI를 사용하려면 다음 방법 중 하나를 사용해 시스템에 대한 로컬 또는 원격 연결을 설정해야 합니다.

- 시스템의 직렬 콘솔 포트를 통해 연결하는 경우 터미널 콘솔을 포트에 연결하고 통신 설정은 9600보드, 8데이터 비트, 패리티 없음 및 1 정지 비트를 사용합니다.
- 시스템에서 키보드 및 모니터 포트를 제공하는 경우 키보드 및 모니터를 이러한 포트에 연결합니다.
- 이더넷을 통해 연결하는 경우 SSH 또는 Telnet 클라이언트 소프트웨어를 시스템과 통신할 수 있는 이더넷 네트워크에 연결합니다.

절차

1. SSH 또는 Telnet 연결을 사용해 CLI에 액세스하는 경우 SSH 또는 Telnet 클라이언트를 시작하고 시스템의 IP 주소 또는 호스트 이름을 지정합니다.

   연결을 시작하는 방법에 대한 자세한 내용은 클라이언트 소프트웨어의 설명서를 참조하십시오. 사용자 이름을 묻는 메시지가 표시됩니다.
2. 메시지가 표시되면 시스템 사용자 이름을 입력합니다.
3. 메시지가 표시되면 시스템 암호를 입력합니다.

다음 예는 SSH 클라이언트 소프트웨어를 사용해 *mysystem*이라는 이름의 시스템에 로그인하는 SSH 로그인을 보여 줍니다.

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
Password:
```

CLI 온라인 도움말 지침

CLI에는 구문만 제공하는 도움말과 명령 구문이 포함된 명령과 설명을 제공하는 도움말의 두 가지 유형의 도움말이 표시됩니다. 두 유형의 도움말 모두 필요한 정보를 찾는 데 소요되는 시간을 줄여줍니다.

다음 지침은 구문만 제공하는 도움말의 사용 방법을 설명합니다.

- 최상위 CLI 명령을 나열하려면 물음표(?)를 입력하거나 프롬프트에서 `help` 명령을 입력합니다.
- 최상위 명령의 모든 형식을 나열하려면 프롬프트에서 옵션 없이 명령을 입력하거나 *command*?를 입력합니다.
- 특정 키워드를 사용하는 모든 명령을 나열하려면 `help`*keyword* 또는 ?*keyword*를 입력합니다.
  예를 들어 `? password`는 암호 인수를 사용하는 모든 Data Domain 시스템 명령을 표시합니다.

다음 지침은 명령과 설명을 제공하는 도움말의 사용 방법을 설명합니다.

- 최상위 CLI 명령을 나열하려면 물음표(?)를 입력하거나 프롬프트에서 `help` 명령을 입력합니다.
- 소개가 포함된 최상위 명령의 모든 형식을 나열하려면 `help`*command* 또는 ?*command*를 입력합니다.
- 각 도움말 설명의 끝부분은 `END`로 표시됩니다. Enter 키를 눌러 CLI 프롬프트로 돌아갑니다.
- 전체 도움말 설명이 화면에 맞지 않을 경우 화면 맨 아래에 콜론 프롬프트(:)가 나타납니다. 다음 지침은 이 프롬프트가 나타날 경우 할 수 있는 동작을 설명합니다.
  - 도움말 화면을 이동하려면 위/아래 화살표 키를 사용합니다.
  - 현재 도움말 화면을 종료하고 CLI 프롬프트로 돌아가려면 **q**를 누릅니다.
  - 도움말 화면을 탐색하기 위한 도움말을 표시하려면 **h**를 누릅니다.
  - 도움말 화면에서 텍스트를 검색하려면 슬래시 문자(/)를 입력하고 그 뒤에 검색 조건으로 사용할 패턴을 입력한 뒤 Enter 키를 누릅니다. 일치하는 텍스트가 강조 표시됩니다.

3장

Data Domain 시스템 관리

이 장에는 다음과 같은 내용이 포함됩니다.

시스템 관리 개요

DD System Manager에서는 DD System Manager가 설치된 시스템을 관리할 수 있습니다.

- 복제를 지원하기 위해 DD System Manager는 이전 두 버전, 현재 버전 및 사용할 수 있는 경우 다음 두 버전을 실행하는 시스템의 추가를 지원합니다. 릴리즈 6.0의 경우 DD System Manager가 DD OS 버전 5.6부터 5.7과 다음 두 릴리즈까지의 복제를 위한 시스템의 추가를 지원합니다.

참고

과도한 로드를 처리할 때 시스템의 응답이 보통 때보다 느릴 수 있습니다. 이 경우 DD System Manager 또는 CLI에서 실행한 관리 명령이 완료되는 데 시간이 더 오래 걸릴 수 있습니다. 소요 시간이 허용된 제한을 초과하면 작업이 완료되더라도 시간 초과 오류가 반환됩니다.

다음 표에는 DD System Manager에서 지원되는 최대 사용자 세션 수에 대한 권장 사항이 나열되어 있습니다.

표 23 DD System Manager에서 지원되는 최대 사용자 수

시스템 모델	최대 활성 사용자 수	로그인한 최대 사용자 수
4GB 모델[a]	5	10
8GB 모델[b]	10	15
16GB 이상 모델[c]	10	20

a. DD140 및 DD2200(4TB) 포함
b. DD610 및 DD630 포함
c. DD670, DD860, DD890, DD990, DD2200(7.5TB 초과), DD4200, DD4500, DD6300, DD6800, DD7200, DD9300, DD9500 및 DD9800 포함

참고

초기 HA 시스템 설정 작업은 DD System Manager에서 수행할 수 없지만 이미 구성된 HA 시스템의 상태를 DD System Manager에서 확인할 수 있습니다.

HA 시스템 관리 개요

두 노드, 즉 액티브 노드와 대기 노드 간의 HA 관계는 DDSH CLI를 통해 설정됩니다.

초기 설정은 두 노드 중 어디에서나 실행할 수 있지만 한 번에 하나만 설정할 수 있습니다. HA의 사전 조건으로서 시스템 상호 연결 및 동일한 하드웨어가 두 노드에 먼저 설정되어 있어야 합니다.

참고

두 DDR의 하드웨어가 일치해야 하며, 설치 및 시스템 부팅 시에 일치 여부를 확인합니다.

신규 설치 시스템에서 설정하는 경우 라이센스가 설치된 노드에서 `ha create` 명령을 실행해야 합니다. 기존 시스템과 새로운 신규 설치 시스템(업그레이드)에서 설정하는 경우 기존 시스템에서 실행해야 합니다.

HA 시스템 계획된 유지 보수

HA 아키텍처는 롤링 업그레이드를 제공하여 DD OS 업그레이드를 위한 유지 보수 다운타임을 줄입니다.

롤링 업그레이드를 통해 HA 노드는 한 번에 하나씩, 조직적이며 자동으로 업그레이드됩니다. 대기 노드가 먼저 재부팅되고 업그레이드됩니다. 그런 다음 새로 업그레이드된 노드가 HA 페일오버를 통해 액티브 역할을 넘겨받습니다. 페일오버 후, 두 번째 노드가 재부팅되고 업그레이드 후 대기 노드의 역할을 대신합니다.

데이터 변환이 필요한 시스템 업그레이드 작업은 두 시스템이 모두 동일한 수준으로 업그레이드되고 HA 상태가 완전하게 복구될 때까지 시작되지 않습니다.

시스템 재부팅

표준 시간대를 변경하는 등 일부 구성을 변경할 때 시스템 재부팅이 요구되는 경우 시스템을 재부팅합니다.

절차

1. **Maintenance** > **System** > **Reboot System**을 선택합니다.
2. **OK**를 클릭하여 확인합니다.

시스템 전원 켜기 또는 끄기

파일 시스템 및 구성 무결성을 보존하려면 올바른 절차에 따라 시스템 전원을 끄고 켜야 합니다.

섀시 전원 스위치를 사용하여 시스템 전원을 끄지 마십시오. 이렇게 하면 IPMI를 사용하는 원격 전원 제어가 방지됩니다. 대신, `system poweroff` 명령을 사용합니다. `system poweroff` 명령은 시스템을 종료하고 전원을 끕니다.

IMPI Remote System Power Down 기능은 DD OS를 순서에 따라 종료하지 않습니다. `system poweroff` 명령이 성공하지 못한 경우에만 이 기능을 사용하십시오.

HA 시스템의 경우 두 노드 모두에 대한 접속이 필요합니다.

Data Domain 시스템 전원을 끄려면 다음 단계를 수행하십시오.

절차

1. 시스템에서 입출력이 중지되었는지 확인합니다.

   다음 명령을 실행합니다.

   - `cifs show active`
   - `nfs show active`
   - `system show stats view sysstat interval 2`
   - `system show perf`

2. HA 시스템의 경우 HA 구성 상태를 확인합니다.

   `ha status`
   명령을 실행합니다.

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
```

```
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

참고

이 출력 샘플은 정상 시스템의 출력입니다. 장애가 발생한 구성 요소를 교체하기 위해 시스템을 종료하는 중이라면 HA 시스템이 성능 저하 상태가 되고 한 노드나 두 노드 모두 HA 상태가 오프라인으로 표시됩니다.

3. `alerts show current` 명령을 실행합니다. HA 쌍의 경우 먼저 액티브 노드에서 명령을 실행한 다음 대기 노드에서 명령을 실행합니다.
4. HA 시스템에서는 시스템이 두 노드 모두 온라인인 고가용성 상태인 경우 `ha offline` 명령을 실행합니다. HA가 성능 저하 상태이면 이 단계를 건너뜁니다.
5. `system poweroff` 명령을 실행합니다. HA 쌍의 경우 먼저 액티브 노드에서 명령을 실행한 다음 대기 노드에서 명령을 실행합니다.

   ```
   # system poweroff

   Continue? (yes|no|?) [no]: yes
   ```

   이 명령은 DD OS 프로세스의 순차적 종료를 자동으로 수행하며, 관리 사용자만 사용할 수 있습니다.
6. 하나 이상의 컨트롤러에 있는 전원 공급 장치에서 전원 코드를 분리합니다.
7. 하나 이상의 컨트롤러에서 전원 표시등이 꺼져 있는지 확인하여 시스템 전원이 꺼졌는지 확인합니다.

   컨트롤러의 전원이 꺼지면 외부 확장 셸프(ES30, DS60, FS15)을 끄십시오.

시스템 전원 켜기

시스템 다운타임이 완료되면 Data Domain 시스템 전원을 복구합니다.

절차

1. Data Domain 컨트롤러의 전원을 켜기 전에 확장 셸프의 전원을 켭니다. 모든 확장 셸프의 전원이 켜진 후에 3분 정도 기다립니다.

   참고

   컨트롤러는 섀시 및 내장형 스토리지입니다. *Data Domain 시스템*은 컨트롤러 및 선택적 외부 스토리지를 나타냅니다.
2. 컨트롤러의 전원 코드를 꽂고 컨트롤러에 전원 버튼이 있는 경우 컨트롤러의 전원 버튼을 누릅니다(Data Domain 시스템의 *설치 및 설정 가이드*에 나와 있음). HA 시스템의 경우 먼저 액티브 노드의 전원을 켠 다음 대기 노드의 전원을 켭니다.

   참고

   일부 Data Domain 어플라이언스에는 기존의 전원 버튼이 없으며 "항상 켜져" 있도록 설계되어 있습니다. 또한 AC 전원이 공급되는 즉시 켜집니다.
3. HA 시스템의 경우 HA 구성 상태를 확인합니다.

   `ha status`
   명령을 실행합니다.

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
```

```
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   offline
-------------------------- --------- --------- --------
```

4. HA 시스템에서 노드 중 하나가 오프라인으로 표시되는 경우 해당 노드에서 `ha online` 명령을 실행하여 HA 구성을 복구합니다.
5. Data Domain이 완전히 부팅되었는지와 운영 체제가 실행 중인지 확인합니다. 이 작업은 시스템 콘솔 또는 Data Domain 시스템에 대한 SSH 세션에서 수행할 수 있습니다. 시스템에 로그인할 수 있으면 시스템이 가동됩니다.
6. `alerts show current` 명령을 실행합니다. HA 쌍의 경우 먼저 액티브 노드에서 명령을 실행한 다음 대기 노드에서 명령을 실행합니다.

시스템 업그레이드 관리

DD OS 시스템을 업그레이드하려면 타겟 시스템에 새 소프트웨어를 위한 공간이 있는지 확인하고 소프트웨어를 업그레이드할 시스템으로 전송한 후 업그레이드를 시작해야 합니다. HA 시스템의 경우 소프트웨어를 액티브 노드로 전송하고 액티브 노드에서 업그레이드를 시작합니다.

HA 시스템의 경우 부동 IP 주소로 DD System Manager에 액세스하여 소프트웨어 업그레이드를 수행합니다.

⚠ 주의

DD OS 6.0은 Secure Remote Support 버전 3(ESRSv3)을 사용합니다. DD OS 5.X를 실행하는 시스템을 DD OS 6.0으로 업그레이드하면 시스템에서 기존 ConnectEMC 구성이 제거됩니다. 업그레이드가 완료된 후 수동으로 ConnectEMC를 재구성하십시오.

시스템에 MD5 서명 인증서가 사용되는 경우 업그레이드 프로세스 도중 더 강력한 해시 알고리즘으로 인증서를 재생성하십시오.

운영 중단을 최소화하는 업그레이드

MDU(Minimal Disruptive Upgrade) 기능을 사용하면 시스템을 재부팅하지 않고도 특정 소프트웨어 구성 요소를 업그레이드하거나 버그 수정 사항을 적용할 수 있습니다. 업그레이드되는 구성 요소에 의존하는 서비스만 중단되므로 MDU 기능은 특정 소프트웨어 업그레이드 중에 심각한 다운타임을 방지할 수 있습니다.

모든 소프트웨어 구성 요소가 운영 중단을 최소화할 수 있는 업그레이드로 제공되는 것은 아닙니다. 이러한 구성 요소는 정기적인 DD OS 시스템 소프트웨어 업그레이드의 일부로 업그레이드해야 합니다. DD OS 소프트웨어 업그레이드는 DD OS의 모든 구성 요소에 대해 업그레이드 작업을 수행하는 대규모 RPM(업그레이드 번들)을 사용합니다. MDU는 특정 소프트웨어 구성 요소를 개별적으로 업그레이드하는 더 작은 구성 요소 번들을 사용합니다.

RPM 서명 확인

RPM 서명 확인은 업그레이드를 위해 다운로드한 Data Domain RPM의 유효성을 검사합니다. RPM이 변조되지 않은 경우 디지털 서명이 유효하며 평상시와 마찬가지로 RPM을 사용할 수 있습니다. RPM이 변조되면 손상으로 인해 디지털 서명이 무효화되고 RPM이 DD OS에서 거부됩니다. 해당 오류 메시지가 표시됩니다.

참고

5.6.0.x에서 6.0으로 업그레이드하는 경우 먼저 5.6.0.x 시스템을 5.6.1.x(또는 그 이상)로 업그레이드한 후 6.0으로 업그레이드하십시오.

지원 소프트웨어

DD OS 6.1에는 지원 소프트웨어라는 유형의 소프트웨어 패키지가 도입되었습니다. 지원 소프트웨어는 특정 문제를 해결하기 위해 Data Domain 지원 엔지니어링 팀에서 제공합니다. 기본적으로 Data Domain 시스템에는 지원 소프트웨어를 설치할 수 없습니다. 지원 소프트웨어에 대한 자세한 내용은 지원 팀에 문의하십시오.

업그레이드 전 체크리스트 및 개요

DD OS 업그레이드를 수행하려면, 계속하기 전에 이러한 점검 사항의 항목을 검토해야 합니다. 이렇게 하면 업그레이드 프로세스를 간소화하고 잠재적인 어려움을 피할 수 있습니다.

업그레이드 전 수동 작업

⚠ 주의

이 섹션의 작업을 수행하지 못하면 업그레이드가 실패할 수 있습니다.

업그레이드하기 전에 계획해야 하는 작업입니다. 이러한 작업은 프로세스에 의해 자동으로 수행되지 않습니다.

1. Data Domain 시스템을 재부팅합니다. HA 시스템의 경우 이 섹션의 나머지 검사를 수행한 후에 HA 시스템의 업그레이드 고려 사항(57페이지)에 설명된 재부팅 지침을 따릅니다.
2. 현재 알림을 확인합니다. 여기에 업그레이드 전에 해결해야 하는 이러한 디스크 또는 기타 하드웨어 오류가 표시될 수 있습니다.

   ```
   # alert show current
   ```

3. `config.net.*`, `crontab`에 대한 레지스트리 설정과 네트워킹 관련 레지스트리 설정이 올바른지 확인합니다.

   예를 들어, `reg show config.net` 작업을 사용하고, `noauto.enabled`, `noauto.speed` 및 `noauto.full_duplex`가 제대로 설정되어 있는지 확인합니다. 이렇게 하면 네트워크에서 속도를 협상할 수 있습니다. 또한 이로 인해 IP 주소와 넷마스크 뿐만 아니라 게이트웨이를 빠르게 설정할 수 있으므로 `.use_dhcp=true` 여부를 확인해야 합니다.

   이러한 요소가 잘못 구성되면 재부팅할 경우 네트워크를 사용할 수 없게 될 수 있으므로 이 검사는 중요합니다.

4. 모든 네트워크 인터페이스가 가동 중인지와 적절한 IP 주소가 있는지 확인하고 Data Domain 시스템을 Data Domain System Manager 또는 사용되는 다른 클라이언트를 통해 액세스할 수 있는지를 확인합니다.

   ```
   # net show
   ```

5. 디스크 상태를 확인하고 Data Domain 시스템에 예비 부품이 부족하거나 누락, 실패 또는 재구성 상태를 나타내는 디스크가 있는 경우 업그레이드를 수행하지 않도록 합니다.

   ```
   # disk show state
   ```

   ```
   # disk show reliability-data
   ```

6. 디스크 안정성을 확인하고 재할당된 섹터가 50개 이상 있는 디스크를 교체합니다.

   ```
   # disk show reliability-data
   ```

7. 다음과 같이 엔클로저 상태를 확인합니다.

 # enclosure show all

모든 디바이스에 대해 “OK”를 표시해야 합니다.

8. 엔클로저 토폴로지가 올바른지 여부를 확인합니다.

   # enclosure show topology

   또한 오류에서 **enc.ctrl.port** 필드 옆에 별표(*)가 표시되는지 여부를 확인합니다. 또한 **Error Message** 필드에 "A possible problem was detected for this shelf controller or the cable connected to it."과 같은 오류가 있는지 확인합니다.

9. 디바이스 포트 매핑이 올바른지 확인합니다.

   # system show hardware

10. 연결된 포트의 링크 속도를 확인합니다.

    # system show ports

11. 파일 시스템의 상태를 확인하여 파일 시스템이 활성화되어 있고 정상적으로 실행되고 있는지 확인합니다.

    # filesys status

12. 파일 시스템 정리가 실행 중인지 확인하고, 실행되고 있는 경우 중지하십시오.

    # filesys clean status

    # filesys clean stop

13. 복제가 활성화된 경우 해당 상태를 확인합니다.

    # replication status

14. 시스템이 클러스터 구성에 있는 경우 클러스터가 실행 중인지 여부를 확인합니다.

    # cluster show config

15. 시스템에서 DD Cloud Tier가 활성화된 경우 데이터 이동이 없는지 확인합니다.

    # data-movement status

    # data-movement stop all

16. 클라우드 정리가 실행 중인지 확인하고, 실행되고 있는 경우 중지하십시오.

    # cloud clean status

    # cloud clean stop

17. 백업 및 복원 작업이 진행 중인지 확인하고, 진행 중이면 중지합니다.

    # system show stats

18. kern.info 로그를 확인하고 하드웨어에 오류가 자주 발생하는지 확인한 후 업그레이드를 수행하기 전에 Data Domain 지원 서비스에 문의하여 시스템을 검사하십시오.

    # log view debug/platform/kern.info

19. DD OS 업그레이드를 수행하기 직전에 자동 지원 보고서를 실행하여 나머지 문제를 해결해야 하는지 확인합니다.

    # autosupport send <your_email_address>

HA 시스템의 업그레이드 고려 사항

HA 시스템에는 업그레이드 작업을 시작하기 전에 몇 가지 고유한 단계가 필요하며 업그레이드가 완료된 후 고유한 사후 점검이 필요합니다.

⚠ 주의

HA 시스템을 재부팅하기 전에 업그레이드 전 수동 작업(56페이지)에 설명된 수동 검사를 수행하십시오.

HA 시스템을 업그레이드할 때 RPM 업그레이드 패키지를 활성 노드에 업로드합니다.

1. HA 시스템은 DD OS 업그레이드를 수행하기 전에 두 노드가 모두 온라인 상태인 고가용성 상태여야 합니다. `ha status` 명령을 실행하여 HA 시스템 상태를 확인합니다.

```
# ha 상태
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com         0       active    online
apollo-ha3a-p1.emc.com         1       standby   online
--------------------------- --------- --------- --------
```

2. 대기 노드를 재부팅합니다(노드 1).
3. `ha status` 명령을 실행하여 대기 노드가 재부팅된 후 HA 시스템 상태가 `highly available`로 표시되는지 확인합니다.
4. `ha failover` 명령을 실행하여 활성 노드에서 대기 노드로의 페일오버를 시작합니다.
5. `ha status` 명령을 실행하여 노드 1이 활성 노드이고 노드 0이 대기 노드인지 확인합니다.

```
# ha 상태
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com         0       standby   online
apollo-ha3a-p1.emc.com         1       active    online
--------------------------- --------- --------- --------
```

6. 대기 노드(노드 0)를 재부팅합니다.
7. `ha status` 명령을 실행하여 대기 노드가 재부팅된 후 HA 시스템 상태가 `highly available`로 표시되는지 확인합니다.
8. `ha failover` 명령을 실행하여 활성 노드에서 대기 노드로의 페일오버를 시작합니다.
9. `ha status` 명령을 실행하여 노드 0이 활성 노드이고 노드 1이 대기 노드인지 확인합니다.

```
# ha 상태
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com         0       active    online
apollo-ha3a-p1.emc.com         1       standby   online
--------------------------- --------- --------- --------
```

활성 노드에서 업그레이드를 시작합니다. DD OS는 자동으로 HA 시스템을 인식하고 두 노드 모두에서 업그레이드 절차를 수행합니다. HA 업그레이드는 다음 순서로 실행됩니다.

1. 대기 노드가 먼저 업그레이드된 후 재부팅됩니다.
2. 재부팅이 완료되면 HA 시스템이 페일오버를 시작하고 대기 노드가 활성 노드로서 작업을 인계 받습니다.

3. 원래 활성 노드는 업그레이드된 후 재부팅되고 대기 노드로 유지됩니다.

두 노드를 모두 업그레이드한 후에 시스템은 노드를 원래 구성으로 되돌리기 위해 다른 페일오버를 수행하지 않습니다.

업그레이드 절차가 완료된 후 `ha status` 명령을 다시 실행하여 시스템이 고가용성 상태이고 두 노드가 모두 온라인 상태인지 확인합니다.

필요에 따라 `ha failover` 명령을 실행하여 노드를 업그레이드 이전 역할로 되돌립니다.

업그레이드 전에 수행되는 자동 작업

DD OS 업그레이드의 이러한 측면을 이해하면 프로세스를 보다 원활하게 진행할 수 있습니다.

업그레이드하기 전에 DataDomain 시스템의 DD OS 버전은 다음 작업을 수행합니다.

1. 복제 초기화가 진행 중인지 확인합니다. 초기화가 진행되는 동안에는 업그레이드가 수행되지 않습니다.
2. .rpm 파일에 포함된 모든 다이제스트 및 서명을 검사하여 패키지의 무결성과 출처를 확인합니다. 서명이 유효하지 않으면 업그레이드가 진행되지 않습니다.
3. 이전 버전의 DD OS에서 새 버전으로 업그레이드하도록 허용되는지 여부를 확인합니다. DD OS 5.7 x 또는 6.0을 실행하는 Data Domain 시스템은 6.1로 직접 업그레이드할 수 있습니다. 이 제한은 RPM 서명으로 인한 것입니다. 이러한 상황에서는 일반적으로 업그레이드가 허용되지 않습니다.
   a. 업그레이드가 6.0.0.1과 6.0.0.4 사이와 같이 동일한 버전에서 수행됩니다. (경우에 따라 이러한 설정을 재정의할 수 있습니다. 자세한 내용은 Data Domain 지원 담당자에게 문의하십시오.)
   b. 업그레이드가 이전 버전으로 수행됩니다(예: 6.0에서 5.7).
   c. 업그레이드가 두 개 기능 제품군 간격을 초과합니다(예: 5.5에서 6.0으로).
4. NFS 마운트 지점을 알 수 없는지 여부를 확인합니다. NFS 마운트 지점을 알 수 없는 경우 업그레이드가 진행되지 않습니다.
5. 이전 업그레이드가 있는 경우 성공적으로 완료되었는지 확인합니다. 이전 업그레이드가 실패했거나 완료되지 않은 경우 현재 업그레이드가 진행되지 않습니다.

업그레이드 전에 업그레이드 스크립트(.rpm 파일)에서 수행하는 자동 작업

이러한 테스트는 Data Domain 시스템에서 실제 업그레이드 프로세스 보다 먼저 수행됩니다.

1. 두 가지 다른 종류의 NVRAM 카드가 있는지 확인합니다.
2. 공간 활용도를 위해 `/ddr` 파티션 및 `/`(루트) 파티션 크기를 확인합니다.
3. OST 버전을 확인합니다.
4. RAID 메타 그룹이 구성되었는지 확인합니다. 구성되지 않은 경우 업그레이드 프로세스가 시작되지 않습니다.
5. 파일 시스템에 사용할 수 있는 공간을 확인합니다.
6. 업그레이드에 사용할 수 있는 공간이 충분한지 확인합니다.
7. VTL이 있는 경우 VTL 버전을 확인합니다.
8. 파일 시스템이 활성화되었는지 확인하고 활성화되지 않은 경우 파일 시스템을 활성화합니다.
9. VTL이 활성화되었는지 확인합니다.

10. VTL 풀을 MTrees로 변환할 수 있는지 확인합니다.
11. 충분한 VTL 공간을 사용할 수 있는지 확인합니다.
12. MTrees 및 VTL 풀의 수가 100을 초과하지 않는지 확인합니다. (이 확인은 DD OS 버전 5.0 이후부터 적용됩니다.)
13. 모든 dg0 디스크가 헤드 유닛에 있는지 확인합니다. 없는 경우 업그레이드 프로세스가 시작되지 않으며 해당 문제를 해결해야 합니다.
14. ConnectEMC가 구성되었는지 확인합니다. 이 경우 업그레이드 이후에 ConnectEMC를 다시 구성하도록 알려주는 경고 메시지가 고객에게 표시됩니다.

이러한 검사 외에도 시스템은 파일 시스템이 문제 없이 정상적으로 종료될 수 있는지 확인합니다. 파일 시스템을 정상적으로 종료할 수 없는 경우에는 업그레이드 프로세스가 중지됩니다.

업그레이드 프로세스를 방해하는 조건

다음 몇 가지 조건으로 인해 업그레이드 프로세스가 중지될 수 있습니다.

- Data Domain 시스템이 작동 중이지 않습니다. 예:
  - 스토리지에 기능적 결함이 있습니다(예: 엔클로저 누락).
  - 파일 시스템이 비정상적으로 종료되어 코어 덤프가 생성되었습니다.
  - 이전 업그레이드가 제대로 완료되지 않았습니다.
- 공간 사용에 문제가 있습니다. 예:
  - / (루트) 또는 `/ddr` 파티션이 로그 파일, 코어 덤프 등으로 가득 찼습니다.
  - 해당 데이터 업그레이드를 수행하는 데 사용할 수 있는 스토리지 공간이 부족합니다.
- Data Domain 시스템이 올바르게 구성되지 않았습니다. 예를 들어, NFS 마운트 지점이 루트 아래 수동으로 생성되었습니다.
- 스토리지 유닛 이름이 MTree 이름으로 변환되지 않습니다. MTree 이름으로 변환하려면, 스토리지 이름에 대문자와 소문자(a-z, A-Z), 숫자(0-9) 및 밑줄(_)만 포함되어야 하며 50자 이하여야 합니다.

이러한 조건을 확인하는 목적은 문제가 있는 업그레이드 또는 파일 시스템 이상 징후가 발생하거나 전파되지 않도록 예방하기 위해서입니다. 이 조건은 복제에서 소스 및 대상 파트너 시스템과 관련된 업그레이드에도 적용됩니다. 복제 소스로 제공되는 Data Domain 시스템에서 업그레이드에 실패하거나 파일 시스템 이상 징후가 발생하면 복제 대상으로 제공되는 Data Domain 시스템의 파일 시스템은 손상되지 않습니다.

시스템에서 업그레이드 패키지 보기

DD System Manager는 시스템에서 최대 5개의 업그레이드 패키지를 보고 관리할 수 있습니다. 시스템을 업그레이드하기 전에 먼저 온라인 지원 사이트에서 로컬 컴퓨터로 업그레이드 패키지를 다운로드한 후 타겟 시스템에 업로드해야 합니다.

절차

1. **Maintenance** > **System**을 선택합니다.
2. 선택적으로 업그레이드 패키지를 선택하고 **View Checksum**을 클릭하여 업그레이드 패키지의 MD5 및 SHA256 체크섬을 표시할 수 있습니다.

결과

시스템에 저장된 각 패키지에 대한 파일 이름, 파일 크기 및 마지막 수정 날짜가 Upgrade Packages Available on Data Domain System이라는 제목의 목록에 나타납니다.

업그레이드 패키지 획득 및 확인

DD System Manager를 사용해 Data Domain 지원 웹 사이트에서 업그레이드 패키지 파일을 찾고 해당 파일의 복제본을 시스템에 업로드할 수 있습니다.

참고

FTP 또는 NFS를 사용해 시스템에 업그레이드 패키지를 복제할 수 있습니다. DD System Manager는 5개의 시스템 업그레이드 패키지로 제한되지만 `/ddvar/releases` 디렉토리에서 직접 파일을 관리할 때에는 공간 제한 외 다른 제한 사항은 없습니다. FTP는 기본적으로 비활성화되어 있습니다. NFS를 사용하려면 `/ddvar`을 내보내 외부 호스트에서 마운트해야 합니다.

절차

1. **Maintenance** > **System**을 선택합니다.
2. 업그레이드 패키지를 가져오려면 **EMC 온라인 지원** 링크를 클릭하고 Downloads를 클릭한 후 검색 기능을 사용해 지원 담당자가 권장하는 패키지를 찾습니다. 로컬 컴퓨터에 업그레이드 패키지를 저장합니다.
3. Upgrade Packages Available on Data Domain System 목록에 4개 미만의 패키지만 나열되어 있는지 확인합니다.

   DD System Manager는 최대 5개의 업그레이드 패키지를 관리할 수 있습니다. 목록에 5개의 패키지가 표시되면 새 패키지를 업로드하기 전에 최소 하나의 패키지를 제거합니다.
4. **Upload Upgrade Package**를 클릭해 시스템에 업그레이드 패키지의 전송을 시작합니다.
5. Upload Upgrade Package 대화 상자에서 **Browse**를 클릭해 Choose File to Upload 대화 상자를 엽니다. 다운로드한 파일이 있는 폴더로 이동하고 파일을 선택한 다음 **Open**을 클릭합니다.
6. **OK**를 클릭합니다.

   업로드 진행 상태를 보여 주는 대화 상자가 나타납니다. 업로드가 성공적으로 완료되면 다운로드 파일(.rpm 확장명)이 Upgrade Packages Available on Data Domain System이라는 제목의 목록에 나타납니다.
7. 업그레이드 패키지 무결성을 확인하려면 **View Checksum**을 클릭하고 계산된 체크섬이 대화 상자에 표시되면 온라인 지원 사이트의 신뢰 체크섬과 비교합니다.
8. 수동으로 업그레이드 사전 점검을 시작하려면 업그레이드 패키지를 선택하고 **Upgrade Precheck**를 클릭합니다.

Data Domain 시스템 업그레이드

시스템에 업그레이드 패키지 파일이 있는 경우 DD System Manager에서 해당 업그레이드 패키지를 사용한 업그레이드를 수행할 수 있습니다.

시작하기 전에

전체 업그레이드 지침 및 업그레이드에 영향을 미칠 수 있는 모든 문제에 대한 내용은 DD OS 릴리스 노트를 읽어 보십시오.

다음 절차는 DD System Manager를 사용하여 업그레이드를 시작하는 방법을 설명합니다. DD System Manager를 사용하여 시스템을 업그레이드하기 전에 업그레이드를 수행할 시스템의 모든 Data Domain CLI 세션에서 로그아웃합니다.

참고

업그레이드 패키지 파일은 .rpm 파일 확장명을 사용합니다. 이 항목에서는 DD OS만 업데이트한다고 가정합니다. 인터페이스 카드를 추가, 스왑 또는 이동하는 등 하드웨어를 변경할 경우 하드웨어 변경 사항과 일치하도록 DD OS 구성을 업데이트해야 합니다.

절차

1. 업그레이드를 수행할 시스템의 DD System Manager에 로그인합니다.

   참고

   대부분의 릴리스에는 최대 2개의 주요 릴리스 버전부터 업그레이드가 수행됩니다. 릴리스 6.0의 경우 릴리스 5.6 및 5.7에서 업그레이드할 수 있습니다.

   참고

   릴리스 노트에 권장된 대로 업그레이드 전에 Data Domain 시스템을 재부팅하여 하드웨어가 CLEAN 상태에 있는지 확인합니다. 재부팅하는 동안 문제가 발생하면 문제를 해결한 다음 업그레이드를 시작하십시오. MDU 업그레이드에서는 재부팅할 필요가 없을 수 있습니다.

2. **Data Management** > **File System**을 선택하고 파일 시스템이 활성화되고 실행 중인지 확인합니다.
3. **Maintenance** > **System**을 선택합니다.
4. Upgrade Packages Available on Data Domain System 목록에서 업그레이드에 사용할 패키지를 선택합니다.

   참고

   최신 버전의 DD OS에 대한 업그레이드 패키지를 선택해야 합니다. DD OS는 이전 버전으로의 다운그레이드를 지원하지 않습니다.

5. **Perform System Upgrade**를 클릭합니다.

   System Upgrade 대화 상자가 나타나고 업그레이드 정보와 현재 업그레이드할 시스템에 로그인되어 있는 사용자 목록이 표시됩니다.

6. 업그레이드 패키지의 버전(업그레이드 이미지)을 확인하고 **OK**를 클릭해 업그레이드를 계속합니다.

   System Upgrade 대화 상자에 업그레이드 상태와 남은 시간이 표시됩니다.

   시스템을 업그레이드할 때 DD System Manager를 사용해 해당 시스템을 관리하려면 업그레이드가 완료될 때까지 기다려야 합니다. 시스템이 재시작되어도 재시작된 후에도 업그레이드가 계속될 수 있으며 DD System Manager에 로그인하면 업그레이드 상태가 표시됩니다. 가능하면 업그레이드가 완료되거나 시스템 전원이 꺼질 때까지 System Upgrade Progress 대화 상자를 열어 두십시오. DD OS 릴리스 5.5 이상을 최신 버전으로 업그레이드할 때 시스템 업그레이드를 위해 전원을 끄지 않아도 되는 경우 업그레이드가 완료되었을 때 Login 링크가 나타납니다.

참고

CLI를 사용해 업그레이드의 상태를 보려면 `system upgrade status` 명령을 입력합니다. 업그레이드에 대한 로그 메시지는 `/ddvar/log/debug/platform/upgrade-error.log` 및 `/ddvar/log/debug/platform/upgrade-info.log`에 저장됩니다.

7. 시스템의 전원이 꺼지면 시스템에서 AC 전원을 제거하고 이전 구성을 지워야 합니다. 모든 전원 케이블을 30초간 뽑았다가 다시 꽂습니다. 시스템 전원이 켜지고 재부팅됩니다.
8. 시스템의 전원이 자동으로 켜지지 않는 경우 전면 패널에 전원 버튼이 있으면 버튼을 누릅니다.

사후 요구 사항

업그레이드를 완료한 후 다음 요구 사항이 적용될 수 있습니다.

- 자체 서명된 SHA-256 인증서를 사용하는 환경에서는 업그레이드 프로세스가 완료된 후 인증서를 수동으로 다시 생성해야 하며 Data Domain 시스템에 연결하는 외부 시스템과의 신뢰 관계를 다시 설정해야 합니다.
  1. **`adminaccess certificate generate self-signed-cert regenerate-ca`** 명령을 실행하여 차체 서명된 CA 및 호스트 인증서를 재생성합니다. 인증서를 재생성하면 외부 시스템과의 기존 신뢰 관계가 깨집니다.
  2. **`adminaccess trust add host`** ***`hostname`*** **`type mutual`** 명령을 실행하여 Data Domain 시스템과 외부 시스템 사이에 상호 신뢰 관계를 다시 설정합니다.
- 시스템에 WWPN 또는 WWNN 정보가 누락된 기존 또는 구성된 FC 포트가 표시되거나 FC HBA(호스트 버스 어댑터) 드라이버가 설치되어 있지 않다고 보고되면 `scsitarget endpoint enable all` 명령을 실행합니다.

복제 노드

컬렉션 복제를 사용하면, 업그레이드를 시작하기 전에 복제가 완료되지 않은 경우 대상 Data Domain 시스템에 파일이 표시되지 않습니다. 업그레이드를 수행한 후에 파일이 대상 시스템에 표시되게 하려면 복제가 완료될 때까지 기다려야 합니다.

ConnectEMC 참고

이 릴리스에서 ConnectEMC는 Secure Remote Services VE(Secure Remote Service Virtual Edition) 게이트웨이를 지원하도록 변경되었습니다. 이러한 변경 사항을 사용하려면 업그레이드 후에 Data Domain 시스템을 ConnectEMC로 재구성해야 합니다.

참고

ConnectEMC는 Service Remote Services VE(V3)에서만 작동하며, 이전 버전의 Service Remote Services를 사용하거나 자체적으로 이메일을 보낼 수 없습니다. ConnectEMC와 이전 버전의 DD OS(예: 5.7 또는 5.6)를 함께 사용한 경우 Service Remote Services VE 서버 구성이 기술 업그레이드로 인해 업그레이드 프로세스 중에 제거되므로 다시 입력해야 합니다.

참고

이전 Service Remote Services 게이트웨이를 사용하는 경우 보안 통신을 허용하도록 Service Remote Services VE 게이트웨이를 구현해야 합니다.

업그레이드 중에 ConnectEMC가 구성된 것으로 확인되면 기존 구성이 제거됩니다. 또한 이벤트 메시지를 회사로 보내도록 지원 알림 방법이 ConnectEMC로 구성되면 이메

일로 전환됩니다. 업그레이드 후에는 새로운 ConnectEMC 명령을 사용하여 ConnectEMC를 다시 구성할 수 있습니다. `support connectemc device register`.

ConnectEMC를 구성한 후에는 `support notification method set connectemc`를 사용하여 ConnectEMC를 활성화합니다.

업그레이드 패키지 제거

DD System Manager를 사용해 최대 5개의 업그레이드 패키지를 시스템에 업로드할 수 있습니다. 업그레이드하는 시스템에 업그레이드 패키지가 5개 포함되어 있으면 시스템을 업그레이드하기 전에 패키지 중 적어도 하나를 제거해야 합니다.

절차

1. **Maintenance** > **System**을 선택합니다.
2. Upgrade Packages Available on this Data Domain System이라는 제목의 목록에서 제거할 패키지를 선택합니다. 한 번에 하나의 패키지를 제거할 수 있습니다.
3. **Remove Upgrade Package**를 클릭합니다.

e-라이센스 관리

Data Domain 시스템에서 e-라이센스를 추가하거나 삭제합니다. 제품 기능, 소프트웨어 업데이트, 소프트웨어 호환성 가이드에 대한 최신 정보와 제품, 라이센스 등록 및 서비스에 대한 정보는 해당 *Data Domain Operating System Release Notes*를 참조하십시오.

HA 시스템 라이센스 관리

HA는 라이센스를 통해 제공되는 기능이며, DD 시스템에 다른 라이센스를 추가할 때와 같은 단계에 따라 시스템 라이센스 키가 등록됩니다.

시스템은 노드 중 하나가 "대기" 노드로 지정되는 Active-Standby 방식으로 구성됩니다. 노드마다 개별 라이센스가 필요한 것이 아니라 한 세트의 라이센스만 있으면 됩니다. 페일오버 시에는 노드 중 하나에서 다른 노드로 라이센스가 페일오버됩니다.

시스템 스토리지 관리

시스템 스토리지 관리 기능을 사용하면 스토리지 공간의 상태 및 구성을 보고 디스크 상태 표시등을 깜박여 디스크 식별을 용이하게 하며 스토리지 구성을 변경할 수 있습니다.

참고

2노드 Active-Standby HA 시스템에 연결되거나 사용되는 모든 스토리지는 단일 시스템이라고 할 수 있습니다.

CLI를 사용하여 사용할 수 있는 스토리지 공간 계산

다음 값은 RAID 오버헤드를 고려한 후 Data Domain에서 사용 가능한 스토리지를 계산하는 데 필요합니다.

- *N* = 디스크 그룹(dg)에서 사용되는 디스크의 수입니다.
- *C* = 포맷 후 각 디스크의 용량입니다.
- *R* = 2(RAID 6 패리티에 사용되는 디스크의 수)

캐시 계층 디스크는 RAID로 보호되지 않으므로 이 계산이 캐시 계층 스토리지에는 작동하지 않습니다.

`storage show all` 명령을 실행하여 *N* 및 *C* 값을 가져옵니다.

그림 4 `storage show all` 명령 예

```
sysadmin@ddbeta90# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg2       2.1-2.14   14      2.7 TiB
(spare)   2.15       1       2.7 TiB
-------   --------   -----   --------   -----------

Current active tier size: 32.7 TiB
Active tier maximum capacity: 131.0 TiB
```

이 예제에서 dg2에는 14개의 디스크가 사용되고 있고 각 디스크의 용량은 2.7TiB이므로 *N*=14 및 *C*= 2.7TiB가 됩니다.

사용 가능한 용량을 얻으려면 수식 (*N*-*R*) x *C*를 사용합니다. 이 예제에서 이 수식은 (14-2) x 2.7TiB.입니다.

12 x 2.7TiB = 32.4TiB 또는 35.6TB.

참고

용량 값은 표시될 때 반올림되므로 계산된 값이 `storage show all` 명령의 출력과 정확히 일치하지 않을 수도 있습니다. `disk show hardware` 명령은 추가 소수점 자릿수를 사용하여 디스크 용량을 표시합니다.

시스템 스토리지 정보 보기

스토리지 상태 영역에는 Operational 또는 Non-Operational과 같은 스토리지의 현재 상태와 스토리지 마이그레이션 상태가 표시됩니다. Status 영역 아래에는 스토리지 인벤토리가 표시되는 방법을 구성하는 탭이 있습니다.

절차

1. 스토리지 상태를 표시하려면 **Hardware** > **Storage**를 선택합니다.
2. 스토리지 상태 다음에 알림 링크가 표시되면 링크를 클릭하여 스토리지 알림을 봅니다.
3. Storage Migration Status가 Not licensed인 경우 **Add License**를 클릭하여 이 기능에 대한 라이센스를 추가할 수 있습니다.

Overview 탭

Overview 탭에는 Data Domain 시스템에 있는 모든 디스크에 대한 정보가 유형별로 정리되어 표시됩니다. 표시되는 범주는 사용 중인 스토리지 구성 유형에 따라 다릅니다.

Overview 탭에는 검색된 스토리지가 하나 이상의 다음 섹션에 나열됩니다.

- Active Tier
  Active Tier 섹션에는 파일 시스템에서 현재 사용할 수 있는 것으로 표시된 디스크가 나열됩니다. 디스크는 Disks in Use 및 Disks Not in Use의 두 가지 표로 나열됩니다.
- Retention Tier
  선택적 Data Domain Extended Retention(이전 명칭 DD Archiver) 라이선스가 설치된 경우 이 섹션에는 DD Extended Retention 스토리지용으로 구성된 디스크가 표시됩니다. 디스크는 Disks in Use 및 Disks Not in Use의 두 가지 표로 나열됩니다.

- 캐시 계층
  캐시 계층의 SSD는 메타데이터 캐싱에 사용됩니다. SSD는 파일 시스템에서 사용할 수 없습니다. 디스크는 Disks in Use 및 Disks Not in Use의 두 가지 표로 나열됩니다.
- Cloud Tier
  클라우드 계층의 디스크는 클라우드 스토리지에 상주하는 데이터의 메타데이터를 저장하는 데 사용됩니다. 디스크는 파일 시스템에서 사용할 수 없습니다. 디스크는 Disks in Use 및 Disks Not in Use의 두 가지 표로 나열됩니다.
- Addable Storage
  선택적 엔클로저가 있는 시스템의 경우 이 섹션에는 시스템에 추가할 수 있는 디스크와 엔클로저가 표시됩니다.
- Failed/Foreign/Absent Disks (Excluding Systems Disks)
  실패 상태에 있는 디스크를 보여 줍니다. 이 디스크는 활성 또는 보존 계층의 시스템에 추가할 수 없습니다.
- Systems Disks
  Data Domain 컨트롤러에 데이터 스토리지 디스크가 없는 경우 DD OS가 상주하는 디스크가 표시됩니다.
- Migration History
  마이그레이션 기록을 표시합니다.

각 섹션 머리글에는 해당 섹션에 대해 구성된 스토리지 요약이 표시됩니다. Summary에서는 디스크, 사용 중인 디스크, 스페어 디스크, 재구성 중인 스페어 디스크, 사용 가능한 디스크 및 알려진 디스크의 총 개수에 대한 총계를 보여 줍니다.

섹션 더하기(+) 버튼을 클릭하여 자세한 정보를 표시하거나 빼기(-) 버튼을 클릭하여 자세한 정보를 숨깁니다.

표 24 Disks In Use 열 레이블 설명

항목	설명
Disk Group	파일 시스템에서 생성한 디스크 그룹의 이름입니다(예: dg1).
State	디스크의 상태입니다(예: Normal, Warning).
Disks Reconstructing	재구성 중인 디스크가 디스크 ID로 표시됩니다(예: 1.11).
Total Disks	사용 가능한 디스크의 총 개수입니다(예: 14).
Disks	사용 가능한 디스크의 디스크 ID입니다(예: 2.1-2.14).
Size	디스크 그룹의 크기입니다(예: 25.47TiB).

표 25 Disks Not In Use 열 레이블 설명

항목	설명
Disk	디스크 식별자로 다음 중 하나일 수 있습니다. • 엔클로저 및 디스크 번호(Enclosure Slot 형식) • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호 • LUN
Slot	디스크가 위치한 엔클로저입니다.

표 25 Disks Not In Use 열 레이블 설명 (계속)

항목	설명
Pack	엔클로저 내에서 디스크가 위치한 팩 디스크(1~4)입니다. DS60 확장 셸프의 경우 이 값은 2~4 사이입니다.
State	예를 들어 In Use, Available, Spare 같은 디스크의 상태입니다.
Size	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
Type	디스크 접속 구성 및 유형입니다(예: SAS).

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1기비바이트를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

Enclosures 탭

Enclosures 탭에는 시스템에 연결된 엔클로저의 세부 정보를 요약한 테이블이 표시됩니다.

Enclosures 탭은 다음과 같은 세부 정보를 제공합니다.

표 26 Enclosures 탭 열 레이블 설명

항목	설명
Enclosure	엔클로저 번호입니다. 엔클로저 1은 본체입니다.
Serial Number	엔클로저 일련 번호입니다.
Disks	*<Enclosure-number>*.1-*<Enclosure-number>*.*<N>* 형식으로 엔클로저에 포함된 디스크를 나타냅니다.
Model	엔클로저 모델입니다. 엔클로저 1인 경우 모델은 본체입니다.
Disk Count	엔클로저에 있는 디스크의 수입니다.
디스크 크기	Data Domain 시스템에서 사용되는 디스크의 데이터 스토리지 용량입니다.[a]
Failed Disks	엔클로저에서 장애가 발생한 디스크입니다.
Temperature Status	엔클로저의 온도 상태입니다.

a. 디스크 공간 계산을 위한 Data Domain 규칙에서는 1GiB(GibiByte)를 230바이트로 정의해 제조업체의 등급과 다른 디스크 용량을 제공합니다.

Disks 탭

Disks 탭에는 각 시스템 디스크에 대한 정보가 표시됩니다. 표시된 디스크를 필터링하여 모든 디스크, 특정 계층의 디스크 또는 특정 그룹의 디스크를 표시할 수 있습니다.

Disk State 테이블에는 모든 시스템 디스크의 상태를 보여주는 요약 상태 테이블이 표시됩니다.

표 27 Disks State 테이블 열 레이블 설명

항목	설명
Total	Data Domain 시스템에 있는 인벤토리가 작성된 디스크의 총 개수입니다.

표 27 Disks State 테이블 열 레이블 설명 (계속)

항목	설명
In Use	현재 파일 시스템에서 사용 중인 디스크의 개수입니다.
Spare	장애가 발생한 디스크 교체에 사용할 수 있는 스페어 디스크의 개수입니다.
Spare (reconstructing)	데이터 재구성 중인 디스크의 개수입니다(장애가 발생한 디스크를 교체하는 스페어 디스크).
Available	Active 또는 DD Extended Retention 스토리지 계층에 할당할 수 있는 디스크의 개수입니다.
Known	할당되지 않은 것으로 알려진 디스크의 개수입니다.
Unknown	할당되지 않은 것으로 알려지지 않은 디스크의 개수입니다.
Failed	장애가 발생한 디스크의 개수입니다.
Foreign	외부 디스크의 개수입니다.
Absent	누락된 디스크의 개수입니다.
Migrating	스토리지 마이그레이션의 소스로 사용되는 디스크의 개수입니다.
Destination	스토리지 마이그레이션의 대상으로 사용되는 디스크의 개수입니다.
Powered Off	전원이 켜지지 않은 디스크의 수입니다.
Not Installed	시스템이 감지할 수 있는 빈 디스크 슬롯의 개수입니다.

Disks 테이블에는 시스템에 설치된 각 디스크와 관련된 정보가 표시됩니다.

표 28 Disks 테이블 열 레이블 설명

항목	설명
Disk	디스크 식별자로, 다음에 해당할 수 있습니다. • 엔클로저 및 디스크 번호(*Enclosure.Slot* 형식) • DD VTL 및 vDisk에서 사용하는 것과 같은 논리 디바이스의 디바이스 번호입니다. • LUN
Size	디스크 의 크기입니다.
Slot	디스크가 위치한 엔클로저입니다.
Pack	엔클로저 내에서 디스크가 위치한 팩 디스크(1~4)입니다. DS60 확장 셸프의 경우 이 값은 2~4 사이입니다.
State	디스크 상태로, 다음 중 하나에 해당할 수 있습니다. • Absent. 표시된 위치에 설치된 디스크가 없습니다. • Available. 사용 가능한 디스크가 활성 또는 보존 계층에 할당되었지만 현재 사용되고 있지 않습니다. • Copy Recovery. 디스크의 오류 비율이 높지만 실패하지는 않았습니다. RAID에서 콘텐츠를 스페어 드라이브에 현재

표 28 Disks 테이블 열 레이블 설명 (계속)

항목	설명
	복제 중이며 복제 재구성이 완료되는 대로 드라이브가 실패할 것입니다. • Destination. 디스크가 스토리지 마이그레이션의 대상으로 사용되고 있습니다. • Error. 디스크의 오류 비율이 높지만 실패하지는 않았습니다. 디스크가 복제 재구성을 위한 대기열에 있습니다. 복제 재구성이 시작되면 상태가 Copy Recovery로 변경됩니다. • Foreign. 디스크가 계층에 할당되었지만 디스크 데이터를 볼 때 다른 시스템에서 소유한 디스크일 수 있습니다. • In-Use. 디스크가 백업 데이터 스토리지로 사용되고 있습니다. • Known. 할당이 가능한 지원되는 디스크입니다. • Migrating. 디스크가 스토리지 마이그레이션의 소스로 사용되고 있습니다. • Powered Off. 지원 팀에서 디스크 전원을 분리했습니다. • Reconstruction. `disk fail` 명령 또는 RAID/SSM의 지시에 대한 응답으로 디스크를 재구성하고 있습니다. • Spare. 디스크를 스페어로 사용할 수 있습니다. • System. 시스템 디스크에는 DD OS 및 시스템 데이터가 저장됩니다. 백업 데이터는 시스템 디스크에 저장되지 않습니다. • Unknown. 활성 또는 보존 계층에 할당되지 않은 알 수 없는 디스크입니다. 관리상의 이유로 또는 RAID 시스템에 의해 실패한 디스크일 수 있습니다.
Manufacturer/Model	제조업체의 모델 지정입니다. 스토리지 시스템에서 전송하는 공급업체 문자열에 따라 모델 ID 또는 RAID 유형 또는 기타 정보가 포함될 수 있습니다.
Firmware	타사 물리적 디스크 스토리지 컨트롤러에서 사용하는 펌웨어 레벨입니다.
Serial Number	디스크의 제조업체 일련 번호입니다.
Disk Life Used	소비된 SSD 정격 수명의 백분율입니다.
Type	디스크 접속 구성 및 유형입니다(예: SAS).

Reconstruction 탭

Reconstruction 탭에는 디스크 재구성에 대한 추가 정보를 제공하는 표가 표시됩니다. 다음 표에서는 Reconstructing의 항목에 대해 설명합니다.

표 29 Reconstruction 테이블 열 레이블 설명

항목	설명
Disk	재구성 중인 디스크를 식별합니다. 디스크 레이블의 형식은 *enclosure.disk*입니다. 엔클로저 1은 Data Domain 시스템이고 외부 셸프의 번호 지정은 엔클로저 2부터 시작됩니다. 예를 들어 레이블 3.4는 두 번째 셸프에 있는 4번째 디스크입니다.
Disk Group	재구성 중인 디스크에 대한 RAID 그룹(dg#)을 보여 줍니다.
Tier	장애가 발생한 디스크가 재구성 중인 계층의 이름입니다.
Time Remaining	재구성이 완료되기까지 남은 시간입니다.
Percentage Complete	완료된 재구성의 비율입니다.

스페어 디스크를 사용할 수 있는 경우 파일 시스템이 자동으로 장애가 발생한 디스크를 스페어로 교체하고 재구성 프로세스를 시작해 RAID 디스크 그룹에 스페어를 통합합니다. 디스크 사용에 `Spare`가 표시되고 상태가 `Reconstructing`이 됩니다. 재구성은 한 번에 하나의 디스크에서 수행됩니다.

물리적 엔클로저 찾기

DD System Manager에 표시된 엔클로저에 해당하는 물리적 엔클로저를 결정하는 데 어려움이 있는 경우 CLI Beacon 기능을 사용하여 엔클로저 IDENT 상태 표시등 및 정상 작동을 나타내는 모든 디스크 상태 표시등을 깜박이게 할 수 있습니다.

절차

1. 시스템에서 CLI 세션을 설정합니다.
2. `enclosure beacon` ***enclosure***을 입력합니다.
3. **Ctrl+C**를 누르면 LED 깜박임이 중지됩니다.

물리적으로 디스크 찾기

DD System Manager에 표시된 디스크에 해당하는 물리적 디스크를 찾기가 어려운 경우 물리적 디스크의 상태 표시등을 깜박이는 beacon 기능을 사용할 수 있습니다.

절차

1. **Hardware** > **Storage** > **Disks**를 선택합니다.
2. **Disks** 표에서 디스크를 선택하고 **Beacon**을 클릭합니다.

   참고

   한 번에 하나의 디스크를 선택할 수 있습니다.

   Beaconing Disk 대화 상자가 나타나며 디스크의 상태 표시등이 깜박이기 시작합니다.
3. 상태 표시등 표시를 중단하려면 **Stop**을 클릭합니다.

스토리지 구성

스토리지 구성 기능을 사용해 스토리지 확장 엔클로저를 활성, 보존 및 클라우드 계층에 추가하고 이러한 계층에서 제거할 수 있습니다. 확장 엔클로저(확장 셸프라고도 함)의 스토리지는 계층에 추가하기 전까지 사용할 수 없습니다.

참고

스토리지를 추가하려면 해당하는 라이센스가 필요하며 새 스토리지 용량을 지원할 충분한 메모리가 있어야 합니다. 라이센스나 메모리가 더 필요하면 오류 메시지가 표시됩니다.

DD6300 시스템은 라이센스가 부여된 사용 가능한 용량이 정확히 21.8TiB인 경우 활성 계층에서 4TB 드라이브로 구성된 ES30 엔클로저(43.6TiB)를 50% 활용률(21.8TiB)로 사용하는 옵션을 지원합니다. 다음 지침은 부분 용량 셸프를 사용할 경우에 적용됩니다.

- 다른 엔클로저 유형 또는 드라이브 크기는 부분 용량 사용을 지원하지 않습니다.
- 부분 용량 셸프는 활성 계층에만 존재할 수 있습니다.
- 활성 계층에 부분 용량 ES30 하나만 존재할 수 있습니다.
- 계층에 부분 용량 셸프가 존재하는 경우 해당 계층에 ES30을 추가로 구성하려면 먼저 부분 용량 셸프를 전체 용량으로 바꿔야 합니다.

  참고

  이렇게 하려면 부분 용량 셸프의 나머지 21.8TiB를 사용할 수 있도록 충분한 추가 용량 라이센스를 부여해야 합니다.
- 사용 가능한 용량이 21.8TB를 초과하면 부분 용량 셸프를 추가할 수 없습니다.
- 나중에 21TiB 라이센스를 삭제하면 자동으로 전체 용량 셸프가 부분 용량 셸프로 변환되는 것은 아닙니다. 셸프를 제거하고 다시 부분 용량 셸프로 추가해야 합니다.

절차

1. **Hardware** > **Storage** > **Overview**를 선택합니다.
2. 사용 가능한 스토리지 계층 중 하나로 대화 상자를 확장합니다.
   - **Active Tier**
   - **Extended Retention Tier**
   - **Cache Tier**
   - **Cloud Tier**
3. **Configure**를 클릭합니다.
4. Configure Storage 대화 상자의 **Addable Storage** 목록에서 추가할 스토리지를 선택합니다.
5. **Configure** 목록에서 **Active Tier** 또는 **Retention Tier**를 선택합니다.

   활성 계층에 추가할 수 있는 최대 스토리지 양은 사용하는 DD 컨트롤러에 따라 다릅니다.

   참고

   라이센스가 부여된 용량 표시줄에 설치된 엔클로저에 대한 라이센스가 부여된 용량(사용된 용량 및 남은 용량)의 부분이 표시됩니다.
6. 추가할 셸프의 확인란을 선택합니다.
7. **Add to Tier** 버튼을 클릭합니다.
8. **OK**를 클릭하여 스토리지를 추가합니다.

참고

추가된 셸프를 제거하려면 Tier Configuration 목록에서 **Remove from Configuration**과 **OK**를 차례로 클릭합니다.

DD3300 용량 확장

DD3300 시스템은 세 가지 서로 다른 용량 구성으로 사용할 수 있습니다. 한 구성에서 다른 구성으로의 용량 확장이 지원됩니다.

DD3300 시스템은 다음과 같은 용량 구성으로 사용할 수 있습니다.

- 4TB
- 8TB
- 16TB
- 32TB

다음 업그레이드 고려 사항이 적용됩니다.

- 4TB 시스템은 16TB로 업그레이드할 수 있습니다.
- 8TB를 16TB로 업그레이드할 수 있고 16TB를 32TB로 업그레이드할 수 있습니다.
- 16TB 시스템은 32TB로 업그레이드할 수 있습니다.
- 4TB에서 32TB로 업그레이드하는 경로는 없습니다.

Maintenance > **System**을 선택하여 용량 확장 관련 정보에 액세스하고 용량 확장 프로세스를 시작합니다.

용량 확장은 일회성 프로세스입니다. **Capacity Expansion History** 창에는 시스템이 이미 확장되었는지 여부가 표시됩니다. 시스템이 확장되지 않은 경우 **Capacity Expand** 버튼을 클릭하여 용량 확장을 시작합니다.

모든 용량 확장에는 시스템의 추가 디스크 및 메모리 설치가 필요합니다. 하드웨어 업그레이드가 완료될 때까지 용량을 확장하지 마십시오. 다음 표에는 용량 확장을 위한 하드웨어 업그레이드 요구 사항이 나와 있습니다.

표 30 용량 확장을 위한 DD3300 업그레이드 요구 사항

용량 확장	추가 메모리	추가 HDD	추가 SSD
4TB~16TB	32GB	6 x 4TB HDD	1 x 480GB SSD
8TB~16TB	8TB~16TB 확장 시에는 라이선스 등록 및 구성 변경만 필요합니다. 하드웨어 업그레이드는 필요하지 않습니다.		
16TB~32TB	16GB	6 x 4TB HDD	해당 없음

*Data Domain DD3300 현장 교체 및 업그레이드 가이드*에 시스템 용량 확장에 대한 자세한 지침이 나와 있습니다.

용량 확장

Select Capacity 드롭다운 목록에서 타겟 용량을 선택합니다. 메모리가 부족하거나, 물리적 용량(HDD)이 부족하거나, 시스템이 이미 확장되었거나, 용량 확장의 타겟이 지원되지 않는 경우 용량을 확장할 수 없습니다. 용량 확장을 완료할 수 없는 경우 여기에 이유가 표시됩니다.

Capacity expansion history

Capactiy Expansion History 표에는 시스템의 용량에 대한 세부 정보가 표시됩니다. 이 표에는 소프트웨어가 처음 설치되었을 당시의 시스템 용량과 초기 소프트웨어 설치 날짜가 표시됩니다. 용량이 확장된 경우 표에 확장된 용량과 확장이 수행된 날짜도 표시됩니다.

디스크 장애 설정 및 해제

디스크 장애 설정 기능을 사용하면 수동으로 디스크를 장애 상태로 설정하여 디스크에 저장된 데이터를 강제로 재구성할 수 있습니다. 디스크 장애 해제 기능을 사용하면 장애 상태의 디스크를 가져와 작동 상태로 되돌릴 수 있습니다.

디스크 장애 설정

디스크에 장애가 발생하여 재구성을 강제합니다. **Hardware** > **Storage** > **Disks** > **Fail**을 선택합니다.

표에서 디스크를 선택하고 **Fail**을 클릭합니다.

디스크 장애 해제

이전에 Failed 또는 Foreign으로 표시된 디스크를 시스템에 사용할 수 있도록 합니다. **Hardware** > **Storage** > **Disks** > **Unfail**을 선택합니다.

표에서 디스크를 선택하고 **Unfail**을 클릭합니다.

네트워크 연결 관리

네트워크 연결 관리 기능을 사용해 네트워크 인터페이스, 일반 네트워크 설정 및 네트워크 라우트를 보고 구성할 수 있습니다.

HA 시스템 네트워크 연결 관리

HA 시스템은 고정 IP 주소와 유동 IP 주소의 두 가지 IP 주소를 사용합니다. 각 유형마다 고유한 동작과 제한 사항이 있습니다.

HA 시스템에서 고정 IP 주소의 특징은 다음과 같습니다.

- CLI를 통한 노드 관리에 사용됨
- 노드에 연결("고정")됨
- 정적이거나 DHCP, IPv6 SLAAC일 수 있음
- 특정 노드에서 `type fixed` 인수를 선택적으로 사용하여 구성 수행

참고

모든 파일 시스템 액세스는 유동 IP를 통해 이루어져야 합니다.

유동 IP 주소는 2개의 노드로 구성된 HA 시스템에만 존재합니다. 페일오버 시 IP 주소가 새 액티브 노드로 이동하며, 다음과 같은 특징이 있습니다.

- 액티브 노드에서만 구성됨
- 파일 시스템 액세스 및 대부분의 구성에 사용
- 정적일 수만 있음

- `type floating` 인수를 반드시 사용하여 구성해야 함

네트워크 인터페이스 관리

네트워크 인터페이스 관리 기능을 사용하면 시스템을 네트워크에 연결하는 물리적 인터페이스를 관리하고 논리적 인터페이스를 생성하여 Link Aggregation, 로드 밸런싱 및 링크/노드 페일오버를 지원할 수 있습니다.

인터페이스 정보 보기

Interfaces 탭에서 물리적 인터페이스 및 가상 인터페이스, VLAN, DHCP, DDNS와 IP 주소 및 별칭을 관리할 수 있습니다.

IPv6 인터페이스를 관리하는 경우 다음 지침을 고려하십시오.

- CLI(Command Line Interface)는 기본 Data Domain 네트워크 및 복제 명령에 대해 IPv6를 지원하지만 백업 및 DD Extended Retention(`archive`) 명령에 대해서는 지원하지 않습니다. CLI 명령은 IPv6 주소를 관리합니다. DD System Manager를 사용하여 IPv6 주소를 볼 수는 있지만 DD System Manager로 IPv6를 관리할 수는 없습니다.
- IPv6 네트워크를 통한 컬렉션, 디렉토리 및 MTree 복제가 지원되며, 그에 따라 IPv6 주소 공간을 활용할 수 있게 됩니다. DD Boost로 관리되는 파일 복제 기능과 마찬가지로, IPv6 및 IPv4 네트워크를 통한 동시 복제 역시 지원됩니다.
- IPv6 주소를 가진 인터페이스에는 몇 가지 제한 사항이 있습니다. 예를 들어 최소 MTU는 1280입니다. IPv6 주소를 가진 인터페이스에 대해 MTU를 1280보다 낮게 설정하려고 하면 오류 메시지가 나타나고 인터페이스가 서비스에서 제거됩니다. IPv6 주소가 인터페이스에 연결된 VLAN을 기반으로 하고 직접 인터페이스상에 있지 않다고 해도 IPv6 주소는 인터페이스에 영향을 미칠 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.

   다음 표에서는 Interfaces 탭의 정보에 대해 설명합니다.

   표 31 Interface 탭 레이블 설명

항목	설명
Interface	선택한 시스템과 연결된 각 인터페이스의 이름입니다.
Enabled	인터페이스의 활성화 여부입니다. • 인터페이스를 활성화하고 네트워크에 연결하려면 **Yes**를 선택합니다. • 인터페이스를 비활성화하고 네트워크에서 분리하려면 **No**를 선택합니다.
DHCP	인터페이스가 수동으로 구성(`no`)되었는지 여부를 나타냅니다 (DHCP(Dynamic Host Configuration Protocol) IPv4 서버(`v4`) 또는 DHCP IPv6 서버(`v6`) 사용).
IP Address	인터페이스와 연결된 IP 주소입니다. 이 주소는 네트워크에서 인터페이스를 식별하는 데 사용됩니다. 인터페이스가 DHCP를 통해 구성되어 있는 경우 이 값 다음에 별표가 나타납니다.

표 31 Interface 탭 레이블 설명 (계속)

항목	설명
Netmask	인터페이스와 연결된 넷마스크입니다. 표준 IP 네트워크 마스크 형식이 사용됩니다. 인터페이스가 DHCP를 통해 구성되어 있는 경우 이 값 다음에 별표가 나타납니다.
Link	이더넷 연결의 활성 여부를 나타냅니다(Yes/No).
Address Type	HA 시스템에서 주소 유형은 고정, 유동 또는 상호 연결을 나타냅니다.
Additional Info	인터페이스에 대한 추가 설정입니다. 연결 모드를 예로 들 수 있습니다.
IPMI interfaces configured	인터페이스에 대해 IPMI 상태 모니터링 및 전원 관리가 구성되어 있는지 여부를 Yes 또는 No로 나타냅니다.

2. 인터페이스 목록을 인터페이스 이름으로 필터링하려면 **Interface Name** 필드에 값을 입력하고 **Update**를 클릭합니다.

   필터는 eth*, veth*, eth0* 등의 와일드카드를 지원합니다.

3. 인터페이스 목록을 인터페이스 유형으로 필터링하려면 **Interface Type** 메뉴에서 값을 선택하고 **Update**를 클릭합니다.

   HA 시스템에는 IP Address Type(Fixed, Floating 또는 Interconnect)을 기준으로 필터링하는 필터 드롭다운이 있습니다.

4. Interfaces 테이블을 기본 나열로 되돌리려면 **Reset**을 클릭합니다.
5. 표에서 인터페이스를 선택하여 Interface Details 영역을 채웁니다.

표 32 Interface Details 레이블 설명

항목	설명
Auto-generated Addresses	선택한 인터페이스에 대해 자동으로 생성된 IPv6 주소를 표시합니다.
Auto Negotiate	이 기능이 `Enabled`라고 표시된 경우 인터페이스는 자동으로 Speed 및 Duplex 설정을 협상합니다. 이 기능이 `Disabled`라고 표시된 경우 Speed 및 Duplex 값은 수동으로 설정해야 합니다.
Cable	인터페이스가 Copper 또는 Fibre인지 여부를 보여 줍니다. 참고 케이블이 유효한 상태가 되기 전에 일부 인터페이스가 실행되고 있어야 합니다.
Duplex	Speed 값과 함께 데이터 전송 프로토콜을 설정하는 데 사용됩니다. 옵션은 Unknown, Full, Half입니다.
Hardware Address	선택한 인터페이스의 MAC 주소입니다. 예를 들어 00:02:b3:b0:8a:d2와 같습니다.
Interface Name	선택한 인터페이스의 이름입니다.

표 32 Interface Details 레이블 설명 (계속)

항목	설명
Latent Fault Detection (LFD) - HA 시스템만 해당	LFD 필드에는 LFD 주소와 인터페이스가 나열된 팝업을 표시하는 `View Configuration` 링크가 있습니다.
MTU(Maximum Transfer Unit)	인터페이스에 할당된 MTU 값입니다.
Speed	Duplex 값과 함께 데이터 전송 속도를 설정하는 데 사용됩니다. 옵션은 Unknown, 10 Mb/s, 100 Mb/s, 1,000 Mb/s, 10 Gb/s입니다. 참고 Auto-negotiated 인터페이스는 Speed, Duplex, Supported Speeds가 나타나기 전에 설정되어야 합니다.
Supported Speeds	인터페이스가 사용할 수 있는 모든 속도를 나열합니다.

6. IPMI 인터페이스 구성 및 관리 옵션을 보려면 **View IPMI Interfaces**를 클릭합니다.

   이 링크는 **Maintenance** > **IPMI** 정보를 표시합니다.

물리적 인터페이스 이름 및 제한 사항

물리적 인터페이스 이름의 형식은 다양한 Data Domain 시스템 및 옵션 카드에 따라 다르며 일부 인터페이스의 경우 제한 사항이 적용됩니다.

- 대부분의 시스템에서 물리적 인터페이스 이름의 형식은 `eth`*xy*이며, 여기서 *x*는 온보드 포트 또는 옵션 카드의 슬롯 번호이며 *y*는 영숫자 문자열을 말합니다. 예를 들어 eth0a를 사용합니다.
- 대부분의 온보드 NIC 수직 인터페이스에서는 상단 인터페이스는 eth0a, 하단 인터페이스는 eth0b로 이름을 지정합니다.
- 대부분의 온보드 NIC 수평 인터페이스에서는 뒤쪽에서 봤을 때 왼쪽 인터페이스는 eth0a, 오른쪽 인터페이스는 eth0b로 이름을 지정합니다.
- DD990 시스템은 4개의 온보드 인터페이스를 제공하며, 2개는 상단에 2개는 하단에 위치합니다. 좌측 상단 인터페이스는 eth0a, 우측 상단은 eth0b, 좌측 하단은 eth0c, 우측 하단은 eth0d입니다.
- DD2200 시스템은 4개의 온보드 1G Base-T NIC 포트인 ethMa(왼쪽 위), ethMb(오른쪽 위), ethMc(왼쪽 아래) 및 ethMd(오른쪽 아래)를 제공합니다.
- DD2500 시스템은 6개의 온보드 인터페이스를 제공합니다. 4개의 온보드 1G Base-T NIC 포트는 ethMa(좌측 상단), ethMb(우측 상단), ethMc(좌측 하단), ethMd(우측 하단)입니다. 2개의 온보드 10G Base-T NIC 포트는 ethMe(상단) 및 ethMf(하단)입니다.
- DD4200, DD4500, DD7200 시스템은 하나의 온보드 이더넷 포트(ethMa)를 제공합니다.
- DD140 및 DD990 범위에 있는 시스템의 경우 입출력 모듈의 물리적 인터페이스 이름은 모듈의 상단 또는 좌측에서 시작합니다. 첫 번째 인터페이스는 ethxa, 그다음은 ethxb, ethxc 등의 순입니다.

- 수평 DD2500 입출력 모듈의 포트 번호는 모듈 핸들(좌측)의 반대쪽 끝에서 순서대로 레이블이 지정됩니다. 첫 번째 포트는 0으로 레이블이 지정되며 물리적 인터페이스 이름 ethxa에 해당합니다. 그다음은 1/ethxb, 2/ethxc 등의 순입니다.
- 수직 DD4200, DD4500, DD7200 입출력 모듈의 포트 번호는 모듈 핸들(하단)의 반대쪽 끝에서 순서대로 레이블이 지정됩니다. 첫 번째 포트는 0으로 레이블이 지정되며 물리적 인터페이스 이름 ethxa에 해당합니다. 그다음은 1/ethxb, 2/ethxc 등의 순입니다.

일반 인터페이스 구성 지침

시스템 인터페이스를 구성하기 전에 일반 인터페이스 구성 지침을 검토하십시오.

- 백업 및 복제 트래픽을 모두 지원하는 경우에는 가능하면 각 트래픽 유형에 다른 인터페이스를 사용하여 트래픽 유형이 서로 영향을 미치지 않도록 하십시오.
- 복제 트래픽이 1Gb/s 미만으로 예상되는 경우 10GbE 인터페이스가 더 빠른 트래픽에 최적화되어 있으므로 가능하면 복제 트래픽에 10GbE 인터페이스를 사용하지 마십시오.
- Data Domain 서비스가 비표준 포트를 사용하고 사용자가 DD OS 6.0으로 업그레이드하려는 경우 또는 사용자가 DD OS 6.0 시스템에서 비표준 포트를 사용하도록 서비스를 변경하려는 경우 해당 서비스를 사용하는 모든 클라이언트에 대해 net filter 기능을 추가하여 클라이언트 IP 주소가 새 포트를 사용하도록 허용합니다.
- IPMI를 사용하는 DD4200, DD4500, DD7200 시스템에서는 가능하면 인터페이스 ethMa를 IPMI 트래픽과 HTTP, Telnet, SSH 등의 프로토콜을 사용하는 시스템 관리 트래픽에 대해 예약하십시오. 백업 데이터 트래픽은 다른 인터페이스로 이동해야 합니다.

물리적 인터페이스 구성

시스템에서 네트워크에 연결하려면 1개 이상의 물리적 인터페이스를 구성해야 합니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. 구성할 인터페이스를 선택합니다.

   참고

   DD140, DD160, DD610, DD620 및 DD630 시스템은 인터페이스 eth0a(기존 포트 이름을 사용하는 시스템은 eth0) 또는 해당 인터페이스에서 생성된 VLAN에서 IPv6를 지원하지 않습니다.

3. **Configure**를 클릭합니다.
4. Configure Interface 대화 상자에서 인터페이스 IP 주소가 설정되는 방식을 결정합니다.

   참고

   HA 시스템에서 Configure Interface 대화 상자에는 Floating IP(Yes/No)를 지정할지 여부를 선택하는 필드가 있습니다. **Yes**를 선택하면 `Manually Configure IP Address` 라디오 버튼이 자동으로 선택됩니다. 유동 IP 인터페이스는 수동으로만 구성할 수 있습니다.

   - Use DHCP to assign the IP address - IP Settings 영역에서 **Obtain IP Address using DHCP**를 선택하고, IPv4 액세스의 경우 **DHCPv4**, IPv6 액세스의 경우 **DHCPv6**를 선택합니다.

DHCP를 사용하도록 물리적 인터페이스를 설정하면 자동으로 인터페이스가 설정됩니다.

참고

DHCP를 통해 네트워크 설정을 가져오도록 선택한 경우 **Hardware** > **Ethernet** > **Settings**에서 또는 `net set hostname` 명령을 사용하여 수동으로 호스트 이름을 구성할 수 있습니다. IPv6에서 DHCP를 사용할 때에는 수동으로 호스트 이름을 구성해야 합니다.

- Specify IP Settings manually - IP Settings 영역에서 **Manually configure IP Address**를 선택합니다.
  IP Address 및 **Netmask** 필드가 활성화됩니다.

5. IP 주소를 수동으로 입력하기로 선택한 경우 IPv4 또는 IPv6 주소를 입력합니다. IPv4 주소를 입력한 경우 넷마스크 주소를 입력합니다.

   참고

   이 절차에서는 인터페이스에 하나의 IP 주소만 할당할 수 있습니다. 다른 IP 주소를 할당하는 경우 새 주소가 이전 주소를 대신합니다. 추가 IP 주소를 인터페이스에 연결하려면 IP 별칭을 생성합니다.

6. Speed/Duplex 설정을 지정합니다.

   속도 및 이중화 설정은 인터페이스를 통한 데이터 전송 속도를 정의합니다. 다음 중 한 옵션을 선택합니다.

   - **Autonegotiate Speed/Duplex** - 네트워크 인터페이스 카드가 인터페이스의 회선 속도 및 이중화 설정을 자동 조정하도록 하려면 이 옵션을 선택합니다. 자동 조정은 다음 DD2500, DD4200, DD4500, DD7200 입출력 모듈에서 지원되지 *않습니다*.
     - LC 커넥터 이중 포트 10GbE SR Optical(SFP 사용)
     - 이중 포트 10GbE DAC(Direct Attach Copper) (SFP+ 케이블)
     - 4중 포트, 2포트 1GbE Copper(RJ45)/2포트 1GbE SR Optical
   - **Manually configure Speed/Duplex** - 인터페이스 데이터 전송 속도를 수동으로 설정하려면 이 옵션을 선택합니다. 메뉴에서 Speed와 Duplex를 선택합니다.
     - Duplex 옵션은 Half, Full 및 Unknown입니다.
     - 나열되는 Speed 옵션은 하드웨어 디바이스의 성능에 따라 제한됩니다. 옵션은 10Mb, 100Mb, 1,000Mb(1Gb), 10Gb, Unknown입니다. 10G Base-T 하드웨어는 100Mb, 1,000Mb, 10Gb 설정만 지원합니다.
     - Half 옵션은 10Mb 및 100Mb 속도에만 사용할 수 있습니다.
     - 1,000Mb 및 10Gb 회선 속도에는 Full-Duplex를 사용해야 합니다.
     - DD2500, DD4200, DD4500, DD7200 10GbE 입출력 모듈에서 Copper 인터페이스는 10Gb 속도 설정만 지원합니다.
     - 10G Base-T 인터페이스의 기본 설정은 Autonegotiate Speed/Duplex입니다. 속도를 1,000Mb 또는 10Gb로 수동으로 설정한 경우 Duplex 설정을 Full로 설정해야 합니다.

7. 물리적(이더넷) 인터페이스의 MTU(Maximum Transfer Unit) 크기를 지정합니다.

다음을 수행하십시오.

- **Default** 버튼을 클릭하면 설정이 기본값으로 돌아갑니다.
- 전체 네트워크 구성 요소가 이 옵션의 크기 세트를 지원하는지 확인하십시오.

8. 필요에 따라 **Dynamic DNS Registration**를 선택합니다.

   DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다. 이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다.

   이 옵션을 사용하려면 DDNS가 등록되어 있어야 합니다.

   참고

   이 옵션은 이 인터페이스에 DHCP를 비활성화합니다.

9. **Next**를 클릭합니다.

   Configure Interface Settings 요약 페이지가 나타납니다. 새 시스템 및 인터페이스 상태를 반영한 값이 나열되며, 이러한 값은 Finish를 클릭하면 적용됩니다.

10. **Finish** 및 **OK**를 차례대로 클릭합니다.

MTU 크기 값

네트워크 연결의 성능을 최적화하려면 MTU 크기를 올바르게 설정해야 합니다. 잘못된 MTU 크기는 인터페이스 성능에 부정적인 영향을 미칠 수 있습니다.

물리적(이더넷) 인터페이스의 MTU(Maximum Transfer Unit) 크기를 설정하기 위해 지원되는 값의 범위는 350~9000입니다. 100 Base-T 및 기가비트 네트워크의 경우, 표준 기본값은 1500입니다.

참고

IPv6 인터페이스의 최소 MTU는 1280입니다. MTU를 1280보다 낮게 설정하려고 하면 인터페이스에 장애가 발생합니다.

정적 IP 주소 이동

특정 정적 IP 주소는 시스템에 있는 하나의 인터페이스에만 지정해야 합니다. 다른 인터페이스에 구성하려는 경우 먼저 원래 인터페이스에서 정적 IP 주소를 올바르게 제거해야 합니다.

절차

1. 정적 IP 주소를 호스팅하는 인터페이스가 DD Boost 인터페이스 그룹에 속할 경우 해당 그룹에서 인터페이스를 제거합니다.
2. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
3. 이동할 정적 IP 주소를 제거합니다.
   a. 현재 이동하려는 IP 주소를 사용하고 있는 인터페이스를 선택합니다.
   b. Enabled 열에서 **No**를 선택해 인터페이스를 해제합니다.
   c. **구성**을 클릭합니다.
   d. IP 주소를 0으로 설정합니다.

참고

인터페이스에 할당할 다른 IP 주소가 없는 경우에는 IP 주소를 0으로 설정하십시오. 여러 인터페이스에 동일한 IP 주소를 지정해서는 안 됩니다.

e. **Next**를 클릭하고 **Finish**를 클릭합니다.

4. 제거한 정적 IP 주소를 다른 인터페이스에 추가합니다.
   a. IP 주소를 이동할 인터페이스를 선택합니다.
   b. Enabled 열에서 **No**를 선택해 인터페이스를 해제합니다.
   c. **Configure**를 클릭합니다.
   d. 제거한 정적 IP 주소와 일치하도록 IP 주소를 설정합니다.
   e. **Next**를 클릭하고 **Finish**를 클릭합니다.
   f. Enabled 열에서 **Yes**를 선택해 업데이트된 인터페이스를 사용합니다.

가상 인터페이스 구성 지침

가상 인터페이스 구성 지침은 페일오버 및 집계 인터페이스에 적용됩니다. 페일오버 또는 집계 인터페이스에 적용되고 둘 다에 적용되지는 않는 추가 지침도 있습니다.

- *virtual-name*은 `veth`*x* 형식이어야 하며 여기서 *x*는 숫자입니다. 권장되는 최대 숫자는 이름 크기 제한으로 인해 99입니다.
- 가상 인터페이스는 물리적 인터페이스 수 만큼 생성할 수 있습니다.
- 가상 인터페이스에서 사용된 각 인터페이스는 우선 비활성화되어야 합니다. 가상 인터페이스의 일부인 인터페이스는 다른 네트워크 구성 옵션에 대해 비활성화된 것으로 인식됩니다.
- 가상 인터페이스가 제거되면 이와 연결된 물리적 인터페이스도 비활성화된 상태로 남습니다. 따라서 수동으로 물리적 인터페이스를 다시 활성화해야 합니다.
- 설치된 카드의 수와 유형으로 사용 가능한 이더넷 포트 수가 결정됩니다.
- 각 물리적 인터페이스는 하나의 가상 인터페이스에 속할 수 있습니다.
- 한 시스템이 여러 개의 혼합 페일오버 및 집계 가상 인터페이스를 지원할 수 있으며, 이 경우 앞서 언급된 제한 사항이 적용됩니다.
- 가상 인터페이스는 동일한 물리적 인터페이스에서 생성되어야 합니다. 예를 들어, 전체 Copper 또는 전체 Optical 인터페이스, 전체 1Gb 또는 전체 10Gb 인터페이스가 있습니다. 그러나 1Gb 인터페이스는 Copper 인터페이스와 Optical 인터페이스의 혼합 연결을 지원합니다. 이는 Chelsio 카드를 제외한 동일한 물리적 인터페이스를 사용하는 다양한 카드의 가상 인터페이스에 적용됩니다. Chelsio 카드의 경우 페일오버만 지원되고, 이는 동일한 카드의 인터페이스에 대해서만 해당됩니다.
- 페일오버와 집계 링크는 두 개 이상의 네트워크 인터페이스를 병렬로 사용하여 네트워크 성능과 복구 성능을 향상시키므로 단일 인터페이스를 사용할 때보다 집계된 링크의 링크 속도와 신뢰성이 높아집니다.
- **Configure** 버튼을 사용하여 제거 기능을 이용할 수 있습니다. Interfaces 탭의 인터페이스 목록에서 가상 인터페이스를 클릭하고 **Configure**를 클릭합니다. 대화 상자의 인터페이스 목록에서 인터페이스의 확인란을 선택 취소하여 연결(페일오버 또는 집계)을 제거하고 **Next**를 클릭합니다.
- 연결된 인터페이스의 경우 슬레이브 인터페이스에 대한 하드웨어에서 장애가 발생하면 나머지 슬레이브를 사용하여 연결된 인터페이스가 생성됩니다. 슬레이브가 없으면 슬레이브가 없는 상태로 연결된 인터페이스 ID가 생성됩니다. 이 슬레이브 하드웨어 장애는, 장애가 발생한 슬레이브당 하나씩 관리되는 알림을 생성합니다.

참고

장애가 발생한 슬레이브에 대한 알림은 해당 슬레이브가 시스템에서 제거되면 사라집니다. 새 하드웨어를 설치한 경우 재부팅하면 알림이 사라지고 연결된 인터페이스가 새 슬레이브 인터페이스를 사용합니다.

- DD3300, DD4200, DD4500 및 DD7200 시스템에서 ethMa 인터페이스는 페일오버 또는 Link Aggregation을 지원하지 않습니다.

Link Aggregation을 위한 가상 인터페이스 구성 지침

Link Aggregation은 하나 이상의 네트워크 인터페이스를 병렬로 사용하여 향상된 네트워크 성능 및 복구 능력을 제공하므로 단일 인터페이스를 사용하는 경우보다 링크 속도와 신뢰성이 높아집니다. 이 지침은 사용자의 Link Aggregation 사용을 최적화하기 위해 제공되었습니다.

- 해제된 이더넷 인터페이스를 변경하면 라우팅 테이블이 플러시됩니다. 예약된 유지 보수 다운타임 중에만 인터페이스를 변경하는 것이 좋습니다. 그 후에 라우팅 규칙과 게이트웨이를 재구성합니다.
- 물리적 인터페이스와 모드를 지정하고 IP 주소를 제공하여 기존 가상 인터페이스에 Link Aggregation을 설정합니다.
- 10Gb 단일 포트 Optical 이더넷 카드는 Link Aggregation을 지원하지 않습니다.
- 1GbE 인터페이스와 10GbE 인터페이스는 함께 집계될 수 없습니다.
- Copper 인터페이스와 Optical 인터페이스는 함께 집계될 수 없습니다.
- DD4200, DD4500 및 DD7200 시스템에서 ethMA 인터페이스는 Link Aggregation을 지원하지 않습니다.

페일오버를 위한 가상 인터페이스 구성 지침

링크 페일오버는 운영 인터페이스가 작동하지 않을 때 네트워크 트래픽을 지원할 수 있는 백업 인터페이스를 식별하여 네트워크 안정성 및 성능을 개선합니다. 이 지침은 사용자의 링크 페일오버 사용을 최적화하기 위해 제공되었습니다.

- 기본 인터페이스는 페일오버의 일부여야 합니다. 페일오버에서 기본 인터페이스 제거를 시도하면 오류 메시지가 나타납니다.
- 기본 인터페이스가 페일오버 구성에 사용된 경우 이를 명시적으로 지정해야 하며 이는 또한 가상 인터페이스에 연결된 인터페이스여야 합니다. 기본 인터페이스가 중단되고 여전히 여러 인터페이스를 사용할 수 있는 경우, 그 다음 인터페이스는 임의로 선택됩니다.
- 가상 인터페이스의 모든 인터페이스는 동일한 물리적 네트워크에 있어야 합니다. 가상 인터페이스에서 사용된 네트워크 스위치는 동일한 물리적 네트워크에 있어야 합니다.
- 페일오버에 대해 권장되는 물리적 인터페이스 수는 1보다 큽니다. 그러나 다음 경우를 제외하고 하나의 기본 인터페이스와 하나 이상의 페일오버 인터페이스를 구성할 수 있습니다.
  - 동일한 카드에서 하나의 기본 인터페이스와 하나의 페일오버 인터페이스로 제한되는 10Gb CX4 이더넷 카드 및
  - 사용할 수 없는 10Gb 단일 포트 Optical 이더넷 카드
- DD4200, DD4500, DD7200 시스템에서 ethMA 인터페이스는 링크 페일오버를 지원하지 않습니다.

가상 인터페이스 생성

Link Aggregation 또는 페일오버를 지원할 가상 인터페이스를 생성합니다. 가상 인터페이스는 링크의 집계 또는 페일오버용 연결을 위한 컨테이너 역할을 합니다.

Link Aggregation을 위한 가상 인터페이스 생성

Link Aggregation을 위한 가상 인터페이스를 생성하여 집계에 사용될 링크를 연결하는 컨테이너로 사용합니다.

Link Aggregation 인터페이스는 링크 연결 모드를 지정해야 하며 해시 선택이 필요할 수 있습니다. 예를 들어 LACP(Link Aggregation Control Protocol) 및 해시 XOR-L2L3 모드에서 가상 인터페이스 *veth1*과 물리적 인터페이스 *eth1* 및 *eth2* 간에 Link Aggregation을 설정할 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. Interfaces 테이블에서 **Enabled** 열의 **No**를 클릭하여 가상 인터페이스가 추가될 물리적 인터페이스를 해제합니다.
3. **Create** 메뉴에서 **Virtual Interface**를 선택합니다.
4. Create Virtual Interface 대화 상자에서 **veth** 상자에 가상 인터페이스 이름을 지정합니다.

   가상 인터페이스 이름은 *vethx*의 형태로 입력하며, 여기서 *x*는 고유 ID(일반적으로 한 자리 또는 두 자리 숫자)를 뜻합니다. VLAN 및 IP 별칭이 포함된 전체 가상 인터페이스 이름의 일반적인 형태는 *veth56.3999:199*입니다. 전체 이름의 길이는 최대 15자입니다. 특수 문자는 사용할 수 없습니다. 숫자는 0~4094 범위여야 합니다.

5. **Bonding Type** 목록에서 **Aggregate**를 선택합니다.

   참고

   레지스트리 설정은 연결 구성과 다를 수 있습니다. 가상 인터페이스에 인터페이스를 추가할 경우, IP 주소가 부여된 가상 인터페이스가 제공되기 전까지 해당 정보는 연결 모듈로 전송되지 않습니다. 그때까지는 레지스트리 및 연결 구성이 다릅니다.

6. **Mode** 목록에서 연결 모드를 선택합니다.

   인터페이스가 직접 연결되는 시스템의 요구 사항과 호환되는 모드를 지정하십시오.

   - Round-robin
     Link Aggregation 그룹의 사용 가능한 첫 링크부터 마지막 링크까지 패킷을 순차적으로 전송합니다.
   - Balanced
     선택한 해시 방식에 따라 결정된 인터페이스를 통해 데이터가 전송됩니다. 이를 위해서는 스위치에 연결된 인터페이스가 이더넷 채널(트렁크)로 그룹화되어야 하며 로드 밸런싱 매개 변수를 통해 제공되는 해시가 있어야 합니다.
   - LACP
     LACP(Link Aggregation Control Protocol) 모드는 링크의 다른 쪽 끝과 통신하는 제어 프로토콜을 사용하며 연결 내에서 사용할 수 있는 링크를 조율한다는 점을 제외하고 Balanced 모드와 유사합니다. LACP는 일종의 하트비트 페일오버를 제공하며 링크의 양쪽 끝에 구성되어야 합니다.

7. Balanced 또는 LACP 모드를 선택한 경우 **Hash** 목록에서 연결 해시 유형을 지정합니다.

   다음과 같은 옵션이 있음 XOR-L2, XOR-L2L3, XOR-L3L4

   XOR-L2는 Layer 2(인바운드 및 아웃바운드 MAC 주소)의 XOR 해시와 연결된 인터페이스를 통해 전송합니다.

   XOR-L2L3는 Layer 2(인바운드 및 아웃바운드 MAC 주소) 및 Layer 3(인바운드 및 아웃바운드 IP 주소)의 XOR 해시와 연결된 인터페이스를 통해 전송합니다.

   XOR-L3L4는 Layer 3(인바운드 및 아웃바운드 IP 주소) 및 Layer 4(인바운드 및 아웃바운드 포트)의 XOR 해시와 연결된 인터페이스를 통해 전송합니다.

8. Link Aggregation 구성에 추가할 인터페이스를 선택하려면 인터페이스에 해당하는 확인란을 선택한 후 **Next**를 클릭합니다.

   Create virtual interface *veth_name* 대화 상자가 나타납니다.

9. IP 주소를 입력하거나, IP 주소를 지정하지 않으려면 0을 입력합니다.
10. 넷마스크 주소 또는 접두사를 입력합니다.
11. Speed/Duplex 옵션을 지정합니다.

    속도 및 이중화 설정은 인터페이스를 통한 데이터 전송 속도를 정의합니다. 다음 중 하나를 선택합니다.

    - **Autonegotiate Speed/Duplex**
      네트워크 인터페이스 카드가 인터페이스의 회선 속도 및 이중화 설정을 자동 조정하도록 하려면 이 옵션을 선택합니다.
    - **Manually configure Speed/Duplex**
      인터페이스 데이터 전송 속도를 수동으로 설정하려면 이 옵션을 선택합니다.
      - Duplex 옵션은 Half 또는 Full입니다.
      - 나열되는 Speed 옵션은 하드웨어 디바이스의 성능에 따라 제한됩니다. 옵션은 10Mb, 100Mb, 1,000Mb 및 10Gb입니다.
      - Half 옵션은 10Mb 및 100Mb 속도에만 사용할 수 있습니다.
      - 1,000Mb 및 10Gb 회선 속도에는 Full-Duplex를 사용해야 합니다.
      - Optical 인터페이스에는 Autonegotiate 옵션을 사용해야 합니다.
      - 10GbE Copper NIC 기본값은 10Gb입니다. Copper 인터페이스를 1000Mb 또는 10Gb 회선 속도로 설정하는 경우 Duplex가 Full-Duplex이어야 합니다.

12. MTU 설정을 지정합니다.
    - 기본값(1500)을 선택하려면 **Default**를 클릭합니다.
    - 다른 설정을 선택하려면 **MTU** 입력란에 설정을 입력합니다. 전체 네트워크 구성 요소가 이 옵션의 크기 세트를 지원하는지 확인하십시오.

13. 필요에 따라 Dynamic DNS Registration 옵션을 선택합니다.

    DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다. 이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다.

    이 옵션을 사용하려면 DDNS가 등록되어 있어야 합니다.

14. **Next**를 클릭합니다.

Configure Interface Settings 요약 페이지가 나타납니다. 새 시스템 및 인터페이스 상태를 반영한 값이 나열됩니다.

15. **Finish** 및 **OK**를 차례대로 클릭합니다.

링크 페일오버를 위한 가상 인터페이스 생성

링크 페일오버를 위한 가상 인터페이스를 생성하여 페일오버에 사용될 링크를 연결하는 컨테이너로 사용합니다.

페일오버 지원 가상 인터페이스는 보조 인터페이스 그룹을 나타내며, 이 중 하나를 기본 인터페이스로 지정할 수 있습니다. 기본 인터페이스가 작동할 때마다 기본 인터페이스는 활성 인터페이스가 됩니다. 구성 가능한 Down Delay 페일오버 옵션을 사용하면 900밀리초 간격으로 페일오버 지연을 구성할 수 있습니다. 페일오버 지연은 네트워크가 안정적이지 않을 때 여러 페일오버가 발생하지 않도록 합니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. Interfaces 탭에서 **Enabled** 열의 **No**를 클릭하여 가상 인터페이스가 추가된 물리적 인터페이스를 해제합니다.
3. **Create** 메뉴에서 **Virtual Interface**를 선택합니다.
4. Create Virtual Interface 대화상자에서 **veth**란에 가상 인터페이스 이름을 지정합니다.

   가상 인터페이스 이름은 `veth`*x*의의 형태로 입력하며, 여기서 *x*는 고유 ID(일반적으로 한 자리 또는 두 자리 숫자)를 뜻합니다. VLAN 및 IP 별칭이 포함된 전체 가상 인터페이스 이름의 일반적인 형태는 *veth56.3999:199*입니다. 전체 이름의 길이는 최대 15자입니다. 특수 문자는 사용할 수 없습니다. 숫자는 0~4094 범위여야 합니다.

5. **Bonding Type** 목록에서 **Failover**를 선택합니다.
6. 페일오버 구성에 추가할 인터페이스를 선택하고 **Next**를 클릭합니다. 가상 집계 인터페이스는 페일오버에 사용될 수 있습니다.

   Create virtual interface *veth_name* 대화상자가 나타납니다.

7. IP 주소를 입력하거나, IP 주소를 지정하지 않으려면 0을 입력합니다.
8. 넷마스크 또는 접두사를 입력합니다.
9. Speed/Duplex 옵션을 지정합니다.

   속도 및 이중화 설정은 인터페이스를 통한 데이터 전송 속도를 정의합니다.

   - 네트워크 인터페이스 카드가 인터페이스의 회선 속도 및 이중화 설정을 자동 조정하도록 하려면 **Autonegotiate Speed/Duplex**를 선택합니다.
   - 인터페이스 데이터 전송 속도를 수동으로 설정하려면 **Manually configure Speed/Duplex**를 선택합니다.
     - Duplex 옵션은 Half 또는 Full입니다.
     - 나열되는 Speed 옵션은 하드웨어 디바이스의 성능에 따라 제한됩니다. 옵션은 10Mb, 100Mb, 1000Mb 및 10Gb입니다.
     - Half 옵션은 10Mb 및 100Mb 속도에만 사용할 수 있습니다.
     - 1000Mb 및 10Gb 회선 속도에는 Full-Duplex를 사용해야 합니다.
     - Optical 인터페이스에는 Autonegotiate 옵션을 사용해야 합니다.

- Copper 인터페이스의 기본값은 10Gb입니다. Copper 인터페이스를 1000Gb 또는 10Gb 회선 속도로 설정하는 경우 Duplex가 Full-Duplex이어야 합니다.

10. MTU 설정을 지정합니다.
    - 기본값(1500)을 선택하려면 **Default**를 클릭합니다.
    - 다른 설정을 선택하려면 MTU 입력란에 설정을 입력합니다. 전체 네트워크 경로의 구성 요소가 이 옵션의 크기 세트를 지원하는지 확인하십시오.
11. 필요에 따라 Dynamic DNS Registration 옵션을 선택합니다.

    DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다. 이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다.

    이 옵션을 사용하려면 DDNS가 등록되어 있어야 합니다.

    참고

    이 옵션은 이 인터페이스에 DHCP를 비활성화합니다.
12. **Next**를 클릭합니다.

    Configure Interface Settings 요약 페이지가 나타납니다. 새 시스템 및 인터페이스 상태를 반영한 값이 나열됩니다.
13. Interface를 완료하고 **Finish**와 **OK**를 차례로 클릭합니다.

가상 인터페이스 수정

가상 인터페이스를 생성한 후 네트워크 변경에 응답하거나 문제를 해결하기 위해 설정을 업데이트할 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. Interfaces 열에서 인터페이스를 선택하고 **Enabled** 열의 **No**를 클릭하여 가상 인터페이스를 해제합니다. 경고 대화 상자에서 **OK**를 클릭합니다.
3. **Interfaces** 열에서 인터페이스를 선택하고 **Configure**를 클릭합니다.
4. **Configure Virtual Interface** 대화 상자에서 설정을 변경합니다.
5. **Next**와 **Finish**를 차례로 클릭합니다.

VLAN 구성

물리적 인터페이스 또는 가상 인터페이스에서 새 VLAN 인터페이스를 생성합니다.

권장되는 총 VLAN 개수는 80개입니다. 시스템에 의해 더 이상의 생성이 금지되기 전까지 최대 100개(별칭, 물리적 및 가상 인터페이스 수 제외)의 인터페이스를 생성할 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. 인터페이스 표에서 VLAN에 추가하려는 인터페이스를 선택합니다.

   VLAN을 추가하려면 먼저 선택하는 인터페이스에 IP 주소가 구성되어야 합니다.

3. **Create**를 클릭하고 **VLAN**을 선택합니다.
4. Create VLAN 대화 상자에서 **VLAN Id** 입력란에 숫자를 입력하여 VLAN ID를 지정합니다.

   VLAN ID의 범위는 1-4094 사이입니다.

5. IP 주소를 입력하거나, IP 주소를 지정하지 않으려면 0을 입력합니다.

   IP(Internet Protocol) 주소는 인터페이스에 지정된 숫자 레이블입니다. 예: 192.168.10.23.

6. 넷마스크 또는 접두사를 입력합니다.
7. MTU 설정을 지정합니다.

   VLAN MTU는 지정된 물리적 인터페이스 또는 가상 인터페이스에 대해 정의된 MTU보다 작거나 같아야 합니다. 지원하는 물리적 인터페이스 또는 가상 인터페이스에 대해 정의된 MTU가 구성된 VLAN 값 미만으로 감소하는 경우, VLAN 값은 자동으로 지원 인터페이스에 맞춰 감소합니다. 지원 인터페이스에 대한 MTU 값이 구성된 VLAN 값을 초과하여 증가하는 경우, VLAN 값은 변경되지 않습니다.

   - 기본값(1500)을 선택하려면 **Default**를 클릭합니다.
   - 다른 설정을 선택하려면 MTU 입력란에 설정을 입력합니다. DD System Manager에서는 VLAN이 지정된 물리적 인터페이스 또는 가상 인터페이스에 대해 정의된 것보다 큰 MTU 크기를 적용하지 않습니다.

8. Dynamic DNS Registration 옵션을 지정합니다.

   DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다. 이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다.

   이 옵션을 사용하려면 DDNS가 등록되어 있어야 합니다.

9. **Next**를 클릭합니다.

   Create VLAN 요약 페이지가 나타납니다.

10. 구성 설정을 검토하고 **Finish**를 클릭한 다음 **OK**를 클릭합니다.

VLAN 인터페이스 수정

VLAN 인터페이스를 생성한 후 네트워크 변경에 응답하거나 문제를 해결하기 위해 설정을 업데이트할 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. **Interfaces** 열에서 인터페이스의 확인란을 선택하고 **Enabled** 열의 **No**를 클릭하여 VLAN 인터페이스를 해제합니다. 경고 대화 상자에서 **OK**를 클릭합니다.
3. Interfaces 열에서 인터페이스의 확인란을 선택하고 **Configure**를 클릭합니다.
4. **Configure VLAN Interface** 대화 상자에서 설정을 변경합니다.
5. **Next**와 **Finish**를 차례로 클릭합니다.

IP 별칭 구성

IP 별칭은 물리적 인터페이스, 가상 인터페이스 또는 VLAN에 추가 IP 주소를 할당합니다.

시스템에 존재할 수 있는 IP 별칭, VLAN, 물리적 및 가상 인터페이스의 권장되는 총 개수는 80개입니다. 인터페이스는 최대 100개까지 지원되지만 최대 개수에 근접하면 디스플레이가 느려질 수 있습니다.

참고

Data Domain HA 시스템을 사용하는 경우, 생성된 사용자가 액티브 노드에 먼저 로그인하지 않고 대기 노드에 로그인하면 이 사용자가 사용할 기본 별칭이 할당되지 않습니다. 따라서 대기 노드에서 별칭을 사용하려면 사용자가 액티브 노드에 먼저 로그인해야 합니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. **Create**를 클릭하고 **IP Alias**를 선택합니다.

   Create IP Alias 대화 상자가 나타납니다.
3. **IP ALIAS Id** 입력란에 숫자를 입력하여 IP 별칭 ID를 지정합니다.

   범위는 1~4094(포함)입니다.
4. IPv4 또는 IPv6 주소를 입력합니다.
5. IPv4 주소를 입력한 경우 넷마스크 주소를 입력합니다.
6. Dynamic DNS Registration 옵션을 지정합니다.

   DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다. 이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다.

   이 옵션을 사용하려면 DDNS가 등록되어 있어야 합니다.
7. **Next**를 클릭합니다.

   Create IP Alias 요약 페이지가 나타납니다.
8. 구성 설정을 검토하고 **Finish**를 클릭한 다음 **OK**를 클릭합니다.

IP 별칭 인터페이스 수정

IP 별칭을 생성한 후 네트워크 변경 또는 문제 해결을 위해 설정을 업데이트할 수 있습니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. **Interfaces** 열에서 인터페이스의 확인란을 선택하고 **Enabled** 열의 **No**를 클릭하여 IP 별칭 인터페이스를 해제합니다. 경고 대화 상자에서 **OK**를 클릭합니다.
3. **Interfaces** 열에서 인터페이스의 확인란을 선택하고 **Configure**를 클릭합니다.
4. Configure IP Alias 대화 상자에서 IP 별칭 생성 절차에 설명된 것과 같이 설정을 변경합니다.

5. **Next**와 **Finish**를 차례로 클릭합니다.

DDNS에 인터페이스 등록

DDNS(Dynamic DNS)는 DNS(Domain Name System) 서버의 로컬 IP 주소를 등록한 프로토콜입니다.

이 릴리즈에서 DD System Manager는 Windows 모드 DDNS를 지원합니다. UNIX 모드 DDNS를 사용하려면 `net ddns` CLI 명령을 사용합니다. 사용할 수 있는 기능은 다음과 같습니다.

- DDNS 등록 목록에 수동으로 구성된 인터페이스를 등록(추가)합니다.
- DDNS 등록 목록에서 인터페이스를 제거합니다.
- DNS 업데이트를 설정 또는 해제합니다.
- DDNS 등록이 설정되어 있는지 여부를 표시합니다.
- DDNS 등록 목록에 있는 인터페이스를 표시합니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces** > **DDNS Registration**을 선택합니다.
2. DDNS Windows Mode Registration 대화 상자에서 **Add**를 클릭하여 인터페이스를 DDNS에 추가합니다.

   Add Interface 대화 상자가 나타납니다.

   a. **Interface** 필드에 이름을 입력합니다.

   b. **OK**를 클릭합니다.
3. 필요한 경우 DDNS에서 인터페이스를 제거하는 방법:

   a. 제거할 인터페이스를 선택하고 **Remove**를 클릭합니다.

   b. Confirm Remove 대화 상자에서 **OK**를 클릭합니다.
4. DDNS Status를 지정합니다.
   - 이미 등록된 모든 인터페이스에 대해 업데이트를 설정하려면 **Enable**을 선택합니다.
   - DDNS 업데이트에 대해 기본 설정을 선택하려면 **Default**를 클릭합니다.
   - 등록된 인터페이스에 대해 DDNS 업데이트를 해제하려면 **Enable**을 선택 취소합니다.
5. DDNS 등록을 완료하려면 **OK**를 클릭합니다.

인터페이스 제거

DD System Manager를 사용하여 가상, VLAN, IP 별칭 인터페이스를 제거하거나 삭제할 수 있습니다.

가상 인터페이스를 제거하면 시스템에서는 가상 인터페이스가 삭제되고, 연결된 물리적 인터페이스의 연결이 해제되고, 가상 인터페이스에 연결된 모든 VLAN 또는 별칭이 삭제됩니다. VLAN 인터페이스를 삭제하면 OS에서는 해당 OS를 기반으로 생성된 VLAN 및 모든 IP 별칭 인터페이스를 삭제합니다. IP 별칭을 제거하면 OS에서는 해당 별칭 인터페이스만 삭제합니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces**를 선택합니다.
2. 제거할 각 인터페이스(Virtual, VLAN 또는 IP Alias) 옆의 상자를 클릭합니다.

3. **Destroy**를 클릭합니다.
4. **OK**를 클릭하여 확인합니다.

트리 보기에서 인터페이스 계층 보기

Tree View 대화 상자에는 물리적 인터페이스와 가상 인터페이스 간의 연결이 표시됩니다.

절차

1. **Hardware** > **Ethernet** > **Interfaces** > **Tree View**를 선택합니다.
2. Tree View 대화 상자에서 더하기 또는 빼기 상자를 클릭하여 계층을 표시하는 트리 보기를 확장하거나 축소합니다.
3. **Close**를 클릭하여 이 보기를 종료합니다.

일반 네트워크 설정 관리

호스트 이름, 도메인 이름, 검색 도메인, 호스트 매핑 및 DNS 목록에 대한 구성 설정은 모두 Settings 탭에서 관리됩니다.

네트워크 설정 정보 보기

Settings 탭에는 호스트 이름, 도메인 이름, 검색 도메인, 호스트 매핑 및 DNS에 대한 현재 구성이 표시됩니다.

절차

1. **Hardware** > **Ethernet** > **Settings**를 선택합니다.

결과

Settings 탭에는 다음 정보가 표시됩니다.

Host Settings

Host Name
선택한 시스템의 호스트 이름입니다.

Domain Name
선택한 시스템과 연결된 정규화된 도메인 이름입니다.

Search Domain List

Search Domain
선택한 시스템에서 사용하는 검색 도메인 목록입니다. 시스템에서는 호스트 이름에 접미사로 검색 도메인을 적용합니다.

Hosts Mapping

IP Address
확인할 호스트의 IP 주소입니다.

Host Name
IP 주소와 연결된 호스트 이름입니다.

DNS List

DNS IP Address

선택한 시스템과 연결된 현재 DNS IP 주소입니다. 별표(*)는 IP 주소가 DHCP를 통해 할당되었음을 나타냅니다.

DD System Manager 호스트 이름 설정

DD System Manager 호스트 이름과 도메인 이름을 수동으로 구성하거나 DHCP(Dynamic Host Configuration Protocol) 서버로부터 호스트 및 도메인 이름을 자동으로 수신하도록 DD OS를 구성할 수 있습니다.

호스트 이름과 도메인 이름을 수동으로 구성하는 것의 한 가지 장점은 DHCP 서버 및 DHCP 서버로 이어지는 인터페이스에 대한 종속성을 제거할 수 있다는 점입니다. 서비스 중단의 위험을 최소화하기 위해 가능하면 호스트 이름과 도메인 이름을 수동으로 구성하십시오.

호스트 이름과 도메인 이름을 구성할 때는 다음 지침을 고려하십시오.

- 일부 브라우저와 호환되지 않으므로 호스트 이름에 밑줄을 포함시키지 마십시오.
- 복제 및 CIFS 인증은 이름을 변경한 뒤에 재구성해야 합니다.
- 정규화된 이름(도메인 이름 아님) 없이 시스템이 이전에 추가된 경우, 도메인 이름을 변경하려면 영향을 받은 시스템을 제거하고 추가하거나 Search Domain List를 업데이트하여 새 도메인 이름을 포함시켜야 합니다.

절차

1. **Hardware** > **Ethernet** > **Settings**를 선택합니다.
2. **Host Settings** 영역에서 **Edit**를 클릭합니다. Configure Host 대화 상자가 나타납니다.
3. 호스트 이름과 도메인 이름을 수동으로 구성하려면
   a. **Manually configure host**를 선택합니다.
   b. **Hostname** 입력란에 호스트 이름을 입력합니다.
      예: `id##.yourcompany.com`
   c. **Domain Name** 입력란에 도메인 이름을 입력합니다.
      이는 Data Domain 시스템과 연관된 도메인 이름이며 대개는 회사의 도메인 이름입니다. 예: *yourcompany.com*
   d. **OK**를 클릭합니다.
      변경이 적용됨에 따라 진행률 메시지가 표시됩니다.
4. DHCP 서버에서 호스트 이름과 도메인 이름을 가져오려면 **Obtain Settings using DHCP**를 선택하고 **OK**를 클릭합니다.
   최소 한 개의 인터페이스가 DHCP를 사용하도록 구성되어 있어야 합니다.

도메인 검색 목록 관리

도메인 검색 목록을 사용해 시스템이 검색할 수 있는 도메인을 정의합니다.

절차

1. **Hardware** > **Ethernet** > **Settings**를 선택합니다.
2. Search Domain List 영역에서 **Edit**를 클릭합니다.

3. Configure Search Domains 대화 상자를 사용하여 검색 도메인을 추가하려면 다음을 수행합니다.
   a. Add(**+**) 버튼을 클릭합니다.
   b. Add Search Domain 대화 상자의 **Search Domain** 입력란에 이름을 입력합니다.
      예: **`id##.yourcompany.com`**
   c. **OK**를 클릭합니다.
      검색 가능한 도메인의 목록에 새 도메인이 추가됩니다.
   d. **OK**를 클릭하여 변경 내용을 적용하고 Settings 보기로 돌아갑니다.
4. Configure Search Domains 대화 상자를 사용하여 검색 도메인을 제거하려면 다음을 수행합니다.
   a. 제거할 검색 도메인을 선택합니다.
   b. Delete(**X**) 버튼을 클릭합니다.
      선택한 도메인이 검색 가능한 도메인의 목록에서 제거됩니다.
   c. **OK**를 클릭하여 변경 내용을 적용하고 Settings 보기로 돌아갑니다.

호스트 맵 추가 및 삭제

호스트 맵은 IP 주소를 호스트 이름에 연결하여 IP 주소 또는 호스트 이름을 사용해 호스트를 지정할 수 있도록 합니다.

절차

1. **Hardware** > **Ethernet** > **Settings**를 선택합니다.
2. 호스트 맵을 추가하려면 다음을 수행합니다.
   a. Hosts Mapping 영역에서 **Add**를 클릭합니다.
   b. Add Hosts 대화 상자에서 **IP Address** 상자에 호스트의 IP 주소를 입력합니다.
   c. 추가(**+**) 버튼을 클릭합니다.
   d. Add Host 대화 상자에서 **Host Name** 입력란에 호스트 이름을 입력합니다 (예: **`id##.yourcompany.com`**).
   e. **OK**를 클릭하여 새 호스트 이름을 Host Name 목록에 추가합니다.
   f. **OK**를 클릭하여 Settings 탭으로 돌아갑니다.
3. 호스트 맵을 삭제하려면 다음을 수행합니다.
   a. Hosts Mapping 영역에서 삭제할 호스트 매핑을 선택합니다.
   b. 삭제(**X**) 버튼을 클릭합니다.

DNS IP 주소 구성

DNS IP 주소는 시스템에서 호스트 매핑 테이블에 없는 호스트 이름에 대한 IP 주소를 가져올 때 사용할 DNS 서버를 지정합니다.

DNS IP 주소를 수동으로 구성하거나 DHCP 서버에서 IP 주소를 자동으로 수신할 수 있도록 DD OS를 구성할 수 있습니다. DNS IP 주소를 수동으로 구성하는 것의 한 가지 장점은 DHCP 서버 및 DHCP 서버로 이어지는 인터페이스에 대한 종속성을 제거할 수 있다는 점입니다. 서비스 중단의 위험을 최소화하기 위해서는 DNS IP 주소를 수동으로 구성하는 것이 좋습니다.

절차

1. **Hardware** > **Ethernet** > **Settings**를 선택합니다.
2. DNS List 영역에서 **Edit**를 클릭합니다.
3. DNS IP 주소를 수동으로 추가하려면
   a. **Manually configure DNS list**를 선택합니다.
      DNS IP 주소 확인란이 활성화됩니다.
   b. 추가(**+**) 버튼을 클릭합니다.
   c. Add DNS 대화 상자에 추가할 DNS IP 주소를 입력합니다.
   d. **OK**를 클릭합니다.
      DNS IP 주소 목록에 새 IP 주소가 추가됩니다.
   e. **OK**를 클릭하여 변경 내용을 적용합니다.
4. 목록에서 DNS IP 주소를 삭제하려면
   a. **Manually configure DNS list**를 선택합니다.
      DNS IP 주소 확인란이 활성화됩니다.
   b. 삭제하려는 DNS IP 주소를 선택하고 삭제(**X**) 버튼을 클릭합니다.
      DNS IP 주소 목록에서 IP 주소가 제거됩니다.
   c. **OK**를 클릭하여 변경 내용을 적용합니다.
5. DHCP 서버에서 DNS 주소를 가져오려면 **Obtain DNS using DHCP**를 선택하고 **OK**를 클릭합니다.
   최소 한 개의 인터페이스가 DHCP를 사용하도록 구성되어 있어야 합니다.

네트워크 라우트 관리

라우트에서는 localhost(Data Domain 시스템)와 다른 네트워크 또는 호스트 간의 데이터 전송에 사용되는 경로를 결정합니다.

Data Domain 시스템에서는 RIP, EGRP/EIGRP, BGP 등의 네트워크 라우팅 관리 프로토콜을 생성하거나 이러한 프로토콜에 응답하지 않습니다. Data Domain 시스템에 구축되는 유일한 라우팅은 IPv4 정책 기반 라우팅이며, 이 라우팅은 기본 게이트웨이에 대한 경로를 라우팅 테이블당 하나만 허용합니다. 라우팅 테이블과 기본 게이트웨이는 여러 개가 있을 수 있습니다. 라우팅 테이블은 기본 게이트웨이와 동일한 서브넷을 갖는 각 주소에 대해 생성됩니다. 라우팅 규칙은 해당 라우팅 테이블에 대한 테이블을 생성하는 데 사용된 IP 주소와 일치하는 소스 IP 주소를 사용하여 패킷을 보냅니다. 라우팅 테이블과 일치하는 소스 IP 주소가 없는 다른 모든 패킷은 기본 라우팅 테이블로 전송됩니다.

각 라우팅 테이블 내에서 정적 라우트를 추가할 수 있지만 테이블에 대한 패킷에 가져오는 데 소스 라우팅이 사용되기 때문에 작동하는 정적 경로는 각 테이블의 소스 주소가 있는 인터페이스를 사용하는 정적 경로뿐입니다. 그렇지 않은 경우 정적 라우트를 기본 테이블에 배치해야 합니다.

이러한 다른 라우팅 테이블에 대해 수행되는 IPv4 소스 라우팅 외에도 Data Domain 시스템은 기본 라우팅 IPv4 및 IPv6 테이블에 대해 소스 기반 라우팅을 사용합니다. 즉, 여러 인터페이스의 서브넷과 일치하는 아웃바운드 네트워크 패킷은 IP 주소가 패킷의 소스 IP 주소(패킷 발생 주소)와 일치하는 물리적 인터페이스를 통해서만 라우팅됩니다.

IPv6에서는, 여러 인터페이스에 동일한 IPv6 서브넷이 포함되어 있으며 해당 서브넷을 통해 IPv6 주소로 연결되는 경우 정적 라우트를 설정합니다. 보통 동일한 서브넷을 사용하는 IPv4 주소에는 백업용 라우트와 같은 정적 라우트가 필요하지 않습니다. Data

Domain 시스템에서 원격 시스템으로의 연결과 같은 작업에 대해 연결을 허용하기 위해 정적 주소가 필요할 경우가 있습니다.

라우트 지정 항목에서 테이블을 추가하거나 삭제하여 개별 라우팅 테이블에서 정적 라우트를 추가하거나 삭제할 수 있습니다. 이렇게 하여 특정 라우트 테이블을 통해 특정 소스 주소로 패킷을 보내는 규칙을 제공합니다. 이러한 소스 주소를 사용하는 패킷에 정적 라우트가 필요한 경우 해당 IP 주소가 라우팅되는 특정 테이블에 라우트를 추가해야 합니다.

참고

복제용 라우팅과 같이 Data Domain 시스템에서 시작된 연결을 위한 라우팅은 동일한 서브넷의 인터페이스에 사용되는 소스 주소에 따라 달라집니다. 특정 인터페이스에서 특정 대상으로의 트래픽을 강제로 적용하려면(해당 인터페이스가 다른 인터페이스와 동일한 서브넷에 있는 경우라도) 두 시스템 간의 정적 라우팅 항목을 구성합니다. 이 정적 라우팅이 소스 라우팅을 재정의합니다. 소스 주소가 IPv4이고 기본 게이트웨이가 연결되어 있는 경우 정적 라우팅이 필요하지 않습니다. 이 경우 소스 라우팅은 자체 라우팅 테이블을 통해 처리됩니다.

라우트 정보 보기

Routes 탭에는 기본 게이트웨이, 정적 라우트 및 동적 라우트가 표시됩니다.

절차

1. **Hardware** > **Ethernet** > **Routes**를 선택합니다.

결과

Static Routes 영역에 각 정적 라우트를 구성하는 데 사용되는 라우트 사양이 나열됩니다. Dynamic Routes 테이블에 동적으로 할당된 각 라우트에 대한 정보가 나열됩니다.

표 33 Dynamic Routes 열 레이블 설명

항목	설명
Destination	네트워크 트래픽(데이터)이 전송되는 대상 호스트/네트워크입니다.
Gateway	DD 네트워크의 라우터 주소가 표시되거나 게이트웨이가 설정되지 않은 경우 0.0.0.0으로 표시됩니다.
Genmask	대상 넷에 대한 넷마스크입니다. 호스트 대상은 255.255.255.255로, 기본 라우트는 0.0.0.0으로 설정되어 있습니다.
Flags	가능한 플래그는 다음과 같습니다. U - 라우트 실행 중, H - 타겟이 호스트임, G - 게이트웨이 사용, R - 정적 라우팅에 대한 라우트 복원, D - 데몬 또는 리디렉션에 의해 동적으로 설치됨, M - 라우팅 데몬 또는 리디렉션에서 수정됨, A - addrconf에 의해 설치됨, C - 캐시 입력, ! - 라우트 거부
Metric	타겟까지의 거리로 보통 홉으로 계산됩니다. DD OS에서는 사용되지 않으나 라우팅 데몬에서 필요할 수 있습니다.
MTU	물리적(이더넷) 인터페이스의 MTU(Maximum Transfer Unit) 크기입니다.
Window	이 라우트를 통한 TCP 연결에 대한 기본 창 크기입니다.
IRTT	가능한 답변 지연을 기다리지 않고 최상의 TCP 프로토콜 매개 변수를 예측하기 위해 커널에서 사용하는 초기 RTT(Round Trip Time)입니다.
Interface	라우팅 인터페이스와 연결된 인터페이스 이름입니다.

기본 게이트웨이 설정

기본 게이트웨이를 수동으로 구성하거나 DHCP 서버에서 기본 게이트웨이 IP 주소를 자동으로 수신할 수 있도록 DD OS를 구성할 수 있습니다.

기본 게이트웨이를 수동으로 구성하는 것의 한 가지 장점은 DHCP 서버 및 DHCP 서버로 이어지는 인터페이스에 대한 종속성을 제거할 수 있다는 점입니다. 서비스 중단의 위험을 최소화하기 위해 가능하면 기본 게이트웨이 IP 주소를 수동으로 구성하십시오.

절차

1. **Hardware** > **Ethernet** > **Routes**를 선택합니다.
2. 구성하려는 기본 게이트웨이 유형(IPv4 또는 IPv6) 옆의 **Edit**를 클릭합니다.
3. 기본 게이트웨이 주소를 수동으로 구성하려면
   a. **Manually Configure**를 선택합니다.
   b. **Gateway** 입력란에 게이트웨이 주소를 입력합니다.
   c. **OK**를 클릭합니다.
4. DHCP 서버에서 기본 게이트웨이 주소를 가져오려면 **Use DHCP value**를 선택하고 **OK**를 클릭합니다.

   최소 한 개의 인터페이스가 DHCP를 사용하도록 구성되어 있어야 합니다.

정적 라우트 생성

정적 라우트는 시스템에서 통신할 수 있는 대상 호스트 또는 네트워크를 정의합니다.

절차

1. **Hardware** > **Ethernet** > **Routes**를 선택합니다.
2. Static Routes 영역에서 **Create**를 클릭합니다.
3. **Create Routes** 대화 상자에서 정적 라우트를 호스팅할 인터페이스를 선택하고 **Next**를 클릭합니다.
4. Destination을 지정합니다.
   - 대상 네트워크를 지정하려면 **Network**를 선택하고 대상 네트워크의 네트워크 주소와 넷마스크를 입력합니다.
   - 대상 호스트를 지정하려면 **Host**를 선택하고 대상 호스트의 호스트 이름 또는 IP 주소를 입력합니다.
5. 선택적으로 대상 네트워크 또는 호스트에 접속하는 데 사용할 게이트웨이를 지정합니다.
   a. **Specify a gateway for this route**를 선택합니다.
   b. **Gateway** 입력란에 게이트웨이 주소를 입력합니다.
6. 구성을 검토하고 **Next**를 클릭합니다.

   Create Routes Summary 페이지가 나타납니다.
7. **Finish**를 클릭합니다.
8. 프로세스가 완료되면 **OK**를 클릭합니다.

   Route Spec 목록에 새 라우트 사양이 나열됩니다.

정적 라우트 삭제

시스템에서 대상 호스트 또는 네트워크와 더 이상 통신하지 않도록 하려면 정적 라우트를 삭제합니다.

절차

1. **Hardware** > **Ethernet** > **Routes**를 선택합니다.
2. Route Spec 목록에서 삭제할 라우트 사양을 선택합니다.
3. **Delete**를 클릭합니다.
4. **Delete**를 클릭하여 확인한 다음 **Close**를 클릭합니다.

   선택한 라우트 사양이 Route Spec 목록에서 제거됩니다.

시스템 암호 관리

시스템 암호는 Data Domain 시스템을 시스템에 있는 암호화 키로 전송할 수 있도록 하는 키입니다. 암호화 키는 데이터를 보호하고 시스템 키는 암호화 키를 보호합니다.

시스템 암호는 육안으로 확인이 가능하며 이해할 수 있는, 스마트 카드와 유사한 키로 시스템에서 사용할 수 있는 AES 256 암호화 키를 생성하는 데 사용됩니다. 전송 중에 시스템을 도난당하더라도 공격자가 데이터를 쉽게 복구할 수 없습니다. 암호화된 사용자 데이터와 암호화된 키를 복구하는 것만 가능합니다.

암호는 Data Domain 스토리지 서브시스템의 숨겨진 부분에 내부적으로 저장됩니다. 따라서 관리자 개입 없이도 Data Domain 시스템을 부팅하고 데이터 액세스 서비스를 계속할 수 있습니다.

시스템 암호 설정

시스템에서 데이터 암호화를 지원하거나 디지털 인증서를 요청할 수 있도록 하려면 시스템 암호를 설정해야 합니다.

시작하기 전에

최소 시스템 암호 길이는 DD OS를 설치할 때 구성되지 않지만 CLI에서 명령을 사용하여 최소 길이를 설정할 수 있습니다. 암호에 대한 최소 길이가 구성되었는지 확인하려면 `system passphrase option show` CLI 명령을 입력합니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.

   시스템 암호가 설정되지 않은 경우 Passphrase 영역에 **Set Passphrase** 버튼이 나타납니다. 시스템 암호가 구성된 경우 **Change Passphrase** 버튼이 나타나며 사용자는 암호 변경만 수행할 수 있습니다.

2. **Set Passphrase** 버튼을 클릭합니다.

   Set Passphrase 대화 상자가 나타납니다.

3. 상자에 시스템 암호를 입력하고 **Next**를 클릭합니다.

   시스템 암호에 대한 최소 길이가 구성된 경우 입력하는 암호에 최소 문자 수가 포함되어야 합니다.

결과

시스템 암호가 설정되고 **Set Passphrase** 버튼이 **Change Passphrase** 버튼으로 바뀝니다.

시스템 암호 변경

관리자는 실제 암호화 키를 조작하지 않고도 암호를 변경할 수 있습니다. 암호를 간접적으로 변경할 경우 키의 암호가 변경되지만 사용자 데이터나 기본 암호화 키는 영향을 받지 않습니다.

암호를 변경하려면 데이터가 폐기되는 것을 방지하기 위해 두 명의 사용자 인증이 필요합니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. 시스템 암호를 변경하려면 **Change Passphrase**를 클릭합니다.

   Change Passphrase 대화 상자가 나타납니다.

   참고

   암호를 변경하려면 파일 시스템을 해제해야 합니다. 파일 시스템이 실행 중인 경우 해제하라는 메시지가 표시됩니다.

3. 텍스트 필드에 다음을 입력합니다.
   - 보안 책임자 계정(해당 Data Domain 시스템의 보안 사용자 그룹에 속한 권한이 부여된 사용자)의 사용자 이름 및 암호
   - 암호를 변경할 때 현재 암호
   - 새 암호(`system passphrase option set min-length` 명령을 사용하여 구성된 최소 문자 수가 포함되어야 함)
4. **Enable file system now**의 확인란을 클릭합니다.
5. **OK**를 클릭합니다.

   알림

   암호를 세심하게 관리해야 합니다. 암호를 잃어버릴 경우 파일 시스템의 잠금을 해제할 수 없어 데이터에 액세스할 수 없고, 데이터는 영구적으로 손실됩니다.

시스템 액세스 관리

시스템 액세스 관리 기능을 사용하면 로컬 데이터베이스 또는 네트워크 디렉토리의 사용자에 대한 시스템 액세스를 제어할 수 있습니다. 추가 제어를 통해 여러 액세스 수준을 정의하고 시스템에 액세스할 수 있는 프로토콜을 제어할 수 있습니다.

역할 기반 액세스 제어

RBAC(Role-Based Access Control)는 사용자가 시스템에서 액세스할 수 있는 DD System Manager 컨트롤과 CLI 명령을 제어하는 인증 정책입니다.

예를 들어 *admin* 역할이 할당된 사용자는 전체 시스템을 구성하고 모니터링할 수 있는 반면에 *user* 역할이 할당된 사용자는 시스템 모니터링만 수행할 수 있습니다. 사용자가 DD System Manager에 로그인하면 해당 사용자에게 할당된 역할을 기반으로 사용할

수 있도록 허용된 프로그램 기능만 표시됩니다. DD OS를 관리하기 위해 사용할 수 있는 역할은 다음과 같습니다.

admin

admin 역할 사용자는 전체 Data Domain 시스템을 구성하고 모니터링할 수 있습니다. 대부분의 구성 기능 및 명령은 *admin* 역할 사용자만 사용할 수 있습니다. 그러나 일부 기능과 명령의 경우 *security* 역할 사용자의 승인이 있어야 작업이 완료될 수 있습니다.

limited-admin

limited-admin 역할은 Data Domain 시스템을 구성하고 모니터링할 수 있지만 몇 가지 제한 사항이 있습니다. 이 역할이 할당된 사용자는 데이터 삭제 작업을 수행하거나, 레지스트리를 편집하거나, bash 또는 SE 모드를 시작할 수 없습니다.

user

user 역할 사용자는 시스템을 모니터링하고 자신의 암호를 변경할 수 있습니다. *user* 관리 역할이 할당된 사용자는 시스템 상태를 볼 수 있지만 시스템 구성을 변경할 수는 없습니다.

security(보안 책임자)

보안 책임자라고도 하는 *security* 역할 사용자는 다른 보안 책임자를 관리하고, 보안 책임자 승인이 필요한 절차를 승인하며, user 역할 사용자에게 지원되는 모든 작업을 수행할 수 있습니다.

security 역할은 WORM(Write Once Read Many) 규정을 준수하기 위해 제공됩니다. 이 규정에 따라, 전자적으로 저장된 회사 데이터는 eDiscovery와 같은 용도를 위해 변경되지 않은 원래 상태로 보존되어야 합니다. Data Domain에서는 이 기능을 향상시키기 위해 감사 및 로깅 기능이 추가되었습니다. 규정 준수 요건으로 인해 DD Encryption, DD Retention Lock Compliance, 아카이빙 등의 중요한 작업을 관리하기 위한 대부분의 명령 옵션에는 이제 보안 책임자 승인이 필요합니다.

일반적인 시나리오에서 *admin* 역할 사용자가 명령을 실행할 때 보안 책임자 승인이 필요하면 승인을 요청하는 메시지가 표시됩니다. 원래 작업을 진행하려면 명령을 실행한 것과 동일한 콘솔에 보안 책임자가 자신의 사용자 이름과 암호를 입력해야 합니다. 시스템이 보안 책임자 자격 증명을 인식하면 절차가 승인됩니다. 그렇지 않으면 보안 알림이 생성됩니다.

security 역할 사용자에게 적용되는 몇 가지 지침은 다음과 같습니다.

- *sysadmin* 사용자(DD OS 설치 중에 생성된 기본 사용자)만 첫 번째 보안 책임자를 생성할 수 있습니다. 그 후 보안 책임자를 생성할 수 있는 권한이 *sysadmin* 사용자에게서 제거됩니다.
- 첫 번째 보안 책임자가 생성된 후에는 보안 책임자만 다른 보안 책임자를 생성할 수 있습니다.
- 보안 책임자를 생성해도 승인 정책이 활성화되지는 않습니다. 승인 정책을 활성화하려면 보안 책임자가 로그인하여 승인 정책을 활성화해야 합니다.
- 권한과 의무의 분리가 적용됩니다. *admin* 역할 사용자는 보안 책임자 작업을 수행할 수 없으며, 보안 책임자는 시스템 구성 작업을 수행할 수 없습니다.
- 업그레이드 중에 시스템 구성에 보안 책임자가 포함된 경우, 모든 현재 보안 책임자의 목록이 포함된 sec-off-defaults 사용 권한이 생성됩니다.

backup-operator

backup-operator 역할 사용자는 모든 *user* 역할 사용자에게 허용된 모든 작업을 수행할 수 있고, MTree의 스냅샷을 생성할 수 있으며, VTL(Virtual Tape Library)의 요소 간에 테이프를 가져오고 내보내고 이동하고 풀 전체의 테이프를 복제할 수 있습니다.

backup-operator 역할 사용자는 암호가 필요하지 않은 로그인의 SSH 공개 키를 추가하고 삭제할 수도 있습니다. (이 기능은 주로 자동화된 스크립팅에 사용됩니다.) 이 역할 사용자는 CLI 명령 별칭을 추가, 삭제, 재설정 및 조회할 수 있고, 수정된 파일을 동기화할 수 있으며, 복제가 대상 시스템에서 완료될 때까지 기다릴 수 있습니다.

none

none 역할은 DD Boost 인증과 테넌트 유닛 사용자만을 위한 것입니다. *none* 역할 사용자는 Data Domain 시스템에 로그인할 수 있고 자신의 암호를 변경할 수 있지만 운영 시스템을 모니터링, 관리 또는 구성할 수 없습니다. 운영 시스템이 테넌트 유닛으로 분할된 경우 *tenant-admin* 또는 *tenant-user* 역할이 특정 테넌트 유닛과 관련된 사용자의 역할을 정의하는 데 사용됩니다. 테넌트 사용자에게는 운영 시스템에 대한 액세스를 최소화하기 위해 먼저 *none* 역할이 할당된 다음 *tenant-admin* 또는 *tenant-user* 역할이 추가됩니다.

tenant-admin

tenant-admin 역할은 SMT(Secure Multi-Tenancy) 기능이 활성화된 경우 다른(비 테넌트) 역할에 추가될 수 있습니다. *tenant-admin* 사용자는 특정 테넌트 유닛을 구성하고 모니터링할 수 있습니다.

tenant-user

tenant-user 역할은 SMT 기능이 활성화된 경우 다른(비 테넌트) 역할에 추가될 수 있습니다. *tenant-user* 역할 사용자는 특정 테넌트 유닛을 모니터링하고 자신의 암호를 변경할 수 있습니다. *tenant-user* 관리 역할이 할당된 사용자는 테넌트 유닛 상태를 볼 수 있지만 테넌트 유닛 구성을 변경할 수는 없습니다.

IP 프로토콜에 대한 액세스 관리

이 기능은 FTP, FTPS, HTTP, HTTPS, SSH, SCP 및 Telnet 프로토콜에 대한 시스템 액세스를 관리합니다.

IP 서비스 구성 보기

Administrator Access 탭에는 시스템에 액세스하는 데 사용될 수 있는 IP 프로토콜에 대한 구성 상태가 표시됩니다. 관리자만 사용할 수 있는 유일한 프로토콜은 FTP 및 FTPS입니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.

결과

Access Management 페이지에는 Administrator Access, Local Users, Authentication 및 Active Users 탭이 표시됩니다.

표 34 Administrator Access 탭 정보

항목	설명
Passphrase	암호가 설정되지 않은 경우 **Set Passphrase** 버튼이 나타납니다. 암호가 설정된 경우 **Change Passphrase** 버튼이 나타납니다.
Services	시스템에 액세스할 수 있는 서비스/프로토콜의 이름입니다.
Enabled (Yes/No)	서비스의 상태입니다. 서비스가 비활성화된 경우 목록에서 서비스를 선택하고 **Configure**를 클릭하여 서비스를 활성화합니다. 대화상자의 General 탭에 내용을 입력합니다. 서비스가 활성화된 경우에

표 34 Administrator Access 탭 정보 (계속)

항목	설명
	는 목록에서 서비스를 선택하고 **Configure**를 클릭하여 설정을 수정합니다. 대화 상자의 General 탭에서 설정을 편집합니다.
Allowed Hosts	서비스에 액세스할 수 있는 하나 이상의 호스트입니다.
Service Options	목록에서 선택된 서비스에 대한 포트 또는 세션 시간 초과 값입니다.
FTP/FTPS	세션 시간 초과만 설정할 수 있습니다.
HTTP port	HTTP 프로토콜에 대해 열린 포트 번호(기본적으로 포트 80)입니다.
HTTPS port	HTTPS 프로토콜에 대해 열린 포트 번호(기본적으로 포트 443)입니다.
SSH/SCP port	SSH/SCP 프로토콜에 대해 열린 포트 번호(기본적으로 포트 22)입니다.
Telnet	포트 번호를 설정할 수 없습니다.
Session Timeout	접속이 닫히기 전에 허용되는 비활성 기간입니다. 기본값은 Infinite입니다. 즉, 접속이 닫히지 않습니다. 가능하면 세션 시간 초과 최대값을 5분으로 설정하십시오. 대화 상자의 **Advanced** 탭을 사용하여 시간 초과를 초 단위로 설정합니다.

FTP 액세스 관리

관리자는 FTP(File Transfer Protocol)를 통해 Data Domain 시스템의 파일에 액세스할 수 있습니다.

Admin 관리 역할이 할당된 사용자를 대상으로 FTP 또는 FTPS 액세스 권한을 설정할 수 있습니다. FTP 액세스 권한을 통해 admin 사용자 이름과 암호를 일반 텍스트로 네트워크 전체에서 사용할 수 있기 때문에 FTP는 안전한 액세스 방법이 아닙니다. 안전한 액세스 방법으로 FTPS가 권장됩니다. FTP 또는 FTPS 액세스 권한을 설정하면 다른 액세스 방법이 해제됩니다.

참고

admin 관리 역할이 할당된 사용자만 FTP를 사용하여 시스템에 액세스할 수 있습니다.

참고

FTPS 또는 FTP를 통해 Data Domain 시스템에 연결하는 LFTP 클라이언트는 설정된 시간 초과 제한에 도달한 후에 연결이 끊깁니다. 그러나 LFTP 클라이언트는 시간 초과 이후에도 명령을 실행하는 동안에 캐싱된 사용자 이름과 암호를 사용해 다시 연결할 수 있습니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. **FTP**를 선택하고 **Configure**를 클릭합니다.
3. FTP 액세스 권한과 연결할 수 있는 호스트를 관리하려면 General 탭을 선택하고 다음을 수행합니다.
   a. FTP 액세스 권한을 설정하려면 **Allow FTP Access**를 선택합니다.
   b. 모든 호스트가 접속할 수 있도록 설정하려면 **Allow all hosts to connect**를 선택합니다.

c. 선택한 호스트로만 액세스를 제한하려면 **Limit Access to the following systems**를 선택하고 Allowed Hosts 목록을 수정합니다.

참고

정규화된 호스트 이름, IPv4 주소 또는 IPv6 주소를 사용해 호스트를 식별할 수 있습니다.

- 호스트를 추가하려면 추가(**+**) 버튼을 클릭합니다. 호스트 ID를 입력하고 **OK**를 클릭합니다.
- 호스트 ID를 수정하려면 **Hosts** 목록에서 호스트를 선택하고 연필 모양의 편집 버튼을 클릭합니다. 호스트 ID를 변경하고 **OK**를 클릭합니다.
- 호스트 ID를 제거하려면 **Hosts** 목록에서 호스트를 선택하고 Delete(**X**) 버튼을 클릭합니다.

4. 세션 시간 초과를 설정하려면 **Advanced** 탭을 선택하고 초 단위로 시간 초과 값을 입력합니다.

참고

세션 시간 초과 기본값은 Infinite이므로 연결이 끊기지 않습니다.

5. **OK**를 클릭합니다.

FTPS가 설정된 경우 경고 메시지와 함께 계속하려면 **OK**를 클릭하라는 프롬프트가 나타납니다.

FTPS 액세스 관리

관리자는 FTPS(FTP Secure) 프로토콜을 통해 Data Domain 시스템의 파일에 액세스할 수 있습니다.

FTPS는 TLS(Transport Layer Security) 및 SSL(Secure Sockets Layer) 암호화 프로토콜 지원과 같은 FTP 사용에 대한 보안을 추가로 제공합니다. FTPS를 사용할 때는 다음 지침을 고려하십시오.

- admin 관리 역할이 할당된 사용자만 FTPS를 사용하여 시스템에 액세스할 수 있습니다.
- FTPS 액세스를 설정하면 FTP 액세스가 해제됩니다.
- DD OS 5.3 이상을 실행하는 DD 시스템에서 관리되는 DD OS 5.2를 실행하는 DD 시스템의 경우 FTPS가 서비스로 표시되지 않습니다.
- `get` 명령을 실행할 때 치명적인 오류 메시지 `SSL_read: wrong version number lftp`가 나타나면 일치하는 버전의 SSL이 Data Domain 시스템에 설치되어 있지 않고 LFTP 클라이언트에 컴파일되지 않은 것을 나타냅니다. 이러한 경우 동일한 파일에 대해 `get` 명령을 다시 실행해 보는 것도 한 가지 대안입니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. **FTPS**를 선택하고 **Configure**를 클릭합니다.
3. FTPS 액세스와 접속할 수 있는 호스트를 관리하려면 General 탭을 선택하고 다음을 수행합니다.
   a. FTPS 액세스를 설정하려면 **Allow FTPS Access**를 선택합니다.
   b. 모든 호스트가 접속할 수 있도록 설정하려면 **Allow all hosts to connect**를 선택합니다.

c. 선택한 호스트로만 액세스를 제한하려면 **Limit Access to the following systems**를 선택하고 호스트 목록을 수정합니다.

참고

정규화된 호스트 이름, IPv4 주소 또는 IPv6 주소를 사용해 호스트를 식별할 수 있습니다.

- 호스트를 추가하려면 추가(**+**) 버튼을 클릭합니다. 호스트 ID를 입력하고 **OK**를 클릭합니다.
- 호스트 ID를 수정하려면 **Hosts** 목록에서 호스트를 선택하고 연필 모양의 편집 버튼을 클릭합니다. 호스트 ID를 변경하고 **OK**를 클릭합니다.
- 호스트 ID를 제거하려면 **Hosts** 목록에서 호스트를 선택하고 삭제(**X**) 버튼을 클릭합니다.

4. 세션 시간 초과를 설정하려면 **Advanced** 탭을 선택하고 초 단위로 시간 초과 값을 입력합니다.

참고

세션 시간 초과 기본값은 Infinite이므로 연결이 끊기지 않습니다.

5. **OK**를 클릭합니다. FTP가 설정된 경우 경고 메시지와 함께 계속하려면 **OK**를 클릭하라는 프롬프트가 나타납니다.

HTTP 및 HTTPS 액세스 관리

DD System Manager에 대한 브라우저 액세스를 지원하려면 HTTP 또는 HTTPS 액세스가 필요합니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. **HTTP** 또는 **HTTPS**를 선택하고 **Configure**를 클릭합니다.

   Configure HTTP/HTTPS Access 대화 상자가 나타나며 일반 구성, 고급 구성, 인증서 관리 탭이 표시됩니다.
3. 액세스 방법과 접속할 수 있는 호스트를 관리하려면 General 탭을 선택하고 다음을 수행합니다.
   a. 허용하려는 액세스 방법에 해당하는 확인란을 선택합니다.
   b. 모든 호스트가 접속할 수 있도록 설정하려면 **Allow all hosts to connect**를 선택합니다.
   c. 선택한 호스트로만 액세스를 제한하려면 **Limit Access to the following systems**를 선택하고 호스트 목록을 수정합니다.

참고

정규화된 호스트 이름, IPv4 주소 또는 IPv6 주소를 사용해 호스트를 식별할 수 있습니다.

- 호스트를 추가하려면 Add(**+**) 버튼을 클릭합니다. 호스트 ID를 입력하고 **OK**를 클릭합니다.
- 호스트 ID를 수정하려면 **Hosts** 목록에서 호스트를 선택하고 연필 모양의 편집 버튼을 클릭합니다. 호스트 ID를 변경하고 **OK**를 클릭합니다.

- 호스트 ID를 제거하려면 **Hosts** 목록에서 호스트를 선택하고 삭제(**X**) 버튼을 클릭합니다.

4. 시스템 포트 및 세션 시간 초과 값을 구성하려면 **Advanced** 탭을 선택하고 양식을 작성합니다.
   - **HTTP Port** 입력란에 포트 번호를 입력합니다. 기본적으로 Port 80이 지정되어 있습니다.
   - **HTTPS Port** 입력란에 숫자를 입력합니다. 기본적으로 Port 443이 지정되어 있습니다.
   - **Session Timeout** 입력란에 연결을 종료하기 전 경과 시간을 초 단위로 입력합니다. 최소 단위는 60초이며 최대 단위는 31,536,000초(1년)입니다.

   참고

   세션 시간 초과 기본값은 10,800초입니다.

5. **OK**를 클릭합니다.

HTTP 및 HTTPS의 호스트 인증서 관리

호스트 인증서를 사용하면 관리 세션을 설정할 때 브라우저에서 시스템의 ID를 확인할 수 있습니다.

HTTP 및 HTTPS의 호스트 인증서 요청

DD System Manager를 사용해 CA(Certificate Authority)에 전달할 호스트 인증서 요청을 생성할 수 있습니다.

참고

CSR을 생성하려면 먼저 시스템 암호(시스템 암호 세트)를 구성해야 합니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. Services 영역에서 **HTTP** 또는 **HTTPS**를 선택하고 **Configure**를 클릭합니다.
3. **Certificate** 탭을 선택합니다.
4. 추가를 클릭합니다.

   이 절차의 앞부분에서 선택한 프로토콜을 위한 대화 상자가 나타납니다.

5. **Generate the CSR for this Data Domain system**을 클릭합니다.

   CSR 양식을 표시하기 위해 대화 상자가 확장됩니다.

   참고

   DD OS는 한 번에 하나의 활성 CSR을 지원합니다. CSR이 생성된 후에는 **Generate the CSR for this Data Domain system** 링크가 **Download the CSR for this Data Domain system** 링크로 바뀝니다. CSR을 삭제하려면 `adminaccess certificate cert-signing-request delete` CLI 명령을 사용하십시오.

6. CSR 양식을 작성하고 **Generate and download a CSR**을 클릭합니다.

CSR 파일이 다음 경로에 저장됩니다./ddvar/certificates/CertificateSigningRequest.csr . 시스템에서 CSR을 CA로 보낼 수 있는 컴퓨터로 CSR 파일을 전송하려면 SCP, FTP 또는 FTPS를 사용합니다.

HTTP 및 HTTPS의 호스트 인증서 추가

DD System Manager를 사용해 호스트 인증서를 시스템에 추가할 수 있습니다.

절차

1. 호스트 인증서를 요청하지 않은 경우 인증 기관에 요청하십시오.
2. 호스트 인증서를 받으면 DD Service Manager를 실행하는 컴퓨터로 복사하거나 이동합니다.
3. **Administration** > **Access** > **Administrator Access**를 선택합니다.
4. Services 영역에서 **HTTP** 또는 **HTTPS**를 선택하고 **Configure**를 클릭합니다.
5. **Certificate** 탭을 선택합니다.
6. **추가**를 클릭합니다.

   이 절차의 앞부분에서 선택한 프로토콜을 위한 대화 상자가 나타납니다.

7. .p12 파일로 호스트 인증서를 추가하려면 다음을 수행합니다.
   a. **I want to upload the certificate as a .p12 file**을 선택합니다.
   b. **Password** 입력란에 암호를 입력합니다.
   c. **Browse**를 클릭하고 시스템에 업로드할 호스트 인증서 파일을 선택합니다.
   d. **Add**를 클릭합니다.
8. .pem 파일로 호스트 인증서를 추가하려면 다음을 수행합니다.
   a. **I want to upload the public key as a .pem file and use a generated private key**를 선택합니다.
   b. **Browse**를 클릭하고 시스템에 업로드할 호스트 인증서 파일을 선택합니다.
   c. **Add**를 클릭합니다.

HTTP 및 HTTPS의 호스트 인증서 삭제

DD OS는 HTTP 및 HTTPS용으로 하나의 호스트 인증서를 지원합니다. 현재 시스템에서 호스트 인증서를 사용 중인 경우 다른 호스트 인증서를 사용하려면 현재 인증서를 삭제한 다음 새 인증서를 추가해야 합니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. Services 영역에서 **HTTP** 또는 **HTTPS**를 선택하고 **Configure**를 클릭합니다.
3. **Certificate** 탭을 선택합니다.
4. 삭제할 인증서를 선택합니다.
5. **Delete**를 클릭하고 **OK**를 클릭합니다.

SSH 및 SCP 액세스 관리

SSH는 SCP(Secure Copy)를 사용하거나 사용하지 않고 시스템 CLI에 대한 네트워크 액세스를 지원하는 보안 프로토콜입니다. DD System Manager에서 SSH 프로토콜을 사용한 시스템 액세스를 설정할 수 있습니다. SCP에는 SSH가 필요하므로 SSH가 해제되면 SCP가 자동으로 해제됩니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.
2. **SSH** 또는 **SCP**를 선택하고 **Configure**를 클릭합니다.
3. 액세스 방법과 접속할 수 있는 호스트를 관리하려면 **General** 탭을 선택합니다.
   a. 허용하려는 액세스 방법에 해당하는 확인란을 선택합니다.
   b. 모든 호스트가 접속할 수 있도록 설정하려면 **Allow all hosts to connect**를 선택합니다.
   c. 선택한 호스트로만 액세스를 제한하려면 **Limit Access to the following systems**를 선택하고 호스트 목록을 수정합니다.

   참고

   정규화된 호스트 이름, IPv4 주소 또는 IPv6 주소를 사용해 호스트를 식별할 수 있습니다.

   - 호스트를 추가하려면 추가(**+**) 버튼을 클릭합니다. 호스트 ID를 입력하고 **OK**를 클릭합니다.
   - 호스트 ID를 수정하려면 **Hosts** 목록에서 호스트를 선택하고 연필 모양의 편집 버튼을 클릭합니다. 호스트 ID를 변경하고 **OK**를 클릭합니다.
   - 호스트 ID를 제거하려면 **Hosts** 목록에서 호스트를 선택하고 삭제(**X**) 버튼을 클릭합니다.
4. 시스템 포트 및 세션 시간 초과 값을 구성하려면 **Advanced** 탭을 클릭합니다.
   - **SSH/SCP** Port 텍스트 입력란에 포트 번호를 입력합니다. 기본적으로 Port 22가 지정되어 있습니다.
   - **Session Timeout** 입력란에 연결을 종료하기 전 경과 시간을 초 단위로 입력합니다.

   참고

   세션 시간 초과 기본값은 Infinite이므로 연결이 끊기지 않습니다.

   참고

   기본값으로 되돌리려면 **Default**를 클릭합니다.
5. **OK**를 클릭합니다.

Telnet 액세스 관리

Telnet은 시스템 CLI에 대한 네트워크 액세스를 가능하게 하는 비보안 프로토콜입니다.

참고

Telnet 액세스를 통해 사용자 이름과 암호가 일반 텍스트로 네트워크를 교차할 수 있으므로 Telnet은 비보안 액세스 방법이 됩니다.

절차

1. **Administration** > **Access** > **Administrator Access**를 선택합니다.

2. **Telnet**을 선택하고 **Configure**를 클릭합니다.
3. Telnet 액세스 및 접속 가능 호스트를 관리하려면 **General** 탭을 선택합니다.
   a. Telnet 액세스를 설정하려면 **Allow Telnet Access**를 선택합니다.
   b. 모든 호스트가 접속할 수 있도록 설정하려면 **Allow all hosts to connect**를 선택합니다.
   c. 선택한 호스트로만 액세스를 제한하려면 **Limit Access to the following systems**를 선택하고 호스트 목록을 수정합니다.

   참고

   정규화된 호스트 이름, IPv4 주소 또는 IPv6 주소를 사용해 호스트를 식별할 수 있습니다.

   - 호스트를 추가하려면 Add(**+**) 버튼을 클릭합니다. 호스트 ID를 입력하고 **OK**를 클릭합니다.
   - 호스트 ID를 수정하려면 **Hosts** 목록에서 호스트를 선택하고 연필 모양의 편집 버튼을 클릭합니다. 호스트 ID를 변경하고 **OK**를 클릭합니다.
   - 호스트 ID를 제거하려면 **Hosts** 목록에서 호스트를 선택하고 삭제(**X**) 버튼을 클릭합니다.
4. 세션 시간 초과를 설정하려면 Advanced 탭을 선택하고 초 단위로 시간 초과 값을 입력합니다.

   참고

   세션 시간 초과 기본값은 Infinite이므로 연결이 끊기지 않습니다.

5. **OK**를 클릭합니다.

로컬 사용자 계정 관리

로컬 사용자는 Windows Active Directory, Windows 워크그룹 또는 NIS 디렉토리에서 정의되지 않고 Data Domain 시스템에 구성된 사용자 계정(사용자 이름 및 암호)입니다.

트러스트된 도메인이 구성되면 해당 도메인에 속한 사용자는 트러스트된 도메인이 오프라인 상태인 경우에도 Data Domain 시스템에 로그인할 수 있게 됩니다.

UID 충돌: 로컬 사용자 계정 및 NIS 사용자 계정

NIS 환경에서 Data Domain 시스템을 설정할 때는 로컬 사용자 계정과 NIS 사용자 계정 간에 UID 충돌이 발생할 수 있다는 점에 유의해야 합니다.

Data Domain 시스템의 로컬 사용자 계정은 UID 500에서 시작합니다. 충돌을 방지하려면 잠재적 로컬 계정의 크기를 고려하여 NIS 사용자에 대한 허용 가능한 UID 범위를 정의하십시오.

로컬 사용자 정보 보기

로컬 사용자는 Active Directory, 워크그룹 또는 UNIX가 아니라 시스템에 정의된 사용자 계정을 의미합니다. 로컬 사용자의 사용자 이름, 관리 역할, 로그인 상태 및 타겟 해제 날짜를 표시할 수 있습니다. 또한 사용자의 암호 제어 및 사용자가 액세스할 수 있는 테넌트 유닛도 표시할 수 있습니다.

참고

사용자 인증 모듈은 GMT(Greenwich Mean Time)를 사용합니다. 사용자 계정 및 암호가 올바르게 만료되도록 하려면 타겟 현지 시간에 해당하는 GMT를 사용하도록 설정을 구성하십시오.

절차

1. **Administration** > **Access** > **Local Users**를 선택합니다.

   Local Users 보기가 나타나고 Local Users 표와 Detailed Information 영역이 표시됩니다.

   표 35 Local user 목록 열 레이블 설명

항목	설명
Name	시스템에 추가된 사용자 ID입니다.
Management Role	표시되는 역할은 admin, user, security, backup-operator 또는 none입니다. 이 탭에서 테넌트 사용자 역할은 *none*으로 표시됩니다. 할당된 테넌트 역할을 보려면 사용자를 선택하고 Detailed Information 영역에서 역할을 확인하십시오.
Status	• Active - 계정에 대한 사용자 액세스가 허용됩니다. • Disabled - 계정이 관리상의 이유로 해제되었거나 현재 날짜가 계정 만료 날짜 이후이거나 잠긴 계정의 암호를 갱신해야 하기 때문에 계정에 대한 사용자 액세스가 거부됩니다. • Locked - 암호가 만료되었기 때문에 사용자 액세스가 거부됩니다.
Disable Date	계정이 해제되도록 설정된 날짜입니다.
Last Login From	사용자가 마지막으로 로그인한 위치입니다.
Last Login Time	사용자가 마지막으로 로그인한 시간입니다.

   참고

   admin 또는 보안 책임자 역할로 구성된 사용자 계정은 모든 사용자를 볼 수 있습니다. 다른 역할의 사용자는 자신의 사용자 계정만 볼 수 있습니다.

2. 사용자 목록에서 확인할 사용자를 선택합니다.

   선택한 사용자에 대한 정보가 Detailed Information 영역에 표시됩니다.

   표 36 자세한 사용자 정보, 행 레이블 설명

항목	설명
Password Last Changed	암호가 마지막으로 변경된 날짜입니다.
Minimum Days Between Change	사용자 암호 변경 주기의 최소 일수입니다. 기본값은 0입니다.
Maximum Days Between Change	사용자 암호 변경 주기의 최대 일수입니다. 기본값은 90입니다.

표 36 자세한 사용자 정보, 행 레이블 설명 (계속)

항목	설명
Warn Days Before Expire	사용자에게 알림을 전송할 암호 만료 전 일수입니다. 기본값은 7입니다.
Disable Days After Expire	암호가 만료된 후 사용자 계정이 비활성화되기까지의 일수입니다. 기본값은 Never입니다.

참고

기본값은 암호 정책의 초기 기본값입니다. 시스템 관리자(admin 역할)는 **More Tasks** > **Change Login Options**를 선택해 기본값을 변경할 수 있습니다.

로컬 사용자 생성

외부 디렉토리가 아닌 로컬 시스템에서 액세스를 관리하려는 경우 로컬 사용자를 생성합니다. Data Domain 시스템은 최대 500개의 로컬 사용자 계정을 지원합니다.

절차

1. **Administration** > **Access** > **Local Users**를 선택합니다.

   Local Users 보기가 나타납니다.

2. **Create**를 클릭하여 새 사용자를 만듭니다.

   Create User 대화 상자가 나타납니다.

3. General 탭에 사용자 정보를 입력합니다.

   표 37 Create User 대화 상자, 일반 컨트롤

항목	설명
User	사용자 ID 또는 이름입니다.
Password	사용자 암호입니다. 기본 암호를 설정하면 사용자가 나중에 변경할 수 있습니다.
Verify Password	사용자 암호를 다시 입력합니다.
Management Role	사용자에게 할당된 역할로, admin, user, security, backup-operator 또는 none이 될 수 있습니다. 참고 sysadmin 사용자(DD OS 설치 중에 생성된 기본 사용자)만 첫 번째 security 역할 사용자를 생성할 수 있습니다. 첫 번째 security 역할 사용자가 생성된 후에는 security 역할 사용자가 다른 security 역할 사용자를 생성할 수 있습니다.
Force Password Change	사용자가 DD System Manager 또는 CLI에 SSH 또는 Telnet으로 처음 로그인할 때 암호를 변경하도록 하려면 이 확인란을 선택합니다.

최소 암호 길이의 기본값은 6자입니다. 사용자 암호에 필요한 최소 문자 클래스의 기본값은 1입니다. 허용되는 문자 클래스는 다음과 같습니다.

- 소문자(a-z)

- 대문자(A-Z)
- 숫자(0-9)
- 특수 문자($, %, #, + 등)

참고

sysadmin은 기본 admin 역할 사용자로, 삭제하거나 수정할 수 없습니다.

4. 암호 및 계정 만료를 관리하려면 Advanced 탭을 선택하고 다음 표에 설명된 컨트롤을 사용합니다.

표 38 Create User 대화 상자, 고급 컨트롤

항목	설명
Minimum Days Between Change	사용자 암호 변경 주기의 최소 일수입니다. 기본값은 0입니다.
Maximum Days Between Change	사용자 암호 변경 주기의 최대 일수입니다. 기본값은 90입니다.
Warn Days Before Expire	사용자에게 알림을 전송할 암호 만료 전 일수입니다. 기본값은 7입니다.
Disable Days After Expire	암호가 만료된 후 사용자 계정이 비활성화되기까지의 일수입니다. 기본값은 Never입니다.
Disable account on the following date	확인란을 선택하고 이 계정을 비활성화할 날짜(mm/dd/yyyy)를 입력합니다. 달력을 클릭하여 날짜를 선택해도 됩니다.

5. **OK**를 클릭합니다.

참고

참고: admin 역할의 사용자가 **More Tasks** > **Change Login Options**에서 기본 암호 정책을 변경할 경우 정책이 변경될 수 있습니다. 기본값은 암호 정책의 초기 기본값입니다.

로컬 사용자 프로필 수정

사용자를 생성한 후 DD System Manager를 사용해 사용자 구성을 수정할 수 있습니다.

절차

1. **Administration** > **Access** > **Local Users**를 선택합니다.

   Local Users 보기가 나타납니다.

2. 목록에서 사용자 이름을 클릭합니다.
3. 사용자 계정을 변경하려면 **Modify**를 클릭합니다.

   Modify User 대화 상자가 나타납니다.
4. General 탭의 정보를 업데이트합니다.

참고

SMT가 설정되고 역할이 없는 상태에서 다른 역할로의 역할 변경이 요청된 경우 변경 요청은 사용자가 관리 사용자로 테넌트 유닛에 할당되지 않았고, 기본 테넌트 유닛 세트가 있는 DD Boost 사용자가 아니며, 테넌트 유닛에 할당된 스토리지 유닛의 소유자가 아닌 경우에만 허용됩니다.

참고

스토리지 유닛을 소유하고 있지 않은 DD Boost 사용자의 역할을 변경하려면 DD Boost 사용자로 역할 할당을 해제하고 사용자 역할을 변경한 다음 DD Boost 사용자로 역할을 다시 할당합니다.

표 39 Modify User 대화 상자, 일반 컨트롤

항목	설명
User	사용자 ID 또는 이름입니다.
Role	목록에서 역할을 선택합니다.

5. Advanced 탭의 정보를 업데이트합니다.

표 40 Modify User 대화 상자, 고급 컨트롤

항목	설명
Minimum Days Between Change	사용자 암호 변경 주기의 최소 일수입니다. 기본값은 0입니다.
Maximum Days Between Change	사용자 암호 변경 주기의 최대 일수입니다. 기본값은 90입니다.
Warn Days Before Expire	사용자에게 알림을 전송할 암호 만료 전 일수입니다. 기본값은 7입니다.
Disable Days After Expire	암호가 만료된 후 사용자 계정이 비활성화되기까지의 일수입니다. 기본값은 Never입니다.

6. **OK**를 클릭합니다.

로컬 사용자 삭제

사용자 역할을 기준으로 특정 사용자를 삭제할 수 있습니다. 선택한 사용자 중 한 명을 삭제할 수 없는 경우 Delete 버튼이 비활성화됩니다.

sysadmin 사용자는 삭제할 수 없습니다. Admin 사용자는 보안 책임자를 삭제할 수 없습니다. 보안 책임자만 다른 보안 책임자를 삭제 및 설정, 해제할 수 있습니다.

절차

1. **Administration** > **Access** > **Local Users**를 선택합니다.

   Local Users 보기가 나타납니다.

2. 목록에서 사용자 이름을 하나 이상 클릭합니다.
3. **Delete**을 클릭해 사용자 계정을 삭제합니다.

   Delete User 대화 상자가 나타납니다.

4. **OK** 및 **Close**를 차례로 클릭합니다.

로컬 사용자 활성화 및 비활성화

관리 사용자는 sysadmin 사용자 및 보안 역할의 사용자를 제외한 모든 사용자를 활성화하거나 비활성화할 수 있습니다. sysadmin 사용자는 비활성화할 수 없습니다. 보안 책임자만 다른 보안 책임자를 활성화하거나 비활성화할 수 있습니다.

절차

1. **Administration** > **Access** > **Local Users**를 선택합니다.

   Local Users 보기가 나타납니다.

2. 목록에서 사용자 이름을 하나 이상 클릭합니다.
3. 사용자 계정을 활성화 또는 비활성화하려면 **Enable** 또는 **Disable**을 클릭합니다.

   Enable or Disable User 대화 상자가 나타납니다.

4. **OK** 및 **Close**를 차례로 클릭합니다.

보안 인증 활성화

Data Domain 시스템 CLI(Command Line Interface)를 사용하여 보안 인증 정책을 활성화 및 비활성화할 수 있습니다.

이 절차에 사용되는 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

참고

DD Retention Lock Compliance 라이센스가 설치되어 있어야 합니다. 사용자는 DD Retention Lock Compliance 시스템에 대한 인증 정책을 비활성화할 권한이 없습니다.

절차

1. 보안 책임자의 사용자 이름과 암호를 사용하여 CLI에 로그인합니다.
2. 보안 책임자 인증 정책을 활성화하려면 다음을 입력합니다. `# authorization policy set security-officer enabled`

사용자 암호 변경

사용자를 생성한 후 DD System Manager를 사용해 사용자 암호를 변경할 수 있습니다. 개별 사용자도 자신의 암호를 변경할 수 있습니다.

절차

1. **Administration** > **Access** > **Local Users**를 클릭합니다.

   로컬 사용자 보기가 표시됩니다.

2. 목록에서 사용자 이름을 클릭합니다.
3. 사용자 암호를 변경하려면 **Change Password**를 클릭합니다.

   Change Password 대화 상자가 표시됩니다.

4. 이전 암호를 **Old Password** 상자에 입력합니다.
5. 새 암호를 **New Password** 상자에 입력합니다.
6. 새 암호를 **Verify New Password** 상자에 다시 입력합니다.
7. **OK**를 클릭합니다.

"admin" 역할의 사용자만 다른 사용자의 암호를 변경할 수 있습니다. 관리자는 `user change password [<user>]` 명령을 실행하여 CLI에서 다른 사용자의 암호를 변경할 수 있습니다.

참고

보안상의 이유로 "admin" 역할이 있는 사용자는 다른 "admin" 사용자의 암호를 변경할 수 없습니다. 다른 사용자로 로그인하여 "admin" 사용자 암호를 변경해야 하는 경우 지원 요청 또는 지원 채팅 요청을 작성하여 DELL EMC 지원 센터에 문의하십시오.

암호 정책 및 로그인 제어 수정

암호 정책 및 로그인 제어는 모든 사용자에 대한 로그인 요구 사항을 정의합니다. 관리자는 암호 변경 주기, 유효한 암호 생성에 필요한 조건 및 잘못된 로그인 시도에 대한 시스템 응답을 지정할 수 있습니다.

절차

1. **Administration** > **Access**를 선택합니다.
2. **More Tasks** > **Change Login Options**를 선택합니다.

   Change Login Options 대화 상자가 나타납니다.

3. 각 옵션에 대한 상자에 새 구성을 지정합니다. 기본값을 선택하려면 해당하는 옵션 옆의 **Default**를 클릭합니다.
4. **OK**를 클릭하여 암호 설정을 저장합니다.

Change Login Options 대화 상자

암호 정책을 설정하고 최대 로그인 시도 및 잠금 기간을 지정하려면 이 대화 상자를 사용합니다.

표 41 Change Login Options 대화 상자 컨트롤

항목	설명
Minimum Days Between Change	사용자 암호 변경 주기의 최소 일수입니다. 이 값은 **Maximum Days Between Change** 값에서 **Warn Days Before Expire** 값을 뺀 값보다 작아야 합니다. 기본 설정은 0입니다.
Maximum Days Between Change	사용자 암호 변경 주기의 최대 일수입니다. 최소값은 1입니다. 기본값은 90입니다.
Warn Days Before Expire	사용자에게 알림을 전송할 암호 만료 전 일수입니다. 이 값은 **Maximum Days Between Change** 값에서 **Minimum Days Between Change** 값을 뺀 값보다 작아야 합니다. 기본 설정은 7입니다.
Disable Days After Expire	암호가 만료되면 시스템이 이 옵션에 지정된 일 수를 바탕으로 사용자 계정을 비활성화합니다. 유효한 항목은 *never* 또는 0보다 크거나 같은 수입니다. 기본 설정은 never입니다.
Minimum Length of Password	요구되는 최소 암호 길이이며 기본값은 6입니다.
Minimum Number of Character Classes	사용자 암호에 요구되는 문자 클래스의 최소 개수이며 기본값은 1입니다. 문자 클래스에는 다음이 포함됩니다.

표 41 Change Login Options 대화 상자 컨트롤 (계속)

항목	설명
	• 소문자(a-z) • 대문자(A-Z) • 숫자(0-9) • 특수 문자($, %, #, + 등)
Lowercase Character Requirement	1개 이상의 소문자에 대한 요구 사항을 활성화 또는 비활성화합니다. 기본 설정은 비활성화입니다.
Uppercase Character Requirement	1개 이상의 대문자에 대한 요구 사항을 활성화 또는 비활성화합니다. 기본 설정은 비활성화입니다.
One Digit Requirement	1개 이상의 숫자에 대한 요구 사항을 활성화 또는 비활성화합니다. 기본 설정은 비활성화입니다.
Special Character Requirement	1개 이상의 특수 문자에 대한 요구 사항을 활성화 또는 비활성화합니다. 기본 설정은 비활성화입니다.
Max Consecutive Character Requirement	최대 3개의 반복 문자에 대한 요구 사항을 활성화 또는 비활성화합니다. 기본 설정은 비활성화입니다.
차단할 이전 암호 수	저장된 암호의 수를 지정합니다. 범위는 0부터 24까지이고, 기본 설정은 1입니다. 참고 이 설정을 줄일 경우 저장된 암호 목록은 다음에 암호를 변경하기 전까지 그대로 유지됩니다. 예를 들어 이 설정을 4에서 3으로 변경할 경우 다음에 암호를 변경하기 전까지 최근 4개의 암호가 저장됩니다.
Maximum login attempts	사용자 계정에 강제적(Mandatory) 잠금이 적용되기 전까지 시도할 수 있는 최대 로그인 횟수를 지정합니다. 이 제한은 sysadmin을 포함하여 모든 사용자 계정에 적용됩니다. 잠긴 사용자는 계정이 잠겨 있는 동안 로그인할 수 없습니다. 범위는 4부터 10까지이고, 기본값은 4입니다.
Unlock timeout(초)	최대 로그인 시도 횟수를 넘은 후 사용자 계정이 잠기는 시간을 지정합니다. Unlock timeout에 구성된 시간이 지나면 사용자가 로그인을 시도할 수 있습니다. 범위는 120초부터 600초까지이고 기본 기간은 120초입니다.
최대 활성 로그인	허용할 활성 로그인의 최대 수를 지정합니다. 기본값은 100입니다.

디렉토리 사용자 및 그룹 관리

DD System Manager를 사용해 Windows Active Directory, Windows 워크그룹 및 NIS 사용자 및 그룹의 시스템 액세스를 관리할 수 있습니다. Kerberos 인증은 CIFS 및 NFS 클라이언트에서 사용할 수 있습니다.

Active Directory 및 Kerberos 정보 보기

Active Directory Kerberos 구성은 CIFS 및 NFS 클라이언트에서 인증에 사용할 방식을 결정합니다. 이 구성은 Active Directory/Kerberos Authentication 패널에 표시됩니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
2. Active Directory/Kerberos Authentication 패널을 확장합니다.

표 42 Active Directory/Kerberos Authentication 레이블 설명

항목	설명
Mode	인증 모드의 유형입니다. Windows/Active Directory 모드에서 CIFS 클라이언트는 Active Directory 및 Kerberos 인증을 사용하고 NFS 클라이언트는 Kerberos 인증을 사용합니다. Unix 모드에서 CIFS 클라이언트는 워크그룹 인증(Kerberos 사용 안 함)을 사용하고 NFS 클라이언트는 Kerberos 인증을 사용합니다. Disabled 모드에서는 Kerberos 인증이 해제되고 CIFS 클라이언트는 워크그룹 인증을 사용합니다.
Realm	워크그룹 또는 Active Directory의 영역 이름입니다.
DDNS	Dynamic Domain Name System의 설정 여부를 나타냅니다.
Domain Controllers	워크그룹 또는 Active Directory의 도메인 컨트롤러 이름입니다.
Organizational Unit	워크그룹 또는 Active Directory의 조직 단위 이름입니다.
CIFS Server Name	사용 중인 CIFS 서버의 이름입니다(Windows 모드 전용).
WINS Server	사용 중인 WINS 서버의 이름입니다(Windows 모드 전용).
Short Domain Name	도메인의 축약된 이름입니다.
NTP	설정/해제(UNIX 모드 전용)
NIS	설정/해제(UNIX 모드 전용)
Key Distribution Center	사용 중인 KDC의 호스트 이름 또는 IP입니다(UNIX 모드 전용).
Active Directory Administrative Access	설정/해제: 클릭하여 Active Directory(Windows) 그룹에 대한 관리 액세스를 설정하거나 해제합니다.

표 43 Active Directory 관리 그룹 및 역할

항목	설명
Windows Group	Windows 그룹의 이름입니다.
Management Role	그룹의 역할(admin, user 등)입니다.

Active Directory 및 Kerberos 인증 구성

Active Directory 인증을 구성하면 Data Domain 시스템이 Windows Active Directory 영역에 포함됩니다. CIFS 클라이언트와 NFS 클라이언트는 Kerberos 인증을 사용합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. Active Directory/Kerberos Authentication 패널을 확장합니다.
3. Mode 옆의 **Configure...**를 클릭하여 구성 마법사를 시작합니다.

   Active Directory/Kerberos Authentication 대화 상자가 나타납니다.

4. **Windows/Active Directory**를 선택하고 **Next**를 클릭합니다.
5. 시스템의 전체 영역 이름(예: domain1.local), Data Domain 시스템의 사용자 이름 및 암호를 입력합니다. 그런 후 **다음**을 클릭합니다.

   참고

   전체 영역 이름을 사용합니다. 도메인에 시스템을 연결할 수 있는 충분한 권한을 사용자에게 할당하십시오. 사용자 이름과 암호는 Active Directory 도메인에 대한 Microsoft 요구 사항과 호환되어야 합니다. 이 사용자에게는 이 도메인에서 계정을 생성할 수 있는 사용 권한도 할당되어야 합니다.

6. 기본 CIFS 서버 이름을 선택하거나 **Manual**을 선택하고 CIFS 서버 이름을 입력합니다.
7. 도메인 컨트롤러를 선택하려면 **Automatically assign**을 선택하거나 **Manual**을 선택하고 도메인 컨트롤러 이름을 최대 3개까지 입력합니다.

   정규화된 도메인 이름, 호스트 이름 또는 IP(IPv4 또는 IPv6) 주소를 입력할 수 있습니다.
8. 조직 단위를 선택하려면 **Use default Computers**를 선택하거나 **Manual**을 선택하고 조직 단위 이름을 입력합니다.

   참고

   계정이 새 조직 단위로 이동합니다.

9. **Next**를 클릭합니다.

   구성에 대한 Summary 페이지가 나타납니다.
10. **Finish**를 클릭합니다.

    Authentication 보기에 구성 정보가 표시됩니다.
11. 관리 액세스를 설정하려면 **Active Directory Administrative Access** 오른쪽에 있는 **Enable**을 클릭합니다.

인증 모드 선택

선택한 인증 모드에 따라 Active Directory, 워크그룹 및 Kerberos 인증을 사용한 CIFS 및 NFS 클라이언트의 인증 방식이 달라집니다.

DD OS는 다음 인증 옵션을 지원합니다.

- Disabled: CIFS 및 NFS 클라이언트에 대해 Kerberos 인증이 해제됩니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.
- Windows/Active Directory: CIFS 및 NFS 클라이언트에 대해 Kerberos 인증이 설정됩니다. CIFS 클라이언트에서는 Active Directory 인증이 사용됩니다.
- Unix: NFS 클라이언트에 대해서만 Kerberos 인증이 설정됩니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.

Active Directory용 관리 그룹 관리

Active Directory/Kerberos Authentication 패널을 사용해 Active Directory(Windows) 그룹을 생성, 수정 및 삭제하고 이러한 그룹에 관리 역할(admin, backup-operator 등)을 할당할 수 있습니다.

그룹을 관리할 준비하려면 **Administration** > **Access** > **Authentication**을 선택하고 Active Directory/Kerberos Authentication 패널을 확장하여 Active Directory Administrative Access **Enable** 버튼을 클릭합니다.

Active Directory용 관리 그룹 생성

Active Directory 그룹에 구성된 모든 사용자에게 관리 역할을 할당하려면 관리 그룹을 생성합니다.

시작하기 전에

Administration > **Access** > **Authentication** 페이지의 Active Directory/Kerberos Authentication 패널에서 Active Directory Administrative Access를 사용하도록 설정합니다.

절차

1. **Create...**를 클릭합니다.
2. 도메인 이름과 그룹 이름을 백슬래시로 구분하여 입력합니다. 예를 들어 domainname\groupname과 같이 입력합니다.
3. 드롭다운 메뉴에서 그룹의 관리 역할을 선택합니다.
4. **OK**를 클릭합니다.

Active Directory용 관리 그룹 수정

Active Directory 그룹에 대해 구성된 관리 그룹 이름 또는 관리 역할을 변경하려면 관리 그룹을 수정합니다.

시작하기 전에

Administration > **Access** > **Authentication** 페이지의 Active Directory/Kerberos Authentication 패널에서 Active Directory Administrative Access를 사용하도록 설정합니다.

절차

1. **Active Directory Administrative Access** 제목 아래에서 수정할 그룹을 선택합니다.
2. **Modify...**를 클릭합니다.
3. 도메인 이름과 그룹 이름을 수정합니다. 이 이름들은 백슬래시로 구분합니다. 예를 들어 domainname\groupname과 같이 입력합니다.
4. 드롭다운 메뉴에서 다른 역할을 선택하여 그룹의 관리 역할을 수정합니다.

Active Directory용 관리 그룹 삭제

Active Directory 그룹에 구성된 모든 사용자에 대한 시스템 액세스를 종료하려면 관리 그룹을 삭제합니다.

시작하기 전에

Administration > **Access** > **Authentication** 페이지의 Active Directory/Kerberos Authentication 패널에서 Active Directory Administrative Access를 사용하도록 설정합니다.

절차

1. **Active Directory Administrative Access** 제목 아래에서 삭제할 그룹을 선택합니다.
2. **Delete**를 클릭합니다.

UNIX Kerberos 인증 구성

UNIX Kerberos 인증을 구성하면 NFS 클라이언트에서 Kerberos 인증을 사용할 수 있습니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.

시작하기 전에

UNIX 모드 Kerberos 인증이 제대로 작동하려면 NIS가 실행 중이어야 합니다. Kerberos 설정에 대한 지침은 NIS 서비스 설정에 대한 섹션을 참조하십시오.

UNIX용 Kerberos를 구성하면 NFS 클라이언트에서 Kerberos 인증을 사용할 수 있습니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. Active Directory/Kerberos Authentication 패널을 확장합니다.
3. Mode 옆의 **Configure...**를 클릭하여 구성 마법사를 시작합니다.

   Active Directory/Kerberos Authentication 대화 상자가 나타납니다.
4. **Unix**를 선택하고 **Next**를 클릭합니다.
5. KDC(Key Distribution Center)에 대한 영역 이름(예: domain1.local)과 최대 세 개의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
6. 필요에 따라 **Browse**를 클릭하여 keytab 파일을 업로드하고 **Next**를 클릭합니다.

   구성에 대한 Summary 페이지가 나타납니다.

   참고

   keytab 파일은 인증 서버(KDC)에 생성되며 KDC 서버와 DDR 간의 공유 암호를 포함하고 있습니다.

   알림

   Kerberos 인증이 올바르게 작동하려면 keytab 파일을 업로드하고 가져와야 합니다.
7. **Finish**를 클릭합니다.

   Active Directory/Kerberos Authentication 패널에 구성 정보가 표시됩니다.

Kerberos 인증을 사용하지 않도록 설정

Kerberos 인증을 해제하면 CIFS 및 NFS 클라이언트에서 Kerberos 인증이 사용되지 않습니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.

절차

1. **Administration** > **Access Management** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. Active Directory/Kerberos Authentication 패널을 확장합니다.
3. Mode 옆의 **Configure...**를 클릭하여 구성 마법사를 시작합니다.

   Active Directory/Kerberos Authentication 대화 상자가 나타납니다.
4. **Disabled**를 선택하고 **Next**를 클릭합니다.

변경 사항이 굵은 텍스트로 나타나는 요약 페이지가 표시됩니다.

5. **Finish**를 클릭합니다.

   Active Directory/Kerberos Authentication 패널의 Mode 모드 옆에 Disabled라고 표시됩니다.

워크그룹 인증 정보 보기

Workgroup Authentication 패널을 사용하여 Workgroup 구성 정보를 봅니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
2. Workgroup Authentication 패널을 확장합니다.

표 44 Workgroup Authentication 레이블 설명

항목	설명
Mode	인증 모드 유형입니다(Workgroup 또는 Active Directory).
Workgroup name	지정된 워크그룹입니다.
CIFS Server Name	사용 중인 CIFS 서버의 이름입니다.
WINS Server	사용 중인 WINS 서버의 이름입니다.

워크그룹 인증 매개 변수 구성

워크그룹 인증 매개 변수를 사용해 워크그룹 이름 및 CIFS 서버 이름을 구성할 수 있습니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. Workgroup Authentication 패널을 확장합니다.
3. **구성**을 클릭합니다.

   Workgroup Authentication 대화 상자가 나타납니다.

4. Workgroup Name에서 **Manual**을 선택하고 연결할 워크그룹 이름을 입력하거나 기본값을 사용합니다.

   Workgroup 모드가 Data Domain 시스템을 워크그룹 도메인에 연결합니다.

5. CIFS Server Name에서 **Manual**을 선택하고 서버 이름(DDR)을 입력하거나 기본값을 사용합니다.
6. **OK**를 클릭합니다.

LDAP 인증 정보 보기

LDAP Authentication 패널에는 LDAP 구성 매개 변수와 LDAP 인증 설정 여부가 표시됩니다.

LDAP를 활성화하면 기존 OpenLDAP 서버 또는 구축을 시스템 수준 사용자 인증, NFSv4 ID 매핑용, LDAP를 사용한 NFSv3 Kerberos 및 LDAP 사용한 NFSv4 Kerberos를 위해 Data Domain 시스템에서 사용할 수 있습니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.
2. LDAP Authentication 패널을 확장합니다.

결과

표 45 LDAP Authentication 패널 항목

항목	설명
LDAP 상태	Enabled 또는 Disabled입니다.
Base Suffix	LDAP 기본 접미사입니다.
Bind DN	LDAP 서버와 연결된 계정 이름입니다.
SSL	Enabled 또는 Disabled입니다.
Server	인증 서버입니다.
LDAP 그룹	LDAP 그룹의 이름입니다.
Management Role	그룹의 역할(admin, user 등)입니다.

LDAP 인증 활성화 및 비활성화

LDAP Authentication 패널을 사용하여 LDAP 인증을 활성화, 비활성화 또는 재설정합니다.

절차

1. **Maintenance** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.
2. LDAP Authentication 패널을 확장합니다.
3. LDAP Status 옆에서 **Enable**을 클릭하여 LDAP 인증을 활성화하거나 **Disable**을 클릭하여 비활성화합니다.
   Enable or Disable LDAP Authentication 대화 상자가 나타납니다.

   참고

   LDAP 인증을 활성화하려면 먼저 LDAP 서버가 존재해야 합니다.
4. **OK**를 클릭합니다.

LDAP 인증 재설정

Reset 버튼을 클릭하면 LDAP 인증이 비활성화되고 LDAP 구성 정보가 지워집니다.

LDAP 인증 구성

LDAP Authentication 패널을 사용하여 LDAP 인증을 구성합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.

2. LDAP Authentication 패널을 확장합니다.
3. **Configure**를 클릭합니다.

   Configure LDAP Authentication 대화 상자가 나타납니다.

4. **Base Suffix** 필드에 기본 접미사를 지정합니다.
5. **Bind DN** 필드에 LDAP 서버와 연결할 계정 이름을 지정합니다.
6. **Bind Password** 필드에 바인딩 DN 계정의 암호를 지정합니다.
7. 필요에 따라 **Enable SSL**을 선택합니다.
8. 필요에 따라 **Demand Server Certificate**를 선택하여 Data Domain 시스템이 LDAP 서버에서 CA 인증서를 가져오도록 요구합니다.
9. **OK**를 클릭합니다.
10. 나중에 필요한 경우 **Reset**을 클릭하여 LDAP 구성을 기본값으로 되돌립니다.

LDAP 인증 서버 지정

LDAP Authentication 패널을 사용하여 LDAP 인증 서버를 지정합니다.

시작하기 전에

LDAP 서버를 구성하려면 LDAP 인증을 비활성화해야 합니다.

참고

LDAP를 사용하여 로그인하면 Data Domain 시스템과 LDAP 서버 간의 홉 수가 늘어나므로 때 DD SM 성능이 저하됩니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. LDAP Authentication 패널을 확장합니다.
3. **+** 버튼을 클릭하여 서버를 추가합니다.
4. 다음 형식 중 하나로 LDAP 서버를 지정하십시오.
   - IPv4 주소 — `10.26.16.250`
   - IPv6 주소 — `[::ffff:9.53.96.21]`
   - 호스트 이름 — `myldapserver`
5. **OK**를 클릭합니다.

LDAP 그룹 구성

LDAP Authentication 패널을 사용하여 LDAP 그룹을 구성합니다.

LDAP 그룹 구성은 Data Domain 시스템에서 사용자 인증에 LDAP를 사용할 때만 적용됩니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. LDAP Authentication 패널을 확장합니다.

3. LDAP Group 테이블에서 LDAP 그룹을 구성합니다.
   - LDAP 그룹을 추가하려면 Add(+)를 클릭하고 LDAP 그룹 이름 및 역할을 입력한 다음, **OK**를 클릭합니다.
   - LDAP 그룹을 수정하려면 LDAP 그룹 목록에서 그룹 이름의 확인란을 선택하고 연필 모양의 편집 버튼을 클릭합니다. LDAP 그룹 이름을 변경하고 **OK**를 클릭합니다.
   - LDAP 그룹 이름을 제거하려면 목록에서 LDAP 그룹을 선택하고 삭제(**X**)를 클릭합니다.

CLI(Command Line Interface)를 사용하여 LDAP 인증 구성

Data Domain 명령줄 인터페이스를 사용하여, 시스템 수준 사용자 인증, NFSv4 ID 매핑, LDAP를 사용하는 NFSv3 Kerberos 또는 LDAP를 사용하는 NFSv4 Kerberos를 위해 Data Domain 시스템을 사용하는 기존 OpenLDAP 서버 또는 구축을 구성할 수 있습니다.

LDAP 서버 구성

한 번에 하나 이상의 LDAP 서버를 구성할 수 있습니다.

참고

구성을 변경할 때 LDAP를 비활성화해야 합니다.

다음 형식 중 하나로 LDAP 서버를 지정하십시오.

- IPv4 주소—**10.*<A>*.*<B>*.*<C>***
- IPv4 주소와 포트 번호—**10.*<A>*.*<B>*.*<C>*:400**
- IPv6 주소 — **[::ffff:9.53.96.21]**
- IPv6 주소와 포트 번호 — **[::ffff:9.53.96.21]:400**
- 호스트 이름 — **myldapserver**
- 호스트 이름과 포트 번호 — **myldapserver:400**

여러 서버를 구성하는 경우:

- 각 서버를 공백으로 구분합니다.
- `authentication ldap servers add` 명령을 사용할 때 나열된 첫 번째 서버가 운영 서버가됩니다.
- 서버 중 하나라도 구성할 수 없으면 나열된 모든 서버에서 명령이 실패합니다.

절차

1. `authentication ldap servers add` 명령을 사용하여 하나 이상의 LDAP 서버를 추가합니다.

```
# authentication ldap servers add 10.A.B.C 10.X.Y.Z:400
LDAP server(s) added
LDAP Server(s):        2
#     IP Address/Hostname
---   --------------------
1.    10.A.B.C (primary)
2.    10.X.Y.Z:400
---   --------------------
```

2. `authentication ldap servers del` 명령을 사용하여 하나 이상의 LDAP 서버를 제거합니다.

```
# authentication ldap servers del 10.X.Y.Z:400
LDAP server(s) deleted.
LDAP Servers: 1
#   Server
-   ------------   ---------
1   10.A.B.C       (primary)
-   ------------   ---------
```

3. `authentication ldap servers reset` 명령을 사용하여 모든 LDAP 서버를 제거합니다.

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

LDAP 기본 접미사 구성

기본 접미사는 검색을 위한 기본 DN이며 LDAP 디렉토리가 검색을 시작하는 위치입니다.

절차

1. `authentication ldap base set` 명령을 사용하여 LDAP 기본 접미사를 설정합니다.

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. `authentication ldap base reset` 명령을 사용하여 LDAP 기본 접미사를 재설정합니다.

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```

LDAP 클라이언트 인증 구성

LDAP 서버로 인증하고 쿼리를 수행하는 데 사용되는 계정(Bind DN) 및 암호(Bind PW)를 구성합니다.

Bind DN 및 암호는 항상 구성해야 합니다. 일반적으로 LDAP 서버에는 기본적으로 인증된 바인드가 필요합니다. `client-auth`가 설정되지 않으면 이름이나 암호를 제공하지 않고 익명 액세스가 요청됩니다. `authentication ldap show`의 출력은 다음과 같습니다.

```
# authentication ldap show
LDAP configuration
        Enabled:          yes (*)
        Base-suffix:      dc=u2,dc=team
        Binddn:           (anonymous)
        Server(s):        1
#   Server
-   -------------   ---------
1   10.207.86.160   (primary)
-   -------------   ---------

Secure LDAP configuration
        SSL Enabled:      no
        SSL Method:       off
        tls_reqcert:      demand

(*) Requires a filesystem restart for the configuration to take
effect.
```

`client-auth` CLI를 사용하여 binddn을 설정하지만 bindpw를 제공하지 않은 경우 인증되지 않은 액세스가 요청됩니다.

```
# authentication ldap client-auth set binddn
"cn=Manager,dc=u2,dc=team"
```

```
Enter bindpw:
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

절차

1. `authentication ldap client-auth set binddn` 명령을 사용하여 Bind DN 및 암호를 설정합니다.

   ```
   # authentication ldap client-auth set binddn
   "cn=Administrator,cn=Users,dc=anvil,dc=team"
       Enter bindpw:
       LDAP client authentication binddn set to
   "cn=Administrator,cn=Users,dc=anvil,dc=team".
   ```

2. `authentication ldap client-auth reset` 명령을 사용하여 Bind DN 및 암호를 재설정합니다.

   ```
   # authentication ldap client-auth reset
   LDAP client authentication configuration reset to empty.
   ```

LDAP 활성화

시작하기 전에

LDAP를 활성화하려면 먼저 LDAP 구성이 있어야 합니다. 또한 NIS를 비활성화하고, LDAP 서버에 연결할 수 있는지 확인하고, LDAP 서버의 루트 DSE를 쿼리할 수 있어야 합니다.

절차

1. `authentication ldap enable` 명령을 사용하여 LDAP를 활성화합니다.

   ```
   # authentication ldap enable
   ```

   계속하기 전에 확인할 수 있도록 LDAP 구성의 세부 정보가 표시됩니다. 계속하려면 **yes**를 입력하여 LDAP 구성이 적용되도록 파일 시스템을 재시작합니다.

2. `authentication ldap show` 명령을 사용하여 현재 LDAP 구성을 확인합니다.

   ```
   # authentication ldap show
   LDAP configuration
           Enabled:          no
           Base-suffix:      dc=anvil,dc=team
           Binddn:
   cn=Administrator,cn=Users,dc=anvil,dc=team
           Server(s):        2
   #    Server
   -    ----------------    ---------
   1    10.26.16.250        (primary)
   2    10.26.16.251:400
   -    ----------------    ---------

   Secure LDAP configuration
           SSL Enabled:      no
           SSL Method:       off
           tls_reqcert:      demand
   ```

   기본 LDAP 및 보안 LDAP 구성 세부 정보가 표시됩니다.

3. `authentication ldap status` 명령을 사용하여 현재 LDAP 상태를 확인합니다.

   ```
   # authentication ldap status
   ```

LDAP 상태가 표시됩니다. LDAP 상태가 `good`이 아닌 경우 문제는 출력 내용에서 확인됩니다. 예를 들면 다음과 같습니다.

```
# authentication ldap status
Status: invalid credentials
```

또는

```
# authentication ldap status
Status: invalid DN syntax
```

4. `authentication ldap disable` 명령을 사용하여 LDAP를 비활성화합니다.

```
# authentication ldap disable
LDAP is disabled.
```

Secure LDAP 활성화

SSL을 활성화하여 보안 LDAP를 사용하도록 DDR을 구성할 수 있습니다.

시작하기 전에

LDAP CA 인증서가 없고 `tls_reqcert`가 `demand`로 설정된 경우 작업이 실패합니다. LDAP CA 인증서를 가져와서 다시 시도하십시오.

`tls_reqcert`가 `never`로 설정된 경우 LDAP CA 인증서가 필요하지 않습니다. 자세한 내용은 가져온 CA 인증서로 LDAP 서버 인증서 확인 구성(123페이지) 섹션을 참조하십시오.

절차

1. `authentication ldap ssl enable` 명령을 사용하여 SSL을 활성화합니다.

```
# authentication ldap ssl enable
Secure LDAP is enabled with 'ldaps' method.
```

기본 방법은 보안 LDAP 또는 *ldaps*입니다. TLS와 같은 다른 방법을 지정할 수 있습니다.

```
# authentication ldap ssl enable method start_tls
Secure LDAP is enabled with 'start_tls' method.
```

2. `authentication ldap ssl disable` 명령을 사용하여 SSL을 비활성화합니다.

```
# authentication ldap ssl disable
Secure LDAP is disabled.
```

가져온 CA 인증서로 LDAP 서버 인증서 확인 구성

TLS 요청 인증서 동작을 변경할 수 있습니다.

절차

1. `authentication ldap ssl set tls_reqcert` 명령을 사용하여 TLS 요청 인증서 동작을 변경합니다.

인증서를 확인하지 않습니다.

```
# authentication ldap ssl set tls_reqcert never
"tls_reqcert" set to "never". LDAP server certificate will not
be verified.
```

인증서를 확인합니다.

```
# authentication ldap ssl set tls_reqcert demand
"tls_reqcert" set to "demand". LDAP server certificate will be
verified.
```

2. `authentication ldap ssl reset tls_reqcert` 명령을 사용하여 TLS 요청 인증서 동작을 재설정합니다. 기본 동작은 `demand`입니다.

```
# authentication ldap ssl reset tls_reqcert
tls_reqcert has been set to "demand". LDAP Server certificate
will be verified with imported CA certificate.Use "adminaccess"
CLI to import the CA certificate.
```

LDAP용 CA 인증서 관리

인증서를 가져오거나 삭제하고 현재 인증서 정보를 표시할 수 있습니다.

절차

1. `adminaccess certificate import` 명령을 사용하여 LDAP 서버 인증서 확인을 위한 CA 인증서를 가져옵니다.

   `ca application`에 `ldap`를 지정합니다.

```
# adminaccess certificate import{host application {all | aws-
federal | ddboost | https| keysecure | rkm | <application-
list>}| ca application { ldap }} [file <file-name>] Import host
or ca certificate
```

2. `adminaccess certificate delete` 명령을 사용하여 LDAP 서버 인증서 확인을 위한 CA 인증서를 삭제합니다.

   `application`에 `ldap`를 지정합니다.

```
# adminaccess certificate delete
{ subject <subject-name> | fingerprint <fingerprint>}
[application { ldap }]
```

   `imported-ca application`에 `ldap`를 지정합니다.

```
# adminaccess certificate delete
{ imported-host application { all | aws-federal | ddboost |
https
| keysecure | rkm | <application-list>}
| imported-ca application { ldap }}
```

3. `adminaccess certificate show` 명령을 사용하여 LDAP 서버 인증서 확인을 위한 현재 CA 인증서 정보를 표시합니다.

```
# adminaccess certificate show imported-ca ldap
```

NIS 인증 정보 보기

NIS Authentication 패널에는 NIS 구성 매개 변수와 NIS 인증 설정 여부가 표시됩니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. NIS Authentication 패널을 확장합니다.

결과

표 46 NIS Authentication 패널 항목

항목	설명
NIS Status	설정 또는 해제입니다.

표 46 NIS Authentication 패널 항목 (계속)

항목	설명
Domain Name	이 서비스의 도메인 이름입니다.
Server	인증 서버입니다.
NIS Group	NIS 그룹의 이름입니다.
Management Role	그룹의 역할(admin, user 등)입니다.

NIS 인증 설정 및 해제

NIS Authentication 패널을 사용해 NIS 인증을 설정하고 해제합니다.

절차

1. **Maintenance** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.
2. NIS Authentication 패널을 확장합니다.
3. NIS Status 옆에서 **Enable**을 클릭하여 NIS 인증을 사용하도록 설정하거나 **Disable**을 클릭해 사용하지 않도록 설정합니다.
   Enable or Disable NIS 대화 상자가 나타납니다.
4. **OK**를 클릭합니다.

NIS 도메인 이름 구성

NIS Authentication 패널을 사용해 NIS 도메인 이름을 구성합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.
2. NIS Authentication 패널을 확장합니다.
3. Domain Name 옆의 **Edit**을 클릭해 NIS 도메인 이름을 편집합니다.
   Configure NIS Domain Name 대화 상자가 나타납니다.
4. **Domain Name** 상자에 도메인 이름을 입력합니다.
5. **OK**를 클릭합니다.

NIS 인증 서버 지정

NIS Authentication 패널을 사용해 NIS 인증 서버를 지정합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.
   Authentication 보기가 나타납니다.
2. NIS Authentication 패널을 확장합니다.
3. Domain Name 아래에서 다음 중 하나를 선택합니다.
   - **Obtain NIS Servers from DHCP** 시스템에서 DHCP를 사용하여 자동으로 NIS 서버를 가져옵니다.

- **Manually Configure** 다음 절차를 사용하여 수동으로 NIS 서버를 구성합니다.
- 인증 서버를 추가하려면 서버 테이블에서 Add(**+**) 버튼을 클릭하고 서버 이름을 입력한 뒤 **OK**를 클릭합니다.
- 인증 서버를 수정하려면 인증 서버 이름을 선택한 뒤 연필 모양의 편집 아이콘을 클릭합니다. 서버 이름을 변경하고 **OK**를 클릭합니다.
- 인증 서버 이름을 제거하려면 서버를 선택하고 X 아이콘을 클릭한 뒤 **OK**를 클릭합니다.

4. **OK**를 클릭합니다.

NIS 그룹 구성

NIS Authentication 패널을 사용해 NIS 그룹을 구성합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다.

   Authentication 보기가 나타납니다.

2. NIS Authentication 패널을 확장합니다.
3. NIS 그룹을 NIS Group 테이블에 구성합니다.
   - NIS 그룹을 추가하려면 Add(**+**)를 클릭하고 NIS 그룹 이름 및 역할을 입력한 다음 **Validate**를 클릭합니다. **OK**를 클릭하여 Add NIS Group 대화 상자를 종료합니다. **OK**를 다시 한 번 클릭해 **Configure Allowed NIS Groups** 대화 상자를 종료합니다.
   - NIS 그룹을 수정하려면 NIS 그룹 목록에서 NIS 그룹 이름의 확인란을 선택하고 연필 모양의 편집 버튼을 클릭합니다. NIS 그룹 이름을 변경하고 **OK**를 클릭합니다.
   - NIS 그룹 이름을 제거하려면 목록에서 NIS 그룹을 선택하고 삭제(**X**)를 클릭합니다.
4. **OK**를 클릭합니다.

인증 문제 진단

Data Domain Operating System은 Data Domain System Manager 인터페이스 내에서 Active Directory의 인증 문제를 진단하는 기능을 제공합니다.

절차

1. **Administration** > **Access** > **Authentication**을 선택합니다
2. Active Directory/Kerberos Authentication 패널을 확장합니다.
3. **Diagnose**를 클릭합니다.
4. 조사할 문제를 선택하고 **Diagnose**를 클릭합니다.
5. 요청된 정보를 제공합니다.

   Active Directory 사용자로 로그인할 때의 문제를 진단하려면 다음을 제공합니다.
   - Active Directory 서버 IP 주소
   - Active Directory 서버 FQDN
   - Active Directory 서비스 사용자

참고

여기에 지정된 Active Directory 사용자 계정에는 다음 권한이 필요합니다.

- 도메인 이름으로 식별되는 기본 DN에 대한 읽기 전용 액세스 권한
- 기본 DN에 있는 모든 사용자의 쿼리 속성에 대한 읽기 전용 액세스 권한
- Data Domain 시스템의 컴퓨터 계정 쿼리 특성에 대한 읽기 전용 액세스 권한

- Active Directory 서비스 암호
- 로그인 실패가 발생한 Data Domain 사용자 이름

Data Domain 시스템을 Active Directory 도메인에 가입할 때의 문제를 진단하려면 다음을 제공합니다.

- Active Directory 서버 IP 주소
- Active Directory 서버 FQDN
- Active Directory 서비스 사용자 이름
- Active Directory 서비스 암호

6. **Diagnose**를 클릭합니다.
7. 보고서를 확인합니다.
   - **View Report**를 클릭하여 온라인으로 보고서를 봅니다. 작업 항목 테이블의 각 항목을 클릭하여 추가 정보를 확인할 수 있습니다.
   - 보고서 사본을 다운로드하려면 **Download**를 클릭합니다.
8. 문제에 대해 제안된 수정 사항을 검토하고 구현한 후 작업을 다시 시도합니다.

시스템 인증 방법 변경

Data Domain 시스템은 암호 기반 인증 또는 인증서 기반 인증을 지원합니다. 암호 기반 인증이 기본 방법입니다.

시작하기 전에

인증서 기반 인증에는 SSH 키가 필요하며 암호 기반 인증이 비활성화될 때 사용자가 시스템에서 인증할 수 있도록 CA 인증서를 가져와야 합니다.

암호 기반 인증에서 인증서 기반 인증으로 시스템 인증 방법을 변경하려면 다음 단계를 완료합니다.

절차

1. **Administration** > **Access**를 선택합니다.

   Access Management 보기가 나타납니다.
2. **Manage CA Certificates**를 클릭합니다.
3. **Add**를 클릭하여 새 인증서를 생성합니다.
4. 인증서를 추가합니다.
   - **I want to upload the certificate as a .pem file**을 선택하고 **Choose File**을 클릭하여 인증서 파일을 선택하고 시스템에 업로드합니다.
   - **I want to copy and paste the certificate text**를 선택하여 인증서 텍스트를 복사하여 텍스트 필드에 붙여 넣습니다.

5. **Add**를 클릭합니다.
6. **More Tasks** > **Change Login Options**를 선택합니다.
7. **Password Based Login** 드롭다운 메뉴에서 **Disable**을 선택합니다.

   참고

   필요한 SSH 키 및 CA 인증서가 시스템에 구성되어 있지 않으면 드롭다운 메뉴가 비활성화됩니다.

8. **OK**를 클릭합니다.

   보안 정책이 구성되어 있으면 보안 책임자 자격 증명을 묻는 메시지가 나타납니다. 자격 증명을 제공하고 **OK**를 클릭합니다.

시스템 인증 방법을 암호 기반 인증으로 재설정합니다.

인증서 기반 인증에서 암호 기반 인증으로 시스템 인증 방법을 변경하려면 다음 단계를 완료합니다.

절차

1. **Administration** > **Access**를 선택합니다.

   Access Management 보기가 나타납니다.

2. **More Tasks** > **Change Login Options**를 선택합니다.
3. **Password Based Login** 드롭다운 메뉴에서 **Enable**을 선택합니다.
4. **OK**를 클릭합니다.

   보안 정책이 구성되어 있으면 보안 책임자 자격 증명을 묻는 메시지가 나타납니다. 자격 증명을 제공하고 **OK**를 클릭합니다.

메일 서버 설정 구성

Mail Server 탭에서 DD OS가 e-메일 보고서를 전송할 메일 서버를 지정할 수 있습니다.

절차

1. **Administration** > **Settings** > **Mail Server**를 선택합니다.
2. **More Tasks** > **Set Mail Server**를 선택합니다.

   Set Mail Server 대화 상자가 나타납니다.

3. **Mail Server** 필드에 메일 서버의 이름을 지정합니다.
4. **Credentials** 버튼을 사용하여 메일 서버에 대한 자격 증명 사용을 활성화하거나 비활성화합니다.
5. 자격 증명이 활성화된 경우 **User Name** 필드에 메일 서버 사용자 이름을 지정합니다.
6. 자격 증명이 활성화된 경우 **Password** 필드에 메일 서버 암호를 지정합니다.
7. **Set**을 클릭합니다.
8. 필요에 따라 CLI를 사용하여 메일 서버 구성을 확인하고 문제를 해결합니다.

   a. **`config show mailserver`** 명령을 실행하여 메일 서버가 구성되어 있는지 확인합니다.

   b. **`net ping <mailserver-hostname> count 4`** 명령을 실행하여 메일 서버를 ping합니다.

c. 메일 서버가 올바르게 구성되지 않은 경우 **config set mailserver *<mailserver-hostname>*** 명령을 실행하여 메일 서버를 설정한 후 ping을 다시 시도합니다.

d. **net show dns** 명령을 실행하여 DNS 서버가 구성되어 있는지 확인합니다.

e. **net ping *<DNS-hostname>* count 4** 명령을 실행하여 DNS 서버를 ping합니다.

f. DNS 서버가 올바르게 구성되지 않은 경우 **config set dns *<dns-IP>*** 명령을 실행하여 DNS 서버를 설정한 후 ping을 다시 시도합니다.

g. 선택적으로 **net hosts add <IP-address> <hostname>** 명령을 실행하여 로컬 확인을 위해 Data Domain 호스트 파일에 메일 서버 IP 주소 및 호스트 이름을 추가합니다.

h. **net ping *<mailserver-hostname>* count 4** 명령을 실행하여 메일 서버를 ping합니다.

시간 및 날짜 설정 관리

Time and Date Settings 탭에서 시스템 시간 및 날짜를 보고 구성하거나 NTP를 구성하여 시간과 날짜를 설정합니다.

절차

1. 현재 시간 및 날짜 구성을 보려면 **Administration** > **Settings** > **Time and Date Settings**를 선택합니다.

   Time and Date Settings 페이지에는 현재 시스템의 날짜와 시간이 제공되며, NTP의 설정 여부가 표시되고 구성된 NTP 서버의 IP 주소 또는 호스트 이름이 나열됩니다.

2. 구성을 변경하려면 **More Tasks** > **Configure Time Settings**를 선택합니다.

   Configure Time Settings 대화 상자가 나타납니다.

3. **Time Zone** 드롭다운 목록에서 Data Domain 시스템이 상주하는 표준 시간대를 선택합니다.
4. 수동으로 시간과 날짜를 설정하려면 **None**을 선택하고, **Date** 상자에 날짜를 입력한 뒤 **Time** 드롭다운 목록에서 시간을 선택합니다.
5. NTP를 사용해 시간을 동기화하려면 NTP를 선택하고 NTP 서버의 액세스 방식을 설정합니다.
   - 서버를 자동으로 선택하는 데 DHCP를 사용하려면 **Obtain NTP Servers using DHCP**를 선택합니다.
   - NTP 서버 IP 주소를 구성하려면 **Manually Configure**를 선택하고 서버의 IP 주소를 추가한 뒤 **OK**를 클릭합니다.

   참고

   Active Directory 도메인 컨트롤러의 시간 동기화를 사용하면 NTP와 도메인 컨트롤러 모두 시간을 수정할 경우 시스템에 과도한 시간 변경이 일어날 수 있습니다.

   ---

6. **OK**를 클릭합니다.

7. 표준 시간대를 변경한 경우 시스템을 재부팅해야 합니다.
   a. **Maintenance** > **System**을 선택합니다.
   b. More Tasks 메뉴에서 Reboot System을 선택합니다.
   c. OK를 클릭하여 확인합니다.

시스템 속성 관리

System Properties 탭에서 관리 대상 시스템의 위치, 관리자 e-메일 주소 및 호스트 이름을 식별하는 시스템 속성을 보고 구성할 수 있습니다.

절차

1. 현재 구성을 보려면 **Administration** > **Settings** > **System Properties**를 선택합니다.

   System Properties 탭에 시스템 위치, 관리자 e-메일 주소, 관리자 호스트 이름이 표시됩니다.

2. 구성을 변경하려면 **More Tasks** > **Set System Properties**를 선택합니다.

   Set System Properties 대화 상자가 나타납니다.

3. **Location** 상자에 Data Domain 시스템의 위치 정보를 입력합니다.
4. **Admin Email** 상자에 시스템 관리자의 e-메일 주소를 입력합니다.
5. **Admin Host** 상자에 관리 서버의 이름을 입력합니다.
6. **OK**를 클릭합니다.

SNMP 관리

SNMP(Simple Network Management Protocol)는 네트워크 관리 정보를 교환하는 표준 프로토콜이며, TCP(Transmission Control Protocol)/IP(Internet Protocol) 프로토콜 제품군의 일부입니다. SNMP는 관리자가 주의할 수 있는 조건이 되도록 Data Domain 시스템과 같은 네트워크 연결 디바이스를 관리하고 모니터링할 수 있는 툴을 네트워크 관리자에게 제공합니다.

SNMP를 사용해 Data Domain 시스템을 모니터링하려면 SNMP 관리 시스템에 Data Domain MIB를 설치해야 합니다. 또한 DD OS는 표준 MIB-II를 지원하므로 사용자는 네트워크 통계와 같은 일반 데이터에 대한 MIB-II 통계를 쿼리할 수 있습니다. 가용 데이터를 모두 운영하려면 Data Domain MIB와 표준 MIB-II MIB를 모두 활용해야 합니다.

Data Domain 시스템 SNMP 에이전트는 SNMP v1, v2c 및 v3를 사용하여 관리 시스템에서 Data Domain 관련 정보에 대한 쿼리를 받습니다. SNMP V3는 인증에 사용되는 일반 텍스트 커뮤니티 문자열을 MD5 또는 SHA1을 사용하는 사용자 기반 인증으로 교체함으로써 v2c 및 v1보다 우수한 보안 수준을 제공합니다. 또한 SNMP v3에서는 사용자 인증 패킷을 암호화하고 DES 또는 AES로 패킷 무결성을 확인할 수 있습니다.

Data Domain 시스템은 SNMP v2c 및 SNMP v3를 사용하여 SNMP 트랩(알림 메시지)을 보낼 수 있습니다. SNMP v1 트랩은 지원되지 않으므로 가능하면 SNMP v2c 또는 v3를 사용하십시오.

SNMP를 활성화하면 열리는 기본 포트는 포트 161입니다. 포트 162를 통해 트랩이 전송됩니다.

- SNMP 모니터링을 사용하기 위한 Data Domain 시스템 설정 방법은 *Data Domain Operating System 초기 구성 가이드*에 설명되어 있습니다.

- Data Domain MIB 분기에 포함된 전체 MIB 매개 변수 세트는 *Data Domain Operating System MIB 참조 가이드*에 설명되어 있습니다.

SNMP 상태 및 구성 보기

SNMP 탭에는 현재 SNMP 상태 및 구성이 표시됩니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.

   SNMP 보기에는 SNMP 상태, SNMP 속성, SNMP V3 구성 및 SNMP V2C 구성이 표시됩니다.

SNMP 탭 레이블

SNMP 탭 레이블은 전반적인 SNMP 상태, SNMP 속성 값 및 SNMPv3 및 SNMPv2에 대한 구성을 식별합니다.

상태
Status 영역에는 시스템에 있는 SNMP 에이전트의 작동 상태(Enabled 또는 Disabled)가 표시됩니다.

SNMP 속성

표 47 SNMP 속성 설명

항목	설명
SNMP System Location	모니터링되는 Data Domain 시스템의 위치입니다.
SNMP System Contact	Data Domain 시스템 관리를 위해 연락할 사람으로 지정된 사용자입니다.
SNMP System Notes	(선택 사항) 추가적인 SNMP 구성 데이터입니다.
SNMP Engine ID	Data Domain 시스템의 고유한 16진수 식별자입니다.

SNMP V3 구성

표 48 SNMP Users 열 설명

항목	설명
Name	Data Domain 시스템용 에이전트에 액세스할 수 있는 권한을 가진 SNMP 관리자에 있는 사용자의 이름입니다.
Access	SNMP 사용자의 액세스 권한으로, 읽기 전용 또는 읽기-쓰기 권한일 수 있습니다.
Authentication Protocols	SNMP 사용자를 확인하는 데 사용되는 인증 프로토콜로, MD5, SHA1 또는 None일 수 있습니다.
Privacy Protocol	SNMP 사용자 인증 중에 사용되는 암호화 프로토콜로, AES, DES 또는 None일 수 있습니다.

표 49 Trap Hosts 열 설명

항목	설명
Host	SNMP 관리 호스트의 IP 주소 또는 도메인 이름입니다.

표 49 Trap Hosts 열 설명 (계속)

항목	설명
Port	SNMP 트랩이 호스트와 통신하는 데 사용되는 포트입니다. 예를 들어 162가 기본값입니다.
User	Data Domain SNMP 정보에 액세스할 권한이 있는 트랩 호스트의 사용자입니다.

SNMP V2C 구성

표 50 Communities 열 설명

항목	설명
Community	커뮤니티의 이름입니다. 예: public, private 또는 localCommunity.
Access	할당된 액세스 권한으로, 읽기 전용 또는 읽기-쓰기일 수 있습니다.
Hosts	이 커뮤니티의 호스트입니다.

표 51 Trap Hosts 열 설명

항목	설명
Host	Data Domain 시스템에 의해 생성된 SNMP 트랩을 수신하도록 지정된 시스템입니다. 이 매개 변수가 설정되어 있으면 SNMP 에이전트가 비활성화되어 있어도 시스템에서 알림 메시지를 받습니다.
Port	SNMP 트랩이 호스트와 통신하는 데 사용되는 포트입니다. 예를 들어 162가 기본값입니다.
Community	커뮤니티의 이름입니다. 예: public, private 또는 localCommunity.

SNMP 설정 및 해제

SNMP 탭을 사용해 SNMP를 설정하거나 해제합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. Status 영역에서 **Enable** 또는 **Disable**을 클릭합니다.

SNMP MIB 다운로드

SNMP 탭을 사용해 SNMP MIB를 다운로드합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. **Download MIB file**을 클릭합니다.
3. Opening DATA_DOMAIN.mib 대화 상자에서 **Open**을 선택합니다.
4. 브라우저 창에서 MIB를 보려면 **Browse**를 클릭하고 브라우저를 선택합니다.

참고

Microsoft Internet Explorer 브라우저를 사용하는 경우 Automatic을 설정하여 파일 다운로드 메시지를 표시합니다.

5. MIB를 저장하거나 브라우저를 종료합니다.

SNMP 속성 구성

SNMP 탭을 사용해 시스템 위치 및 시스템 연락처에 대한 텍스트 항목을 구성합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. SNMP Properties 영역에서 **Configure**를 클릭합니다.

   SNMP Configuration 대화 상자가 표시됩니다.

3. 텍스트 필드에서 다음과 같은 정보를 지정합니다.
   - SNMP System Location: Data Domain 시스템이 위치한 장소에 대한 설명입니다.
   - SNMP System Contact: Data Domain 시스템의 시스템 관리자 이메일 주소입니다.
   - SNMP System Notes: (선택 사항) 추가적인 SNMP 구성 정보입니다.
   - SNMP Engine ID: SNMP 개체에 대한 고유 식별자입니다. 엔진 ID는 5~34자의 16진수 문자여야 합니다(SNMPv3만 해당).

     참고

     SNMP 엔진 ID가 길이 요구 사항을 충족시키지 못하거나 잘못된 문자가 사용된 경우 시스템에 오류가 표시됩니다.

4. **OK**를 클릭합니다.

SNMP V3 사용자 관리

SNMP 탭을 사용해 SNMPv3 사용자 및 트랩 호스트를 생성, 수정 및 삭제합니다.

SNMP V3 사용자 생성

SNMPv3 사용자를 생성할 때는 사용자 이름을 정의하고 읽기 전용 또는 읽기/쓰기 액세스를 지정하고 인증 프로토콜을 선택합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. SNMP Users 영역에서 **Create**를 클릭합니다.

   Create SNMP User 대화 상자가 나타납니다.

3. **Name** 텍스트 필드에 Data Domain 시스템 에이전트에 대한 액세스를 부여하려는 사용자의 이름을 입력합니다. 이름은 8자 이상이어야 합니다.
4. 이 사용자에 대한 읽기 전용 또는 쓰기-읽기 액세스 권한을 선택합니다.
5. 사용자를 인증하려면 **Authentication**을 선택합니다.

a. MD5 또는 SHA1 프로토콜을 선택합니다.

b. **Key** 텍스트 필드에 인증 키를 입력합니다.

c. 인증 세션에 암호화를 제공하려면 **Privacy**를 선택합니다.

d. AES 또는 DES 프로토콜을 선택합니다.

e. **Key** 텍스트 필드에 암호화 키를 입력합니다.

6. **OK**를 클릭합니다.

   새로 추가된 사용자 계정이 SNMP Users 테이블에 나타납니다.

SNMP V3 사용자 수정

기존 SNMPv3 사용자에 대한 액세스 수준(읽기 전용 또는 읽기/쓰기) 및 인증 프로토콜을 수정할 수 있습니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. **SNMP Users** 영역에서 사용자에 해당하는 확인란을 선택하고 **Modify**를 클릭합니다.

   Modify SNMP User 대화 상자가 나타납니다. 다음 설정을 추가하거나 변경합니다.

3. 이 사용자에 대한 읽기 전용 또는 쓰기-읽기 액세스 권한을 선택합니다.
4. 사용자를 인증하려면 **Authentication**을 선택합니다.

   a. MD5 또는 SHA1 프로토콜을 선택합니다.

   b. Key 텍스트 필드에 인증 키를 입력합니다.

   c. 인증 세션에 암호화를 제공하려면 **Privacy**를 선택합니다.

   d. AES 또는 DES 프로토콜을 선택합니다.

   e. **Key** 텍스트 필드에 암호화 키를 입력합니다.

5. **OK**를 클릭합니다.

   이 사용자 계정의 새 설정이 SNMP Users 테이블에 나타납니다.

SNMP V3 사용자 제거

SNMP 탭을 사용해 기존 SNMPv3 사용자를 삭제합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. SNMP Users 영역에서 사용자 확인란을 선택하고 **Delete**를 클릭합니다.

   Delete SNMP User 대화 상자가 나타납니다.

참고

Delete 버튼이 비활성화되어 있으면 선택한 사용자를 하나 이상의 트랩 호스트에서 사용 중인 것입니다. 이 경우 트랩 호스트를 삭제한 다음 사용자를 삭제합니다.

---

3. 삭제할 사용자 이름을 확인하고 **OK**를 클릭합니다.
4. Delete SNMP User Status 대화 상자에서 **Close**를 클릭합니다.

   해당 사용자 계정이 SNMP Users 테이블에서 제거됩니다.

SNMP V2C 커뮤니티 관리

SNMP v2c 커뮤니티(암호로 사용됨)를 정의해 Data Domain 시스템에 대한 관리 시스템 액세스를 제어합니다. 지정된 커뮤니티를 사용하는 특정 호스트에 대한 액세스를 제한하려면 호스트를 커뮤니티에 할당합니다.

참고

SNMP V2C Community 문자열은 일반 텍스트로 전송되며 차단하기 용이합니다. 이러한 상황이 발생하는 경우 인터셉터는 네트워크상의 디바이스에서 정보를 검색해, 구성을 수정하고 종료할 수도 있습니다. SNMP V3는 인증 및 암호화 기능을 제공하여 차단을 방지합니다.

참고

SNMP 커뮤니티를 정의한다고 해서 SNMP 트랩이 관리 스테이션에 전송되지는 않습니다. 관리 스테이션에 트랩이 제출되도록 하려면 트랩 호스트를 정의해야 합니다.

SNMP V2C 커뮤니티 생성

커뮤니티를 생성하여 DDR 시스템에 대한 액세스를 제한하거나 트랩 호스트에 트랩을 전송하는 데 사용할 수 있습니다. 트랩 호스트에 사용할 커뮤니티를 선택하려면 먼저 커뮤니티를 생성하고 호스트에 할당해야 합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. Communities 영역에서 **Create**를 클릭합니다.

   Create SNMP V2C Community 대화 상자가 나타납니다.

3. **Community** 상자에 Data Domain 시스템 에이전트에 액세스할 수 있는 커뮤니티의 이름을 입력합니다.
4. 이 커뮤니티에 대한 읽기 전용 또는 쓰기-읽기 액세스 권한을 선택합니다.
5. 커뮤니티를 하나 이상의 호스트에 연결하려는 경우 다음과 같이 호스트를 추가합니다.
   a. **+**를 클릭하여 호스트를 추가합니다.

      Host 대화 상자가 나타납니다.

   b. **Host** 텍스트 필드에 호스트의 IP 주소 또는 도메인 이름을 입력합니다.

   c. **OK**를 클릭합니다.

      호스트 목록에 호스트가 추가됩니다.
6. **OK**를 클릭합니다.

   새 커뮤니티 항목이 **Communities** 테이블에 나타나고 선택한 호스트가 나열됩니다.

SNMP V2C 커뮤니티 수정

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. Communities 영역에서 커뮤니티에 대한 확인란을 선택하고 **Modify**를 클릭합니다.

   Modify SNMP V2C Community 대화 상자가 나타납니다.

3. 이 커뮤니티에 대한 액세스 모드를 변경하려면 **read-only** 또는 **read-write** 액세스를 선택합니다.

   참고

   동일한 시스템에서 트랩 호스트가 해당 커뮤니티의 일부로 구성된 경우 선택한 커뮤니티에 대한 Access 버튼이 비활성화됩니다. 액세스 설정을 수정하려면 커뮤니티를 수정한 후 트랩 호스트를 삭제하고 다시 추가하십시오.

4. 하나 이상의 호스트를 이 커뮤니티에 추가하려면 다음을 수행합니다.
   a. **+**를 클릭하여 호스트를 추가합니다.

      Host 대화 상자가 나타납니다.

   b. **Host** 텍스트 필드에 호스트의 IP 주소 또는 도메인 이름을 입력합니다.
   c. **OK**를 클릭합니다.

      호스트 목록에 호스트가 추가됩니다.
5. 호스트 목록에서 하나 이상의 호스트를 삭제하려면 다음을 수행합니다.

   참고

   동일한 시스템에서 트랩 호스트가 해당 커뮤니티의 일부로 구성된 경우 DD System Manager를 사용해 호스트를 삭제할 수 없습니다. 커뮤니티에서 트랩 호스트를 삭제하려면 커뮤니티를 수정한 후 트랩 호스트를 삭제하고 다시 추가하십시오.

   참고

   트랩 호스트가 IPv6 주소를 사용하고 IPv6를 지원하지 않는 이전 DD OS를 통해 시스템이 관리되는 경우 선택한 커뮤니티에 대한 Access 버튼이 비활성화되지 않습니다. 가능하면 항상 시스템의 DD OS 버전 이상을 사용하는 관리 시스템을 선택하십시오.

   a. 각 호스트에 대한 확인란을 선택하거나 테이블의 Host 확인란을 클릭하여 나열된 모든 호스트를 선택합니다.
   b. 삭제 버튼(X)을 클릭합니다.
6. 호스트 이름을 편집하려면 다음을 수행합니다.
   a. 호스트에 대한 확인란을 선택합니다.
   b. 편집 버튼(연필 아이콘)을 클릭합니다.
   c. 호스트 이름을 편집합니다.

d. **OK**를 클릭합니다.

7. **OK**를 클릭합니다.

   Communities 테이블에 수정된 커뮤니티 항목이 나타납니다.

SNMP V2C 커뮤니티 삭제

SNMP 탭을 사용해 기존 SNMPv2 커뮤니티를 삭제합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. **Communities** 영역에서 커뮤니티에 해당하는 확인란을 선택하고 **Delete**를 클릭합니다.

   Delete SNMP V2C Community 대화 상자가 나타납니다.

   참고

   Delete 버튼이 비활성화되어 있으면 선택한 커뮤니티를 하나 이상의 트랩 호스트에서 사용 중인 것입니다. 이 경우 트랩 호스트를 삭제한 다음 커뮤니티를 삭제합니다.

   ---

3. 삭제할 커뮤니티 이름을 확인하고 **OK**를 클릭합니다.
4. Delete SNMP V2C Communities Status 대화 상자에서 **Close**를 클릭합니다. 해당 커뮤니티 항목이 Communities 테이블에서 제거됩니다.

SNMP 트랩 관리

트랩 호스트 정의를 사용해 Data Domain 시스템에서 SNMP 관리 스테이션에 SNMP 트랩 메시지로 알림 메시지를 전송하도록 할 수 있습니다.

SNMP V3 및 V2C 트랩 호스트 생성

트랩 호스트 정의는 시스템의 SNMP 트랩 메시지를 수신하는 원격 호스트를 식별합니다.

시작하기 전에

기존 SNMP v2c 커뮤니티를 트랩 호스트에 할당하려는 경우 먼저 Communities 영역을 사용해 트랩 호스트를 커뮤니티에 할당해야 합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. SNMP V3 Trap Hosts 또는 SNMP V2C Trap Hosts 영역에서 **Create**를 클릭합니다.

   Create SNMP [V3 or V2C] Trap Hosts 대화 상자가 나타납니다.

3. **Host** 상자에 트랩을 받을 SNMP 호스트의 IP 주소 또는 도메인 이름을 입력합니다.
4. **Port** 상자에 전송 트랩의 포트 번호를 입력합니다. 포트 162가 일반적인 포트입니다.
5. 드롭다운 메뉴에서 사용자(SNMP V3) 또는 커뮤니티(SNMP V2C)를 선택합니다.

참고

Community 목록에는 트랩 호스트가 이미 할당된 커뮤니티만 표시됩니다.

6. 새 커뮤니티를 생성하려면 다음을 수행합니다.
   a. Community 드롭다운 메뉴에서 **Create New Community**를 선택합니다.
   b. **Community** 상자에 새 커뮤니티의 이름을 입력합니다.
   c. 액세스 유형을 선택합니다.
   d. 추가(+) 버튼을 클릭합니다.
   e. 트랩 호스트 이름을 입력합니다.
   f. **OK**를 클릭합니다.
   g. **OK**를 클릭합니다.
7. **OK**를 클릭합니다.

SNMP V3 및 V2C 트랩 호스트 수정

기존 트랩 구성에 대한 포트 번호 및 커뮤니티 선택을 수정할 수 있습니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. **SNMP V3 Trap Hosts** 또는 **SNMP V2C Trap Hosts** 영역에서 Trap Host 항목 하나를 선택하고 **Modify**를 클릭합니다.

   Modify SNMP [V3 or V2C] Trap Hosts 대화 상자가 나타납니다.
3. 포트 번호를 수정하려면 **Port** 상자에 새 포트 번호를 입력합니다. 포트 162가 일반적인 포트입니다.
4. 드롭다운 메뉴에서 사용자(SNMP V3) 또는 커뮤니티(SNMP V2C)를 선택합니다.

   참고

   Community 목록에는 트랩 호스트가 이미 할당된 커뮤니티만 표시됩니다.
5. 새 커뮤니티를 생성하려면 다음을 수행합니다.
   a. Community 드롭다운 메뉴에서 **Create New Community**를 선택합니다.
   b. **Community** 상자에 새 커뮤니티의 이름을 입력합니다.
   c. 액세스 유형을 선택합니다.
   d. 추가(+) 버튼을 클릭합니다.
   e. 트랩 호스트 이름을 입력합니다.
   f. **OK**를 클릭합니다.
   g. **OK**를 클릭합니다.
6. **OK**를 클릭합니다.

SNMP V3 및 V2C 트랩 호스트 제거

SNMP 탭을 사용해 기존 트랩 호스트 구성을 삭제합니다.

절차

1. **Administration** > **Settings** > **SNMP**를 선택합니다.
2. **Trap Hosts** 영역(V3 또는 V2C의 경우) 트랩 호스트에 해당하는 확인란을 선택하고 **Delete**를 클릭합니다.

   Delete SNMP [V3 or V2C] Trap Hosts 대화 상자가 나타납니다.
3. 삭제할 호스트 이름을 확인하고 **OK**를 클릭합니다.
4. Delete SNMP [V3 or V2C] Trap Hosts Status 대화 상자에서 **Close**를 클릭합니다.

   트랩 호스트 항목이 **Trap Hosts** 테이블에서 제거됩니다.

자동 지원 보고서 관리

자동 지원 기능은 ASUP라는 보고서를 생성합니다. ASUP는 시스템 식별 정보, Data Domain 시스템 명령의 통합 출력 결과 및 각종 로그 파일에 입력된 정보를 보여 줍니다. 보고서의 끝에는 광범위하고 자세한 내부 통계가 나타납니다. 이 보고서는 시스템 문제의 디버깅 시 Data Domain 지원 팀에게 도움이 되도록 설계되었습니다.

ASUP는 파일 시스템이 시작될 때마다 생성되며 일반적으로 하루 한 번 생성됩니다. 그러나 파일 시스템이 하루에 두 번 이상 시작될 수도 있습니다.

이메일 주소를 구성하여 일일 ASUP를 받아 볼 수 있으며, 이러한 보고서를 Data Domain으로 전송하는 기능을 활성화 또는 비활성화할 수 있습니다. 일일 ASUP를 전송하는 기본 시간은 오전 6시이며 이 시간은 구성할 수 있습니다. Data Domain에 ASUP를 전송하는 경우 기존의 비보안 방식을 선택하거나 전송 전에 정보를 암호화하는 ConnectEMC 방식을 선택할 수 있습니다.

HA 시스템 자동 지원 및 지원 번들 관리

구성 작업은 액티브 노드에서 수행하며, 구성 내용이 대기 노드에 미러링됩니다. 따라서 두 노드에 동일한 구성이 적용되지만 통합 ASUP 및 지원 번들은 없습니다.

액티브 노드의 자동 지원 및 지원 번들에는 로컬 노드 정보와 함께 파일 시스템, 복제, 프로토콜 및 전체 HA 정보가 포함됩니다. 대기 노드의 자동 지원 및 지원 번들에는 로컬 노드 정보와 일부 HA 정보(구성 및 상태)만 있지만 파일 시스템/복제/프로토콜 정보는 없습니다. HA 시스템 상태(파일 시스템, 복제, 프로토콜 및 HA 구성)와 관련한 문제를 디버그하려면 두 노드의 자동 지원 및 지원 번들이 필요합니다.

Data Domain에 대한 자동 지원 보고 활성화 및 비활성화

Data Domain으로의 알림 전송 여부에 영향을 미치지 않고 Data Domain에 대한 자동 지원 보고를 활성화하거나 비활성화할 수 있습니다.

절차

1. 자동 지원 보고 상태를 보려면 **Maintenance** > **Support** > **Autosupport**를 선택합니다.

   자동 지원 보고 상태는 Support 영역의 Scheduled autosupport 레이블 옆에 강조 표시됩니다. 현재 구성에 따라 **Enable** 또는 **Disable** 버튼이 Scheduled autosupport 행에 표시됩니다.
2. Data Domain에 대한 자동 지원 보고를 활성화하려면 Scheduled autosupport 행에서 **Enable**을 클릭합니다.

3. Data Domain에 대한 자동 지원 보고를 비활성화하려면 Scheduled autosupport 행에서 **Disable**을 클릭합니다.

생성된 자동 지원 보고서 검토

자동 지원 보고서를 검토해 이전에 캡처된 시스템 통계 및 구성 정보를 봅니다. 시스템에는 자동 지원 보고서가 최대 14개까지 저장됩니다.

절차

1. **Maintenance** > **Support** > **Autosupport**를 선택합니다.

   Autosupport Reports 페이지에는 자동 지원 보고서 파일 이름 및 파일 크기, 그리고 보고서의 생성 날짜가 표시됩니다. 보고서의 이름은 자동으로 만들어집니다. 가장 최근 보고서는 autosupport이며, 전날에 생성된 보고서는 autosupport.1이고, 보고서 생성 날짜가 오래된 것일수록 숫자가 커집니다.

   CLI 절차

   ```
   # autosupport show history
   ```

2. 파일 이름 링크를 클릭하면 텍스트 편집기를 사용해 보고서를 볼 수 있습니다. 브라우저의 요구 사항인 경우 먼저 파일을 다운로드합니다.

자동 지원 메일 목록 구성

자동 지원 메일 목록에는 이메일을 통해 자동 지원 메시지를 수신하는 구독자가 나열됩니다. Autosupport 탭을 사용해 구독자를 추가, 수정 및 삭제합니다.

자동 지원 이메일은 구성된 메일 서버를 통해 자동 지원 이메일 목록에 있는 모든 구독자에게 전송됩니다. 메일 서버와 자동 지원 이메일 목록을 구성한 후에는 설정을 테스트하여 자동 지원 메시지가 의도된 대상에게 잘 전송되는지 확인하는 것이 좋습니다.

절차

1. **Maintenance** > **Support** > **Autosupport**를 선택합니다.
2. **Configure**를 클릭합니다.

   Configure Autosupport Subscribers 대화 상자가 나타납니다.

3. 구독자를 추가하려면 다음을 수행합니다.
   a. 추가(**+**) 버튼을 클릭합니다.

      Email 대화 상자가 나타납니다.

   b. Email 상자에 받는 사람 이메일 주소를 입력합니다.

   c. OK를 클릭합니다.

   CLI 절차

   ```
   # autosupport add asup-detailed emails djones@company.com # autosupport add alert-summary emails djones@company.com
   ```

4. 구독자를 삭제하려면 다음을 수행합니다.
   a. Configure Autosupport Subscribers 대화 상자에서 삭제할 구독자를 선택합니다.

   b. 삭제(**X**) 버튼을 클릭합니다.

   CLI 절차

```
 # autosupport del asup-detailed emails djones@company.com #
autosupport del alert-summary emails djones@company.com
```

5. 구독자 이메일 주소를 수정하려면 다음을 수행합니다.
   a. Configure Autosupport Subscribers 대화 상자에서 편집할 구독자 이름을 선택합니다.
   b. 수정 버튼(연필 아이콘)을 클릭합니다.
      Email 대화 상자가 나타납니다.
   c. 필요한 대로 이메일 주소를 수정합니다.
   d. OK를 클릭합니다.
6. **OK**를 클릭하여 Configure Autosupport Subscribers 대화 상자를 닫습니다.
   수정된 자동 지원 이메일 목록이 Autosupport Mailing List 영역에 나타납니다.

Data Domain이 외부 수신자에게 ASUP 및 알림 이메일을 보낼 수 있는지 확인

외부 이메일 수신자가 사용자가 Data Domain 디바이스에서 보내는 자동 지원(ASUP) 및 알림 이메일을 받을 수 있는지 확인합니다.

자동 지원(ASUP)이 교환 서버에 의해 릴레이되는지 확인합니다.

절차

1. ASUP을 동일한 메일 서버의 이메일 주소인 로컬 이메일 주소로 보낼 수 있는지 확인합니다.

   ```
   # autosupport send [internal-email-addr]
   ```

2. ASUP을 로컬 메일 서버 외부의 이메일 주소로 보낼 수 있는지 확인합니다.

   ```
   # autosupport send [external email-addr]
   ```

3. 이메일이 메일 서버의 외부 이메일 주소로 전송되지 않으면 다음과 같은 오류가 나타날 수 있습니다.

   ```
   **** Unable to send message: (errno 51: Unrecoverable errors
   from server--giving up)
   ```

   이 경우 https://support.emc.com/kb/181900에서 사용할 수 있는 KB 문서, *MS Exchange에서 이메일 릴레이 구성*에 설명된 단계를 사용하여 로컬 메일 서버의 Data Domain 시스템에 대해 전달을 활성화해야 할 수 있습니다.

4. ASUP을 외부 이메일 주소로 보낼 수 있지만 Data Domain으로 전달되지 않으면 방화벽 구성 또는 스팸 필터에 문제가 있는 것일 수 있습니다.
5. ASUP 알림이 Data Domain으로 전송되지만 사례가 생성되지 않을 경우 알림 이메일의 제목 또는 본문에 잘못된 문자가 있기 때문일 수 있습니다. 확인하려면 다음을 수행합니다.
   a. 현재 자동 지원을 살펴보고 HOSTNAME, SYSTEM_ID, LOCATION에 작은따옴표 또는 아포스트로피가 있는지 확인합니다. 이것은 DD OS 버전 4.9.2.0 및 이전 버전에서 잘못된 문자이므로 제거해야 합니다.

   ```
   Example:


   ==========  GENERAL INFO  ==========
   GENERATED_ON=Thu Apr 28 06:54:55 PDT 2011
   ```

```
VERSION=Data Domain OS 4.9.2.6-226914
SYSTEM_ID=7FP5105000


MODEL_NO=DD510
HOSTNAME=system.datadomain.com


LOCATION=123 O Malley Lane
```

b. 시스템 HOSTNAME 및/또는 LOCATION에서 잘못된 문자를 제거합니다. 명령은 다음과 같습니다.

```
net set hostname <host>

config set location "location"
```

c. 알림을 시뮬레이트하여 새 설정을 테스트합니다. 가장 쉬운 방법은 예비 디스크 드라이브를 수동으로 장애 처리하고, 전송된 알림을 확인한 후, 같은 드라이브의 장애 처리를 즉시 해제하여 예비 상태로 되돌리는 것입니다.

지원 번들 관리

지원 번들은 시스템 구성 및 작업 정보를 포함하는 파일입니다. 소프트웨어 업그레이드 또는 컨트롤러 업그레이드 등의 시스템 토폴로지 변경 전에 지원 번들을 생성하는 것이 좋습니다.

Data Domain 지원 팀에서는 지원을 제공할 때 지원 번들을 요청하는 경우가 많습니다.

https://support.emc.com/kb/180563에서 사용할 수 있는 KB 문서, *DDR(Data Domain Restorer)에서 지원 번들(SUB)을 수집/업로드하는 방법*에서는 지원 번들 사용에 대한 추가 정보를 제공합니다.

지원 번들 생성

문제 해결 과정에서 Data Domain 고객 지원 팀이 지원 번들을 요청할 수 있습니다. 지원 번들은 자동 지원 헤더가 포함되어 있는 README 파일과 선택한 로그 파일을 tar-g-zip 압축한 파일입니다.

절차

1. **Maintenance** > **Support** > **Support Bundles**를 선택합니다.
2. **Generate Support Bundle**을 클릭합니다.

   참고

   시스템에서는 최대 5개의 지원 번들을 지원합니다. 여섯 번째 지원 번들을 생성하면 자동으로 가장 오래된 지원 번들이 삭제됩니다. CLI 명령 `support bundle delete`를 사용하여 지원 번들을 삭제할 수도 있습니다.

   또한 이전 형식 `support-bundle.tar.gz`를 사용해 만든 이름의 지원 번들이 있는 업그레이드한 시스템에서 지원 번들을 생성하면 해당 파일은 새 이름 형식을 사용하도록 이름이 바뀝니다.

3. 고객 지원 팀에 이메일(support@emc.com)로 파일을 보냅니다.

참고

번들이 너무 커서 이메일로 보낼 수 없는 경우에는 온라인 지원 사이트를 이용하여 번들을 업로드하십시오. https://support.emc.com으로 이동합니다.

지원 번들 목록 보기

Support Bundles 탭을 사용해 시스템에 있는 지원 번들 파일을 봅니다.

절차

1. **Maintenance** > **Support** > **Support Bundles**를 선택합니다.

   지원 번들 목록이 나타납니다.

   여기에는 지원 번들 파일 이름, 파일 크기, 번들이 생성된 날짜가 표시됩니다. 번들의 이름은 자동으로 *hostname*-support-bundle-*datestamp*.tar.gz라고 지정됩니다. 예제 파일 이름인 localhost-support-bundle-1127103633.tar.gz는 지원 번들이 11월 27일 10시 36분 33초에 localhost 시스템에서 생성되었음을 나타냅니다.

2. 파일 이름 링크를 클릭하고 gz/tar 압축 해제 툴을 선택해 번들의 ASCII 컨텐츠를 봅니다.

coredump 관리

coredump로 인해 DD OS가 충돌하면 문제를 설명하는 core 파일이 /ddvar/core 디렉토리에 생성됩니다. 이 파일은 크고 Data Domain 시스템에서 복사하기가 어려울 수 있습니다.

코어 파일이 너무 커서 Data Domain 시스템에서 복사할 수 없는 경우 **support coredump split *<filename>* by *<n>* {MiB|GiB}** 명령을 실행합니다. 여기서 다음이 적용됩니다.

- *<filename>*은 /ddvar/core 디렉토리에 있는 core 파일의 이름입니다.
- *<n>*은 core 파일을 분할할 더 작은 청크의 수입니다.

  참고

  단일 core 파일을 최대 20개 청크로 분할할 수 있습니다. 지정된 크기로 인해 20개를 초과하는 청크가 발생하면 명령이 실패하고 오류가 발생합니다.

예를 들어 이름이 cpmdb.core.19297.1517443767인 42.1MB core 파일을 10MB 청크로 분할하면 5개 청크가 발생합니다.

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                                Size       Time Created
---------------------------------   --------   ------------------------
cpmdb.core.19297.1517443767_5_01    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05    2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5     0 MiB      Mon Feb  5 11:50:58 2018
---------------------------------   --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

support coredump save *<file-list>* 명령을 실행하여 지정된 코어 덤프 파일을 USB 드라이브에 저장합니다.

알림 관리

알림 기능은 구성 가능한 이메일 목록과 Data Domain에 배포할 수 있는 이벤트 및 요약 보고서를 생성합니다.

이벤트 보고서는 즉시 전송되어 시스템 이벤트에 대한 자세한 정보를 제공합니다. 이벤트 알림에 대한 배포 목록을 *알림 그룹*이라고 합니다. 알림 그룹에 하나 이상의 이메일 주소가 포함되도록 구성하여 해당 주소로 전송되는 이벤트 보고서의 유형과 심각도 수준을 구성할 수 있습니다. 예를 들어 중요한 이벤트에 대해 알아야 하는 개인을 위한 알림 그룹과, 덜 중요한 이벤트를 모니터링하는 개인을 위한 알림 그룹을 구성할 수 있습니다. 또 다른 옵션은 서로 다른 기술에 대해 그룹을 구성하는 것입니다. 예를 들어 모든 네트워크 이벤트에 대한 이메일 메시지를 받는 알림 그룹을 구성하고 스토리지 문제에 대한 메시지를 받는 그룹을 구성할 수 있습니다.

요약 보고서는 매일 전송되며 지난 24시간 동안 발생한 이벤트의 요약을 제공합니다. 이벤트 보고서에 제공되는 모든 정보가 요약 보고서에 포함되지는 않습니다. 일일 보고서의 기본 생성 시간은 오전 8시이며, 이 시간은 변경될 수 있습니다. 요약 보고서는 이벤트 알림 그룹과 분리된 전용 이메일 목록을 사용하여 전송됩니다.

Data Domain에 대한 알림 배포는 활성화하거나 비활성화할 수 있습니다. Data Domain에 보고서를 전송하는 경우 기존의 비보안 방식을 선택하거나 보안이 설정된 전송을 위한 Secure Remote Services 방식을 선택할 수 있습니다.

HA 시스템 알림 관리

HA 시스템의 알림 기능은 비 HA 시스템처럼 이벤트와 요약 보고서를 생성하지만, 2개의 노드로 이루어진 시스템 구성으로 인해 HA 시스템에서는 알림을 관리하는 방식이 다릅니다.

초기 알림 구성은 액티브 노드에서 수행되어 대기 노드에 미러링됩니다. 따라서 두 노드에 동일한 구성이 적용됩니다. 알림 설정에 따라 로컬 및 AM 알림이 e-메일로 전송되며, 이 알림에는 HA 시스템에서 발생한 알림임을 나타내는 정보와 알림이 생성된 노드에 대한 정보(액티브 또는 대기)가 포함됩니다.

페일오버 시에 파일 시스템, 복제 또는 프로토콜에 대한 활성 알림이 있는 경우, 알림 조건을 지우지 않는 한 페일오버 후에도 해당 활성 알림이 새 액티브 노드에 계속 표시됩니다.

파일 시스템, 복제 및 프로토콜에 대한 이전 알림은 페일오버 시에 파일 시스템과 함께 페일오버되지 않고 원래 생성되었던 노드에 그대로 유지됩니다. 즉, 액티브 노드의 CLI에는 파일 시스템, 복제 및 프로토콜에 대한 이전 알림의 완전한/지속적인 보기가 표시되지 않습니다.

페일오버를 수행하는 동안 이전 로컬 알림은 생성되었던 노드에 유지되지만, 파일 시스템, 복제 및 프로토콜에 대한 이전 알림("논리적 알림"으로 통칭)은 파일 시스템과 함께 페일오버됩니다.

참고

Health > **High Availability** 패널에는 HA와 관련된 알림만 표시됩니다. 해당 알림은 HA Manager, 노드, 상호 연결, 스토리지, SAS 연결 등의 주요 HA 구성 요소별로 필터링할 수 있습니다.

알림 그룹 목록 보기

알림 그룹은 다양한 알림 유형(클래스) 및 이메일 주소(구독자의 이메일) 그룹을 정의합니다. 알림 목록에서 선택된 유형의 알림이 생성될 때마다 알림이 목록의 구독자에게 전송됩니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.

   CLI 절차

   ```
   # alerts notify-list show
   ```

2. Group Name 목록의 항목을 제한(필터링)하려면 Group Name 상자에 그룹 이름을 입력하거나 Alert Email 상자에 구독자 이메일을 입력하고 **Update**를 클릭합니다.

   참고

   모든 구성된 그룹을 표시하려면 **Reset**을 클릭합니다.

3. 그룹에 대한 자세한 정보를 표시하려면 Group Name 목록에서 해당 그룹을 선택합니다.

Notification 탭

Notification 탭에서는 선택한 알림 유형 및 심각도 수준에 대한 시스템 알림을 수신할 e-메일 주소 그룹을 구성할 수 있습니다.

표 52 Group Name 목록, 열 레이블 설명

항목	설명
Group Name	그룹의 구성된 이름입니다.
Classes	그룹에 보고되는 알림 클래스의 수입니다.
Subscribers	e-메일을 통해 알림을 수신하도록 구성된 구독자의 수입니다.

표 53 Detailed Information, 레이블 설명

항목	설명
Class	알림을 전달할 수 있는 서비스 또는 서브시스템입니다. 알림 그룹은 여기에 나열된 클래스에 대한 알림을 수신합니다.
Severity	알림 그룹에 전송되는 e-메일을 트리거하는 심각도 수준입니다. 지정된 심각도 수준 이상의 모든 알림이 알림 그룹에 전송됩니다.
Subscribers	Subscribers 영역에는 알림 그룹에 대해 구성된 모든 e-메일 주소 목록이 표시됩니다.

표 54 Notification 탭 컨트롤

컨트롤	설명
Add 버튼	알림 그룹 생성을 시작하려면 **Add** 버튼을 클릭합니다.

표 54 Notification 탭 컨트롤 (계속)

컨트롤	설명
Class Attributes Configure 버튼	선택한 알림 그룹에 대한 알림을 생성하는 클래스 및 심각도 수준을 변경하려면 이 Configure 버튼을 클릭합니다.
Delete 버튼	선택한 알림 그룹을 삭제하려면 **Delete** 버튼을 클릭합니다.
Filter By: Alert Email 상자	특정 텍스트가 있는 e-메일 주소가 포함된 그룹으로 Group Name 목록의 항목을 제한하려면 이 상자에 텍스트를 입력합니다.
Filter By: Group Name 상자	특정 텍스트가 포함된 그룹 이름으로 Group Name 목록의 항목을 제한하려면 이 상자에 텍스트를 입력합니다.
Modify 버튼	선택한 알림 그룹에 대한 구성을 수정하려면 **Modify** 버튼을 클릭합니다.
Reset 버튼	Filter By 상자의 항목을 제거하고 모든 그룹 이름을 표시하려면 이 버튼을 클릭합니다.
Subscribers Configure 버튼	선택한 알림 그룹에 대한 e-메일 목록을 변경하려면 이 Configure 버튼을 클릭합니다.
Update 버튼	필터 상자에 텍스트를 입력한 후 그룹 이름 목록을 업데이트하려면 이 버튼을 클릭합니다.

알림 그룹 생성

알림 그룹을 추가하고 각 그룹에 대한 심각도 수준을 선택하려면 Notification 탭을 사용합니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.
2. **Add**를 클릭합니다.

   Add Group 대화 상자가 나타납니다.

3. **Group Name** 상자에 그룹 이름을 입력합니다.
4. 알려야 하는 하나 이상의 알림 클래스에 대한 확인란을 선택합니다.
5. 클래스의 기본 심각도(Warning)를 변경하려면 연결된 목록 상자에서 다른 레벨을 선택합니다.

   심각도 레벨은 오름차순으로 나열됩니다. *Emergency*가 가장 높은 심각도 레벨입니다.

6. **OK**를 클릭합니다.

   CLI 절차

   ```
   # alerts notify-list create eng_grp class hardwareFailure
   ```

그룹의 구독자 목록 관리

Notification 탭을 사용해 알림 그룹 구독자 목록에서 이메일 주소를 추가, 수정 또는 삭제합니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.
2. Notifications 그룹 목록에서 그룹의 확인란을 선택하고 다음 중 하나를 수행합니다.
   - **Modify**를 클릭하고 **Subscribers**를 선택합니다.
   - Subscribers 목록에서 **Configure**를 클릭합니다.
3. 그룹에 구독자를 추가하려면 다음을 수행합니다.
   a. **+** 아이콘을 클릭합니다.

      Email Address 대화 상자가 나타납니다.

   b. 구독자의 이메일 주소를 입력합니다.

   c. **OK**를 클릭합니다.

      CLI 절차

      ```
      # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      ```

4. 이메일 주소를 수정하려면 다음을 수행합니다.
   a. **Subscriber Email** 목록에서 이메일 주소의 확인란을 클릭합니다.

   b. 연필 모양 아이콘을 클릭합니다.

   c. Email Address 대화 상자에서 이메일 주소를 편집합니다.

   d. **OK**를 클릭합니다.
5. 이메일 주소를 삭제하려면 **Subscriber Email** 목록에서 이메일 주소의 확인란을 클릭하고 **X** 아이콘을 클릭합니다.

   CLI 절차

   ```
   # alerts notify-list del eng_lab emails bob@urcompany.com
   ```

6. **Finish**를 클릭하거나 **OK**를 클릭합니다.

알림 그룹 수정

Notification 테이블을 사용해 기존 그룹의 속성 클래스를 수정합니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.
2. 그룹 목록에서 수정할 그룹의 확인란을 선택합니다.
3. 그룹에 대한 클래스 속성을 수정하려면 다음을 수행합니다.
   a. Class Attributes 영역에서 **Configure**를 클릭합니다.

      Edit Group 대화 상자가 나타납니다.

   b. 하나 이상의 클래스 속성에 해당하는 확인란을 선택하거나 선택을 취소합니다.

c. 클래스 속성의 심각도를 변경하려면 해당 목록 상자에서 레벨을 선택합니다.

d. **OK**를 클릭합니다.

CLI 절차

```
# alerts notify-list add eng_lab class cloud severity warning
# alerts notify-list del eng_lab class cloud severity notice
```

4. 그룹에 대한 구독자 목록을 수정하려면 다음을 수행합니다.

a. Subscribers 영역에서 **Configure**를 클릭합니다.

Edit Subscribers 대화 상자가 나타납니다.

b. 그룹 목록에서 구독자를 삭제하려면 삭제할 구독자의 확인란을 선택하고 삭제 아이콘(X)을 클릭합니다.

c. 구독자를 추가하려면 추가 아이콘(+)을 클릭하고 구독자 이메일 주소를 입력한 후 OK를 클릭합니다.

d. **OK**를 클릭합니다.

CLI 절차

```
# alerts notify-list add eng_lab emails
mlee@urcompany.com,bob@urcompany.com
# alerts notify-list del eng_lab emails bob@urcompany.com
```

5. **OK**를 클릭합니다.

알림 그룹 삭제

Notification 탭을 사용해 하나 이상의 기존 알림 그룹을 삭제합니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.
2. Notifications 그룹 목록에서 하나 이상의 그룹 확인란을 선택하고 **Delete**를 클릭합니다.

   Delete Group 대화 상자가 나타납니다.

3. 삭제를 확인하고 **OK**를 클릭합니다.

   CLI 절차

```
# alerts notify-list destroy eng_grp
```

알림 그룹 구성 재설정

Notification 탭을 사용해 Default 그룹에 추가된 모든 알림 그룹과 Default 그룹의 변경 내용을 제거합니다.

절차

1. **Health** > **Alerts** > **Notification**을 선택합니다.
2. **More Tasks** > **Reset Notification Groups**를 선택합니다.
3. Reset Notification Groups 대화 상자의 Verification 대화 상자에서 **Yes**를 클릭합니다.

   CLI 절차

```
# alerts notify-list reset
```

일일 요약 스케줄 및 배포 목록 구성

매일 각 관리 대상 시스템에서는 alertssummary.list 이메일 그룹에 대해 구성된 구독자들에게 Daily Alert Summary 이메일을 보냅니다. Daily Alert Summary 이메일에는 현재 및 이전 알림이 포함되며 곧 해결해야 할 심각하지 않은 하드웨어 상황 및 디스크 공간 사용량 수에 대한 메시지를 보여 줍니다.

가급적 빨리 해결해야 하는 심각하지 않은 문제의 예로 팬 장애를 들 수 있습니다. 고객 서비스는 장애 알림을 수신하면 사용자에게 연락하여 구성 요소 교체 일정을 수립합니다.

절차

1. **Health** > **Alerts** > **Daily Alert Summary**를 선택합니다.
2. 기본 제공 시간 오전 8시가 허용되지 않는 경우 다음을 수행합니다.
   a. **Schedule**을 클릭합니다.

      Schedule Alert Summary 대화 상자가 나타납니다.

   b. 목록 상자를 사용하여 요약 보고서에 대해 시, 분 및 AM 또는 PM을 선택합니다.
   c. **OK**를 클릭합니다.

      CLI 절차

      ```
      # autosupport set schedule alert-summary daily 1400
      ```

3. 일일 알림 구독자 목록을 구성하려면 다음을 수행합니다.
   a. **Configure**를 클릭합니다.

      Daily Alert Summary Mailing List 대화 상자가 나타납니다.

   b. 일일 알림 구독자 목록을 다음과 같이 수정합니다.
      - 구독자를 추가하려면 **+** 아이콘을 클릭하고 이메일 주소를 입력한 뒤 **OK**를 클릭합니다.
        CLI 절차

        ```
        # autosupport add alert-summary emails djones@company.com
        ```
      - 이메일 주소를 수정하려면 구독자 확인란을 선택하고 연필 아이콘을 클릭하여 이메일 주소를 편집한 뒤 **OK**를 클릭합니다.
      - 이메일 주소를 삭제하려면 구독자 확인란을 선택하여 **X**를 클릭합니다.
        CLI 절차

        ```
        # autosupport del alert-summary emails djones@company.com
        ```

   c. **Finish**를 클릭합니다.

Daily Alert Summary 탭

Daily Alert Summary 탭에서는 모든 시스템 알림의 요약을 매일 수신할 사용자의 e-메일 목록을 구성할 수 있습니다. 이 목록의 사용자에게는 개별 알림이 전송되지 않습니다. 개별 알림을 받으려면 알림 그룹에도 추가되어야 합니다.

표 55 Daily Alert Summary, 레이블 설명

항목	설명
Delivery Time	전달 시간은 일별 e-메일에 구성된 시간을 보여 줍니다.
Email List	이 목록에는 일별 e-메일을 수신하는 사용자의 e-메일 주소가 표시됩니다.

표 56 Daily Alert Summary 탭 컨트롤

컨트롤	설명
Configure 버튼	구독자 e-메일 목록을 편집하려면 **Configure** 버튼을 클릭합니다.
Schedule 버튼	일별 보고서가 전송되는 시간을 구성하려면 **Schedule** 버튼을 클릭합니다.

Data Domain에 대한 알림 활성화 및 비활성화

Data Domain으로의 자동 지원 보고서 전송 여부에 영향을 미치지 않고 Data Domain에 대한 알림 통지를 활성화하거나 비활성화할 수 있습니다.

절차

1. 알림 보고 상태를 보려면 **Maintenance** > **Support** > **Autosupport**를 선택합니다.

   Support 영역의 Real-time alert 레이블 옆에 알림 통지 상태가 녹색으로 강조 표시됩니다. 현재 구성에 따라 **Enable** 또는 **Disable** 버튼이 Real-time alert 행에 표시됩니다.
2. Data Domain에 대한 알림 보고를 활성화하려면 Real-time alert 행에서 **Enable**을 클릭합니다.
3. Data Domain에 대한 알림 보고를 비활성화하려면 Real-time alert 행에서 **Disable**을 클릭합니다.

알림 이메일 기능 테스트

선택한 알림 그룹 또는 이메일 주소로 테스트 이메일을 보내려면 Notification 탭을 사용합니다. 이 기능을 활용해 시스템이 알림 메시지를 전송할 수 있도록 올바르게 구성되어 있는지 확인할 수 있습니다.

절차

1. 테스트 알림을 Data Domain으로 전송할지 여부를 제어하려면 다음을 수행합니다.

   a. **Maintenance** > **Support** > **Autosupport**를 선택합니다.

   b. 테스트 이메일의 전송 여부를 제어하려면 **Alert Support** 영역에서 **Enable** 또는 **Disable**을 클릭합니다.

   이메일 주소는 변경할 수 없습니다.
2. **Health** > **Alerts** > **Notification**을 선택합니다.
3. **More Tasks** > **Send Test Alert**를 선택합니다.

   Send Test Alert 대화 상자가 나타납니다.

4. **Notification Groups** 목록에서 테스트 이메일을 받을 그룹을 선택한 뒤 **Next**를 클릭합니다.
5. 필요에 따라 이메일을 받을 이메일 주소를 더 추가합니다.
6. **Send Now**를 클릭하고 **OK**를 클릭합니다.

   CLI 절차

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```

7. Data Domain에 테스트 알림을 전송하는 기능을 비활성화했지만, 지금 활성화하고자 한다면 다음을 수행합니다.

   a. **Maintenance** > **Support** > **Autosupport**를 선택합니다.

   b. **Alert Support** 영역에서 **Enable**을 클릭합니다.

결과

메일러 문제 확인을 위해 새로 추가된 알림 이메일을 테스트하려면 **autosupport test email***email-addr*을 입력합니다.

예를 들어, 목록에 이메일 주소 djones@yourcompany.com을 추가하고 나서 **autosupport test email***djones@yourcompany.com* 명령을 사용하여 주소를 확인합니다.

지원 제공 관리

제공 관리는 알림 및 자동 지원 보고서를 Data Domain으로 보내는 방법을 정의합니다. 기본적으로 알림 및 자동 지원 보고서는 표준(비보안) 이메일을 사용해 Data Domain 고객 지원 팀으로 전송됩니다. ConnectEMC 방식은 Secure Remote Services VE(Virtual Edition) 게이트웨이를 통해 안전한 형식으로 메시지를 전송합니다.

ConnectEMC 방식을 Secure Remote Services 게이트웨이와 함께 사용할 때의 장점 중 하나는 단일 게이트웨이로 여러 시스템의 메시지를 전달할 수 있으므로 여러 시스템이 아닌 Secure Remote Services 게이트웨이에 대한 네트워크 보안만 구성하면 된다는 것입니다. 또한 전자 라이센스를 채택한 경우 사용 정보 보고서가 생성되어 전송됩니다.

Secure Remote Services 게이트웨이를 구성할 때 Data Domain 시스템은 이중화를 보장하기 위해 다중 게이트웨이 등록을 지원합니다.

Data Domain으로 표준 이메일 제공 선택

표준(비보안) 이메일 제공 방법을 선택하면 이 제공 방법이 알림 및 자동 지원 보고에 모두 적용됩니다.

절차

1. **Maintenance** > **Support** > **Autosupport**를 선택합니다.
2. Support 영역의 Channel 행에서 **Configure**를 클릭합니다.

   Configure EMC Support Delivery 대화 상자가 나타납니다. 제공 방법은 Support 영역의 Channel 레이블 다음에 표시됩니다.
3. **Channel** 목록 상자에서 **Email to datadomain.com**을 선택합니다.
4. **OK**를 클릭합니다.

   CLI 절차

```
# support notification method set email
```

Secure Remote Services 제공 선택 및 구성

Secure Remote Services VE(Virtual Edition) Gateway는 종합적인 보안 시스템으로 강화된 IP 기반 솔루션을 통해 자동화된 connect home 및 원격 지원 기능을 제공합니다.

운영 환경 내부 Secure Remote Services 버전 3 게이트웨이는 운영 환경 내부 Data Domain 시스템 및 DD VE 인스턴스와 클라우드 기반 DD VE 인스턴스를 모두 모니터링하는 기능을 제공합니다.

절차

1. **Maintenance** > **Support** > **Autosupport**를 선택합니다.
2. Support 영역의 Channel 행에서 **Configure**를 클릭합니다.

   Configure Dell EMC Support Delivery 대화 상자가 나타납니다. 제공 방법은 Support 영역의 Channel 레이블 다음에 표시됩니다.
3. **Channel** 목록 상자에서 **Secure Remote Services**를 선택합니다.
4. 게이트웨이 호스트 이름을 입력하고 Data Domain 시스템의 로컬 IP 주소를 선택합니다.
5. **OK**를 클릭합니다.
6. 서비스 링크 사용자 이름 및 암호를 입력한다.
7. **Register**를 클릭합니다.

   Autosupport 패널에 Secure Remote Services 세부 정보가 표시됩니다.

CLI 절차

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

⚠ 주의

Data Domain HA 쌍에서 Secure Remove Services 제공을 구성하는 경우

- **두 노드를 등록할 Data Domain HA 쌍에서 Secure Remote Services를 구성할 때 `ha-peer` 매개변수가 필요합니다.**
- **사용자는 HA 쌍을 등록하려고 하면 실패하고 RSA 키 토큰이 동기화되지 않으므로 서비스 링크 자격 증명을 제공하여 HA 쌍에 대해 `support connectemc device register` 명령을 실행해야 합니다.**

ConnectEMC 작업 테스트

CLI 명령을 사용하면 Secure Remote Services 게이트웨이를 통해 Support에 테스트 메시지를 전송하여 ConnectEMC 작업을 테스트할 수 있습니다.

절차

1. ConnectEMC 작업을 테스트하려면 CLI를 사용합니다.

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

로그 파일 관리

Data Domain 시스템은 발생할 수 있는 시스템 문제 해결에 도움을 받기 위해 번들로 묶어 지원 팀에 보낼 수 있는 로그 파일 세트를 유지합니다. 어떠한 사용자도 DD System Manager를 사용해 로그 파일을 수정하거나 삭제할 수 없지만 로그 디렉토리에서 복사하고 시스템에서 관리할 수 있습니다.

참고

HA 시스템의 로그 메시지는 로그 파일이 원래 생성된 노드에 유지됩니다.

로그 파일은 매주 교체됩니다. 매주 일요일 오전 0시 45분에 시스템에서 기존 로그에 대한 새 로그 파일을 자동으로 열고 이전 파일의 이름을 추가된 번호로 변경합니다. 예를 들어 작업 첫 주가 지난 후에 지난주 `messages` 파일의 이름이 `messages.1`로 바뀌고, 새 메시지가 새 메시지 파일에 저장됩니다. 번호가 매겨진 파일은 매주 다음 번호로 넘어갑니다. 예를 들어 둘째 주가 지난 후에 `messages.1` 파일이 `messages.2`로 넘어갑니다. `messages.2` 파일이 이미 있는 경우 `messages.3`으로 넘어갑니다. 보존 기간(아래 테이블 참조)이 종료되면 만료된 로그가 삭제됩니다. 예를 들어 `messages.8`이 `messages.9`로 넘어가면 기존 `messages.9` 파일이 삭제됩니다.

`audit.log`는 주단위로 순환되지 않습니다. 대신 파일 크기가 70MB에 도달하면 순환됩니다.

이 항목에 나와 있는 경우를 제외하고 로그 파일은 `/ddvar/log`에 저장됩니다.

참고

`/ddvar` 디렉토리에 있는 파일은 Linux 사용자에게 해당 디렉토리에 대한 *쓰기* 권한이 할당된 경우 Linux 명령을 사용해 삭제할 수 있습니다.

각 시스템에 있는 로그 파일 세트는 시스템에서 구성된 기능과 발생하는 이벤트에 따라 결정됩니다. 다음 표에는 시스템에서 생성할 수 있는 로그 파일을 설명합니다.

표 57 시스템 로그 파일

로그 파일	설명	보존 기간
audit.log	로그인 이벤트에 대한 메시지입니다.	15주
cifs.log	CIFS 서브시스템의 로그 메시지는 `debug/cifs/cifs.log`에만 기록됩니다. 크기는 50MiB로 제한됩니다.	10주
messages	실행한 명령을 포함해 일반 시스템 이벤트에 대한 메시지입니다.	9주
secure.log	로그인 성공 및 실패, 사용자 추가 및 삭제, 암호 변경 등 사용자 이벤트와 관련된 메시지입니다. admin 역할 사용자만 이 파일을 볼 수 있습니다.	9주
space.log	시스템 구성 요소의 디스크 공간 사용량에 대한 메시지 및 정리 프로세스에서 보낸 메시지입니다. 공간 사용량 메시지는 매시간 생성됩니다. 정리 프로세스가 실행될 때마다 약 100개의 메시지가 생성됩니다. 모든 메시지는 쉼표로 구분된 값 형식이며, 디스크 공간 메시지를 정리 메시지로부터 구분하는 데 사용할 수 있는 태그를 포함하고 있습니다. 타사 소프트웨어를 사용하여 메시지 세트를 분석할 수 있습니다. 로그 파일은 다음 태그를 사용합니다.	단일 파일은 영구적으로 보관됩니다. 이 로그에 대해서는 로그 파일 교체가 없습니다.

표 57 시스템 로그 파일 (계속)

로그 파일	설명	보존 기간
	• CLEAN은 정리 작업의 데이터 줄에 해당합니다. • CLEAN_HEADER는 정리 작업 데이터 줄을 위한 헤더를 포함하고 있는 줄에 해당합니다. • SPACE는 디스크 공간 데이터 줄에 해당합니다. • SPACE_HEADER는 디스크 공간 데이터 줄을 위한 헤더를 포함하고 있는 줄에 해당합니다.	

DD System Manager에서 로그 파일 보기

Logs 탭을 사용해 DD System Manager에서 시스템 로그 파일을 보고 엽니다.

절차

1. **Maintenance** > **Logs**를 선택합니다.

   로그 목록에는 로그 파일 이름과 크기 및 각 로그 파일의 생성 날짜가 표시됩니다.

2. 로그 파일 이름을 클릭하여 해당 컨텐츠를 봅니다. 파일을 열기 위해 Notepad.exe 같은 애플리케이션을 선택하라는 메시지가 표시될 수 있습니다.

CLI에 로그 파일 표시

`log view` 명령을 사용해 CLI에서 로그 파일을 봅니다.

절차

1. CLI에서 로그 파일을 보려면 `log view` 명령을 사용합니다.

   인수 없이 사용할 경우 이 명령은 현재 메시지 파일을 표시합니다.

2. 로그를 볼 때는 위쪽 화살표와 아래쪽 화살표를 사용하여 파일을 스크롤하고 종료할 때는 q 키를 사용합니다. 파일 내에서 검색하려면 슬래시 문자(/)와 패턴을 입력합니다.

메시지 파일은 다음과 같이 표시됩니다. 아래 예의 마지막 메시지는 Data Domain 시스템이 자동으로 생성하는 시간별 시스템 상태 메시지입니다. 이 메시지는 시스템 가동 시간, 저장 데이터 양, NFS 작업 및 데이터 스토리지에 사용된 데이터 공간(%)을 보고합니다. 시간별 메시지는 시스템 로그와 직렬 콘솔(연결된 경우)로 전송됩니다.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

참고

GiB = 기비바이트(Gibibyte) = 기가바이트의 2진 표기법

로그 메시지에 대한 자세한 내용

사용자의 현재 DD OS 버전에 대한 Error Message Catalog에서 오류 메시지를 조회합니다.

로그 파일에는 다음과 같은 텍스트가 표시됩니다.

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

메시지의 구성 요소는 다음과 같습니다.

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: Message
```

심각도에 따라 내림차순으로 나열하면 Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug입니다.

절차

1. 온라인 지원 웹 사이트(https://support.emc.com)로 이동하여 검색 상자에 *Error Message Catalog*를 입력한 뒤 검색 버튼을 클릭합니다.
2. 결과 목록에서 사용자 시스템의 카탈로그를 찾고 링크를 클릭합니다.
3. 사용자의 브라우저 검색 툴을 사용해 메시지에서 고유한 텍스트 문자열을 검색합니다.

   오류 메시지 설명은 다음과 유사하게 나타납니다.

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience:
   customerMessage: No replication throttle schedules found:
   setting throttle to unlimited. Description: The restorer
   cannot find a replication throttle schedule. Replication
   is running with throttle set to unlimited. Action: To set
   a replication throttle schedule, run the replication
   throttle add command.
   ```

4. 문제를 해결하려면 권장 조치를 실행합니다.

   예제 메시지 설명에 따라 `replication throttle add` 명령을 실행하여 스로틀을 설정할 수 있습니다.

로그 파일 복제본 저장

로그 파일 복제본을 아카이빙할 경우 다른 디바이스에 저장하십시오.

NFS, CIFS 마운트 또는 FTP를 사용하여 파일을 다른 시스템에 복제할 수 있습니다. CIFS 또는 NFS를 사용할 경우 데스크톱에 /ddvar을 마운트하고 마운트 지점에서 파일을 복제하십시오. 다음 절차는 FTP를 사용하여 다른 시스템으로 파일을 이동하는 방법에 대해 설명합니다.

절차

1. Data Domain 시스템에서 `adminaccess show ftp` 명령을 사용하여 FTP 서비스의 설정 여부를 확인합니다. 서비스가 해제되어 있다면 `adminaccess enable ftp`명령을 사용합니다.

2. Data Domain 시스템에서 `adminaccess show ftp` 명령을 사용하여 FTP 액세스 목록에 사용자의 원격 시스템 IP 주소가 있는지 확인합니다. 목록에 주소가 없으면 `adminaccess add ftp` *ipaddr* 명령을 사용합니다.
3. 원격 시스템에서 웹 브라우저를 엽니다.
4. 다음 예와 같이, 웹 브라우저 상단의 **Address** 상자에서 FTP를 사용하여 Data Domain 시스템에 액세스합니다.

   ftp://Data Domain system_name.yourcompany.com/

   참고

   시스템에서 익명 로그인을 허용하지 않으면 일부 웹 브라우저는 자동으로 로그인을 요청하지 않습니다. 이 경우에는 FTP 라인에 사용자 이름과 암호를 추가합니다. 예를 들면 다음과 같습니다. **ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/**

5. 로그인 팝업에서 사용자 **sysadmin**으로 Data Domain 시스템에 로그인합니다.
6. 사용자는 Data Domain 시스템에서 로그 디렉토리 바로 위에 있는 디렉토리에 있게 됩니다. 로그 디렉토리를 열어서 메시지 파일을 나열합니다.
7. 저장할 파일을 복제합니다. 파일 아이콘을 마우스 오른쪽 버튼으로 클릭하여 메뉴에서 **Copy To Folder**를 선택합니다. 파일 복제 위치를 선택합니다.
8. 파일 복제를 마친 뒤 Data Domain 시스템에서 FTP 서비스를 해제하려면 SSH를 사용하여 sysadmin으로 Data Domain 시스템에 로그인한 뒤 `adminaccess disable ftp`명령을 호출합니다.

원격 시스템으로의 로그 메시지 전송

Data Domain 시스템에서 다른 시스템으로 일부 로그 메시지가 전송될 수 있습니다. DD OS에서는 syslog를 사용하여 로그 메시지를 원격 시스템에 게시합니다.

Data Domain 시스템은 로그 파일에 대한 다음 facility.priority 선택기를 내보냅니다. 선택기를 관리하고 타사 시스템에서 메시지를 수신하는 방법에 대한 자세한 내용은 공급업체에서 제공한 수신 시스템에 대한 설명서를 참조하십시오.

- *.notice - 통지 우선 순위 이상의 모든 메시지를 전송합니다.
- *.alert - 알림 우선 순위 이상의 모든 메시지를 전송합니다. 알림은 *.notice에 포함됩니다.
- kern.* - 모든 커널 메시지, 즉 kern.info 로그 파일을 전송합니다.

`log host` 명령은 다른 시스템으로 로그 메시지를 전송하는 프로세스를 관리합니다.

로그 파일 전송 구성 보기

`log host show` CLI 명령을 사용해 로그 파일 전송이 설정되었는지 여부와 로그 파일을 수신하는 호스트를 표시합니다.

절차

1. 구성을 표시하려면 `log host show` 명령을 입력합니다.

```
# log host show
Remote logging is enabled.
Remote logging hosts
     log-server
```

로그 메시지 전송 설정 및 해제

로그 메시지 전송을 설정하거나 해제하려면 CLI 명령을 사용해야 합니다.

절차

1. 다른 시스템으로의 로그 메시지 전송을 설정하려면 `log host enable` 명령을 사용합니다.
2. 다른 시스템으로 로그 메시지를 보내지 않으려면 `log host disable` 명령을 사용합니다.

수신 호스트 추가 또는 제거

수신 호스트를 추가하거나 제거하려면 CLI 명령을 사용해야 합니다.

절차

1. Data Domain 시스템 로그 메시지를 수신하는 목록에 시스템을 추가하려면 `log host add` 명령을 사용합니다.
2. 시스템 로그 메시지를 수신하는 목록에서 시스템을 제거하려면 다음 명령을 사용합니다. `log host del`.

다음 명령은 로그 메시지를 수신하는 호스트에 *log-server*라는 이름의 시스템을 추가합니다.

```
log host add log-server
```

다음 명령은 로그 메시지를 수신하는 호스트에서 *log-server*라는 이름의 시스템을 제거합니다.

```
log host del log-server
```

다음 명령은 로그 전송을 비활성화하고 대상 호스트 이름 목록을 지웁니다.

```
log host reset
```

IPMI를 사용한 원격 시스템 전원 관리

DD 시스템에서는 IPMI(Intelligent Platform Management Interface)를 사용한 원격 전원 관리를 지원하며, SOL(Serial over LAN)을 사용한 부팅 시퀀스 원격 모니터링도 지원합니다.

IPMI 전원 관리는 IPMI 이니시에이터와 IPMI 원격 호스트 간에 이루어집니다. IPMI 이니시에이터는 원격 호스트의 전원을 제어하는 호스트입니다. 이니시에이터의 원격 전원 관리를 지원하려면 원격 호스트를 IPMI 사용자 이름 및 암호로 구성해야 합니다. 이니시에이터에서 원격 호스트의 전원을 관리하려 할 때 이 사용자 이름과 암호를 제공해야 합니다.

DD OS와 별개로 실행되는 IPMI를 사용하면 원격 시스템이 전원과 네트워크에 접속되어 있는 한 시스템 전원을 관리할 수 있습니다. 이니시에이터와 원격 시스템은 IP 네트워크로 연결되어야 합니다. 구성 및 접속이 적절히 이루어지면 IPMI 관리를 통해 물리적 디바이스 없이 원격 시스템의 전원을 켜고 끌 수 있습니다.

원격 시스템에 IPMI 사용자를 구성할 때는 DD System Manager와 CLI를 모두 사용할 수 있습니다. 원격 시스템에 IPMI를 구성한 후에는 다른 시스템에서 IPMI 이니시에이터 기능을 사용하여 로그인하고 전원을 관리할 수 있습니다.

참고

시스템에서 하드웨어 또는 소프트웨어 제한으로 인해 IPMI를 지원할 수 없는 경우 구성 페이지로 이동하려고 하면 DD System Manager에서 알림 메시지를 표시합니다.

SOL을 사용해 원격 시스템의 전원을 껐다 켠 후의 부팅 시퀀스를 볼 수 있습니다. SOL을 사용하면 일반적으로 직렬 포트나 연결된 콘솔로 전송되는 텍스트 콘솔 데이터를 LAN을 통해 전송하고 관리 호스트에 표시되도록 할 수 있습니다.

DD OS CLI를 사용하면 SOL용 원격 시스템을 구성하고 원격 콘솔 출력을 볼 수 있습니다. 이 기능은 CLI 에서만 지원됩니다.

알림

DD OS 명령을 사용한 전원 종료 시도가 실패하게 되는 긴급 상황을 위해 IPMI 전원 차단 기능이 제공됩니다. IPMI 전원 차단 기능을 사용하면 단순히 시스템에서 전원이 제거되며, DD OS 파일 시스템의 순차 종료가 실행되지는 않습니다. 전원을 차단한 후 다시 공급하는 적절한 방법은 DD OS `system reboot` 명령을 사용하는 것입니다. 시스템 전원을 차단하는 적절한 방법은 DD OS `system poweroff` 명령을 사용한 후 명령에 따라 파일 시스템이 제대로 종료될 때까지 기다리는 것입니다.

IPMI 및 SOL 제한 사항

일부 Data Domain 시스템에서 IPMI 및 SOL 지원은 제한되어 있습니다.

- IPMI는 다음 시스템을 제외하고 이 릴리즈에서 지원하는 모든 시스템에서 지원됩니다. DD140, DD610 및 DD630.
- IPMI 사용자 지원은 다음과 같이 다양합니다.
  - DD990 모델: 최대 사용자 ID 수 = 15개. 세 가지 기본 사용자(NULL, 익명, 루트). 사용 가능한 최대 사용자 ID 수 = 12개.
  - DD640, DD4200, DD4500, DD7200 및 DD9500 모델: 최대 사용자 ID 수 = 10개. 두 가지 기본 사용자(NULL, 루트). 사용 가능한 최대 사용자 ID 수 = 8개.
- SOL은 다음 시스템에서 지원됩니다. DD160, DD620, DD640, DD670, DD860, DD890, DD990, DD2200, DD2500(DD OS 5.4.0.6 이상 필요), DD4200, DD4500, DD7200 및 DD9500

참고

DD160 시스템의 IPMI 연결에 대해서는 루트 사용자가 지원되지 않습니다.

DD System Manager를 사용해 IPMI 사용자 추가 및 삭제

각 시스템에는 구성된 IPMI 사용자의 고유한 목록이 있으며 이 목록은 로컬 전원 관리 기능에 대한 액세스를 제어할 때 사용됩니다. IPMI 이니시에이터로 작동하는 다른 시스템에서 원격 시스템 전원을 관리하려면 유효한 사용자 이름과 암호를 제공해야 합니다.

IPMI 사용자에게 여러 원격 시스템에서 전원을 관리할 수 있는 권한을 부여하려면 원격 시스템 각각에 해당 사용자를 추가해야 합니다.

참고

각 원격 시스템의 IPMI 사용자 목록은 관리자 액세스 및 로컬 사용자에 대한 DD System Manager 목록과 별개입니다. 관리자와 로컬 사용자는 IPMI 전원 관리에 대한 권한을 상속하지 않습니다.

절차

1. **Maintenance** > **IPMI**를 선택합니다.
2. 사용자를 추가하려면 다음 단계를 완료합니다.
   a. IPMI Users 테이블 위에서 **Add**를 클릭합니다.
   b. Add User 대화 상자의 해당 상자에 사용자 이름(16자 미만)과 암호를 입력하고 **Verify Password** 상자에 암호를 다시 입력합니다.
   c. **Create**를 클릭합니다.

   IPMI Users 테이블에 사용자 항목이 나타납니다.
3. 사용자를 삭제하려면 다음 단계를 완료합니다.
   a. IPMI Users 목록에서 사용자를 선택하고 **Delete**를 클릭합니다.
   b. Delete User 대화 상자에서 **OK**를 클릭해 사용자 삭제를 확인합니다.

IPMI 사용자 암호 변경

이전 암호가 전원 관리에 사용되지 않도록 IPMI 사용자 암호를 변경합니다.

절차

1. **Maintenance** > **IPMI**를 선택합니다.
2. IPMI Users 테이블에서 사용자를 선택하고 **Change Password**를 클릭합니다.
3. Change Password 대화 상자에서 해당 입력란에 암호를 입력하고 **Verify Password** 입력란에 암호를 다시 입력합니다.
4. **Update**를 클릭합니다.

IPMI 포트 구성

시스템의 IPMI 포트를 구성할 때 네트워크 포트 목록에서 포트를 선택하고 해당 포트에 대한 IP 구성 매개 변수를 지정합니다. 표시되는 IPMI 포트 선택 항목은 Data Domain 시스템 모델에 따라 결정됩니다.

일부 시스템에서는 IPMI 트래픽에만 사용할 수 있는 하나 이상의 전용 포트를 지원합니다. 다른 시스템의 경우 IPMI 트래픽과 **Hardware** > **Ethernet** > **Interfaces** 보기의 물리적 인터페이스가 지원하는 모든 IP 트래픽에 모두 사용할 수 있는 포트를 지원합니다. 전용 IPMI 포트를 제공하는 시스템에서는 공유 포트가 제공되지 않습니다.

IPMI Network Ports 목록에 나와 있는 포트 이름은 베이스보드 관리 컨트롤러를 나타내는 접두사 bmc를 사용합니다. 포트가 전용 포트인지 공유 포트인지 결정하려면 나머지 포트 이름을 네트워크 인터페이스 목록에 있는 포트와 비교하십시오. 나머지 IPMI 포트 이름이 네트워크 인터페이스 목록에 있는 인터페이스와 일치하면 해당 포트는 공유 포트입니다. 나머지 IPMI 포트 이름이 네트워크 인터페이스 목록에 있는 인터페이스와 다르면 해당 포트는 전용 IPMI 포트입니다.

참고

DD4200, DD4500 및 DD7200 시스템은 앞서 설명한 명명 규칙에서 예외입니다. 이 시스템에서 IPMI 포트 bmc0a는 네트워크 인터페이스 목록의 공유 포트 ethMa에 해당합니다. 가능하면 공유 포트 ethMa는 IPMI 트래픽 및 시스템 관리 트래픽을 위해 예약하십시오(HTTP, Telnet 및 SSH 같은 프로토콜 사용). 백업 데이터 트래픽은 다른 포트로 전송해야 합니다.

IPMI 및 IPMI가 아닌 IP 트래픽이 이더넷 포트를 공유할 경우 연결 상태 변화가 IPMI 접속 구성에 방해가 될 수 있기 때문에 가능하면 공유 인터페이스에서는 Link Aggregation 기능을 사용하지 마십시오.

절차

1. **Maintenance** > **IPMI**를 선택합니다.

   IPMI Configuration 영역에 관리 대상 시스템의 IPMI 구성이 표시됩니다. Network Ports 테이블에 IPMI를 설정하고 구성할 수 있는 포트가 나열됩니다. IPMI Users 테이블에 관리 대상 시스템에 액세스할 수 있는 IPMI 사용자가 나열됩니다.

   표 58 Network Ports 목록 열 설명

항목	설명
Port	IPMI 통신을 지원하는 포트의 논리적 이름입니다.
Enabled	IPMI에 대해 포트가 설정되어 있는지 여부입니다(Yes 또는 No).
DHCP	포트가 해당 IP 주소를 설정하는 데 DHCP를 사용하는지 여부입니다(Yes 또는 No).
MAC Address	포트의 하드웨어 MAC 주소입니다.
IP Address	포트 IP 주소입니다.
Netmask	포트의 서브넷 마스크입니다.
Gateway	포트의 게이트웨이 IP 주소입니다.

   표 59 IPMI Users 목록 열 설명

항목	설명
User Name	원격 시스템의 전원을 관리할 수 있는 권한이 있는 사용자의 이름입니다.

2. **Network Ports** 테이블에서 구성할 포트를 선택합니다.

   참고

   IPMI 포트가 IP 트래픽(관리자 액세스 또는 백업 트래픽용)도 지원할 경우, IPMI를 구성하기 전에 인터페이스 포트를 사용하도록 설정해야 합니다.

3. **Network Ports** 테이블 위에서 **Configure**를 클릭합니다.

   Configure Port 대화 상자가 나타납니다.

4. 네트워크 주소 정보를 할당할 방법을 선택합니다.
   - DHCP 서버에서 IP 주소, 넷마스크 및 게이트웨이 구성을 수집하려면 **Dynamic(DHCP)**을 선택합니다.
   - 네트워크 구성을 수동으로 정의하려면 **Static(Manual)**을 선택하고 IP 주소, 넷마스크 및 게이트웨이 주소를 입력합니다.

5. **Network Ports** 테이블에서 네트워크 포트를 선택하고 **Enable**을 클릭해 비활성화된 IPMI 포트를 활성화합니다.
6. **Network Ports** 테이블에서 네트워크 포트를 선택하고 **Disable**을 클릭해 활성화된 IPMI 포트를 비활성화합니다.

7. **Apply**를 클릭합니다.

CLI를 사용한 원격 전원 관리 및 콘솔 모니터링 준비

원격 콘솔 모니터링은 SOL(Serial over LAN) 기능을 사용하여 직렬 서버 없이 텍스트 기반 콘솔 출력을 볼 수 있게 해 줍니다. 시스템에서 원격 전원 관리 및 콘솔 모니터링을 설정하려면 CLI를 사용해야 합니다.

원격 콘솔 모니터링은 일반적으로 `ipmi remote power cycle` 명령과 함께 사용되므로 사용자는 원격 시스템의 부팅 시퀀스를 볼 수 있습니다. 부팅 시퀀스 동안 원격으로 콘솔을 보려는 모든 시스템에서 이 절차를 사용해야 합니다.

절차

1. 콘솔을 시스템에 직접 또는 원격으로 연결합니다.
   - 직접 연결의 경우 다음 커넥터를 사용합니다.
     - PS/2 키보드용 DIN 유형 커넥터
     - USB 키보드용 USB-A 콘센트 포트
     - VGA 모니터용 DB15 암 커넥터

     참고

     DD4200, DD4500, DD7200 시스템은 KVM을 포함한 직접 연결을 지원하지 않습니다.

   - 직렬 연결의 경우 표준 DB9 수 커넥터 또는 Micro-DB9 암 커넥터를 사용합니다. DD4200, DD4500, DD7200 시스템에서는 Micro-DB9 커넥터가 제공됩니다. 수 Micro-DB9 커넥터 및 표준 암 DB9 커넥터를 사용하는 Null 모뎀 케이블이 일반적인 노트북 컴퓨터 접속용으로 포함되어 있습니다.
   - 원격 IPMI/SOL 연결의 경우 다음과 같이 적절한 RJ45 콘센트를 사용합니다.
     - DD990 시스템의 경우 기본 포트 eth0d를 사용합니다.
     - 다른 시스템의 경우 유지 보수 또는 서비스 포트를 사용합니다. 포트 위치는 하드웨어 개요 또는 설치 및 설정 가이드 등과 같은 시스템 설명서를 참조하십시오.
2. 원격 콘솔 모니터링을 지원하려면 기본 BIOS 설정을 사용합니다.
3. IPMI 포트 이름을 표시하려면 `ipmi show config`를 입력합니다.
4. IPMI를 설정하려면 `ipmi enable {`***port*** `| all}`을 입력합니다.
5. IPMI 포트를 구성하려면 `ipmi config port { dhcp | ipaddress` ***ipaddr*** `netmask` ***mask*** `gateway` ***ipaddr*** `}` 을 입력합니다.

   참고

   IPMI 포트에서 관리자 액세스 또는 백업 트래픽을 위해 IP 트래픽도 지원하는 경우 IPMI를 구성하기 전에 `net enable` 명령을 이용해 인터페이스 포트를 설정해야 합니다.

6. IPMI를 처음 사용하는 경우 `ipmi user reset`을 실행하여 두 포트 간의 동기화가 중단 상태일 수 있는 IPMI 사용자를 지우고 기본 사용자를 해제합니다.
7. 새 IPMI 사용자를 추가하려면 `ipmi user add` ***user***를 입력합니다.

8. SOL을 설정하려면 다음을 수행합니다.
   a. `system option set console lan`을 입력합니다.
   b. 메시지가 표시되면 `y`를 입력하여 시스템을 재부팅합니다.

DD System Manager를 사용한 전원 관리

원격 시스템에서 IPMI를 올바르게 설정한 후에 DD System Manager를 IPMI 이니시에이터로 사용해 원격 시스템에 로그인하고, 전원 상태를 보고, 전원 상태를 변경할 수 있습니다.

절차

1. **Maintenance** > **IPMI**를 선택합니다.
2. **Login to Remote System**을 클릭합니다.

   IPMI Power Management 대화 상자가 나타납니다.
3. 원격 시스템 IPMI IP 주소 또는 호스트 이름과 IPMI 사용자 이름 및 암호를 입력한 다음 **Connect**를 클릭합니다.
4. IPMI 상태를 봅니다.

   IPMI Power Management 대화 상자가 나타나고 타겟 시스템 식별 및 현재 전원 상태가 표시됩니다. Status 영역에는 항상 현재 상태가 표시됩니다.

   참고

   상태 옆의 Refresh 아이콘(파란색 화살표)는 구성 상태를 새로 고치는 데 사용할 수 있습니다(예: 지난 15분 안에 CLI 명령을 사용하여 IPMI IP 주소 또는 사용자 구성이 변경된 경우).
5. IPMI 전원 상태를 변경하려면 해당 버튼을 클릭합니다.
   - **Power Up** - 원격 시스템의 전원이 꺼질 때 나타납니다. 원격 시스템의 전원을 켜려면 이 버튼을 클릭합니다.
   - **Power Down** - 원격 시스템의 전원이 켜질 때 나타납니다. 원격 시스템의 전원을 끄려면 이 버튼을 클릭합니다.
   - **Power Cycle** - 원격 시스템의 전원이 켜질 때 나타납니다. 원격 시스템의 전원을 껐다 켜려면 이 버튼을 클릭하십시오.
   - **Manage Another System** - IPMI 전원 관리를 위해 다른 원격 시스템에 로그인하려면 이 버튼을 클릭합니다.
   - **Done** - IPMI Power Management 대화 상자를 닫으려면 클릭합니다.

   알림

   IPMI Power Down 기능은 DD OS를 정상적인 절차대로 종료하지 않습니다. 이 옵션은 DD OS가 중단될 경우 사용할 수 있으며, 시스템을 정상적으로 종료하는 데 사용할 수 없습니다.

CLI를 사용한 전원 관리

CLI를 사용해 원격 시스템의 전원을 관리하고 원격 콘솔 모니터링을 시작할 수 있습니다.

참고

원격 시스템은 전원을 관리하거나 시스템을 모니터링하기 전에 적절히 설정되어야 합니다.

절차

1. 원격 시스템을 모니터링하려는 시스템에서 CLI 세션을 설정합니다.
2. 원격 시스템에서 전원을 관리하려면 `ipmi remote power {on | off | cycle | status} ipmi-target <`*ipaddr* | *hostname*`> user` *user*를 입력합니다.
3. 원격 콘솔 모니터링을 시작하려면 `ipmi remote console ipmi-target <`*ipaddr* | *hostname*`> user` *user*를 입력합니다.

   참고

   사용자 이름은 원격 시스템의 IPMI에 대해 정의된 IPMI 사용자 이름입니다. DD OS 사용자 이름은 자동으로 IPMI에서 지원되지는 않습니다.

4. 원격 콘솔 모니터링 세션의 연결을 해제하고 명령줄로 돌아가려면 @ 기호를 입력합니다.
5. 원격 콘솔 모니터링을 종료하려면 물결표(~)를 입력합니다.

4장

Data Domain 시스템 모니터링

이 장에는 다음과 같은 내용이 포함됩니다.

개별 시스템 상태 및 ID 정보 보기

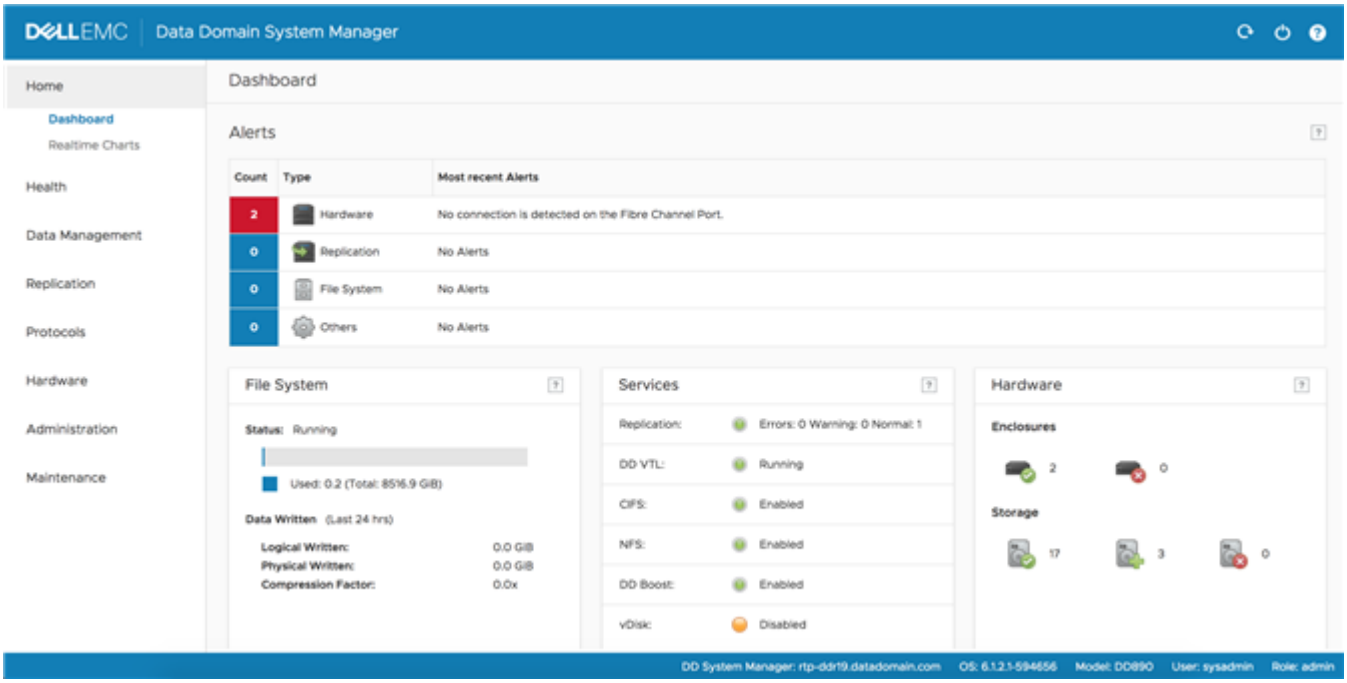
Dashboard 영역에는 알림, 파일 시스템, 라이센스가 등록된 서비스 및 하드웨어 엔클로저에 대한 요약 정보 및 상태가 표시됩니다. **Maintenance** 영역에는 시스템 가동 시간 및 시스템/섀시 일련 번호와 같은 추가 시스템 정보가 표시됩니다.

바닥글에는 항상 시스템 이름, 소프트웨어 버전 및 사용자 정보가 나타납니다.

절차

1. 시스템 대시보드를 보려면 **Home** > **Dashboard**를 선택합니다.

   그림 5 시스템 대시보드



2. 시스템 가동 시간 및 ID 정보를 보려면 **Maintenance** > **System**을 선택합니다.

   System 영역에 시스템 가동 시간 및 식별 정보가 나타납니다.

Dashboard Alerts 영역

Dashboard Alerts 영역에는 각 서브시스템(하드웨어, 복제, 파일 시스템 및 기타)에 대해 시스템에 있는 최신 알림의 개수, 유형 및 텍스트가 표시됩니다. 현재 알림에 대한 자세한 정보를 표시하려면 Alerts 영역의 아무 곳이나 클릭합니다.

표 60 Dashboard Alerts 열 설명

열	설명
Count	인접 열에 지정된 서브시스템 유형에 대한 현재 알림의 개수입니다. 배경색은 알림의 심각도를 나타냅니다.
Type	알림을 생성한 서브시스템입니다.

표 60 Dashboard Alerts 열 설명 (계속)

열	설명
Most recent alerts	인접 열에 지정된 서브시스템 유형에 대한 최신 알림의 텍스트입니다.

Dashboard File System 영역

Dashboard File System 영역에는 전체 파일 시스템에 대한 통계가 표시됩니다. 자세한 정보를 표시하려면 File System 영역의 아무 곳이나 클릭합니다.

표 61 File System 영역 레이블 설명

열	설명
Status	파일 시스템의 현재 상태입니다.
X.Xx	파일 시스템의 평균 압축 감소율 요인입니다.
Used	사용 중인 총 파일 시스템 공간입니다.
Data Written: Pre-compression	압축 전에 시스템에서 받은 데이터 양입니다.
Data Written: Post-compression	압축 후에 시스템에 저장된 데이터 양입니다.

Dashboard Services 영역

Dashboard Services 영역에는 복제, DD VTL, CIFS, NFS, DD Boost 및 vDisk 서비스의 상태가 표시됩니다. 서비스에 대한 자세한 정보를 표시하려면 해당 서비스를 클릭합니다.

표 62 Services 영역 열 설명

열	설명
왼쪽 열	왼쪽 열에는 시스템에서 사용할 수 있는 서비스가 나열됩니다. 이러한 서비스에는 복제, DD VTL, CIFS, NFS, DD Boost, vDisk가 포함될 수 있습니다.
오른쪽 열	오른쪽 열에는 서비스의 작동 상태가 표시됩니다. 대부분의 경우 서비스 상태는 Enabled, Disabled 또는 Not Licensed입니다. 복제 서비스 행에는 정상, 경고 및 오류 상태의 복제 컨텍스트 수가 표시됩니다. 색상으로 구분된 상자의 경우 녹색은 정상 작동, 노란색은 경고 상황, 빨간색은 오류가 있음을 나타냅니다.

Dashboard HA Readiness 영역

HA(High-Availability) 시스템에서 HA 패널에는 필요한 경우 액티브 노드에서 대기 노드로 시스템을 페일오버할 수 있는지 여부가 표시됩니다.

HA 패널을 클릭하여 **HEALTH**의 **High Availability** 섹션으로 이동할 수 있습니다.

Dashboard Hardware 영역

Dashboard Hardware 영역에는 시스템 엔클로저 및 드라이브의 상태가 표시됩니다. 이러한 구성 요소에 대한 자세한 정보를 표시하려면 Hardware 영역의 아무 곳이나 클릭합니다.

표 63 Hardware 영역 레이블 설명

레이블	설명
엔클로저	엔클로저 아이콘은 정상 상태(녹색 선택 표시) 및 성능 저하 상태(빨간색 X)로 작동하는 엔클로저의 수를 표시합니다.
스토리지	스토리지 아이콘은 정상 상태(녹색 선택 표시), 스페어 상태(녹색 +) 및 실패 상태(빨간색 X)로 작동하는 디스크 드라이브의 수를 표시합니다.

Maintenance System 영역

Maintenance System 영역에는 시스템 모델 번호, DD OS 버전 시스템 가동 시간 및 섀시 일련 번호가 표시됩니다.

표 64 System 영역 레이블 설명

레이블	설명
모델 번호	Data Domain 시스템에 할당된 모델 번호입니다.
버전	DD OS 버전과 시스템에서 실행되는 소프트웨어의 빌드 번호입니다.
System Uptime	마지막으로 시스템을 시작한 이후로 시스템이 실행된 시간이 표시됩니다. 괄호 안의 시간은 시스템 가동 시간이 마지막으로 업데이트된 시간을 나타냅니다.
System Serial No.	시스템에 할당된 일련 번호입니다. DD4500 및 DD7200과 같은 새 시스템에서는 시스템 일련 번호가 섀시 일련 번호와 무관하며, 섀시 교체 등 다양한 유형의 유지 보수 작업에서 동일하게 유지됩니다. DD990 이하의 기존 시스템에서는 시스템 일련 번호가 섀시 일련 번호로 설정되어 있습니다.
Chassis Serial No.	현재 시스템 섀시의 일련 번호입니다.

Health Alerts 패널

알림은 시스템 이벤트를 보고하는 시스템 서비스 및 서브시스템의 메시지입니다. Health > Alerts 탭에는 현재 및 이전 알림, 구성된 알림 통지 그룹 및 일일 알림 요약 보고서를 받을 사용자에 대한 구성을 볼 수 있는 탭이 표시됩니다.

알림은 SNMP 트랩으로도 전송됩니다. 트랩의 전체 목록은 *MIB Quick Reference Guide* 또는 SNMP MIB를 참조하십시오.

현재 알림 보기 및 지우기

Current Alerts 탭에는 모든 현재 알림의 목록이 표시되며 선택한 알림에 대한 자세한 정보가 표시될 수 있습니다. 근본적인 원인이 되는 상황을 수정하거나 알림을 수동으로 지울 경우 Current Alerts 목록에서 알림이 자동으로 제거됩니다.

절차

1. 모든 현재 알림을 보려면 **Health** > **Alerts** > **Current Alerts**를 선택합니다.
2. 현재 알림 목록의 항목 수를 제한하려면 다음을 수행합니다.
   a. Filter By 영역에서 **Severity** 및 **Class**를 선택해 해당 선택과 관련된 알림만 표시합니다.
   b. **Update**를 클릭합니다.
   Severity 및 Class와 일치하지 않는 모든 알림은 목록에서 제거됩니다.
3. **Details** 영역의 특정 알림에 대한 추가 정보를 표시하려면 목록에서 알림을 클릭합니다.
4. 알림을 지우려면 목록에서 알림 확인란을 선택하고 **Clear**를 클릭합니다.
   지워진 알림은 Current Alerts 목록에 더 이상 나타나지 않지만 Alerts History 목록에서 확인할 수 있습니다.
5. 필터링을 제거하고 현재 알림의 전체 목록으로 돌아가려면 **Reset**을 클릭합니다.

Current Alerts 탭

Current Alerts 탭에는 알림 목록과 선택한 알림에 대한 자세한 정보가 표시됩니다.

표 65 Alerts 목록, 열 레이블 설명

항목	설명
Message	알림 메시지 텍스트입니다.
Severity	알림의 심각도입니다. 예를 들어 경고, 심각, 정보 또는 긴급이 있습니다.
Date	알림이 발생한 시간과 날짜입니다.
Class	알림이 발생한 서브시스템입니다.
Object	알림이 발생한 물리적 구성 요소입니다.

표 66 Details 영역, 행 레이블 설명

항목	설명
Name	알림의 텍스트 식별자입니다.
Message	알림 메시지 텍스트입니다.
Severity	알림의 심각도입니다. 예를 들어 경고, 심각, 정보, 긴급이 있습니다.
Class	알림이 발생한 서브시스템과 디바이스입니다.

표 66 Details 영역, 행 레이블 설명 (계속)

항목	설명
Date	알림이 발생한 시간과 날짜입니다.
Object ID	알림이 발생한 물리적 구성 요소입니다.
Event ID	이벤트 식별자입니다.
Tenant Units	영향을 받은 테넌트 유닛을 나열합니다.
Description	알림에 대한 보다 상세한 정보입니다.
Action	알림을 해결하기 위한 제안입니다.
Object Info	영향을 받은 객체에 대한 추가 정보입니다.
SNMP OID	SNMP 객체 ID입니다.

알림 기록 보기

Alerts History 탭에는 지워진 모든 알림의 목록이 표시되며 선택한 알림에 대한 자세한 정보가 표시될 수 있습니다.

절차

1. 모든 알림 기록을 보려면 **Health** > **Alerts** > **Alerts History**를 선택합니다.
2. 현재 알림 목록의 항목 수를 제한하려면 다음을 수행합니다.
   a. Filter By 영역에서 **Severity** 및 **Class**를 선택해 해당 선택과 관련된 알림만 표시합니다.
   b. **Update**를 클릭합니다.
   Severity 및 Class와 일치하지 않는 모든 알림은 목록에서 제거됩니다.
3. **Details** 영역의 특정 알림에 대한 추가 정보를 표시하려면 목록에서 알림을 클릭합니다.
4. 필터링을 제거하고 지워진 알림의 전체 목록으로 돌아가려면 **Reset**을 클릭합니다.

Alerts History 탭

Alerts History 탭에는 지워진 알림 목록과 선택한 알림에 대한 세부 정보가 표시됩니다.

표 67 Alerts 목록, 열 레이블 설명

항목	설명
Message	알림 메시지 텍스트입니다.
Severity	알림의 심각도입니다. 예를 들어 경고, 심각, 정보 또는 긴급이 있습니다.
Date	알림이 발생한 시간과 날짜입니다.
Class	알림이 발생한 서브시스템입니다.
Object	알림이 발생한 물리적 구성 요소입니다.

표 67 Alerts 목록, 열 레이블 설명 (계속)

항목	설명
Status	알림 상태가 게시되었는지, 지워졌는지 여부를 나타냅니다. 게시된 알림은 지우지 않은 것입니다.

표 68 Details 영역, 행 레이블 설명

항목	설명
Name	알림의 텍스트 식별자입니다.
Message	알림 메시지 텍스트입니다.
Severity	알림의 심각도입니다. 예를 들어 경고, 심각, 정보, 긴급이 있습니다.
Class	알림이 발생한 서브시스템과 디바이스입니다.
Date	알림이 발생한 시간과 날짜입니다.
Object ID	알림이 발생한 물리적 구성 요소입니다.
Event ID	이벤트 식별자입니다.
Tenant Units	영향을 받은 테넌트 유닛을 나열합니다.
Additional Information	알림에 대한 보다 상세한 정보입니다.
Status	알림 상태가 게시되었는지, 지워졌는지 여부를 나타냅니다. 게시된 알림은 지우지 않은 것입니다.
Description	알림에 대한 보다 상세한 정보입니다.
Action	알림을 해결하기 위한 제안입니다.

하드웨어 구성 요소 상태 보기

Hardware Chassis 패널에는 섀시 일련 번호, 엔클로저 상태 등 시스템의 각 엔클로저에 대한 블록 드로잉이 표시됩니다. 디스크, 팬, 전원 공급 장치, NVRAM, CPU 및 메모리 등의 엔클로저 구성 요소가 각 블록 드로잉에 표시됩니다. 표시되는 구성 요소는 시스템 모델에 따라 다릅니다.

DD OS 5.5.1 이상을 실행하는 시스템에서는 시스템 일련 번호도 표시됩니다. DD4500 및 DD7200과 같은 새 시스템에서는 시스템 일련 번호가 섀시 일련 번호와 무관하며, 섀시 교체 등 다양한 유형의 유지 보수 작업에서 동일하게 유지됩니다. DD990 이하의 기존 시스템에서는 시스템 일련 번호가 섀시 일련 번호로 설정되어 있습니다.

절차

1. **Hardware** > **Chassis**를 선택합니다.

   Chassis 보기에 시스템 엔클로저가 표시됩니다. Enclosure 1은 시스템 컨트롤러이며 나머지 엔클로저가 Enclosure 1 아래에 나타납니다.

   문제가 있는 구성 요소는 노란색(경고) 또는 빨간색(오류)으로 나타나며, 그 외의 구성 요소는 OK로 표시됩니다.

2. 커서를 구성 요소 위로 이동하면 자세한 상태를 볼 수 있습니다.

팬 상태

팬에는 번호가 매겨져 있으며 섀시의 각 위치에 해당합니다. 시스템을 마우스로 가리키면 해당 디바이스에 대한 툴 설명이 표시됩니다.

표 69 팬 툴 설명, 열 레이블 설명

항목	설명
Description	팬의 이름입니다.
Level	현재 작동 속도 범위(Low, Medium, High)로, 작동 속도는 섀시 내 온도에 따라 변합니다.
Status	팬의 상태입니다.

온도 상태

Data Domain 시스템 및 일부 구성 요소는 구성할 수 없는 온도 프로파일에 의해 정의되는 특정 온도 범위 내에서 작동하도록 구성됩니다. 온도 툴 설명을 표시하려면 Temperature 상자를 마우스로 가리키십시오.

표 70 온도 툴 설명, 열 레이블 설명

항목	설명
Description	측정 중인 섀시 내의 위치입니다. 나열되는 구성 요소는 모델에 따라 다르며 주로 약어로 표시됩니다. 예를 들면 다음과 같습니다. • CPU 0 Temp(Central Processing Unit) • MLB Temp 1(Main Logic Board) • BP middle temp(백플레인) • LP temp(로우 프로파일의 입출력 라이저 FRU) • FHFL temp(전체 높이 전체 길이의 입출력 라이저 FRU) • FP temp(전면 패널)
C/F	C/F 열에는 온도가 섭씨 및 화씨의 도 단위로 표시됩니다. CPU에 대한 설명이 *상대적*(CPU *n* Relative)으로 지정된 경우 이 열에는 각 CPU가 허용 가능한 최대 온도 미만인 도 수와 섀시 내부(섀시 주위)의 실제 온도가 표시됩니다.
Status	다음과 같이 온도 상태를 표시합니다. • OK - 온도가 적절합니다. • Critical - 온도가 종료 온도보다 높습니다. • Warning - 온도가 경고 온도보다 높지만 종료 온도보다는 낮습니다. • Dash (-) - 이 구성 요소에 구성된 온도 임계값이 없으므로 보고할 상태가 없습니다.

관리 패널 상태

DD6300, DD6800 및 DD9300 시스템에는 고정된 관리 패널이 있으며, 섀시 후면에 관리 네트워크용 이더넷 포트가 있습니다. 이더넷 포트를 마우스로 가리키면 툴 설명이 표시됩니다.

표 71 관리 패널 툴 설명, 열 레이블 설명

항목	설명
Description	관리 패널에 설치된 NIC의 유형입니다.
Vendor	관리 NIC의 제조업체입니다.
Ports	관리 네트워크의 이름입니다(Ma).

SSD 상태(DD6300에만 해당)

DD6300은 섀시 후면의 슬롯에서 최대 두 개의 SSD를 지원합니다. SSD 슬롯에는 번호가 매겨져 있으며 섀시의 각 위치에 해당합니다. SSD를 마우스로 가리키면 해당 디바이스에 대한 툴 설명이 표시됩니다.

표 72 SSD 툴 설명, 열 레이블 설명

항목	설명
Description	SSD의 이름입니다.
Status	SSD의 상태입니다.
Life Used	SSD가 사용한 정격 작동 수명의 백분율입니다.

전원 공급 장치 상태

툴 설명에서는 전원 공급 장치의 상태가 표시됩니다. 전원 공급 장치에 누락이나 장애가 발생한 경우 OK 또는 DEGRADED로 나타납니다. 엔클로저의 후면 패널을 보고 각 전원 공급 장치의 상태 표시등을 확인하여 교체가 필요한 부분을 파악할 수도 있습니다.

PCI 슬롯 상태

Chassis 보기에 표시된 PCI 슬롯은 PCI 슬롯의 수와 각 슬롯의 수를 나타냅니다. 툴 설명에서는 PCI 슬롯에 있는 각 카드에 대한 구성 요소 상태를 제공합니다. 예를 들어 NVRAM 카드 모델의 툴 설명에는 메모리 크기, 온도 데이터 및 배터리 레벨이 표시됩니다.

NVRAM 상태

NVRAM(Non-Volatile RAM), 배터리 및 기타 구성 요소에 대한 정보를 표시하려면 NVRAM을 마우스로 가리키십시오.

표 73 NVRAM 툴 설명, 열 레이블 설명

항목	설명
Component	Component 목록의 항목은 시스템에 설치된 NVRAM에 따라 다르며 다음 항목이 포함될 수 있습니다. • 펌웨어 버전 • 메모리 크기 • 오류 수 • 플래시 컨트롤러 오류 수 • 보드 온도 • CPU 온도 • 배터리 개수(배터리 개수는 시스템 유형에 따라 다름) • NVRAM의 현재 슬롯 번호
C/F	선택된 구성 요소의 온도가 섭씨/화씨 형식으로 표시됩니다.
Value	Value는 선택된 구성 요소에 대해 제공되며 다음 내용에 대해 설명합니다. • 펌웨어 버전 번호 • 표시된 유닛의 메모리 크기 값 • 메모리, PCI 및 컨트롤러에 대한 오류 수 • 다음 그룹으로 정렬되는 플래시 컨트롤러 오류 수: 구성 오류(Cfg Err), 패닉 상태(Panic), Bus Hang, 손상된 블록 경고(Bad Blk Warn), 백업 오류(Bkup Err) 및 복구 오류(Rstr Err) • 충전 비율 및 상태(설정 또는 해제) 같은 배터리 정보

시스템 통계 보기

Realtime Charts 패널에는 CPU 사용량, 디스크 트래픽 등의 실시간 서브시스템 성능 통계를 보여 주는 최대 7개의 그래프가 표시됩니다.

절차

1. **Home** > **Realtime Charts**를 선택합니다.

   Performance Graphs 영역에 현재 선택한 그래프가 표시됩니다.
2. 표시할 그래프 선택을 변경하려면 목록 상자에서 그래프의 확인란을 선택하거나 선택 취소합니다.
3. 특정 데이터 지점의 정보를 보려면 마우스로 특정 그래프 지점을 가리킵니다.
4. 그래프에 여러 데이터가 포함된 경우 그래프의 오른쪽 위에 있는 확인란을 사용해 표시하려는 항목을 선택할 수 있습니다. 예를 들어 디스크 상태 그래프의 오른쪽 위에 Read가 선택되어 있지 않으면 쓰기 데이터만 그래프로 표시됩니다.

결과

각 그래프에는 지난 200여 초 동안의 사용량이 표시됩니다. 표시를 일시 중지하려면 **Pause**를 클릭합니다. 다시 시작하여 일시 중지 중에 누락된 지점을 표시하려면 **Resume**을 클릭합니다.

성능 통계 그래프

성능 통계 그래프는 주요 시스템 구성 요소 및 기능에 대한 통계를 보여 줍니다.

DD Boost Active Connections

DD Boost Active Connections 그래프는 지난 200초 동안의 활성 DD Boost 접속 수를 표시합니다. 그래프 안의 각 줄은 읽기(복구) 접속 및 쓰기(백업) 접속에 대한 수를 표시합니다.

DD Boost Data Throughput

DD Boost Data Throughput 그래프는 지난 200초 동안의 초당 전송 바이트를 표시합니다. 그래프 안의 각 줄은 DD Boost 클라이언트가 시스템에서 읽은 데이터와 DD Boost 클라이언트가 시스템에 기록한 데이터의 속도를 표시합니다.

Disk

Disk 그래프는 초당 KiB, MiB 등 수신한 데이터를 기준으로 하는 적절한 단위로 시스템의 모든 디스크에서 전송 및 수신하는 데이터의 양을 표시합니다.

File System Operations

File System Operations 그래프는 지난 200초 동안 발생한 초당 작업 수를 표시합니다. 그래프 안의 각 줄은 초당 NFS 및 CIFS 작업을 표시합니다.

Network

Network 그래프는 초당 KiB 또는 MiB 등 수신한 데이터를 기준으로 하는 적절한 단위로 각 이더넷 접속을 통과하는 데이터의 양을 표시합니다. 이더넷 포트마다 한 줄이 표시됩니다.

Recent CPU Usage

Recent CPU Usage 그래프는 지난 200초 동안의 초당 CPU 사용 비율을 표시합니다.

Replication(DD Replicator의 라이센스를 등록해야 함)

Replication 그래프는 지난 200초 동안의 초당 네트워크에서 전송된 복제 데이터 양을 표시합니다. 각 줄은 In 및 Out 데이터를 다음과 같이 표시합니다.

- In: DD Replicator 페어의 한쪽에서 다른 쪽으로부터 받은 KB/초 같은 측정 단위의 총 수입니다. 대상의 값에는 백업 데이터, 복제 오버헤드 및 네트워크 오버헤드가 포함됩니다. 소스의 값에는 복제 오버헤드 및 네트워크 오버헤드가 포함됩니다.
- Out: DD Replicator 페어의 한쪽에서 다른 쪽에 보낸 KB/초 같은 측정 단위의 총 수입니다. 소스의 값에는 백업 데이터, 복제 오버헤드 및 네트워크 오버헤드가 포함됩니다. 대상의 값에는 복제 및 네트워크 오버헤드가 포함됩니다.

활성 사용자 보기

Active Users 탭에는 시스템에 로그인한 사용자의 이름과 현재 사용자 세션에 대한 통계가 표시됩니다.

절차

1. **Administration** > **Access** > **Active Users**를 선택합니다.

   Active Users 목록이 나타나며 각 사용자의 정보가 표시됩니다.

표 74 Active Users 목록, 열 레이블 설명

항목	설명
Name	로그인한 사용자의 사용자 이름입니다.
Idle	사용자의 마지막 활동 이후 시간입니다.
Last Login From	사용자가 로그인한 시스템입니다.
Last Login Time	사용자가 로그인한 Datestamp입니다.
TTY	로그인에 대한 터미널 표기법입니다. DD System Manager 사용자에 대한 GUI가 나타납니다.

참고

로컬 사용자를 관리하려면 **Go to Local Users**를 클릭합니다.

기록 보고서 관리

DD System Manager를 사용하여 지난 2년간의 Data Domain 시스템의 공간 사용량을 추적하는 보고서를 생성할 수 있습니다. 복제 진행률을 확인하는 데 도움이 되는 보고서를 생성하고 파일 시스템에 대한 일일 및 누적 보고서를 볼 수도 있습니다.

보고서 보기는 2개의 섹션으로 구분됩니다. 상단 섹션에서는 다양한 유형의 보고서를 생성할 수 있습니다. 하단 섹션에서는 저장된 보고서를 보고 관리할 수 있습니다.

보고서는 보고서 유형에 따라 표 형식 및 차트로 표시됩니다. 특정 Data Domain 시스템에 대한 보고서를 선택하여 특정 기간을 제공할 수 있습니다.

보고서에는 실시간 데이터가 아닌 기간별 데이터가 표시됩니다. 보고서가 생성된 후 차트는 정적 상태가 되어 더 이상 업데이트되지 않습니다. 보고서에서 얻을 수 있는 정보 유형의 예는 다음과 같습니다.

- 시스템으로 백업되는 데이터의 양 및 처리된 데이터 중복 제거의 양
- 주별 공간 사용량 추세에 따른 Data Domain 시스템 공간이 꽉 차게 되는 예측 시기
- 선택 간격 기준에 따른 백업 및 압축 사용률
- 정리 주기 기간, 정리될 수 있는 공간의 양, 확보된 공간의 양 등 기간별 정리 성능
- 소스 및 대상에 대해 복제에서 사용하는 WAN 대역폭의 양, 대역폭이 복제 요구 사항을 충족하기에 충분한지 여부
- 시스템 성능 및 리소스 활용도

보고서 유형

New Report 영역에는 시스템에서 생성할 수 있는 보고서 유형이 나열됩니다.

참고

복제 보고서는 시스템에 복제 라이센스가 포함되어 있고 유효한 복제 컨텍스트가 구성된 경우에만 생성할 수 있습니다.

File System Cumulative Space Usage 보고서

File System Cumulative Space Usage Report에는 지정된 기간 동안 시스템의 공간 사용량을 자세히 나타내는 3개의 차트가 표시됩니다. 이 보고서는 백업되는 데이터의 양, 수행되는 중복 제거의 양, 사용되는 공간의 양을 분석하는 데 사용됩니다.

표 75 File System - Usage 차트 레이블 설명

항목	설명
Data Written (GiB)	압축 전에 기록된 데이터의 양이며, 보고서에 보라색 음영이 있는 영역으로 표시됩니다.
Time	데이터가 기록된 일정입니다. 이 보고서에 표시된 시간은 차트가 생성되었을 때의 Duration 선택에 따라 달라집니다.
Total Compression Factor	총 압축 비율은 압축률을 보고합니다.

표 76 File System - Consumption 차트 레이블 설명

항목	설명
Used (GiB)	압축 후 사용된 공간의 양입니다.
Time	데이터가 기록된 날짜입니다. 이 보고서에 표시된 시간은 차트가 생성되었을 때의 Duration 선택에 따라 달라집니다.
Used (Post Comp)	압축 후에 사용된 스토리지 용량입니다.
Usage Trend	검은색 점선은 스토리지 사용량 추세를 보여 줍니다. 점선이 상단의 빨간색 선에 가까워지면 스토리지가 거의 꽉 찬 것입니다.
Capacity	Data Domain 시스템의 총 용량입니다.
Cleaning	Cleaning은 정리 주기(각 정리 주기의 시작 및 종료 시간)입니다. 관리자는 이 정보를 사용해 공간 정리에 가장 적절한 시간과 최적의 임계치 조절(throttle) 설정을 선택할 수 있습니다.

표 77 File System Weekly Cumulative Capacity 차트 레이블 설명

항목	설명
Date (or Time for 24 hour report)	보고서에 설정된 기준을 바탕으로 매주 마지막 날입니다. 보고서에서 24시간은 당일 정오에서 다음 날 정오까지입니다.
Data Written (Pre-Comp)	지정된 기간 동안 압축 전에 기록된 누적 데이터입니다.
Used (Post-Comp)	지정된 기간 동안 압축 후에 기록된 누적 데이터입니다.
Compression Factor	총 압축 비율입니다. 보고서에서 검은색 선으로 표시됩니다.

File System Daily Space Usage 보고서

File System Daily Space Usage 보고서에는 지정된 기간 동안 공간 사용량을 자세히 보여 주는 5개의 차트가 표시됩니다. 이 보고서는 일일 작업을 분석하는 데 사용됩니다.

표 78 File System Daily Space Usage 차트 레이블 설명

항목	설명
Space Used (GiB)	사용된 공간의 용량입니다. Post-Comp는 빨간색으로 음영 처리된 영역입니다. Pre-Comp는 보라색으로 음영 처리된 영역입니다.
Time	데이터가 기록된 날짜입니다.
Compression Factor	총 압축 비율입니다. 보고서에 검은색 사각형으로 표시됩니다.

표 79 File System Daily Capacity Utilization 차트 레이블 설명

항목	설명
Date	데이터가 기록된 날짜입니다.
Data Written (Pre-Comp)	압축 전에 기록한 데이터 양입니다.
Used (Post-Comp)	압축 후에 사용된 스토리지 용량입니다.
Total Compression Factor	총 압축 비율입니다.

표 80 File System Weekly Capacity Utilization 차트 레이블 설명

항목	설명
Start Date	이 요약의 첫 번째 요일입니다.
End Date	이 요약의 마지막 요일입니다.
Available	사용 가능한 총 스토리지 용량입니다.
Consumed	사용한 총 스토리지 용량입니다.
Data (Post -Comp)	지정된 기간 동안 압축 전에 기록된 누적 데이터입니다.
Replication (Post-Comp)	지정된 기간 동안 압축 후에 기록된 누적 데이터입니다.
Overhead	비데이터 스토리지에 사용된 추가 공간입니다.
Reclaimed by Cleaning	정리 후 재확보된 총 공간입니다.

표 81 File System Compression Summary 차트 레이블 설명

항목	설명
Time	이 보고서에 대한 데이터 취합 기간입니다.
Data Written (Pre-Comp)	압축 전에 기록한 데이터 양입니다.
Used (Post-Comp)	압축 후에 사용된 스토리지 용량입니다.
Total Compression Factor	총 압축 비율입니다.

표 82 File System Cleaning Activity 차트 레이블 설명

항목	설명
Start Time	정리 작업을 시작한 시간입니다.
End Time	정리 작업을 마친 시간입니다.

표 82 File System Cleaning Activity 차트 레이블 설명 (계속)

항목	설명
Duration (Hours)	정리에 필요한 총 시간입니다.
Space Reclaimed	GiB(Gibibyte) 단위로 재확보된 공간입니다.

Replication Status 보고서

Replication Status 보고서에는 시스템에서 실행 중인 현재 복제 작업의 상태를 제공하는 차트 3개가 표시됩니다. 이 보고서는 모든 복제 컨텍스트에서 진행되고 있는 작업에 대한 간단한 정보를 제공하므로 Data Domain 시스템의 전체적인 복제 상태를 파악하는 데 도움이 됩니다.

표 83 Replication Context Summary 차트 레이블 설명

항목	설명
ID	복제 컨텍스트 식별 표시입니다.
Source	소스 시스템 이름입니다.
Destination	대상 시스템 이름입니다.
Type	복제 컨텍스트의 유형으로, MTree, Directory, Collection 또는 Pool이 있습니다.
Status	복제 상태 유형에는 Error, Normal이 포함됩니다.
Sync as of Time	마지막 동기화의 시간 및 날짜 스탬프입니다.
Estimated Completion	복제를 완료해야 하는 예상 시간입니다.
Pre-Comp Remaining	복제할 압축 전 데이터의 양입니다. Collection 유형에만 적용됩니다.
Post-Comp Remaining	복제해야 하는 압축 후 데이터 양입니다. Directory 및 Pool 유형에만 적용됩니다.

표 84 Replication Context Error Status 차트 레이블 설명

항목	설명
ID	복제 컨텍스트 식별 표시입니다.
Source	소스 시스템 이름입니다.
Destination	대상 시스템 이름입니다.
Type	복제 컨텍스트 유형으로 Directory 또는 Pool입니다.
Status	복제 상태 유형에는 Error, Normal, Warning이 포함됩니다.
Description	오류에 대한 설명입니다.

표 85 Replication Destination Space Availability 차트 레이블 설명

항목	설명
Destination	대상 시스템 이름입니다.

표 85 Replication Destination Space Availability 차트 레이블 설명 (계속)

항목	설명
Space Availability (GiB)	사용 가능한 총 스토리지 용량입니다.

Replication Summary 보고서

Replication Summary 보고서에는 복제 시 시스템의 전반적인 네트워크 입출력 사용량에 대한 성능 정보와 지정된 기간에 걸친 컨텍스트당 레벨이 표시됩니다. 목록에서 분석할 컨텍스트를 선택합니다.

표 86 Replication Summary 보고서 레이블 설명

항목	설명
Network In (MiB)	시스템에 입력되는 데이터 양입니다. Network In은 가는 녹색 선으로 표시됩니다.
Network Out (MiB)	시스템으로부터 전송되는 데이터 양입니다. Network Out은 굵은 주황색 선으로 표시됩니다.
Time	데이터가 기록된 날짜입니다.
Pre-Comp Remaining (MiB)	복제할 압축 전 데이터의 양입니다. Pre-Comp Remaining은 파란색 선으로 표시됩니다.

작업 로그 보기

작업 로그에는 복제 또는 시스템 업그레이드 등 현재 실행 중인 작업 목록이 표시됩니다. DD System Manager는 여러 시스템을 관리하고 해당 시스템에서 작업을 시작할 수 있습니다. 원격 시스템에서 작업을 시작한 경우 원격 시스템 작업 로그가 아니라 관리 스테이션 작업 로그에서 해당 작업의 진행률이 추적됩니다.

절차

1. **Health** > **Jobs**를 선택합니다.

   Tasks 보기가 나타납니다.

2. Filter By 목록 상자에서 Task Log를 표시할 때 사용할 필터를 선택합니다. **All**, **In Progress**, **Failed** 또는 **Completed**를 선택할 수 있습니다.

   Tasks 보기에 사용자가 선택한 필터를 기준으로 모든 작업의 상태가 표시되고 60초마다 새로 고쳐집니다.

3. Tasks 목록을 수동으로 새로 고치려면 다음 중 하나를 수행합니다.
   - **Update**를 클릭해 작업 로그를 업데이트합니다.
   - **Reset**을 클릭해 모든 작업을 표시하고 설정된 필터를 제거합니다.

4. 작업에 대한 자세한 정보를 표시하려면 작업 목록에서 해당 작업을 선택합니다.

표 87 Detailed Information, 레이블 설명

항목	설명
System	파일 시스템 이름입니다.
Task Description	작업에 대한 설명입니다.
Status	작업의 상태입니다(completed, failed 또는 in progress).
Start Time	작업을 시작한 날짜와 시간입니다.
End Time	작업을 종료한 날짜와 시간입니다.
Error Message	있는 경우 해당 오류 메시지입니다.

시스템의 HA(High Availability) 상태 보기

High Availability 패널을 사용하여 시스템의 HA 상태에 대한 자세한 정보와 필요한 경우 시스템에서 페일오버를 수행할 수 있는지 여부를 확인할 수 있습니다.

절차

1. DD System Manager에서 **Health > High Availability**를 선택합니다.

   Health High Availability 화면이 나타납니다.
   녹색 체크 표시는 시스템이 정상 작동 중이고 페일오버할 준비가 된 상태임을 나타냅니다.

   화면에 액티브 노드가 표시됩니다. 일반적으로 액티브 노드는 Node 0으로 표시됩니다.

2. 노드 위에 커서를 올려 놓으면 상태를 확인할 수 있습니다.

   노드가 활성 상태인 경우 파란색으로 표시됩니다.

3. 보기를 액티브 노드에서 대기 노드(일반적으로 Node 1)로 변경하려면 배너의 드롭다운 메뉴를 클릭합니다.

HA(High Availability) 상태

Health High Availability 보기에는 시스템의 상태에 대한 정보가 노드와 연결된 스토리지의 다이어그램으로 표시됩니다. 또한 현재 알림과 모든 시스템에 대한 세부 정보도 표시됩니다.

액티브 노드와 스토리지 위에 커서를 올려 놓으면 정상 작동 중인지를 확인할 수 있습니다. 정상 작동 중인 구성 요소는 파란색으로 표시됩니다. 대기 노드는 회색으로 표시됩니다.

구성 요소를 클릭하여 알림 테이블을 필터링할 수도 있습니다. 선택한 구성 요소와 관련한 알림만 표시됩니다.

그림 6 상태/HA(High Availability) 표시

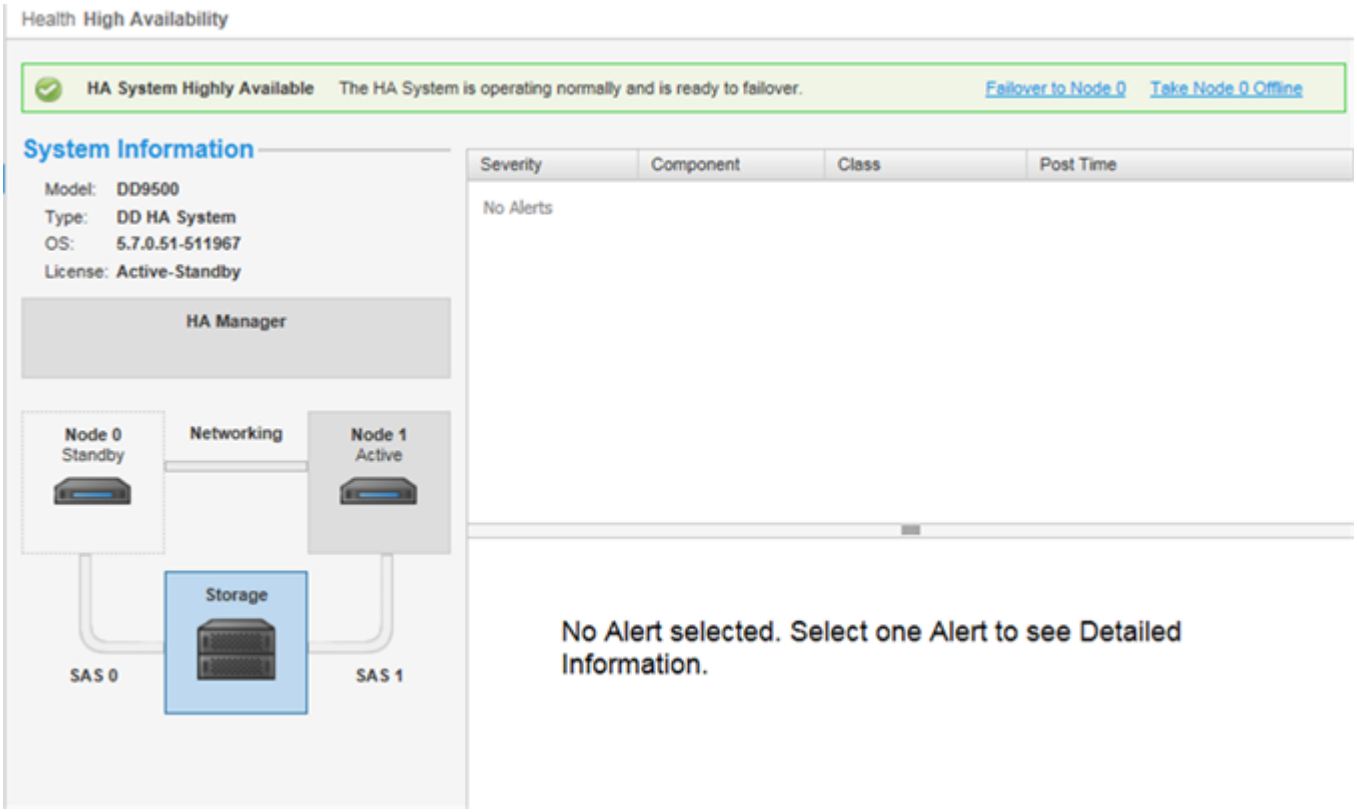


표 88 HA(High Availability) 상태 표시

항목	설명
HA 시스템 표시줄	시스템이 정상 작동 중이고 페일오버할 준비가 된 경우 녹색 체크 표시가 나타납니다.
Failover to Node 0	수동으로 대기 노드로 페일오버할 수 있습니다.
Take Node 1 Offline	필요한 경우 액티브 노드를 오프라인으로 전환할 수 있습니다.
System Information	Data Domain 시스템 모델, 시스템 유형, 사용 중인 Data Domain Operating System의 버전, 적용된 HA 라이센스가 표시됩니다.
HA Manager	노드, 노드에 연결된 스토리지, HA 상호 연결 및 케이블 연결이 표시됩니다.
Severity	시스템의 HA 상태에 영향을 줄 수 있는 모든 알림의 심각도 나타냅니다.
Component	영향을 받는 구성 요소를 나타냅니다.
Class	하드웨어, 환경 등, 수신된 알림의 클래스를 나타냅니다.
Post Time	알림이 게시된 날짜와 시간을 나타냅니다.

5장

파일 시스템

이 장에는 다음과 같은 내용이 포함됩니다.

파일 시스템 개요

파일 시스템을 사용하는 방법을 학습합니다.

파일 시스템의 데이터 저장 방식

Data Domain 스토리지 용량은 여러 백업을 만들고 다음 정리까지 백업을 수용하는 20%의 빈 공간을 유지하는 최적의 방식으로 관리됩니다. 공간 사용은 주로 데이터의 크기 및 압축 가능성과 보존 기간에 영향을 받습니다.

Data Domain 시스템은 백업 및 아카이브 데이터용의 매우 안정적인 온라인 시스템으로 설계되었습니다. 새 백업이 시스템에 추가됨에 따라 이전 백업은 제거됩니다. 이러한 제거 작업은 보통 구성된 보존 기간에 따라 백업 또는 아카이브 소프트웨어의 제어 하에 수행됩니다.

백업 소프트웨어에서 Data Domain 시스템의 이전 백업을 만료시키거나 삭제하는 경우, Data Domain 시스템의 이 공간은 Data Domain 시스템이 디스크에서 만료된 백업의 데이터를 정리하고 난 후에야 사용 가능합니다. Data Domain 시스템의 공간을 관리하는 바람직한 방법은 일부 빈 공간(총 사용 가능 공간의 약 20%)을 사용하여 가능한 한 많은 온라인 백업을 보존함으로써 기본적으로 주 1회 실행되는 다음 예약된 정리일까지 원활하게 백업을 수용하게끔 하는 것입니다.

일부 스토리지 용량은 내부 인덱스 및 기타 메타데이터용으로 Data Domain 시스템에서 사용됩니다. 시간이 지남에 따라 메타데이터용으로 사용되는 스토리지의 양은 저장된 데이터의 유형 및 저장된 파일의 크기에 따라 달라집니다. 두 개의 동일한 시스템에서 서로 다른 데이터 세트가 각 시스템으로 전송된 경우, 시간이 지남에 따라 한 시스템에서 다른 시스템보다 메타데이터용으로 더 많은 공간을 예약하고 실제 백업 데이터 공간이 더 적을 수 있습니다.

Data Domain 시스템의 공간 사용률은 주로 다음의 영향을 받습니다.

- 백업 데이터의 크기 및 압축률
- 백업 소프트웨어에 지정된 보존 기간

많은 중복을 이용해 데이터 세트를 백업하고 장기간 이러한 데이터 세트를 보존하는 경우 압축 수준이 높아집니다.

파일 시스템의 공간 사용량 보고 방식

모든 DD System Manager 창과 시스템 명령은 2진 표기법으로 계산하여 스토리지 용량을 표시합니다. 예를 들어 디스크 공간의 1GiB가 사용된 것으로 표시하는 명령은 2^{30} 바이트 = 1,073,741,824바이트를 보고합니다.

- 1KiB = 2^{10} = 1,024바이트
- 1MiB = 2^{20} = 1,048,576바이트
- 1GiB = 2^{30} = 1,073,741,824바이트
- 1TiB = 2^{40} = 1,099,511,627,776바이트

파일 시스템의 압축 사용 방식

파일 시스템은 압축을 사용해 데이터 저장 시 사용 가능한 디스크 공간을 최적화하므로 디스크 공간이 두 가지 방법 즉, 물리적과 논리적으로 계산됩니다. (압축 유형에 대한 섹션 참조) 물리적 공간은 Data Domain 시스템에서 사용되는 실제 디스크 공간입니다. 논리적 공간은 시스템에 기록된 압축되지 않은 데이터의 양입니다.

파일 시스템 공간 보고 툴(DD System Manager 그래프 및 `filesys show space` 명령 또는 별칭 `df`)은 물리적 공간과 논리적 공간을 모두 표시합니다. 또한 이 툴은 사용 중이거나 사용 가능한 공간의 크기 및 양도 보고합니다.

Data Domain 시스템이 마운트된 경우에는 파일 시스템의 물리적 공간 활용을 표시하는 일반적인 툴을 사용할 수 있습니다.

Data Domain 시스템은 파일 시스템이 90%, 95% 및 100% 용량에 이르면 경고 메시지를 생성합니다. 데이터 압축에 대한 다음 정보는 시간 경과에 따른 디스크 사용에 대한 지침으로 활용할 수 있습니다.

시간이 지나면서 Data Domain 시스템이 사용하는 디스크 공간의 양은 다음에 따라 달라집니다.

- 초기 전체 백업의 크기
- 시간이 지나면서 보존되는 추가 백업(증분 및 전체)의 수
- 백업 데이터 세트의 증가율
- 데이터 변경률

일반적인 변경률 및 증가율을 가진 데이터 세트의 경우 데이터 압축은 일반적으로 다음 지침과 같습니다.

- Data Domain 시스템에 대한 첫 번째 전체 백업의 경우 압축 비율은 일반적으로 3:1입니다.
- 초기 전체 백업에 대한 각 증분 백업의 경우 압축 비율은 일반적으로 6:1의 범위에 있습니다.
- 다음 전체 백업의 경우 압축 비율은 약 60:1입니다.

시간이 지나면서, 주 단위 전체 백업 및 매일 증분 백업 스케줄에 따라 모든 데이터에 대한 총 압축 비율은 20:1이 됩니다. 압축 비율은 증분 전용 데이터 또는 중복 데이터가 적은 백업의 경우 더 낮습니다. 모든 백업이 전체 백업인 경우에는 압축 비율이 더 높습니다.

압축 유형

Data Domain 시스템에서는 글로벌 및 로컬의 두 수준으로 데이터를 압축합니다. 글로벌 압축은 수신된 데이터를 디스크에 이미 저장된 데이터와 비교합니다. 중복 데이터는 다시 저장될 필요가 없지만 새 데이터는 디스크에 기록되기 전에 압축됩니다.

로컬 압축

Data Domain 시스템에서는 데이터가 디스크에 기록될 때의 처리량을 극대화하기 위해 특별히 개발된 로컬 압축 알고리즘을 사용합니다. 기본 알고리즘(lz)을 사용하면 백업 작업에 드는 백업 기간이 단축되지만 공간을 더 많이 사용합니다. 사용 가능한 다른 두 유형의 로컬 압축은 gzfast 및 gz입니다. 둘 모두 lz보다 향상된 압축을 제공하지만 CPU 로드가 늘어납니다. 로컬 압축 옵션을 사용하면 느린 성능과 공간 사용량 간의 균형을 맞출 수 있습니다. 로컬 압축을 해제할 수도 있습니다. 압축을 변경하려면 로컬 압축 변경(205페이지) 항목을 참조하십시오.

압축 유형을 변경한 후에는 모든 새 쓰기에 새 압축 유형을 사용합니다. 기존 데이터는 정리되는 동안 새 압축 유형으로 변환됩니다. 압축 유형 변경 전에 있었던 데이터를 모두 다시 압축하려면 몇 번에 걸친 정리 작업이 필요합니다.

압축 유형 변경 후 처음으로 하는 정리 작업은 평소보다 시간이 더 걸릴 수 있습니다. 압축 유형을 변경할 때마다 1~2주간 시스템을 주의 깊게 모니터링하여 제대로 작동하는지 확인하도록 합니다.

파일 시스템의 데이터 무결성 실행 방식

DD OS 파일 시스템은 백업 애플리케이션에서 수신한 데이터에 대해 여러 계층의 데이터 검증을 실행하여 데이터가 Data Domain 시스템 디스크에 올바르게 기록되도록 합니다. 또한 오류 없이 데이터를 검색할 수 있도록 해 줍니다.

DD OS는 데이터 보호를 위해 특별히 제작되었으며 데이터 손상을 차단하는 아키텍처로 설계되었습니다. 다음 섹션에서 네 가지 주요 중점 영역에 대해 살펴봅니다.

철저한 데이터 검증

철저한 검사를 통해 모든 파일 시스템 데이터와 메타데이터를 보호합니다. 데이터가 시스템에 수신되면 강력한 체크섬 계산이 수행됩니다. 데이터는 중복이 제거되어 파일 시스템에 저장됩니다. 모든 데이터가 디스크에 플러시되면 다시 읽고 체크섬이 재수행됩니다. 체크섬을 비교하여 데이터와 파일 시스템 메타데이터가 모두 제대로 저장되었는지 검증합니다.

장애 방지 및 억제

Data Domain에서는 기존 데이터를 업데이트하거나 여기에 덮어쓰지 않는 로그 구조 파일 시스템을 사용합니다. 새 데이터는 항상 새 컨테이너에 기록되어 기존의 컨테이너에 추가됩니다. 기존 컨테이너 및 참조는 그대로 유지되며, 새 백업을 저장할 때 소프트웨어 버그나 하드웨어 장애가 발생해도 안전하게 보호됩니다.

지속적인 장애 감지 및 복구

지속적인 장애 감지 및 복구 기능을 통해 스토리지 시스템을 장애로부터 보호합니다. 시스템은 정기적으로 RAID 스트라이프의 무결성을 재검사하고, 오류가 있을 경우 RAID 시스템의 이중화 기능을 통해 오류를 복구합니다. 읽기 작업 시 데이터 무결성이 다시 검증되고 오류가 있으면 즉시 복구됩니다.

파일 시스템 복구 성능

데이터가 자가 설명 형식으로 기록됩니다. 필요한 경우 로그를 스캔하고 데이터와 함께 저장된 메타데이터를 재구성하여 파일 시스템을 다시 생성할 수 있습니다.

파일 시스템 정리를 통한 파일 시스템의 스토리지 공간 확보

NetWorker, NetBackup 등의 백업 애플리케이션에서 데이터가 만료되면 데이터가 Data Domain 시스템에서 삭제 대상으로 표시됩니다. 그러나 데이터는 즉시 삭제되지 않고 정리 작업이 진행되는 동안 제거됩니다.

- 정리 작업 도중에도 파일 시스템을 사용하여 쓰기 작업인 백업과 읽기 작업인 복구를 포함한 정상적인 작업을 모두 수행할 수 있습니다.
- 정리 작업에 상당한 양의 시스템 리소스가 사용되긴 하지만 정리의 임계치가 자가 조절되며 사용자 트래픽이 있을 경우에는 시스템 리소스가 정리에 사용되지 않습니다.
- Data Domain 시스템에 대한 첫 번째 전체 백업 후 정리 작업을 실행하는 것이 좋습니다. 전체 백업에서 초기 로컬 압축 비율은 일반적으로 1.5에서 2.5 정도입니다. 즉시 정리 작업을 수행하면 1.15에서 1.2 정도의 비율만큼 추가 압축이 이루어지고 그에 해당하는 양의 디스크 공간이 재확보됩니다.
- 정리 작업이 끝나면 메시지가 시스템 로그에 전송되어 확보된 스토리지 공간의 비율을 제공합니다.

기본 스케줄에 따라 매주 화요일 오전 6시(tue 0600)에 정리 작업을 실행합니다. 스케줄을 변경하거나 수동으로 작업을 실행할 수 있습니다. 정리 스케줄 수정에 관한 섹션을 참조하십시오.

Data Domain에서는 매주 한 번씩 정리 작업을 실행하는 것이 좋습니다.

파일 시스템을 해제하거나 시스템 전원 끄기 또는 재부팅 등 정리 작업 동안 Data Domain 시스템을 중단하는 모든 작업은 정리 작업을 중단시킵니다. 정리 작업은 시스템 재시작 시 즉시 재시작되지 않습니다. 정리 작업을 수동으로 재시작하거나 다음 예약된 정리 작업까지 기다릴 수 있습니다.

컬렉션 복제를 사용하면 복제되지 않은 소스 시스템의 복제 컨텍스트에 있는 데이터를 파일 시스템 정리를 위해 처리할 수 없습니다. 소스 및 대상 시스템이 동기화되지 않아 파일 시스템 정리를 완료할 수 없는 경우 시스템은 정리 작업의 상태를 `partial`로 보고하며 정리 작업에 대해 제한적인 시스템 상태 통계만 사용할 수 있습니다. 컬렉션 복제를 비활성화하면 복제 소스 및 대상 시스템이 동기화되지 않은 상태로 유지되기 때문에 파일 시스템 정리에서 처리할 수 없는 데이터의 양이 증가합니다. KB 문서 *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*에서 자세한 정보를 제공하며, 이 문서는 온라인 지원 사이트(https://support.emc.com)에서 사용할 수 있습니다.

MTree 복제를 이용해 스냅샷이 복제되는 동안 파일을 생성 및 삭제하면, 다음 스냅샷에 이 파일에 대한 어떠한 정보도 존재하지 않으며 시스템에서 이 파일과 연결된 모든 컨텐츠를 복제하지 않습니다. 디렉토리 복제는 생성과 삭제가 서로 동시에 이루어져도 복제합니다.

디렉토리 복제에서 사용하는 복제 로그를 통해 삭제, 이름 변경 등과 같은 작업이 단일 스트림으로 실행됩니다. 이는 복제 처리량을 줄일 수 있습니다. MTree 복제에 의한 스냅샷 사용은 이 문제를 방지합니다.

지원되는 인터페이스

파일 시스템에서 지원되는 인터페이스는 다음과 같습니다.

- NFS
- CIFS
- DD Boost
- DD VTL

지원되는 백업 소프트웨어

Data Domain 시스템과 함께 사용할 백업 소프트웨어 및 백업 서버의 설정에 대한 지침은 support.emc.com에서 제공됩니다.

Data Domain 시스템에 전송되는 데이터 스트림

최적의 성능을 위해서는 Data Domain 시스템과 사용자의 백업 서버 간의 동시 스트림에 대한 제한값을 따르는 것이 좋습니다.

다음 표에서 데이터 스트림은 백업 파일에 대한 쓰기 스트림 또는 복구 이미지로부터의 읽기 스트림 등 순차적 파일 액세스와 관련된 대규모 바이트 스트림을 의미합니다. 복제 소스 또는 대상 스트림은 디렉토리 복제 작업 스트림 또는 파일 복제 작업과 관련된 DD Boost 파일 복제 스트림을 말합니다.

표 89 Data Domain 시스템에 전송되는 데이터 스트림

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD140, DD160, DD610	4GB 또는 6GB/0.5GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8GB/0.5GB 또는 1GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16GB 또는 20GB/1GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36GB/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72GB[b]/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 또는 64GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885

표 89 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD9800	256/768GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD6300	48/96GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8TB	8GB/512MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16TB	16GB/512MB 또는 24GB/1GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32TB	24GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48TB	36GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64TB	48GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96TB	64GB/2GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4TB	12GB(가상 메모리)/512MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32TB	46GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

표 89 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

a. DirRepl, OptDup, MTreeRepl 스트림
b. Data Domain Extended Retention 소프트웨어 옵션은 확장(최대) 메모리를 지원하는 이러한 디바이스에서만 사용할 수 있습니다.

파일 시스템 제한 사항

파일 시스템에는 파일 수 제한, 배터리 제한 등의 제한 사항이 있습니다.

Data Domain 시스템의 파일 수 제한

10억 개가 넘는 파일을 저장할 경우의 고려 사항과 그로 인한 결과는 다음과 같습니다.

Data Domain에서는 시스템에 저장하는 파일 수가 10억 개 이하인 것이 좋습니다. 그 이상의 파일 수를 저장하는 경우 성능 및 정리 시간에 부정적인 영향을 미칠 수 있으며, 파일 시스템 정리와 같은 일부 프로세스는 파일 수가 너무 많은 이유로 실행에 훨씬 더 많은 시간이 소요될 수 있습니다. 예를 들어, 정리 열거 단계는 시스템 내 파일 수에 따라 몇 분에서 몇 시간까지 걸릴 수 있습니다.

참고

시스템에서 최대 파일 양을 지원해야 하고 클라이언트 시스템에서 워크로드가 신중히 제어되지 않는 경우에는 Data Domain 시스템의 전반적인 성능이 감당할 수 있는 수준을 벗어나게 됩니다.

파일 시스템이 10억 개 파일 제한을 초과하면 다음의 예와 같은 몇 가지 프로세스 또는 작동 성능이 저하될 수 있습니다.

- 정리 완료에 며칠이 걸릴 정도로 매우 오랜 시간이 걸릴 수 있습니다.
- 자동 지원 작업에 더 많은 시간이 소요될 수 있습니다.
- 모든 파일을 열거해야 하는 모든 프로세스 또는 명령에 부정적인 영향이 있을 수 있습니다.

작은 파일이 많은 경우 다른 고려 사항이 발생할 수 있습니다.

- 초당 생성될 수 있는 별도의 파일 수는 파일이 아주 작더라도 Data Domain 시스템으로 이동할 수 있는 초당 MB 수보다 더 많은 제약이 있을 수 있습니다. 파일이 대용량인 경우 파일 생성률이 높지 않지만 파일이 저용량인 경우에는 파일 생성률이 매우 높으며 이는 제약 요인이 될 수 있습니다. 파일 생성률은 MTree 및 CIFS 연결 수에 따라 초당 약 100~200개 파일입니다. 고객 환경에서 대량의 파일을 대량으로 수집해야 하는 경우에는 시스템 사이징 중 이 속도를 고려해야 합니다.
- 파일 액세스 지연 시간은 디렉토리에 있는 파일 수에 영향을 받습니다. 가급적이면 디렉토리 크기를 250,000개 미만의 파일로 제한하는 것이 좋습니다. 디렉토리 크기가 이보다 크면 디렉토리에 파일을 나열하고 파일을 열거나 생성하는 것과 같은 메타데이터 작업에 대한 응답 속도가 느려질 수 있습니다.

배터리 제한

NVRAM을 사용하는 시스템의 경우 배터리 충전율이 80% 아래로 내려가면 운영 체제에서 배터리 부족 알림을 생성하고 파일 시스템이 해제됩니다.

알림

Data Domain DD2200 시스템은 NVRAM을 사용하지 않기 때문에 펌웨어 계산을 통해 배터리 충전율이 데이터를 저장하기에 충분한지 결정하며, AC 전원 손실이 발생할 경우 파일 시스템을 해제합니다.

최대 지원 inode 수

NFS 또는 CIFS 클라이언트가 요청하면 Data Domain 시스템이 약 20억 개의 inode(파일 및 디렉토리) 용량을 보고합니다. Data Domain 시스템에서 그 수치를 초과할 수 있지만 클라이언트에 대한 보고가 올바르지 않을 수도 있습니다.

경로 이름 최대 길이

`/data/col1/backup`의 문자를 포함하는 전체 경로 이름의 최대 길이는 61자입니다. 심볼 링크의 최대 길이도 61자입니다.

HA 페일오버 시 제한된 액세스

HA(High Availability) 시스템에서 페일오버 시에 최장 10분 동안 파일에 대한 액세스가 중단될 수 있습니다. DD Boost 및 NFS의 경우 더 많은 시간이 소요됩니다.

파일 시스템 사용량 모니터링

실시간 데이터 스토리지 통계를 봅니다.

File System 보기에는 실시간 데이터 스토리지 통계, 클라우드 유닛 정보, 암호화 정보에 액세스하고 공간 사용량, 사용 비율 및 데이터 기록 추세 그래프에 액세스할 수 있는 탭과 컨트롤이 있습니다. 또한 파일 시스템 정리, 확장, 복사 및 제거를 관리하는 컨트롤도 있습니다.

File System 보기 액세스

이 섹션에서는 파일 시스템 기능에 대해 설명합니다.

절차

- **Data Management** > **File System**을 선택합니다.

File System Status 패널 정보

파일 시스템 서비스의 상태를 표시합니다.

File System Status 패널에 액세스하려면 **Data Management** > **File System** > **Show Status of File System Services**를 클릭합니다.

파일 시스템

File System 필드에는 **Enable/Disable** 링크가 있으며 파일 시스템의 작업 상태가 표시됩니다.

- Enabled and Running - 최근 연속해서 파일 시스템이 활성화 및 실행 중인 기간도 함께 표시됩니다.
- Disabled and Shutdown
- Enabling and Disabling - 활성화 또는 비활성화 프로세스 중에 표시됩니다.
- Destroyed - 파일 시스템이 삭제된 경우 표시됩니다.
- Error - 파일 시스템 초기화 문제 등 오류가 있을 경우 표시됩니다.

Cloud File Recall

Cloud File Recall 필드에는 Cloud Tier에서 파일 리콜을 시작할 수 있는 **Recall** 링크가 포함되어 있습니다. **Details** 링크는 활성 리콜이 진행 중인 경우에 사용할 수 있습니다. 자세한 내용은 "Cloud Tier에서 파일 리콜" 항목을 참조하십시오.

Physical Capacity Measurement

물리적 용량 측정 상태를 비활성화한 경우 **Physical Capacity Measurement** 필드에 **Enable** 버튼이 표시됩니다. 활성화한 경우에는 **Disable** 및 **View** 버튼이 표시됩니다. **View**를 클릭하면 현재 실행 중인 물리적 용량 측정에 대한 정보가 MTree, 우선 순위, 제출 시간, 시작 시간 및 기간과 함께 표시됩니다.

Data Movement

Data Movement 필드에는 **Start/Stop** 버튼이 있으며 마지막 데이터 이동 작업이 완료된 날짜, 복제된 파일 수 및 복제된 데이터의 양이 표시됩니다. 데이터 이동 작업을 사용할 수 있는 경우 **Start** 버튼이 표시되고 데이터 이동 작업이 실행 중인 경우 **Stop** 버튼이 표시됩니다.

Active Tier Cleaning

Active Tier Cleaning 필드에는 **Start/Stop** 버튼이 있으며, 마지막 정리 작업이 실행된 날짜가 표시되거나 현재 정리 작업을 실행 중인 경우 현재 정리 상태가 표시됩니다. 예:

```
Cleaning finished at 2009/01/13 06:00:43
```

또는 파일 시스템이 비활성화된 경우에는 다음과 같이 표시됩니다.

```
Unavailable
```

Cloud Tier Cleaning

Cloud Tier Cleaning 필드에는 **Start/Stop** 버튼이 있으며, 마지막 정리 작업이 실행된 날짜가 표시되거나 현재 정리 작업을 실행 중인 경우 현재 정리 상태가 표시됩니다. 예:

```
Cleaning finished at 2009/01/13 06:00:43
```

또는 파일 시스템이 비활성화된 경우에는 다음과 같이 표시됩니다.

```
Unavailable
```

Summary 탭 정보

Summary 탭을 클릭하여 활성 및 클라우드 계층의 공간 사용량 통계를 표시하고 파일 시스템 상태 보기, 파일 시스템 설정 구성, 빠른 복제 작업 수행, 용량 확장 및 파일 시스템 제거 작업을 실행할 수 있는 컨트롤에 액세스합니다.

각 계층에 대한 공간 사용량 통계에는 다음이 포함됩니다.

- **Size** - 데이터에 사용 가능한 물리적 디스크 공간의 총 크기입니다.
- **Used** - 압축된 데이터에 사용되는 실제 물리적 공간입니다. 사용량이 90%, 95%, 100%에 도달하면 경고 메시지가 시스템 로그에 전달되고 이메일 알림이 생성됩니다. 100%에 도달하면 Data Domain 시스템이 백업 서버에서 더 이상 데이터를 받지 않습니다.
  Used 공간 크기가 항상 높다면 정리 스케줄을 확인해 정리 작업이 자동으로 얼마나 자주 실행되는지 알아보십시오. 그러고 나서 정리 스케줄 수정 절차를 사용해 정리 작업을 좀 더 자주 실행하십시오. 나아가 데이터 보존 기간을 줄이거나 백업 데이터의 일부를 다른 Data Domain 시스템으로 분할하는 방법도 고려해 보십시오.
- **Available** (GiB) - 데이터 스토리지에 사용 가능한 총 공간 크기입니다. Data Domain 시스템에 데이터가 증가함에 따라 내부 인덱스가 확장되기 때문에 이 값이 변할 수 있습니다. 확장된 인덱스는 Avail GiB의 공간을 점유합니다.

- **Pre-Compression** (GiB) - 압축 전에 기록된 데이터
- **Total Compression Factor (Reduction %)** - 압축 전 / 압축 후
- **Cleanable** (GiB) - 정리 작업 실행 시 재확보가 가능한 공간의 크기입니다.

Cloud Tier의 경우 **Cloud File Recall** 필드에는 Cloud Tier에서 파일 리콜을 시작할 수 있는 **Recall** 링크가 포함되어 있습니다. **Details** 링크는 활성 리콜이 진행 중인 경우에 사용할 수 있습니다. 자세한 내용은 "Cloud Tier에서 파일 리콜" 항목을 참조하십시오.

지난 24시간 동안 각 계층의 다음과 같은 통계가 별도의 패널에 제공됩니다.

- **Pre-Compression** (GiB) - 압축 전에 기록된 데이터
- **Post-Compression** (GiB) - 압축 후에 사용된 스토리지
- **Global Compression Factor** - (압축 전) / (전역 압축 이후의 크기)
- **Local Compression Factor** - (전역 압축 이후의 크기) / (압축 후)
- **Total Compression Factor (Reduction %)** - [(압축 전 - 압축 후) / 압축 전] * 100

파일 시스템 설정 정보

시스템 옵션과 현재 정리 스케줄을 표시하고 변경합니다.

File System Settings 대화 상자에 액세스하려면 **Data Management** > **File System** > **Settings**를 클릭합니다.

표 90 일반 설정

일반 설정	설명
Local Compression Type	사용 중인 로컬 압축의 유형입니다. • 개요는 압축 유형에 관한 섹션을 참조하십시오. • 로컬 압축 유형 변경에 관한 섹션을 참조하십시오.
Cloud Tier Local Comp	클라우드 계층에 사용 중인 압축의 유형입니다. • 개요는 압축 유형에 관한 섹션을 참조하십시오. • 로컬 압축 유형 변경에 관한 섹션을 참조하십시오.
Report Replica as Writable	애플리케이션에서 복제본을 인식하는 방식입니다. • 읽기 전용 설정 변경에 관한 섹션을 참조하십시오.
Staging Reserve	디스크 스테이징을 관리합니다. • 디스크 스테이징 작업에 관한 섹션을 참조하십시오. • 디스크 스테이징 구성에 관한 섹션을 참조하십시오.
Marker Type	데이터 스트림의 백업 소프트웨어 마커(테이프 마커, 태그 헤더 또는 다른 이름이 사용됨)입니다. 테이프 마커 설정에 관한 섹션을 참조하십시오.
Throttle	물리적 용량 측정 스로틀 설정 관련 섹션을 참조하십시오.
Cache	물리적 용량 캐시를 초기화하면 캐시가 정리되고 측정 속도가 향상됩니다.

파일 시스템의 워크로드 밸런스를 조정하여 사용량을 기준으로 성능을 향상시킬 수 있습니다.

표 91 워크로드 밸런스 설정

워크로드 밸런스 설정	설명
Random workloads (%)	랜덤 워크로드를 사용하여 즉각적인 액세스 및 복구의 성능을 향상시킵니다.
Sequential workloads (%)	순차적 워크로드를 사용하여 기존 백업 및 복구의 성능을 향상시킵니다.

표 92 데이터 이동 설정

데이터 이동 정책 설정	설명
File Age Threshold	데이터 이동이 시작되면 지정한 임계값 일수 동안 수정되지 않은 모든 파일이 활성 계층에서 보존 계층으로 이동합니다.
Schedule	일수 및 횟수 데이터를 이동합니다.
Throttle	시스템이 데이터 이동에 사용할 수 있는 리소스의 백분율입니다. 기본 스로틀 값은 100%이며 기본값을 사용할 경우 데이터 이동에 스로틀이 적용되지 않습니다.

표 93 정리 설정

정리 스케줄 설정	설명
Time	정리 작업을 실행하는 날짜/시간입니다. • 정리 스케줄 수정에 관한 섹션을 참조하십시오.
Throttle	시스템 리소스 할당입니다. • 정리 작업의 스로틀링에 관한 섹션을 참조하십시오.

Cloud Units 탭 정보

클라우드 유닛에 대한 요약 정보를 표시하고, 클라우드 유닛을 추가 및 수정하고, 인증서를 관리합니다.

File System 페이지의 Cloud Units 탭은 선택 사항인 DD Cloud Tier 라이센스를 활성화한 경우에만 표시됩니다. 이 보기에는 요약 정보(상태, 네트워크 대역폭, 읽기 액세스, 로컬 압축, 데이터 이동 및 데이터 상태), 클라우드 공급업체, 사용 용량 및 라이센스 용량이 표시됩니다. 클라우드 유닛을 편집하고, 인증서를 관리하고, 새로운 클라우드 유닛을 추가할 수 있는 컨트롤이 제공됩니다.

Retention Units 탭 정보

보존 유닛 및 보존 유닛의 상태와 크기를 표시합니다.

File System 페이지의 Retention Units 탭은 선택적으로 DD Extended Retention 라이센스가 활성화되어 있을 때만 표시됩니다. 이 보기에는 보존 유닛이 나열되어 있으며 New, Sealed, Target 등의 상태, Disabled 또는 Ready 등의 상태와 그 크기가 표시됩니다. 유닛이 봉인되어 있는 경우, 이는 데이터가 더 이상 추가될 수 없음을 뜻하며 봉인된 날짜가 제공됩니다.

열 머리글 오른쪽에 있는 다이아몬드 기호를 선택하면 값의 순서를 역순으로 정렬할 수 있습니다.

DD Encryption 탭 정보

암호화 상태, 진행률, 알고리즘 등을 표시합니다.

표 94 DD 암호화 설정

설정	설명
DD System	상태는 다음 중 하나일 수 있습니다. • Not licensed - 다른 정보가 제공되지 않음 • Not configured - 암호화 라이센스는 있으나 구성되지 않음 • Enabled - 암호화가 활성화되어 실행 중임 • Disabled - 암호화가 비활성화됨
Active Tier	활성 계층의 암호화 상태 보기: • Enabled - 암호화가 활성화되어 실행 중임 • Disabled - 암호화가 비활성화됨
Cloud Unit	클라우드 유닛별 암호화 상태 보기: • Enabled - 암호화가 활성화되어 실행 중임 • Disabled - 암호화가 비활성화됨
Encryption Progress	데이터 재암호화 및 변경 내용 적용과 관련한 활성 계층의 암호화 상태 세부 정보를 봅니다. 상태는 다음 중 하나일 수 있습니다. • None • Pending • Running • Done View Details를 클릭하여 Active Tier에 대한 다음 정보를 포함하는 Encryption Status Details 대화 상자를 표시합니다. • Type(예: 암호화가 이미 시작된 경우 Changes를 적용하거나 이전에 제거된 키 등 암호화가 데이터 유출에 의한 결과인 경우 Re-encryption을 적용합니다.) • Status(예: Pending) • Details: (예: 12월 xx/xx/xx에 요청되었으며 다음 시스템 정리 후에 수행됩니다.)
Encryption Algorithm	데이터 암호화에 사용되는 알고리즘: • AES 256-bit (CBC) (기본값) • AES 256-bit (GCM) (더 안전하지만 느림) • AES 128-bit (CBC) (256비트만큼 안전하지 않음) • AES 128-bit (GCM) (256비트만큼 안전하지 않음) 자세한 내용은 암호화 알고리즘 변경을 참고하십시오.
Encryption Passphrase	구성된 경우 “*****”라고 표시됩니다. 암호 변경은 시스템 암호 관리를 참조하십시오.
File System Lock	

표 94 DD 암호화 설정 (계속)

설정	설명
Status	File System Lock 상태는 다음 중 하나입니다. • Unlocked - 기능이 활성화되지 않음 • Locked - 기능이 활성화됨
Key Management	
Key Manager	내부 Data Domain Embedded Key Manager 또는 선택 사항인 RSA DPM(Data Protection Manager) Key Manager 중 하나입니다. **Configure**를 클릭하여 Key Manager를 서로 전환하거나(둘 모두 구성된 경우) Key Manager 옵션을 수정합니다.
Server	RSA Key Manager Server의 이름입니다.
Server Status	온라인 또는 오프라인이거나 RSA Key Manager Server에서 반환되는 오류 메시지입니다.
Key Class	비슷한 특성을 가진 암호 키를 그룹화하는 RSA DPM(Data Protection Manager) Key Manager 옵션에 의해 사용되는 특수 유형의 보안 클래스입니다. Data Domain 시스템은 키 클래스별로 RSA 서버에서 키를 검색합니다. 키 클래스는 현재 키를 반환하거나 매번 새 키를 생성하도록 설정됩니다. 참고 Data Domain 시스템은 현재 키를 반환하도록 구성된 키 클래스만 지원합니다.
Port	RSA 서버의 포트 번호입니다.
FIPS mode	가져온 호스트 인증서의 FIPS 준수 여부를 나타냅니다. 기본 모드가 활성화되어 있습니다.
Encryption Keys	ID 번호별로 키를 나열합니다. 키의 생성 시기, 유효 기간, 유형(RSA DPM Key Manager 또는 Data Domain 내부 키), 상태(RSA DPM Key Manager 작업, Data Domain이 지원하는 DPM 암호화 키 상태 참조), 키로 암호화된 데이터 양을 보여 줍니다. 시스템에서 키 정보의 마지막 업데이트 시간을 오른쪽 열 위에 표시합니다. 목록에서 선택된 키는 다음과 같을 수 있습니다. • 동기화됨(RSA 서버에 추가된 새 키가 목록에 표시되지만 파일 시스템이 재시작될 때까지는 사용 불가) • 삭제됨 • 제거됨

Space Usage 보기 정보(파일 시스템)

특정 시점의 파일 시스템 데이터 사용에 대한 시각적(정적) 표현을 표시합니다.

Data Management > **File System** > **Charts**를 클릭합니다. Chart 드롭다운 목록에서 **Space Usage**를 선택합니다.

그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 표시합니다. 그래프 선이 의미하는 바는 다음과 같습니다.

- Pre-comp Written - 백업 서버가 MTree에 보낸 총 데이터 양입니다. 백업 서버는 MTree의 압축 전 데이터를 MTree가 스토리지 단위로써 보관하고 있는 압축되지 않은 데이터로 인식합니다. 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다.
- Post-comp Used - MTree에서 사용 중인 총 디스크 스토리지 용량으로 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다.
- Comp Factor - Data Domain 시스템이 수신한 데이터로 수행한 압축의 양, 즉 압축 비율입니다. 그래프의 세로 축 오른쪽에 Compression Factor와 함께 표시됩니다.

기간별 공간 사용량 확인

Space Usage 그래프에서 그래프 위에 기간(1w, 1m, 3m, 1y 또는 All)을 클릭하여 그래프에 표시되는 데이터의 기간을 변경할 수 있습니다. 예를 들어 1w에서 All로 변경합니다.

Consumption 보기 정보

시간별 공간 사용량을 총 시스템 용량과 비교하여 표시합니다.

Data Management > **File System** > **Charts**를 클릭합니다. Chart 드롭다운 목록에서 **Consumption**을 선택합니다.

그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 표시합니다. 그래프 선이 의미하는 바는 다음과 같습니다.

- Capacity - Data Domain 시스템의 데이터에 대해 사용 가능한 총 디스크 스토리지 용량입니다. 용량은 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다. Capacity 확인란을 클릭하여 이 선의 활성화 및 비활성화를 전환할 수 있습니다.
- Post-comp - Data Domain 시스템에서 사용 중인 총 디스크 스토리지 용량입니다. 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다.
- Comp Factor - Data Domain 시스템이 수신한 데이터로 수행한 압축의 양, 즉 압축 비율입니다. 그래프의 세로 축 오른쪽에 Compression Factor와 함께 표시됩니다.
- Cleaning - 파일 시스템 정리 작업이 시작될 때마다 회색 다이아몬드가 차트에 표시됩니다.
- Data Movement - 아카이브 라이센스를 활성화한 경우 아카이빙 스토리지 영역으로 이동된 디스크 공간의 크기입니다.

기간별 사용량 확인

Consumption 그래프에서 그래프 위에 기간(1w, 1m, 3m, 1y 또는 All)을 클릭하여 그래프에 표시되는 데이터의 기간을 변경할 수 있습니다. 예를 들어 1w에서 All로 변경합니다.

Daily Written 보기 정보(파일 시스템)

시간별 데이터 흐름을 표시합니다. 데이터 양은 압축 전 및 압축 후 양을 비교하여 시간별로 표시됩니다.

Data Management > **File System** > **Charts**를 클릭합니다. Chart 드롭다운 목록에서 **Daily Written**을 선택합니다.

그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 보여 주는 상자를 표시합니다. 그래프의 선이 의미하는 바는 다음과 같습니다.

- Pre-Comp Written은 백업 서버에 의해 파일 시스템에 기록된 총 데이터 양입니다. 백업 서버에서는 파일 시스템의 압축 전 데이터를 파일 시스템에서 보관하고 있는 압축되지 않은 총 데이터로 인식합니다.
- Post-Comp Written은 압축 수행 후 파일 시스템에 기록된 GiB 단위의 총 데이터 양입니다.

- Total Comp Factor - Data Domain 시스템이 수신한 데이터에 대해 수행한 압축 양, 즉 압축 비율입니다. 그래프의 세로 축 오른쪽에 Total Compression Factor와 함께 표시됩니다.

기간별 기록된 데이터 확인

Daily Written 그래프에서 그래프 위에 기간(1w, 1m, 3m, 1y 또는 All)을 클릭하여 그래프에 표시되는 데이터의 기간을 변경할 수 있습니다. 예를 들어 1w에서 All로 변경합니다.

파일 시스템이 꽉 찼거나 거의 꽉 찬 경우

Data Domain 시스템에는 꽉 찬 정도에 따라 세 가지 진행 레벨이 있습니다. 각 레벨에 도달함에 따라 허용되지 않는 작업은 점점 더 늘어납니다. 각 레벨에서 데이터를 삭제하고 파일 시스템 정리 작업을 수행하면 디스크 공간이 마련됩니다.

참고

파일을 삭제하고 스냅샷을 제거한다고 디스크 공간이 즉시 재확보되는 것은 아니며 후속 정리 작업을 통해 공간을 재확보할 수 있습니다.

- 레벨 1 - 꽉 찬 정도의 첫 번째 레벨에서는 더 이상 새로운 데이터를 파일 시스템에 기록할 수 없습니다. 공간 부족 정보 알림이 생성됩니다.
  해결책 - 불필요한 데이터 세트를 삭제하고, 보존 기간을 줄이고, 스냅샷을 삭제하고, 파일 시스템 정리 작업을 수행합니다.
- 레벨 2 - 꽉 찬 정도의 두 번째 레벨에서는 파일을 삭제할 수 없습니다. 파일을 삭제하는 데에도 사용 가능한 공간이 필요한데 시스템에 사용 가능한 공간이 너무 적어 파일을 삭제할 수 없기 때문입니다.
  해결책 - 스냅샷을 만료 처리하고 파일 시스템 정리 작업을 수행합니다.
- 레벨 3 - 꽉 찬 정도의 세 번째이자 마지막 레벨에서는 스냅샷의 만료 처리, 파일 삭제 또는 새 데이터 쓰기 시도가 실패합니다.
  해결책 - 파일 시스템 정리 작업을 수행하여 일부 파일을 삭제하거나 일부 스냅샷을 만료 처리한 뒤 정리를 다시 실행하는 데 최소한으로 필요한 여유 공간을 확보합니다.

e-메일 알림을 통한 공간 사용량 모니터링

파일 시스템이 90%, 95%, 100% 꽉 찬 시점에 알림이 생성됩니다. 이러한 알림을 전송하려면 알림 e-메일 목록에 사용자를 추가합니다.

참고

알림 e-메일 목록에 가입하려면 알림 보기 및 지우기를 참조하십시오.

파일 시스템 작업 관리

이 섹션에서는 파일 시스템 정리, 완전 삭제 및 기본 작업 수행에 대해 설명합니다.

기본 작업 수행

기본 파일 시스템 작업에는 파일 시스템의 설정 및 해제가 포함되며, 간혹 파일 시스템의 제거가 포함됩니다.

파일 시스템 생성

Data Management > File System 페이지에서 Summary 탭을 사용해 파일 시스템을 생성합니다.

파일 시스템은 다음 세 가지 경우에 생성합니다.

- 새 Data Domain 시스템인 경우
- 정리 설치 후 시스템을 시작하는 경우
- 파일 시스템이 제거된 경우

파일 시스템을 생성하려면 다음을 수행합니다.

절차

1. 스토리지가 설치 및 구성되었는지 확인합니다. 자세한 내용은 시스템 스토리지 정보 보기에 대한 섹션을 참조하십시오. 시스템이 이 사전 요구 사항을 충족하지 못하면 경고 메시지가 표시됩니다. 파일 시스템을 생성하려고 시도하기 전에 스토리지를 설치 및 구성하십시오.
2. **Data Management** > **File System** > **Summary** > **Create**를 선택합니다.

   File System Create 마법사가 시작됩니다. 제공하는 지시를 따릅니다.

파일 시스템 활성화 또는 비활성화

파일 시스템을 활성화하거나 비활성화하는 옵션은 파일 시스템의 현재 상태에 따라 다릅니다. 활성화되어 있는 경우 비활성화하고, 비활성화되어 있는 경우 활성화할 수 있습니다.

- 파일 시스템을 활성화하면 Data Domain 시스템 작업을 시작할 수 있습니다. 이 권한은 관리 사용자만 사용할 수 있습니다.
- 파일 시스템을 비활성화하면 정리 작업을 비롯해 모든 Data Domain 시스템 작업이 중단됩니다. 이 권한은 관리 사용자만 사용할 수 있습니다.

⚠ 주의

백업 애플리케이션이 시스템에 데이터를 보내는 동안에 파일 시스템을 비활성화하면 백업 프로세스가 실패할 수 있습니다. 일부 백업 소프트웨어 애플리케이션에서는 파일 복제를 성공적으로 재개할 수 있는 경우 중지된 시점부터 재시작해 복구할 수 있습니다. 그러나 그 밖의 애플리케이션에서는 복구가 실패할 수 있어 백업이 완료되지 않은 상태로 남게 됩니다.

절차

1. **Data Managment** > **File System** > **Summary**를 선택합니다.
2. **File System**에 대해 **Enable** 또는 **Disable**을 클릭합니다.
3. 확인 대화 상자에서 **Close**를 클릭합니다.

파일 시스템 확장

"파일 시스템이 꽉 찼거나 거의 꽉 찬 경우"에서의 제안을 통해서도 정상적인 작업을 위한 공간이 충분한지 분명치 않으면 파일 시스템의 크기를 확장해야 할 수 있습니다.

그러나 다음과 같은 이유로 파일 시스템을 확장하지 못할 수도 있습니다.

- 파일 시스템을 활성화할 수 없는 경우
- 활성, 보존 또는 클라우드 계층에 사용하지 않는 디스크 또는 엔클로저가 없는 경우
- 확장된 스토리지 라이센스가 설치되지 않은 경우
- 충분한 용량 라이센스가 설치되지 않은 경우

DD6300 시스템은 라이센스가 부여된 사용 가능한 용량이 정확히 21.8TiB인 경우 활성 계층에서 4TB 드라이브로 구성된 ES30 엔클로저(43.6TiB)를 50% 활용률(21.8TiB)로

사용하는 옵션을 지원합니다. 다음 지침은 부분 용량 셸프를 사용할 경우에 적용됩니다.

- 다른 엔클로저 유형 또는 드라이브 크기는 부분 용량 사용을 지원하지 않습니다.
- 부분 용량 셸프는 활성 계층에만 존재할 수 있습니다.
- 활성 계층에 부분 용량 ES30 하나만 존재할 수 있습니다.
- 계층에 부분 용량 셸프가 존재하는 경우 해당 계층에 ES30을 추가로 구성하려면 먼저 부분 용량 셸프를 전체 용량으로 바꿔야 합니다.

  참고

  이렇게 하려면 부분 용량 셸프의 나머지 21.8TiB를 사용할 수 있도록 충분한 추가 용량 라이센스를 부여해야 합니다.

- 사용 가능한 용량이 21.8TB를 초과하면 부분 용량 셸프를 추가할 수 없습니다.
- 나중에 21TiB 라이센스를 삭제하면 자동으로 전체 용량 셸프가 부분 용량 셸프로 변환되는 것은 아닙니다. 셸프를 제거하고 다시 부분 용량 셸프로 추가해야 합니다.

파일 시스템을 확장하려면 다음을 수행합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Expand Capacity**를 선택합니다.

   Expand File System Capacity 마법사가 시작됩니다. **Storage Tier** 드롭다운 목록에는 항상 Active Tier가 포함되며 2차 선택 항목으로 Extended Retention Tier 또는 Cloud Tier를 포함할 수 있습니다. 이 마법사에는 각 계층에 대한 파일 시스템의 현재 용량이 표시되고 확장을 위해 얼마나 많은 추가 스토리지 공간을 사용할 수 있는지가 나타납니다.

   참고

   파일 시스템 용량은 물리적 디스크가 시스템에 설치되어 있고 파일 시스템이 활성화된 경우에만 확장할 수 있습니다.

2. **Storage Tier** 드롭다운 목록에서 계층을 선택합니다.
3. **Addable Storage** 영역에서 사용할 스토리지 디바이스를 선택하고 **Add to Tier**를 클릭합니다.
4. 마법사의 지침을 따릅니다. 확인 페이지가 표시되면 **Close**를 클릭합니다.

파일 시스템 제거

파일 시스템 제거는 고객 지원 팀의 지시 하에서만 실행되어야 합니다. 이 조치는 가상 테이프 등 파일 시스템의 모든 데이터를 삭제합니다. 삭제된 데이터는 복구할 수 없습니다. 이 작업은 또한 Replication 구성 설정을 제거합니다.

기존 데이터 정리, 새 컬렉션 복제 대상 생성 또는 컬렉션 소스 교체를 위해서나 시스템이 작업에서 제거되고 있어 보안 목적을 위해 필요한 경우에 이 작업을 사용합니다.

⚠ 주의

선택 사항인 Write zeros to disk 작업은 모든 파일 시스템 디스크에 0을 기록하여 효과적으로 모든 데이터 추적을 제거합니다. Data Domain 시스템에 대량의 데이터가 포함되어 있는 경우 이 작업은 완료하는 데 많은 시간이 걸리거나 하루 종일 걸릴 수도 있습니다.

참고

이는 재구축 절차이므로 이 작업은 관리자만 사용할 수 있습니다.

절차

1. **Data Management** > **File System** > **Summary** > **Destroy**를 선택합니다.
2. Destroy File System 대화 상자에서 sysadmin 암호를 입력합니다. 이것이 유일하게 허용되는 암호입니다.
3. 필요에 따라 **Write zeros to disk** 확인란을 클릭하여 데이터를 완전히 제거합니다.
4. **OK**를 클릭합니다.

정리 수행

이 섹션에서는 정리에 대한 정보를 제공하고 정리 스케줄을 시작, 중지 및 수정하는 방법에 대해 설명합니다.

DD OS는 활성 계층에 대해 'Cleanable GiB'라는 카운터를 유지 관리하려고 합니다. 이 값은 정리/가비지 수집을 실행하여 활성 계층에서 잠재적으로 회수할 수 있는 물리적(postcomp) 공간을 예측한 것입니다. 이 카운터는 `filesys show space` 및 `df` 명령을 사용하여 표시됩니다.

```
Active Tier:
Resource Size GiB Used GiB Avail GiB Use% Cleanable GiB*
---------------- -------- --------- --------- ----
--------------
/data: pre-comp - 7259347.5 - - -
/data: post-comp 304690.8 251252.4 53438.5 82% 51616.1 <=== NOTE
/ddvar 29.5 12.5 15.6 44% -
---------------- -------- --------- --------- ----
--------------
```

다음 중 하나에 해당할 경우 활성 계층을 실행합니다.

- 'Cleanable GiB' 값이 큰 경우
- DDFS가 100% 가득 찬 경우(따라서 읽기 전용임)

정리 작업을 한 번만 실행해서 모든 잠재적 공간을 회수할 수는 없습니다. 매우 큰 데이터 세트가 포함된 Data Domain 시스템에서, 정리 작업은 대부분의 불필요한 데이터를 포함하는 파일 시스템 부분에 작동하며, 모든 잠재적 공간을 회수하려면 여러 번 실행해야 할 수 있습니다.

정리 시작

정리 작업을 즉시 시작하려면 다음을 수행합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Settings** > **Cleaning**을 선택합니다.

   File System Setting 대화 상자의 **Cleaning** 탭에 각 계층에 대해 구성할 수 있는 설정이 표시됩니다.

2. 활성 계층의 경우:

   a. Throttle % 입력란에 시스템 스로틀 양을 입력합니다. 이는 정리 관련 CPU 사용량 비율입니다. 기본값은 50%입니다.

   b. Frequency 드롭다운 목록에서 빈도로 Never, Daily, Weekly, Biweekly 및 Monthly 중 하나를 선택합니다. 기본값은 Weekly입니다.

c. At에서 특정 시간을 구성합니다.

d. On에서 요일을 선택합니다.

3. 클라우드 계층의 경우:

a. Throttle % 입력란에 시스템 스로틀 양을 입력합니다. 이는 정리 관련 CPU 사용량 비율입니다. 기본값은 50%입니다.

b. Frequency 드롭다운 목록에서 빈도로 Never, After every 'N' Active Tier cleans 중 하나를 선택합니다.

참고

클라우드 계층 정리가 실행될 때 클라우드 유닛에 액세스할 수 없는 경우 해당 클라우드 유닛은 실행을 건너뜁니다. 클라우드 유닛을 사용할 수 있게 되면 다음번 실행에서 해당 클라우드 유닛의 정리가 실행됩니다. 정리 스케쥴은 두 실행 사이의 기간을 결정합니다. 클라우드 유닛을 사용할 수 있으며 다음번 스케줄이 실행될 때까지 기다릴 수 없는 경우 수동으로 정리를 시작할 수 있습니다.

4. **Save**를 클릭합니다.

참고

CLI를 사용하여 정리 작업을 시작하려면 `filesys clean start` 명령을 사용합니다.

```
# filesys clean start
Cleaning started. Use 'filesys clean watch' to monitor progress.
```

정리가 진행 중인지 확인하려면 `filesys status` 명령을 사용합니다.

```
# filesys status
The filesystem is enabled and running.
Cleaning started at 2017/05/19 18:05:58: phase 1 of 12 (pre-merge)
50.6% complete, 64942 GiB free; time: phase 0:01:05, total 0:01:05
```

정리가 이미 실행 중인 경우 시작하려고 하면 다음 메시지가 표시됩니다.

```
**** Cleaning already in progress. Use 'filesys clean watch' to monitor
progress.
```

참고

정리를 시작할 수 없는 경우 계약된 지원 공급업체에 문의하여 도움을 받으십시오. 이 문제는 시스템에 세그먼트 누락 오류가 발생하여 정리가 비활성화됨을 나타낼 수 있습니다.

정리 예약 또는 중지

정리 작업을 즉시 중지하거나 예약하려면 다음을 수행합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Settings** > **Cleaning**을 선택합니다.

File System Setting 대화 상자의 Cleaning 탭에 각 계층에 구성할 수 있는 설정이 표시됩니다.

2. 활성 계층의 경우:

a. Frequency 드롭다운 목록에서 원하는 빈도를 선택합니다.

3. 클라우드 계층의 경우:

a. Frequency 드롭다운 목록에서 원하는 빈도를 선택합니다.

4. **Save**를 클릭합니다.

참고

CLI를 사용하여 정리 일정이 설정되었는지 확인할 수 있습니다.

```
# filesys clean show schedule
```

필요한 경우 활성 계층 정리 일정을 설정합니다. 다음 예제에서는 매주 화요일 오전 6시에 정리를 실행하도록 설정합니다.

```
# filesys clean set schedule Tue 0600
Filesystem cleaning is scheduled to run "Tue" at "0600".
```

ER(Extended Retention)로 구성된 시스템에서는 데이터 이동이 완료된 후에 정리가 실행되도록 구성할 수 있으며 고유한 별도 일정이 없을 수도 있습니다.

완전 삭제 수행

정부 지침을 준수하려면 분류된 데이터 또는 중요 데이터를 해당 데이터를 저장하도록 승인되지 않은 시스템에 기록할 때 데이터 폐기라고도 하는 시스템 완전 삭제를 수행해야 합니다.

인시던트가 발생하면 시스템 관리자가 즉각적인 조치를 취해 실수로 기록한 데이터를 완벽하게 삭제해야 합니다. 목표는 이벤트가 발생하지 않은 상태로 스토리지 디바이스를 효과적으로 복원하는 것입니다. 데이터 유출이 중요 데이터에 발생할 경우 Data Domain Professional Services의 Secure Data 지우기 방법을 사용해 전체 스토리지를 완전 삭제해야 합니다.

Data Domain 완전 삭제 명령은 관리자가 논리적 수준에서 백업 세트 또는 개발 파일에 상관없이 파일을 삭제할 수 있도록 존재합니다. 대부분의 파일 시스템에서 파일을 삭제하는 과정은 파일을 단순히 플래그로 지정하거나 디스크의 데이터에 대한 참조를 삭제해 나중에 사용될 물리적 공간을 확보하는 작업으로 구성됩니다. 그러나 이 간단한 작업은 물리적으로 디스크에 기본 데이터의 잔여량 표시가 남겨질 수 있다는 문제를 불러올 수 있습니다. 중복 제거된 스토리지 환경은 이러한 문제의 영향을 받습니다.

시스템에서 데이터를 폐기하면 해당 데이터의 잔여량 표시가 제거되고 이에 따라 데이터가 폐기된 후에 파일에 액세스할 가능성이 사라집니다. Data Domain의 완전 삭제 방식은 다음 사양의 DoD(Department of Defense) 5220.22의 2007년 버전을 준수합니다.

- *US Department of Defense 5220.22-M Clearing and Sanitization Matrix*
- *NIST(National Institute of Systems and Technology) Special Publication 800-88 Guidelines for Media Sanitization*

중복 제거된 데이터 완전 삭제

Data Domain 시스템은 원래 위치에서 기본 중복 제거된 상태의 데이터를 완전 삭제합니다.

중복 제거 스토리지 시스템은 시스템에 전송된 파일에서 일반적인 데이터 패턴을 추출하고 이 패턴의 고유한 복제본을 저장해 모든 중복 인스턴스를 참조합니다. 이러한 데이터 패턴 또는 세그먼트가 잠재적으로 시스템에 있는 여러 파일 사이에서 공유될 수 있기 때문에 완전 삭제 프로세스는 먼저 손상된 파일의 각 세그먼트가 정리된 파일과 공유되었는지 확인한 후에 손상된 메타데이터와 함께 공유되지 않은 세그먼트만 지웁니다.

삭제된 파일에만 속하는 모든 세그먼트의 복제본이 모두 사용되지 않도록 모든 스토리지 계층, 캐시, 사용되지 않은 용량 및 사용 가능한 공간이 지워집니다. 시스템은 손상된 파일이 해당 시스템에 전혀 존재하지 않은 듯한 상태로 스토리지 디바이스를 효과적으로 복원하기 위해 이 세그먼트가 점유한 모든 스토리지를 재확보하고 덮어씁니다.

완전 삭제 레벨 1: 데이터 지우기 또는 폐기

제거해야 하는 데이터가 "US Department of Defense 5220.22-M Clearing and Sanitization Matrix"에 정의된 대로 미분류 대상인 경우 완전 삭제 레벨 1을 사용해 영향을 받은 스토리지를 한 번 덮어쓸 수 있습니다. 이렇게 하면 대부분의 데이터 폐기 및 시스템 완전 삭제 사례를 처리할 수 있는 기반이 마련됩니다.

Data Domain 시스템 완전 삭제 기능은 단일 패스 제로화(single-pass zeroization) 메커니즘을 사용해 지운 파일에만 속하는 모든 세그먼트의 복제본을 모두 덮어쓰도록 합니다. 완전 삭제되는 시스템에 있는 정리된 데이터는 온라인 상태이며 사용자에게 제공됩니다.

절차

1. 백업 소프트웨어 또는 해당 클라이언트를 통해 손상된 파일 또는 백업을 삭제합니다. 백업의 경우 해당 이미지의 관련 파일이 조정되고 카탈로그 기록이 필요에 맞게 관리되는지 등을 확인하기 위해 백업 소프트웨어를 적절하게 관리해야 합니다.
2. 손상된 Data Domain 시스템에서 `system sanitize start` 명령을 실행해 이 시스템에서 이전에 사용된 모든 공간을 한 번 덮어쓰도록 합니다(아래 그림 참조).
3. 영향을 받은 시스템이 완전히 삭제될 때까지 기다립니다. 완전 삭제는 `system sanitize watch` 명령을 사용해 모니터링할 수 있습니다.

   영향을 받은 Data Domain 시스템에서 복제가 설정된 경우에도 복제본이 포함된 모든 시스템을 비슷한 방법으로 처리해야 합니다. 시스템에 얼마나 많은 데이터가 존재하고 어떤 식으로 분산되는지에 따라 `system sanitize` 명령에 시간이 걸릴 수 있습니다. 그러나 이 시간 동안에 시스템에서 정리된 모든 데이터가 사용자에게 제공됩니다.

완전 삭제 레벨 2: 전체 시스템 완전 삭제

제거해야 하는 데이터가 "US Department of Defense 5220.22-M Clearing and Sanitization Matrix"에 정의된 대로 분류 대상인 경우 완전 삭제 레벨 2(전체 시스템 완전 삭제)를 사용해야 합니다.

Data Domain에서는 덮어쓰기 패턴 및 인증서가 있는 다중 패스 덮어쓰기에 Blancco를 사용하는 것이 좋습니다. Blancco는 전체 시스템 완전 삭제가 필요할 경우 일반적인 국방부 요구 사항을 처리하기 위한 기반을 마련합니다. 자세한 내용은 다음을 참조하십시오.

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

기본 설정 수정

이 섹션에 설명된 대로 사용된 압축 유형, 마커 유형, 복제본 쓰기 상태, 스테이징 예약 비율을 변경합니다.

로컬 압축 변경

File System Settings 대화 상자의 General 탭을 사용하여 로컬 압축 유형을 구성합니다.

참고

반드시 필요한 경우가 아니면 로컬 압축 유형을 변경하지 마십시오.

절차

1. **Data Managment** > **File System** > **Summary** > **Settings** > **General**을 선택합니다.
2. Local Compression Type 드롭다운 목록에서 압축 유형을 선택합니다.

   표 95 압축 유형

옵션	설명
NONE	데이터를 압축하지 않습니다.
LZ	최고 처리량을 제공하는 기본 알고리즘이며 Data Domain에서는 lz 옵션이 권장됩니다.
GZFAST	압축 데이터에 더 적은 공간을 사용하지만 CPU 리소스는 lz에 비해 2배 더 많이 사용하는 zip 방식의 압축으로, 성능 저하를 감수하면서 더 많은 압축을 원하는 사이트에 권장되는 방법입니다.
GZ	데이터 스토리지에 가장 적은 공간을 사용하는 zip 방식의 압축으로, lz에 비해 공간을 평균 10%~20% 적게 사용하며 일부 데이터 세트의 경우 압축률이 더 높습니다. 이 방식은 lz의 최대 5배에 달하는 가장 많은 CPU 리소스를 사용하는 방식이기도 합니다. gz 압축 유형은 성능 요구 사항이 낮은 니어라인 스토리지 애플리케이션에 주로 사용됩니다.

3. **Save**를 클릭합니다.

읽기 전용 설정 변경

복제본을 쓰기 가능하게 변경합니다. 일부 백업 애플리케이션의 경우 복제본에서 복구 또는 볼트(Vault) 작업을 진행하려면 복제본이 쓰기 가능해야 합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Settings** > **General**을 선택합니다.
2. Report Replica as Writable 영역에서 **Disabled** 및 **Enabled**을 적절히 전환합니다.
3. **Save**를 클릭합니다.

디스크 스테이징 작업

디스크 스테이징은 Data Domain 시스템이 스테이징 디바이스 역할을 하도록 합니다. 여기서 시스템은 CIFS 공유 또는 NFS 마운트 지점을 통해 기본 디스크로 보입니다.

디스크 스테이징은 NetWorker 및 Symantec의 NBU(NetBackup) 등과 같은 백업 소프트웨어와 함께 사용할 수 있으며 라이센스가 필요 없고 기본적으로 비활성화되어 있습니다.

참고

Data Domain 시스템이 디스크 스테이징 디바이스로 사용되는 경우에는 DD VTL 기능이 필요하거나 지원되지 않습니다.

일부 백업 애플리케이션에서 디스크 스테이징 디바이스를 사용하는 이유는 테이프 드라이브를 지속적으로 스트리밍할 수 있도록 하기 위해서입니다. 데이터를 테이프로 복제한 뒤에는 공간이 남아 있는 한 디스크에 보존됩니다. 최근 백업에서 복구가 필요한 경우, 데이터가 아직 디스크에 있을 가능성이 높아 테이프에서보다는 더 편리하게 복구할 수 있습니다. 디스크가 차면 이전 백업을 삭제하여 공간을 확보할 수 있습니다. 이러한 필요 시 삭제 정책으로 디스크 사용을 극대화할 수 있습니다.

정상 작동 시, Data Domain 시스템은 정리 작업이 이루어지기 전까지는 삭제된 파일에서 공간을 재확보하지 않습니다. 이는 스테이징 모드로 작동하는 백업 소프트웨어와는 호환되지 않는 사항입니다. 여기서는 파일이 삭제되면 공간이 확보될 것입니다. 디스크 스테이징 구성 시, 총 공간(일반적으로 20~30%)의 비율을 예약하여 시스템이 즉각적인 공간 확보를 시뮬레이션할 수 있도록 합니다.

가용 공간은 스테이징 예약 공간만큼 감소됩니다. 저장된 데이터 양이 가용 공간을 모두 사용하는 경우 시스템은 꽉 차게 됩니다. 그러나 파일이 삭제될 때마다 시스템이 정리 작업으로 복구될 공간을 예상하고, 스테이징 예약 공간에서 용량을 빌려와 가용 공간을 그 예상 공간만큼 늘립니다. 정리 작업을 실행하면 공간이 실제로 복구되고 예약 공간은 초기 크기로 복구됩니다. 파일 삭제로 생기는 가용 공간은 예상치에 불과하기 때문에 정리 작업으로 확보되는 실제 공간은 예상치와 일치하지 않을 수 있습니다. 디스크 스테이징의 목적은 충분한 예약 공간을 구성해 정리 작업 실행이 예약되기 전에 공간이 부족해지지 않도록 하는 것입니다.

디스크 스테이징 구성

디스크 스테이징을 활성화하고 스테이징 예약 비율을 지정합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Settings** > **General**을 선택합니다.
2. Staging Reserve 영역에서 **Disabled** 및 **Enabled** 간에서 적절히 전환합니다.
3. Staging Reserve를 활성화한 경우 **% of Total Space** 상자에 값을 입력합니다.

   이 값은 디스크 스테이징을 위해 예약되는 총 디스크 공간의 비율을 나타내며 일반적으로 20~30%입니다.
4. **Save**를 클릭합니다.

테이프 마커 설정

일부 공급업체의 백업 소프트웨어는 Data Domain 시스템으로 전송되는 모든 데이터 스트림(파일 시스템 및 DD VTL 백업 모두)에서 마커(테이프 마커, 태그 헤더 또는 기타 사용되는 이름)를 삽입합니다.

마커는 Data Domain 시스템에서 데이터 압축의 성능을 크게 저하시킵니다. 따라서 기본 마커 유형이 auto로 설정되어 있고 사용자가 변경할 수 없게 되어 있습니다. 이 설정이 사용 중인 백업 소프트웨어와 호환되지 않으면 계약된 지원 서비스 공급업체에 연락하시기 바랍니다.

참고

Data Domain 환경에서 애플리케이션이 작동하는 방법에 대한 정보는 *EMC Data Domain 시스템이 스토리지 환경에 통합되는 방법*을 참조하십시오. 이러한 매트릭스와 통합 가이드를 사용해 공급업체 관련 문제를 해결할 수 있습니다.

SSD 랜덤 워크로드 공유

Data Domain 시스템에서 랜덤 입출력을 제한하는 임계값을 기본값에서 변경 요구 사항과 입출력 패턴에 맞는 값으로 조정할 수 있습니다.

기본적으로 Data Domain 시스템은 SSD 랜덤 워크로드 공유를 40%로 설정합니다. 필요에 따라 이 값을 높이거나 낮출 수 있습니다. **Data Managment** > **File System** > **Summary** > **Settings** > **Workload Balance**를 선택하고 슬라이더를 조정하십시오.

Save를 클릭합니다.

빠른 복제 작업

빠른 복제는 소스 디렉토리의 파일 및 디렉토리 트리를 Data Domain 시스템의 타겟 디렉토리로 복제하는 작업입니다.

`force` 옵션을 사용하면 대상 디렉토리가 있을 경우 이를 덮어쓸 수 있습니다. 빠른 복제 작업을 실행하면 진행 상태 대화 상자가 표시됩니다.

참고

빠른 복제는 대상이 소스와 같아지도록 만들지만 특정 시점에서는 그렇지 않습니다. 이 작업 중에 폴더 중 하나를 변경하는 경우 두 개 폴더가 현재 같거나 이전에 같았다고 보장할 수 없게 됩니다.

빠른 복제 작업 수행

Data Domain 시스템 소스 디렉토리에서 Data Domain 시스템의 다른 대상으로 파일 또는 디렉토리 트리를 복제합니다.

절차

1. **Data Managment** > **File System** > **Summary** > **Fast Copy**를 선택합니다.

   Fast Copy 대화 상자가 표시됩니다.

2. Source 입력란에 복제될 데이터가 상주하는 디렉토리의 경로 이름, 예를 들어 `/data/col1/backup/.snapshot/`*`snapshot-name`*`/dir1`을 입력합니다.

   참고

   col1은 소문자 L 다음에 숫자 1을 사용합니다.

3. Destination 입력란에는 데이터가 복제될 디렉토리의 경로 이름, 예를 들어 `/data/col1/backup/dir2`를 입력합니다. 이 대상 디렉토리는 비워 두어야 하며 그렇지 않으면 작업이 실패합니다.

   - Destination 디렉토리가 있는 경우 **Overwrite existing destination if it exists** 확인란을 클릭합니다.

4. **OK**를 클릭합니다.
5. 나타나는 진행률 대화 상자에서 **Close**를 클릭하여 종료합니다.

6장

MTree

이 장에는 다음과 같은 내용이 포함됩니다.

MTree 개요

MTree는 파일 시스템의 논리적 파티션입니다.

MTree는 DD Boost 스토리지 유닛, DD VTL 풀 또는 NFS/CIFS 공유에 사용할 수 있습니다. MTree를 통해 스냅샷, 할당량 및 DD Retention Lock의 세밀한 관리가 가능합니다. DD Extended Retention을 비롯해 활성 계층에서 보존 계층까지 데이터 마이그레이션 정책의 세부적 관리 기능이 있는 시스템의 경우 전체 파일 시스템과는 달리 특정 MTree에 대해 MTree 작업을 수행할 수 있습니다.

참고

MTree 복제 컨텍스트에 최대 구성 가능한 MTree를 지정할 수 있습니다.

MTree의 최상위 레벨 디렉토리에 사용자 파일을 배치하지 마십시오.

MTree 제한

Data Domain 시스템에 대한 MTree 제한

표 96 지원되는 Mtree

Data Domain 시스템	DD OS 버전	지원되는 구성 가능한 Mtree	지원되는 동시 활성 Mtree
DD9800	6.0 이상	256	256
DD9500	5.7 이상	256	256
DD6800, DD9300	6.0 이상	128	128
DD6300	6.0 이상	100	32
DD990, DD4200, DD4500, DD7200	5.7 이상	128	128
다른 모든 DD 시스템	5.7 이상	100	모델에 따라 최대 32개
DD9500	5.6	100	64
DD990, DD890	5.3 이상	100	모델에 따라 최대 32개
DD7200, DD4500, DD4200	5.4 이상	100	모델에 따라 최대 32개
다른 모든 DD 시스템	5.2 이상	100	모델에 따라 최대 14개

할당량

MTree 할당량은 MTree에 기록한 논리 데이터에만 적용됩니다.

과도한 공간 소비를 방지하기 위해 관리자가 MTree, 스토리지 유닛 또는 DD VTL 풀에 스토리지 공간 제한을 설정할 수 있습니다. 할당량 제한에는 고정적 제한과 유동적 제한의 두 가지 종류가 있습니다. 유동적 제한이나 고정적 제한 중 하나만 설정할 수도 있고 둘 다 설정할 수도 있습니다. 두 값 모두 정수여야 하며, 유동적 값은 고정적 값보다 작아야 합니다.

유동적 제한을 설정하면 MTree 크기가 해당 제한값을 초과할 때마다 알림이 전송되지만 데이터를 여전히 MTree에 기록할 수 있습니다. 고정적 제한을 설정하면 고정적 제

한값에 도달했을 때 MTree에 데이터를 기록할 수 없습니다. 따라서 MTree에서 데이터를 삭제할 때까지 모든 쓰기 작업이 실패합니다.

자세한 내용은 MTree 할당량 구성(222페이지) 섹션을 참조하십시오.

Quota Enforcement

Quota Enforcement를 설정하거나 해제합니다.

MTree 패널 정보

시스템의 모든 활성 MTree가 나열되며 실시간 데이터 스토리지 통계가 표시됩니다. 개요 영역의 정보는 공간 사용량 추세를 시각적으로 보여 주는 데 유용합니다.

Data Management > **MTree**를 선택합니다.

- 목록의 MTree 확인란을 선택하여 세부 정보를 표시하고 Summary 보기에서 구성을 수행합니다.
- Filter By MTree Name 필드에 텍스트(와일드카드 지원됨)를 입력하고 **Update**를 클릭하여 목록에 구체적인 MTree 이름을 나열합니다.
- 기본 목록으로 돌아가려면 필터 텍스트를 삭제하고 **Reset**을 클릭합니다.

표 97 MTree 개요 정보

항목	설명
MTree Name	MTree의 경로 이름입니다.
Quota Hard Limit	사용된 고정적 제한 할당량의 비율입니다.
Last 24 Hr Pre-Comp (pre-compression)	지난 24시간 동안 기록된 백업 애플리케이션으로부터의 원시 데이터 양입니다.
Last 24 Hr Post-Comp (post-compression)	지난 24시간 동안 압축 후 사용된 스토리지 양입니다.
Last 24 hr Comp Ratio	지난 24시간 동안의 압축률입니다.
Weekly Avg Post-Comp	지난 5주 동안 사용된 평균 압축 스토리지 양입니다.
Last Week Post-Comp	지난 7일 동안 사용된 평균 압축 스토리지 양입니다.
Weekly Avg Comp Ratio	지난 5주 동안의 평균 압축률입니다.
Last Week Comp Ratio	지난 7일 동안의 평균 압축률입니다.

Summary 보기 정보

중요한 파일 시스템 통계를 봅니다.

세부 정보 보기

MTree를 선택하여 정보를 봅니다.

표 98 선택한 MTree에 대한 MTree 세부 정보

항목	설명
Full Path	MTree의 경로 이름입니다.

표 98 선택한 MTree에 대한 MTree 세부 정보 (계속)

항목	설명
Pre-Comp Used	MTree에 기록된 백업 애플리케이션의 현재 원시 데이터 양입니다.
Status	MTree의 상태입니다(여러 상태의 조합이 지원됨). 상태는 다음 중 하나일 수 있습니다. • D: 삭제됨 • RO: 읽기 전용 • RW: 읽기/쓰기 • RD: 복제 대상 • RLCE: DD Retention Lock Compliance 활성화 • RLCD: DD Retention Lock Compliance 비활성화 • RLGE: DD Retention Lock Governance 활성화 • RLGD: DD Retention Lock Governance 비활성화
Quota	
Quota Enforcement	Enabled 또는 Disabled입니다.
Pre-Comp Soft Limit	현재 값입니다. 할당량 제한값을 수정하려면 Configure를 클릭합니다.
Pre-Comp Hard Limit	현재 값입니다. 할당량 제한값을 수정하려면 Configure를 클릭합니다.
Quota Summary	사용한 고정적 제한의 비율입니다.
Protocols	
CIFS Shared	CIFS 공유 상태입니다. 상태는 다음 중 하나일 수 있습니다. • Yes - MTree 또는 그 상위 디렉토리가 공유됩니다. • Partial - 이 MTree 아래의 하위 디렉토리가 공유됩니다. • No - 이 MTree와 그 상위 또는 하위 디렉토리가 공유되지 않습니다. CIFS 보기로 이동하려면 CIFS 링크를 클릭합니다.
NFS Exported	NFS 내보내기 상태입니다. 상태는 다음 중 하나일 수 있습니다. • Yes - MTree 또는 그 상위 디렉토리를 내보냅니다. • Partial - 이 MTree 아래의 하위 디렉토리를 내보냅니다. • No - 이 MTree와 그 상위 또는 하위 디렉토리를 내보내지 않습니다. NFS 보기로 이동하려면 NFS 링크를 클릭합니다.
DD Boost Storage Unit	DD Boost 내보내기 상태입니다. 상태는 다음 중 하나일 수 있습니다. • Yes - MTree를 내보냅니다. • No - 이 MTree를 내보내지 않습니다. • Unknown - 정보가 없습니다.

표 98 선택한 MTree에 대한 MTree 세부 정보 (계속)

항목	설명
	DD Boost 보기로 이동하려면 DD Boost 링크를 클릭합니다.
DD VTL Pool	VTL 풀 보고서 상태입니다. 상태는 다음 중 하나일 수 있습니다. • Yes - MTree가 DD VTL MTree 풀입니다. • No - MTree가 DD VTL MTree 풀이 아닙니다. • Unknown - 정보가 없습니다.
vDisk Pool	vDisk 보고서 상태입니다. 상태는 다음 중 하나일 수 있습니다. • Unknown - vDisk 서비스가 활성화되지 않았습니다. • No - vDisk 서비스가 활성화되어 있지만 MTree가 vDisk 풀이 아닙니다. • Yes - vDisk 서비스가 활성화되어 있고 MTree가 vDisk 풀입니다.
Physical Capacity Measurements	
Used (Post-Comp)	압축된 데이터가 수집된 후 사용된 MTree 공간입니다.
Compression	전역 압축 비율입니다.
Last Measurement Time	시스템이 MTree를 측정한 마지막 시간입니다.

Schedules	할당된 스케줄의 수입니다.
	스케줄을 보고 MTree에 할당하려면 **Assign**을 클릭합니다.
	• Name: 스케줄 이름입니다.
	• Status: Enabled 또는 Disabled
	• Priority:
	  ▪ Normal - 측정 작업을 처리 대기열에 제출합니다.
	  ▪ Urgent - 측정 작업을 처리 대기열의 맨 앞에 제출합니다.
	• Schedule: 작업이 실행되는 시간입니다.
	• MTree Assignments: 스케줄이 할당된 MTree의 수입니다.

Submitted Measurements	MTree의 압축 후 상태를 표시합니다. MTree에 대한 수동 압축 후 작업을 제출하고 해당 작업의 우선순위를 선택하려면 **Measure Now**를 클릭합니다. • 0 - 제출된 측정 작업이 없습니다. • 1 - 1개의 측정 작업이 실행 중입니다. • 2 - 2개의 측정 작업이 실행 중입니다.
Snapshot	다음과 같은 통계를 표시합니다. • Total Snapshots • Expired • Unexpired

표 98 선택한 MTree에 대한 MTree 세부 정보 (계속)

항목	설명
	• Oldest Snapshot • Newest Snapshot • Next Scheduled • Assigned Snapshot Schedules **Total Snapshots**를 클릭하여 **Data Management** > **Snapshots** 보기로 이동합니다. **Assign Schedules**를 클릭하여 스냅샷 스케줄을 구성합니다.

MTree 복제 정보 보기

MTree 복제 구성을 표시합니다.

선택된 MTree가 복제되도록 구성된 경우 구성 요약 정보가 이 영역에 표시됩니다. 그렇지 않은 경우 이 영역에 `No Record Found`가 표시됩니다.

- Replication 링크를 클릭해 구성을 위한 Replication 페이지로 이동하여 추가 세부 정보를 봅니다.

표 99 MTree 복제 정보

항목	설명
Source	소스 MTree 경로 이름입니다.
Destination	대상 MTree 경로 이름입니다.
Status	MTree 복제 페어 상태입니다. 상태는 Normal, Error 또는 Warning일 수 있습니다.
Sync As Of	복제 페어가 동기화된 마지막 요일과 시간입니다.

MTree 스냅샷 정보 보기

선택된 MTree가 스냅샷에 대해 구성된 경우 스냅샷 구성 요약 정보가 표시됩니다.

- **Snapshots** 링크를 클릭해 Snapshot 페이지로 이동하여 구성을 수행하거나 추가 세부 정보를 봅니다.
- 선택된 MTree에 대한 스냅샷 스케줄을 할당하려면 **Assign Schedules**를 클릭합니다. 스케줄의 확인란을 선택한 뒤 **OK**와 **Close**를 차례로 클릭합니다. 스냅샷 스케줄을 생성하려면 **Create Snapshot Schedule**을 클릭합니다. 지침은 스냅샷 스케줄 생성에 대한 섹션을 참조하십시오.

표 100 MTree 스냅샷 정보

항목	설명
Total Snapshots	이 MTree에 대해 생성된 스냅샷의 총 개수입니다. MTree마다 총 750개의 스냅샷을 생성할 수 있습니다.
Expired	이 MTree에서 삭제하기 위해 표시해 두었지만 아직 정리 작업을 통해 제거하지 않은 스냅샷의 개수입니다.

표 100 MTree 스냅샷 정보 (계속)

항목	설명
Unexpired	유지하기 위해 표시해 둔 이 MTree에 있는 스냅샷의 개수입니다.
Oldest Snapshot	이 MTree에 대해 가장 오래된 스냅샷의 날짜입니다.
Newest Snapshot	이 MTree에 대해 가장 최신 스냅샷의 날짜입니다.
Next Scheduled	다음으로 예약된 스냅샷의 날짜입니다.
Assigned Snapshot Schedules	이 MTree에 할당된 스냅샷 스케줄의 이름입니다.

MTree Retention Lock 정보 보기

선택한 MTree가 DD Retention Lock 소프트웨어 옵션 중 하나에 대해 구성된 경우 DD Retention Lock 구성에 대한 요약 정보가 표시됩니다.

참고

MTree용 DD Retention Lock을 관리하는 방법에 대한 정보는 DD Retention Lock 작업에 대한 섹션을 참조하십시오.

표 101 DD Retention Lock 정보

항목	설명
Status	DD Retention Lock의 활성화 또는 비활성화 여부를 나타냅니다.
Mode	MTree가 DD Retention Lock 규정 준수용으로 구성되어 있는지 또는 DD Retention Lock 거버넌스용으로 구성되어 있는지를 나타냅니다.
Use	MTree의 사용을 나타냅니다.
Retention period min	최소 DD Retention Lock 기간을 나타냅니다.
Retention period max	최대 DD Retention Lock 기간을 나타냅니다.

DD Retention Lock 설정 활성화 및 관리

GUI의 DD Retention Lock 영역을 사용해 보존 잠금 기간을 수정합니다.

절차

1. **Data Management** > **MTree** > **Summary**를 선택합니다.
2. Retention Lock 영역에서 **Edit**를 클릭합니다.
3. Data Domain 시스템에서 DD Retention Lock을 활성화하려면 Modify Retention Lock 대화 상자에서 **Enable**을 선택합니다.
4. Retention Period 패널에서 최소 또는 최대 보존 기간을 수정합니다. 우선 기능이 활성화되어야 합니다.
5. 간격(minutes, hours, days, years)을 선택합니다. 기본 값을 표시하려면 **Default**를 클릭합니다.
6. **OK**를 클릭합니다.

결과

Modify Retention Lock 대화 상자를 닫고 나면 DD Retention Lock 요약 영역에 업데이트된 MTree 정보가 표시됩니다.

Space Usage 보기 정보(MTree)

특정 시점의 MTree 데이터 사용량에 대한 시각적 표현을 표시합니다.

Data Management > **MTree** > **Space Usage**를 선택합니다.

- 그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 보여 주는 상자를 표시합니다.
- 그래프 하단의 **Print**를 클릭하여 표준 Print 대화 상자를 엽니다.
- **Show in new window**를 클릭하여 그래프를 새 브라우저 창에 표시합니다.

그래프의 선이 의미하는 바는 다음과 같습니다.

- Pre-comp Written - 백업 서버가 MTree에 보낸 총 데이터 양입니다. 백업 서버는 MTree의 압축 전 데이터를 MTree가 스토리지 단위로써 보관하고 있는 압축되지 않은 데이터로 인식합니다. 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다.
- Post-comp Used - 압축 후에 MTree에서 사용된 총 스토리지 용량으로, 그래프의 세로 축 왼쪽에 Space Used와 함께 표시됩니다.
- Comp Factor—MTree에 저장된 데이터의 압축률로, 그래프의 세로 축 오른쪽에 Comp Factor와 함께 표시됩니다.

참고

MTrees Space Usage 보기의 경우 시스템에 압축 전 정보만 표시됩니다. 데이터가 MTree 사이에서 공유될 수 있으므로 단일 MTree에 압축된 사용량을 제공할 수 없습니다.

기간별 공간 사용량 확인

Space Usage 그래프에서 그래프 위 Duration 선의 간격(1w, 1m, 3m, 1y)을 클릭하면 그래프에 나타나는 데이터 기간을 7일~120일로 변경할 수 있습니다.

120일 이상의 간격으로 공간 사용량을 보려면 다음 명령을 실행합니다.

```
# filesys show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

Daily Written 보기 정보(MTree)

최근 24시간의 데이터 흐름을 표시합니다. 데이터 양은 사전 압축 및 사후 압축을 비교하여 시간별로 표시됩니다.

전역 압축 및 로컬 압축의 양과 압축 전 및 압축 후의 양에 대한 정보도 제공합니다.

- 그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 보여 주는 상자를 표시합니다.
- 그래프 하단의 **Print**를 클릭하여 표준 Print 대화 상자를 엽니다.
- **Show in new window**를 클릭하여 그래프를 새 브라우저 창에 표시합니다.

그래프의 선이 의미하는 바는 다음과 같습니다.

- Pre-Comp Written - 백업 서버가 MTree에 기록한 총 데이터 양입니다. 백업 서버는 MTree의 압축 전 데이터를 MTree가 스토리지 단위로써 보관하고 있는 압축되지 않은 데이터로 인식합니다.

- Post-Comp Written - 압축 수행 후 MTree에 기록된 GiB 단위의 총 데이터 양입니다.
- Total Comp Factor - Data Domain 시스템이 수신한 데이터에 대해 수행한 압축 양, 즉 압축 비율입니다. 그래프의 세로 축 오른쪽에 Total Compression Factor와 함께 표시됩니다.

기간별 기록된 데이터 확인

Daily Written 그래프에서 그래프 위 Duration 선의 간격(7d, 30d, 60d, 120d)을 클릭하면 그래프에 나타나는 데이터 기간을 7일~120일로 변경할 수 있습니다.

Daily Written 그래프 아래에는 다음과 같은 현재 기간 값에 대한 합계가 표시됩니다.

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

MTree 사용량 모니터링

MTree에 대한 공간 사용량 및 데이터 기록 추세를 표시합니다.

절차

- **Data Management** > **MTree**를 선택합니다.

  MTree 보기에 구성된 MTree 목록이 나타나며, 목록에서 선택하면 MTree의 세부 정보가 Summary 탭에 나타납니다. Space Usage and Daily Written 탭에 선택한 MTree에 대한 공간 사용량과 데이터가 기록된 추세를 시각적으로 표현한 그래프가 나타납니다. 이 보기에는 또한 CIFS, NFS, DD Boost에 대한 MTree 구성을 허용하는 옵션과 MTree에 대한 스냅샷 및 DD Retention Lock을 관리하기 위한 섹션들도 포함되어 있습니다.

  MTree 보기에는 MTree 개요 패널과 이 섹션들에서 자세히 설명되어 있는 세 개의 탭이 있습니다.

  - MTree 패널 정보(211페이지)
  - Summary 보기 정보(211페이지)
  - Space Usage 보기 정보(MTree)(216페이지)
  - Daily Written 보기 정보(MTree)(216페이지)

  참고

  PCM(Physical Capacity Measurement)은 MTree에 대한 공간 사용량 정보를 제공합니다. PCM에 대한 자세한 내용은 물리적 용량 측정 이해와 관련된 섹션을 참조하십시오.

물리적 용량 측정 이해

PCM(Physical Capacity Measurement)은 스토리지 공간의 하위 집합에 대한 공간 사용량 정보를 제공합니다. DD System Manager에서 PCM은 MTree에 대한 공간 사용량 정보를 제공하지만 명령줄 인터페이스에서는 MTree, 테넌트, 테넌트 유닛 및 경로 세트에 대한 공간 사용량 정보를 볼 수 있습니다.

PCM에 대한 경로를 선택하면 그 아래의 모든 경로가 자동으로 포함됩니다. 이미 상위 경로를 선택한 후 하위 경로를 선택하지 마십시오. 예를 들어 `/data/col1/mtree3`을 선택한 경우 mtree3 아래의 어떤 하위 디렉토리도 선택하지 마십시오.

명령줄에서 PCM을 사용하는 것에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

물리적 용량 측정 활성화, 비활성화 및 보기

물리적 용량 측정은 MTree에 대한 공간 사용량 정보를 제공합니다.

절차

1. **Data Managment** > **File System** > **Summary**를 선택합니다.

   File System 패널의 Summary 탭에 시스템이 표시됩니다.
2. 오른쪽 하단 모서리에 있는 **^**을 클릭하여 상태 패널을 표시합니다.
3. **Physical Capacity Measurement Status** 오른쪽에서 **Enable**을 클릭하여 PCM을 활성화합니다.
4. **Physical Capacity Measurement Status** 오른쪽에서 **Details**를 클릭하여 현재 실행 중인 PCM 작업을 봅니다.
   - **MTree**: PCM이 측정하는 MTree입니다.
   - **Priority**: 작업의 우선 순위(일반 또는 긴급)입니다.
   - **Submit Time**: 작업이 요청된 시간입니다.
   - **Duration**: 작업을 완료하기 위해 PCM이 실행된 시간입니다.
5. **Physical Capacity Measurement Status** 오른쪽에서 **Disable**을 클릭하여 PCM을 비활성화하고 현재 실행 중인 모든 PCM 작업을 취소합니다.

물리적 용량 측정 초기화

PCM(Physical Capacity Measurement) 초기화는 PCM이 설정되고 캐시가 초기화되지 않은 경우에만 수행할 수 있는 일회성 작업입니다. 이 작업을 수행하면 캐시가 정리되어 측정 속도가 개선됩니다. 초기화 프로세스가 진행되는 동안에도 PCM 작업을 관리하고 실행할 수 있습니다.

절차

1. **Data Management** > **File System** > **Configuration**을 선택합니다.
2. Physical Capacity Measurement 아래, Cache 오른쪽에 있는 **Initialize**를 클릭합니다.
3. **Yes**를 클릭합니다.

물리적 용량 측정 스케줄 관리

물리적 용량 측정 스케줄을 생성하고 편집하고 삭제하고 봅니다. 이 대화상자에는 MTree에 대해 생성된 스케줄과 현재 할당이 없는 스케줄만 표시됩니다.

절차

1. **Data Management** > **MTree** > **Manage Schedules**를 선택합니다.
   - **Add**(+) 버튼을 클릭하여 스케줄을 생성합니다.
   - 스케줄을 선택하고 **Modify**(연필 모양) 버튼을 클릭하여 스케줄을 편지합니다.
   - 스케줄을 선택하고 **Delete**(X) 버튼을 클릭하여 스케줄을 삭제합니다.
2. 필요에 따라 머리글 이름을 클릭하여 스케줄을 기준으로 정렬합니다. **Name**, **Status**(Enabled 또는 Disabled) **Priority**(Urgent 또는 Normal), **Schedule**(스케

줄 시기) 및 **MTree Assignments**(스케줄을 적용할 MTree 수)를 정렬할 수 있습니다.

물리적 용량 측정 스케줄 생성

물리적 용량 측정 스케줄을 생성하고 MTree에 할당합니다.

절차

1. **Data Management** > **MTree** > **Manage Schedules**를 선택합니다.
2. **Add**(+) 버튼을 클릭하여 스케줄을 생성합니다.
3. 스케줄의 이름을 입력합니다.
4. 상태를 선택합니다.
   - **Normal**: 측정 작업을 처리 대기열에 제출합니다.
   - **Urgent**: 측정 작업을 처리 대기열의 맨 앞에 제출합니다.
5. 스케줄이 측정을 트리거하는 빈도를 **Day**, **Week** 또는 **Month** 중에서 선택합니다.
   - **Day**의 경우 시간을 선택합니다.
   - **Week**의 경우 시간과 요일을 선택합니다.
   - **Month**의 경우 시간과 날짜를 선택합니다.
6. 스케줄에 대한 MTree 할당을 선택합니다(스케줄을 적용할 MTree).
7. **Create**를 클릭합니다.
8. 필요에 따라 머리글 이름을 클릭하여 스케줄을 기준으로 정렬합니다. **Name**, **Status**(Enabled 또는 Disabled) **Priority**(Urgent 또는 Normal), **Schedule**(스케줄 시기) 및 **MTree Assignments**(스케줄을 적용할 MTree 수)를 정렬할 수 있습니다.

물리적 용량 측정 스케줄 편집

물리적 용량 측정 스케줄을 편집합니다.

절차

1. **Data Management** > **MTree** > **Manage Schedules**를 선택합니다.
2. 스케줄을 선택하고 **Modify**(연필 모양) 버튼을 클릭합니다.
3. 스케줄을 수정하고 **Save**를 클릭합니다.

   스케줄 옵션은 물리적 용량 측정 스케줄 생성 항목에 설명되어 있습니다.
4. 필요에 따라 머리글 이름을 클릭하여 스케줄을 기준으로 정렬합니다. **Name**, **Status**(Enabled 또는 Disabled) **Priority**(Urgent 또는 Normal), **Schedule**(스케줄 시기) 및 **MTree Assignments**(스케줄을 적용할 MTree 수)를 정렬할 수 있습니다.

MTree에 물리적 용량 측정 스케줄 할당

MTree에 스케줄을 연결합니다.

시작하기 전에

PCM(Physical Capacity Measurement) 스케줄을 생성해야 합니다.

참고

관리자는 MTree에 최대 3개의 PCM 스케줄을 할당할 수 있습니다.

절차

1. **Data Management** > **MTree** > **Summary**를 선택합니다.
2. 스케줄을 할당할 Mtree를 선택합니다.
3. Physical Capacity Measurements 영역으로 스크롤한 다음 Schedules 오른쪽에 있는 **Assign**을 클릭합니다.
4. MTree에 할당할 스케줄을 선택하고 **Assign**을 클릭합니다.

물리적 용량 측정 즉시 시작

측정 프로세스를 가능한 한 빨리 시작합니다.

절차

1. **Data Management** > **MTree** > **Summary**를 선택합니다.
2. Physical Capacity Measurements 영역으로 스크롤한 다음 Submitted Measurements 오른쪽에서 **Measure Now**를 클릭합니다.
3. **Normal**(측정 작업을 처리 대기열에 제출) 또는 **Urgent**(측정 작업을 처리 대기열 맨 앞에 제출)를 선택합니다.
4. **Submit**을 클릭합니다.

물리적 용량 측정 스로틀 설정

물리적 용량 측정 전용으로 사용할 시스템 리소스의 백분율을 설정합니다.

절차

1. **Data Management** > **File System** > **Settings**를 선택합니다.
2. Physical Capacity Measurement 영역에서 Throttle 왼쪽의 **Edit**를 클릭합니다.
3.

옵션	설명
Click Default	시스템 기본값인 20%를 입력합니다.
Type throttle percent	물리적 용량 측정 전용으로 사용할 시스템 리소스의 백분율입니다.

4. **Save**를 클릭합니다.

MTree 작업 관리

이 섹션에서는 MTree 생성, 구성, MTree 할당량 설정 및 해제 등에 대해 설명합니다.

MTree 생성

MTree는 파일 시스템의 논리적 파티션입니다. MTree는 DD Boost 스토리지 유닛, DD VTL 풀 또는 NFS/CIFS 공유에 사용됩니다.

MTree는 /data/col1/*mtree_name* 영역에서 생성됩니다.

절차

1. **Data Management** > **MTree**를 선택합니다.
2. MTree 개요 영역에서 **Create**를 클릭합니다.
3. MTree Name 입력란에 MTree의 이름을 입력합니다. MTree 이름은 최대 50자로 제한됩니다. 다음 문자를 사용할 수 있습니다.
   - 알파벳 대문자 및 소문자: A-Z, a-z
   - 숫자: 0-9
   - 공백
   - 쉼표(,)
   - 이름 앞에 오는 경우를 제외한 마침표(.)
   - 느낌표(!)
   - 번호 기호(#)
   - 달러 기호($)
   - 퍼센트 기호(%)
   - 더하기 기호(+)
   - at 기호(@)
   - 등호 기호(=)
   - 앰퍼샌드(&)
   - 세미콜론(;)
   - 괄호[()]
   - 대괄호([])
   - 중괄호({})
   - 캐럿(^)
   - 물결표(~)
   - 아포스트로피(기울지 않은 작은따옴표)
   - 기울어진 작은따옴표(‘)
4. 과도한 공간 소비를 방지하기 위해 MTree에 대한 스토리지 공간 제한을 설정합니다. 할당량의 유동적 제한값 또는 고정적 제한값을 입력하거나 둘 다 입력합니다. MTree 크기가 유동적 제한값을 초과하면 알림이 전송되지만 MTree에 데이터를 계속해서 기록할 수 있습니다. 하지만 고정적 제한값에 도달하면 MTree에 데이터를 기록할 수 없습니다.

참고

할당량 제한값은 압축 전 값입니다.
MTree에 대한 할당량 제한을 설정하려면 **Set to Specific value**를 선택하여 값을 입력합니다. 측정 단위를 MiB, GiB, TiB 또는 PiB 중에서 선택하십시오.

참고

유동적 제한과 고정적 제한을 모두 설정할 경우 할당량의 유동적 제한이 할당량의 고정적 제한을 초과할 수 없습니다.

---

5. **OK**를 클릭합니다.

   MTree 테이블에 새 MTree가 표시됩니다.

참고

전체 경로 이름을 보려면 MTree Name 열의 너비를 확장해야 할 수 있습니다.

MTree 할당량 구성 및 활성화/비활성화

MTree, 스토리지 유닛 또는 DD VTL 풀에 대한 스토리지 공간 제한을 설정합니다.

Data Management > **Quota** 페이지를 통해 관리자는 가변 할당량(soft quota) 또는 고정 할당량(hard quota) 설정이 없는 MTree가 얼마나 되는지 확인할 수 있습니다. 할당량이 설정되어 있는 MTree의 경우, 사용되는 압축 전 유동적 제한 및 고정적 제한의 비율이 페이지에 표시됩니다.

할당량 관리 시 다음 정보를 고려하십시오.

- MTree 할당량은 수집 작업에 적용됩니다. 이 할당량은 상주하는 계층에 관계없이 DD Extended Retention 소프트웨어를 비롯해 DD VTL, DD Boost, CIFS 및 NFS가 있는 시스템의 데이터에 적용될 수 있습니다.
- 스냅샷은 계산되지 않습니다.
- `/data/col1/backup` 디렉토리에서는 할당량을 설정할 수 없습니다.
- 최대 허용되는 할당량 값은 4,096PiB입니다.

MTree 할당량 구성

MTree 탭 또는 Quota 탭을 사용해 MTree 할당량을 구성합니다.

절차

1. 다음 메뉴 경로 중 하나를 선택합니다.
   - **Data Management** > **MTree**를 선택합니다.
   - **Data Management** > **Quota**를 선택합니다.
2. MTree 탭에서 하나의 MTree만 선택하거나 Quota 탭에서 하나 이상의 MTree를 선택합니다.

   참고

   `/data/col1/backup` 디렉토리에서는 할당량을 설정할 수 없습니다.

   ---
3. MTree 탭에서 **Summary** 탭을 클릭한 후 Quota 영역에서 **Configure** 버튼을 클릭합니다.
4. Quota 탭에서 **Configure Quota** 버튼을 클릭합니다.

MTree 할당량 구성

고정 할당량(hard quota) 및 가변 할당량(soft quota)에 대한 값을 입력하고 측정 단위를 선택합니다.

절차

1. Configure Quota for MTrees 대화 상자에서 고정 할당량(hard quota) 및 가변 할당량(soft quota) 값을 입력하고 MiB, GiB, TiB 또는 PiB 중에서 선택하십시오.
2. **OK**를 클릭합니다.

MTree 삭제

MTree 테이블에서 MTree를 제거합니다. MTree 데이터는 다음 정리 시 삭제됩니다.

참고

파일 정리가 실행될 때까지 MTree를 비롯한 관련 데이터는 제거되지 않으므로 정리 작업을 통해 파일 시스템에서 삭제된 MTree가 완전히 제거될 때까지는 삭제된 MTree와 같은 이름의 새 MTree를 생성할 수 없습니다.

절차

1. **Data Management** > **MTree**를 선택합니다.
2. MTree를 선택합니다.
3. MTree 개요 영역에서 **Delete**를 클릭합니다.
4. Warning 대화 상자에서 **OK**를 클릭합니다.
5. 진행률을 본 뒤 Delete MTree Status 대화 상자에서 **Close**를 클릭합니다.

MTree 삭제 취소

삭제를 취소하면 삭제된 MTree와 그 데이터를 가져와 MTree 테이블에 다시 배치합니다.

MTree 삭제를 취소하면 삭제된 MTree와 그 데이터를 가져와 MTree 테이블에 다시 배치합니다.

삭제 취소는 MTree가 삭제로 표시된 후 파일 정리를 실행하지 않은 경우에만 가능합니다.

참고

이 절차를 사용하여 스토리지 유닛의 삭제를 취소할 수도 있습니다.

절차

1. **Data Management** > **MTree** > **More Tasks** > **Undelete**를 선택합니다.
2. 다시 가져오려는 MTree의 확인란을 선택한 뒤 **OK**를 클릭합니다.
3. 진행률을 본 뒤 Undelete MTree Status 대화 상자에서 **Close**를 클릭합니다.

   MTree 테이블에 복구된 MTree가 표시됩니다.

MTree 이름 변경

Data Management MTree GUI를 사용해 MTree의 이름을 바꿉니다.

절차

1. **Data Management** > **MTree**를 선택합니다.
2. MTree 테이블에서 MTree를 선택합니다.
3. Summary 탭을 선택합니다.
4. Detailed Information 개요 영역에서 **Rename**을 클릭합니다.
5. New MTree Name 입력란에 MTree의 이름을 입력합니다.

   허용되는 문자 목록은 MTree 생성에 대한 섹션을 참조하십시오.

6. **OK**를 클릭합니다.
   MTree 테이블에서 이름이 변경된 **MTree**가 표시됩니다.

7장

스냅샷

이 장에는 다음과 같은 내용이 포함됩니다.

스냅샷 개요

이 장에서는 MTree와 함께 스냅샷 기능을 사용하는 방법에 대해 설명합니다.

스냅샷은 특정 시간에 지정된 MTree의 읽기 전용 복제본(*스냅샷*이라고 함)을 저장합니다. 스냅샷을 복구 지점으로 사용할 수 있으며 MTree 스냅샷 및 스케줄을 관리하고 기존 스냅샷의 상태에 대한 정보를 표시할 수 있습니다.

참고

소스 Data Domain 시스템에 생성된 스냅샷은 컬렉션과 MTree 복제를 통해 대상에 복제됩니다. 컬렉션 복제의 복제본인 Data Domain 시스템에는 스냅샷을 생성할 수 없습니다. 또한 MTree 복제의 대상 MTree에도 스냅샷을 생성할 수 없습니다. 디렉토리 복제의 경우 스냅샷이 복제되지 않으며, 대상 시스템에 스냅샷을 별도로 생성해야 합니다.

이름이 `backup`인 MTree가 `/data/col1/backup/.snapshot` 시스템 디렉토리에 생성됩니다. `/data/col1/backup` 아래의 각 디렉토리에도 해당 디렉토리가 포함된 각 스냅샷의 이름을 가진 `.snapshot` 디렉토리가 있습니다. 각 MTree의 구조가 동일한 유형이므로 SantaClara라는 MTree에는 시스템 디렉토리 `/data/col1/SantaClara/.snapshot`이 있고, `/data/col1/SantaClara`의 각 하위 디렉토리에도 `.snapshot` 디렉토리가 있습니다.

참고

`.snapshot` 디렉토리는 `/data`만 마운트된 경우 표시되지 않습니다. MTree 자체가 마운트된 경우에는 .snapshot 디렉토리가 표시됩니다.

만료된 스냅샷은 다음 파일 시스템 정리 작업이 수행될 때까지 사용할 수 있습니다.

MTree당 허용되는 최대 스냅샷 수는 750개입니다. MTree당 스냅샷 수가 허용된 최대 수의 90%(675~749개의 스냅샷)에 도달하면 경고가 전송되고, 최대 수에 도달하면 알림이 생성됩니다. 경고를 지우려면 스냅샷을 만료시킨 다음 파일 시스템 정리 작업을 실행합니다.

참고

최대 스냅샷 수에 근접한 MTree를 식별하려면 MTree 스냅샷 정보 조회와 관련된 MTree 페이지의 Snapshots 패널을 확인하십시오.

MTree의 스냅샷 보존에는 공간이 추가로 필요하지 않지만, 스냅샷이 존재하고 원래 파일이 더 이상 그곳에 없는 경우에는 공간을 재확보할 수 없습니다.

참고

스냅샷 및 CIFS 프로토콜: DD OS 5.0부터 `.snapshot` 디렉토리는 Windows 탐색기나 DOS CMD 셸의 디렉토리 목록에 더 이상 표시되지 않습니다. Windows 탐색기 주소 표시줄이나 DOS CMD 셸에서 이름을 입력하여 `.snapshot` 디렉토리에 액세스할 수 있습니다. 예를 들어 `\\dd\backup\.snapshot` 또는 `Z:\.snapshot`을 입력하면 됩니다(`Z:`가 `\\dd\backup`으로 매핑되는 경우).

스냅샷 및 스냅샷 스케줄 모니터링

이 섹션에서는 스냅샷과 스냅샷 스케줄의 상태에 대한 자세한 정보와 요약 정보를 제공합니다.

Snapshots 보기 정보

이 섹션의 항목에서는 Snapshot 보기에 대해 설명합니다.

Snapshots 개요 패널

전체 스냅샷 수, 만료된 스냅샷 수, 만료되지 않은 스냅샷 수 및 다음 정리 시간을 봅니다.

Data Management > **Snapshots**를 선택합니다.

표 102 Snapshots 개요 패널 정보

필드	설명
Total Snapshots (Across all MTrees)	시스템의 모든 MTree에 있는 활성 스냅샷과 만료된 스냅샷의 총 수입니다.
Expired	삭제 대상으로 표시되었지만 정리 작업을 통해 아직 제거되지 않은 스냅샷의 수입니다.
Unexpired	유지 대상으로 표시된 스냅샷의 수입니다.
Next file system clean scheduled	다음에 예약된 파일 시스템 정리 작업이 수행될 날짜입니다.

Snapshots 보기

이름, MTree, 생성 시간, 활성 여부 및 만료 시기별 스냅샷 정보를 봅니다.

Snapshots 탭에는 스냅샷의 목록과 다음 정보가 표시됩니다.

표 103 스냅샷 정보

필드	설명
Selected Mtree	스냅샷이 작동하는 MTree를 선택하는 드롭다운 목록입니다.
Filter By	표시되는 스냅샷 목록에서 검색할 항목입니다. 다음과 같은 옵션이 있음 • **Name** - 스냅샷의 이름입니다(와일드카드가 허용됨). • **Year** - 연도를 선택할 드롭다운 목록입니다.
Name	스냅샷 이미지의 이름입니다.
Creation Time	스냅샷이 생성된 날짜입니다.
Expires On	스냅샷이 만료되는 날짜입니다.
Status	스냅샷의 상태로, Expired이거나 스냅샷이 활성 상태인 경우 비어 있을 수 있습니다.

Schedules 보기

스냅샷이 생성될 요일, 시간, 보존되는 기간 및 명명 규칙을 봅니다.

표 104 스냅샷 스케줄 정보

필드	설명
Name	스냅샷 스케줄의 이름입니다.
Days	스냅샷이 생성될 요일입니다.
Times	스냅샷이 생성될 시간입니다.
Retention Period	스냅샷이 보존될 기간입니다.
Snapshot Name Pattern	스냅샷 이름으로 변환되는 문자열과 변수입니다(예를 들어 “scheduled-2010-04-12-17-33”으로 변환되는 `scheduled-%Y-%m-%d-%H-%M`).

1. Schedules 탭에서 스케줄을 선택합니다. 선택한 MTree와 동일한 스케줄을 공유하는 MTree가 나열된 Detailed Information 영역이 나타납니다.
2. **Add/Remove** 버튼을 클릭하여 스케줄 목록에서 MTree를 추가하거나 제거합니다.

스냅샷 관리

이 섹션에서는 스냅샷을 관리하는 방법에 대해 설명합니다.

스냅샷 생성

예약되지 않은 스냅샷이 필요한 경우 스냅샷을 생성합니다.

절차

1. **Data Management** > **Snapshots**를 선택하여 Snapshots 보기를 엽니다.
2. Snapshots 보기에서 **Create**를 클릭합니다.
3. Name 텍스트 필드에 스냅샷의 이름을 입력합니다.
4. MTree(s) 영역의 Available MTrees 패널에서 하나 이상의 MTree에 대한 확인란을 선택하고 **Add**를 클릭합니다.
5. Expiration 영역에서 다음 만료 옵션 중 하나를 선택합니다.
   a. **Never Expire**.
   b. In 텍스트 필드에 숫자를 입력하고 드롭다운 목록에서 **Days**, **Weeks**, **Month** 또는 **Years**를 선택합니다. 스냅샷은 생성된 시간과 동일한 시간까지 보존됩니다.
   c. On 텍스트 필드에 *mm/dd/yyyy* 형식을 사용하여 날짜를 입력하거나 **Calendar**를 클릭하고 날짜를 클릭합니다. 스냅샷은 지정된 날짜의 자정(00:00, 하루의 시작 시간)까지 보존됩니다.
6. **OK** 및 **Close**를 차례로 클릭합니다.

스냅샷 만료 날짜 수정

스냅샷 만료 날짜를 수정하여 스냅샷을 제거하거나 감사 또는 규정 준수를 위해 스냅샷 만료 기간을 연장합니다.

절차

1. **Data Management**>**Snapshots**를 선택하여 Snapshots 보기를 엽니다.
2. 목록에서 스냅샷 항목의 확인란을 클릭하고 **Modify Expiration Date**를 클릭합니다.

   참고

   확인란을 추가로 클릭하여 스냅샷을 두 개 이상 선택할 수 있습니다.

3. Expiration 영역에서 만료 날짜에 대해 다음 중 하나를 선택합니다.
   a. **Never Expire**.
   b. In 텍스트 필드에 숫자를 입력하고 드롭다운 목록에서 **Days**, **Weeks**, **Month** 또는 **Years**를 선택합니다. 스냅샷은 생성된 시간과 동일한 시간까지 보존됩니다.
   c. **On** 텍스트 필드에 날짜(*mm/dd/yyyy* 형식 사용)를 입력하거나 **Calendar**를 클릭하고 날짜를 클릭합니다. 스냅샷은 지정된 날짜의 자정(00:00, 하루의 시작 시간)까지 보존됩니다.
4. **OK**를 클릭합니다.

스냅샷 이름 변경하기

Snapshot 탭을 사용해 스냅샷 이름을 변경합니다.

절차

1. **Data Management** > **Snapshots**를 선택하여 Snapshots 보기를 엽니다.
2. 목록에 있는 스냅샷 항목의 확인란을 선택하고 **Rename**을 클릭합니다.
3. Name 텍스트 필드에 새 이름을 입력합니다.
4. **OK**를 클릭합니다.

스냅샷 만료

스냅샷은 삭제할 수 없습니다. 디스크 공간을 확보하기 위해 스냅샷을 만료시킬 수 있으며, 이렇게 만료된 스냅샷은 만료 날짜 후 다음 정리 주기에서 삭제됩니다.

절차

1. **Data Management** > **Snapshots**를 선택하여 Snapshots 보기를 엽니다.
2. 목록의 스냅샷 항목 옆에 있는 확인란을 클릭하고 **Expire**를 클릭합니다.

   참고

   확인란을 추가로 선택하여 스냅샷을 두 개 이상 선택할 수 있습니다.
   스냅샷이 Status 열에서 Expired로 표시되고 다음 정리 작업에서 삭제됩니다.

스냅샷 스케줄 관리

이후에 정기적으로 자동 생성되는 일련의 스냅샷(스냅샷 스케줄)을 설정하고 관리합니다.

여러 스냅샷 스케줄이 동시에 활성화될 수 있습니다.

참고

이름이 같은 여러 스냅샷이 동시에 발생하도록 예약된 경우 그중 하나만 보존됩니다. 어떤 스냅샷이 보존되는지는 확정되지 않기 때문에 지정된 시간에 해당 이름의 스냅샷을 하나만 예약해야 합니다.

스냅샷 스케줄 생성

Data Management GUI를 사용해 주별 또는 월별 스냅샷 스케줄을 생성합니다.

절차

1. **Data Managment** > **Snapshots** > **Schedules**를 선택하여 Schedules 보기를 엽니다.
2. **Create**를 클릭합니다.
3. **Name** 텍스트 필드에 스케줄의 이름을 입력합니다.
4. **Snapshot Name Pattern** 입력란에 이름 패턴을 입력합니다.

   스냅샷 이름으로 변환되는 문자열과 변수를 입력합니다(예를 들어 **`scheduled-%Y-%m-%d-%H-%m`**은 "scheduled-2012-04-12-17-33"으로 변환됨). 현재 값으로 변환되는 영문자, 숫자, _, - 및 변수를 사용합니다.

5. **Validate Pattern & Update Sample**을 클릭합니다.
6. **Next**를 클릭합니다.
7. 스케줄이 실행될 날짜를 선택합니다.
   a. Weekly - 요일 옆의 확인란을 클릭하거나 **Every Day**를 선택합니다.
   b. Monthly - **Selected Days** 옵션을 클릭하고 달력에서 날짜를 클릭하거나, **Last Day of the Month** 옵션을 선택합니다.
   c. **Next**를 클릭합니다.
8. 스케줄이 실행될 시간을 선택합니다.
   a. At Specific Times - **Add**를 클릭하고 나타나는 Time 대화 상자에 *hh:mm* 형식으로 시간을 입력한 다음 **OK**를 클릭합니다.
   b. In Intervals - 드롭다운 화살표를 클릭하여 시작 및 종료 시간 *hh:mm*과 AM 또는 PM을 선택합니다. **Interval** 드롭다운 화살표를 클릭하여 숫자를 선택한 후 간격의 시간 또는 분을 선택합니다.
   c. **Next**를 클릭합니다.
9. Retention Period 텍스트 입력 필드에 숫자를 입력하고 드롭다운 화살표를 클릭하여 일, 월 또는 연을 선택한 후 **Next**를 클릭합니다.

   스케줄은 보존 기간을 명시적으로 지정해야 합니다.

10. 스케줄 요약에서 매개 변수를 검토한 다음 **Finish**를 클릭하여 스케줄을 완료하거나 **Back**을 클릭하여 항목을 변경합니다.

11. MTree가 스케줄과 연결되지 않은 경우 스케줄에 MTree를 추가할 것인지 묻는 경고 대화 상자가 나타납니다. 계속하려면 **OK**를 클릭하고 중단하려면 **Cancel**을 클릭합니다.
12. 스케줄에 MTree를 할당하려면 MTree 영역의 Available MTrees 패널에서 하나 이상의 MTree에 대한 확인란을 클릭한 다음 **Add**를 클릭하고 **OK**를 클릭합니다.

스케줄에 따라 생성된 스냅샷의 명명 규칙

예약된 스냅샷의 명명 규칙은 scheduled라는 단어 뒤에 스냅샷이 생성될 날짜를 붙여 `scheduled-`*yyyy-mm-dd-hh-mm* 형식으로 이름을 지정하는 것입니다. 예를 들어 `scheduled-2009-04-27-13-30`으로 이름을 지정할 수 있습니다.

"mon_thurs"라는 이름은 스냅샷 스케줄의 이름입니다. 이 스케줄에 따라 생성된 스냅샷의 이름은 `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00` 등일 수 있습니다.

스냅샷 스케줄 수정

스냅샷 스케줄의 이름, 날짜 및 보존 기간을 변경합니다.

절차

1. 스케줄 목록에서 스케줄을 선택하고 **Modify**를 클릭합니다.
2. Name 텍스트 필드에 스케줄의 이름을 입력하고 **Next**를 클릭합니다.

   영숫자와 _ 및 -를 사용하십시오.

3. 스케줄이 실행될 날짜를 선택합니다.
   a. Weekly - 요일 옆의 확인란을 클릭하거나 **Every Day**를 선택합니다.
   b. Monthly - **Selected Days** 옵션을 클릭하고 달력에서 날짜를 클릭하거나, **Last Day of the Month** 옵션을 선택합니다.
   c. **Next**를 클릭합니다.
4. 스케줄이 실행될 시간을 선택합니다.
   a. At Specific Times - Times 목록에서 예약된 시간의 확인란을 클릭하고 **Edit**를 클릭합니다. 나타나는 Times 대화상자에 *hh:mm* 형식으로 새 시간을 입력한 다음 **OK**를 클릭합니다. 또는 **Delete**를 클릭하여 예약된 시간을 제거합니다.
   b. In Intervals - 드롭다운 화살표를 클릭하여 시작 및 종료 시간 *hh:mm*과 AM 또는 PM을 선택합니다. Interval 드롭다운 화살표를 클릭하여 숫자를 선택한 후 간격의 시간 또는 분을 선택합니다.
   c. **Next**를 클릭합니다.
5. Retention Period 텍스트 입력 필드에 숫자를 입력하고 드롭다운 화살표를 클릭하여 일, 월 또는 연을 선택한 후 **Next**를 클릭합니다.
6. 스케줄 요약에서 매개 변수를 검토한 다음 **Finish**를 클릭하여 스케줄을 완료하거나 **Back**을 클릭하여 항목을 변경합니다.

스냅샷 스케줄 삭제

스케줄 목록에서 스냅샷 스케줄을 삭제합니다.

절차

1. 스케줄 목록에서 확인란을 클릭하여 스케줄을 선택하고 **Delete**를 클릭합니다.

2. 검증 대화 상자에서 **OK**를 클릭한 다음 **Close**를 클릭합니다.

스냅샷에서 데이터 복구

빠른 복제 작업을 사용하여 스냅샷에 저장된 데이터를 검색합니다. 빠른 복제 작업에 대한 섹션을 참조하십시오.

8장

CIFS

이 장에는 다음과 같은 내용이 포함됩니다.

CIFS 개요

CIFS(Common Internet File System) 클라이언트는 Data Domain 시스템의 시스템 디렉토리에 액세스할 수 있습니다.

- `/data/col1/backup` 디렉토리는 압축된 백업 서버 데이터를 저장하기 위한 대상 디렉토리입니다.
- `/ddvar/core` 디렉토리에는 Data Domain 시스템의 핵심 파일과 로그 파일이 포함되어 있습니다. 이 영역에서 공간을 확보하려면 이전 로그와 핵심 파일을 제거해야 합니다.

  참고

  `/ddvar` 또는 `/ddvar/ext` 디렉토리가 있는 경우 여기서 핵심 파일을 삭제할 수도 있습니다.

Data Domain 시스템을 통해 백업 및 복구 작업을 수행하는 백업 서버와 같은 클라이언트는 적어도 `/data/col1/backup` 디렉토리에 액세스할 수 있어야 합니다. 관리 액세스 권한이 있는 클라이언트는 `/ddvar/core` 디렉토리에 액세스하여 핵심 파일과 로그 파일을 검색할 수 있어야 합니다.

초기 Data Domain 시스템 구성에서는 CIFS 클라이언트가 이러한 디렉토리에 액세스하도록 구성되어 있습니다. 이 장에서는 이러한 설정을 수정하는 방법과 Data DD Manager와 `cifs` 명령을 사용하여 데이터 액세스를 관리하는 방법에 대해 설명합니다.

참고

- DD System Manager **Protocols** > **CIFS** 페이지에서 CIFS 활성화 및 비활성화, 인증 설정, 공유 관리, 구성 및 공유 정보 보기 등의 주요 CIFS 작업을 수행할 수 있습니다.
- `cifs` 명령에는 Windows 클라이언트와 Data Domain 시스템 간의 CIFS 백업 및 복구를 관리하고 CIFS 통계 및 상태를 표시하기 위한 모든 옵션이 포함되어 있습니다. `cifs` 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.
- 초기 시스템 구성에 대한 자세한 내용은 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.
- Data Domain 시스템을 서버로 사용하도록 클라이언트를 설정하는 것에 관한 자세한 내용은 support.emc.com 웹 사이트에서 제공되는 *CIFS Tuning Guide*와 같은 관련 튜닝 가이드를 참조하십시오. 검색 필드를 사용하여 문서의 전체 이름을 검색하십시오.

SMB 서명 구성

이 기능을 지원하는 DD OS 버전에서 서버 서명이라는 CIFS 옵션을 사용해 SMB 서명 기능을 구성할 수 있습니다.

성능 저하 문제 때문에 이 기능은 기본적으로 비활성화되어 있습니다. 활성화할 경우 SMB 서명은 시스템마다 성능에 차이가 있지만 29%(읽기)에서 50%(쓰기) 처리량 성능 저하를 일으킬 수 있습니다. SMB 서명에 가능한 값 세 가지는 Disabled, Auto 및 Mandatory입니다.

- SMB 서명을 Disabled로 설정하면 SMB 서명을 사용할 수 없으며, 이는 기본값입니다.
- SMB 서명을 Mandatory로 설정하면 SMB 서명이 필요하며 SMB 연결에서 컴퓨터 두 대가 SMB 서명을 활성화해야 합니다.

SMB 서명 CLI 명령

`cifs option set "server-signing" required`
서버 서명을 required로 설정합니다.

`cifs option reset "server-signing"`
서버 서명을 기본값(Disabled)으로 재설정합니다.

최상의 방법은 SMB 서명 옵션을 변경할 때마다 다음 CLI 명령을 사용해 CIFS 서비스를 비활성화했다가 활성화(재시작)하는 것입니다.

```
cifs disable
cifs enable
```

DD System Manager 인터페이스에 SMB 서명 옵션이 비활성화되었는지 아니면 Auto 또는 Mandatory로 설정되었는지 표시됩니다. 인터페이스에서 이 설정을 보려면 **Protocols** > **CIFS** > **Configuration** 탭으로 이동합니다. Options 영역에서 SMB 서명 옵션을 위한 값이 비활성화되고 Auto 또는 Mandatory에 CLI 명령을 사용해 설정된 값이 반영됩니다.

CIFS 설정 수행

이 섹션에는 CIFS 서비스 설정 및 CIFS 서버 명명 등에 대한 지침이 포함되어 있습니다.

HA 시스템과 CIFS

HA 시스템은 CIFS와 호환되지만 페일오버 시에 CIFS 작업이 진행 중인 경우 나중에 작업을 다시 시작해야 합니다.

"/ddvar은 ext3 파일 시스템으로, 일반 MTree 기반 공유처럼 공유할 수 없습니다. 액티브 노드가 대기 노드로 페일오버되면 두 노드의 파일 핸들이 서로 달라지므로 /ddvar의 정보가 더 이상 유효하지 않게 됩니다. 로그 파일에 액세스하거나 시스템을 업그레이드하기 위해 /ddvar을 마운트한 경우, /ddvar을 마지막으로 마운트한 후 페일오버가 실행되었다면 /ddvar을 마운트 해제한 후 다시 마운트하십시오."

Data Domain 시스템에 액세스하기 위한 클라이언트 준비

온라인에서 설명서를 찾습니다.

절차

1. 온라인 지원(support.emc.com) 웹 사이트에 로그인합니다.
2. 검색 필드에 찾으려는 문서의 이름을 입력합니다.
3. *CIFS and Data Domain Systems Tech Note*와 같은 해당 문서를 선택합니다.
4. 문서에 나오는 지침을 따릅니다.

CIFS 서비스 설정

클라이언트에서 CIFS 프로토콜을 사용해 시스템에 액세스할 수 있도록 합니다.

Data Domain 시스템에 액세스하도록 클라이언트를 구성한 후에는 CIFS 서비스를 설정하여 클라이언트가 CIFS 프로토콜을 통해 시스템에 액세스할 수 있게 합니다.

절차

1. DD System Manager 탐색 트리에서 선택한 Data Domain 시스템에 대해 **Protocols** > **CIFS**를 클릭합니다.
2. CIFS Status 영역에서 **Enable**을 클릭합니다.

CIFS 서버 이름 지정

CIFS 서버 역할을 수행하는 Data Domain 시스템의 호스트 이름은 시스템의 초기 구성을 수행하는 동안 설정됩니다.

CIFS 서버 이름을 변경하려면 인증 매개 변수 설정과 관련된 섹션의 절차를 참조하십시오.

Data Domain 시스템의 호스트 이름은 DNS 테이블에서 IP 주소에 할당된 이름과 일치해야 합니다. 일치하지 않는 경우에는 인증과 도메인에 연결하려는 시도가 실패할 수 있습니다. Data Domain 시스템의 호스트 이름을 변경해야 한다면 `net set hostname` 명령을 사용합니다. 또한 DNS 테이블에서 시스템 항목도 수정해야 합니다.

Data Domain 시스템은 CIFS 서버 역할을 수행할 때 시스템의 호스트 이름을 사용합니다. 또한 호환성을 위해 NetBIOS 이름도 생성합니다. NetBIOS 이름은 호스트 이름의 첫 번째 구성 요소이며 모두 대문자입니다. 예를 들어, 호스트 이름 `jp9.oasis.local`은 NetBIOS 이름 `JP9`이 됩니다. CIFS 서버는 이 두 이름에 모두 응답합니다.

NetBIOS 호스트 이름을 변경하여 CIFS 서버가 NetBIOS 수준에서 서로 다른 이름에 응답하게 할 수 있습니다.

NetBIOS 호스트 이름 변경

CLI를 사용해 NetBIOS 호스트 이름을 변경합니다.

절차

1. 다음을 입력하여 현재 NetBIOS 이름을 표시합니다.

   ```
   # cifs show config
   ```

2. `cifs set nb-hostname`*`nb-hostname`* 명령을 사용합니다.

인증 매개 변수 설정

CIFS에서 사용할 Data Domain 인증 매개 변수를 설정합니다.

Configure 탭의 Authentication 레이블 왼쪽에 있는 Configuration 링크를 클릭합니다. **Administration** > **Access** > **Authentication** 탭으로 이동하여 Active Directory, Kerberos, 워크그룹 및 NIS 인증을 구성할 수 있습니다.

CIFS 옵션 설정

CIFS 구성을 보고 익명 접속을 제한합니다.

절차

1. **Protocols** > **CIFS** > **Configuration**을 선택합니다.
2. Options 영역에서 **Configure Options**를 클릭합니다.
3. 익명 접속을 제한하려면 Restrict Anonymous Connections 영역에서 **Enable** 옵션의 확인란을 클릭합니다.
4. Log Level 영역에서 드롭다운 목록을 클릭하여 레벨 번호를 선택합니다.

   레벨은 1(일)에서 5(오)까지의 정수입니다. 1이 가장 자세하지 않은 레벨의 CIFS 관련 로그 메시지를 보내는 기본 시스템 레벨이고 5는 가장 자세한 메시지를 생

성합니다. 로그 메시지는 `/ddvar/log/debug/cifs/cifs.log` 파일에 저장됩니다.

참고

로그 레벨 5를 사용하면 시스템 성능이 저하됩니다. 문제를 디버깅한 후 Log Level 영역에서 **Default**를 클릭하십시오. 이렇게 하면 레벨이 다시 1로 설정됩니다.

5. Server Signing 영역에서 다음을 선택합니다.
   - 서버 서명을 활성화하려면 **Enabled** 선택
   - 서버 서명을 비활성화하려면 **Disabled** 선택
   - 서버 서명이 필요한 경우 **Required** 선택

CIFS 서비스 해제

클라이언트에서 Data Domain 시스템에 액세스할 수 없도록 합니다.

절차

1. **Protocols** > **CIFS**를 선택합니다.
2. Status 영역에서 **Disable**을 클릭합니다.
3. **OK**를 클릭합니다.

   CIFS 액세스를 해제한 후에도 CIFS 인증 서비스는 Data Domain 시스템에서 계속 실행됩니다. 이런 연속성은 관리 액세스를 위해 Active Directory 도메인 사용자를 인증하는 데 필수입니다.

공유 작업

데이터를 공유하려면 Data Domain 시스템에서 공유를 생성하십시오.

공유는 Data Domain 시스템 및 CIFS 시스템에서 관리됩니다.

Data Domain 시스템에서 공유 생성

공유를 생성할 때 각 디렉토리별로 클라이언트 액세스를 할당하고 각 디렉토리별로 액세스를 제거해야 합니다. 예를 들어, 클라이언트가 `/ddvar`에서만 제거되고 `/data/col1/backup`에는 계속 액세스하도록 지정할 수 있습니다

Data Domain 시스템은 최대 3,000개의 CIFS 공유를 지원합니다.[1] 600개의 동시 연결이 허용됩니다. 그러나 지원되는 최대 접속 수는 시스템 메모리를 기준으로 합니다. 자세한 내용은 접속에서 열린 최대 파일 수 설정과 관련된 섹션을 참조하십시오.

참고

복제를 구축하는 경우 Data Domain 시스템은 각각에 대해 별도의 디렉토리가 사용되는 한 CIFS 클라이언트와 NFS 클라이언트 모두로부터 백업을 수신할 수 있습니다. 동일한 디렉토리에 CIFS와 NFS 데이터를 함께 저장하지 마십시오.

1. 이 수는 하드웨어 제한에 따라 달라질 수 있습니다.

절차

1. **Protocols** > **CIFS** 탭을 선택하여 CIFS 보기로 이동합니다.
2. 인증 방법 매개 변수 설정과 관련된 섹션에 설명된 대로 인증이 구성되었는지 확인합니다.
3. CIFS 클라이언트에서 공유 디렉토리 권한이나 보안 옵션을 설정합니다.
4. CIFS 보기에서 Shares 탭을 클릭합니다.
5. **Create**를 클릭합니다.
6. Create Shares 대화 상자에서 다음 정보를 입력합니다.

   표 105 Shares 대화 상자 정보

항목	설명
Share Name	공유의 설명 이름입니다.
Directory Path	타겟 디렉토리의 경로입니다(예: `/data/col1/backup/dir1`). 참고 col1은 소문자 L 다음에 숫자 1을 사용합니다.
Comment	공유에 대한 쉽게 알 수 있는 설명입니다.

   참고

   공유 이름은 최대 80자일 수 있으며 \ / : * ? " < > | + [ ] ; , = 또는 확장 ASCII 문자를 포함할 수 없습니다.

7. Clients 영역에서 추가(**+**) 버튼을 클릭하여 클라이언트를 추가합니다. Client 대화 상자가 표시됩니다. Client 입력란에 클라이언트 이름을 입력하고 **OK**를 클릭합니다.

   클라이언트 이름을 입력할 때는 다음을 고려하십시오.

   - 탭이나 공백 문자는 사용할 수 없습니다.
   - 지정된 공유에 별표(*)와 개별 클라이언트 이름 또는 IP 주소를 모두 사용하지 않는 것이 좋습니다. 별표(*)가 있는 경우 해당 공유에 대한 다른 모든 클라이언트 항목이 사용되지 않습니다.
   - 지정된 공유의 동일한 클라이언트에 대해 클라이언트 이름과 클라이언트 IP 주소를 모두 사용할 필요는 없습니다. 클라이언트 이름이 DNS 테이블에 정의된 경우에는 클라이언트 이름을 사용하십시오.
   - 모든 클라이언트가 공유를 사용할 수 있게 하려면 별표(*)를 클라이언트로 지정합니다. 사용자 이름을 하나 이상 지정하지 않는 한 클라이언트 목록의 모든 사용자가 공유에 액세스할 수 있습니다. 사용자 이름을 지정하면 나열된 이름만 공유에 액세스할 수 있습니다.

   구성해야 하는 각 클라이언트에 대해 이 단계를 반복합니다.

8. Max Connections 영역에서 입력란을 선택하고 한 번에 허용되는 공유에 대한 최대 접속 수를 입력합니다. 기본값 0(Unlimited 버튼을 통해서도 설정 가능)을 설정하면 접속 수에 제한이 적용되지 않습니다.
9. **OK**를 클릭합니다.

새로 생성된 공유가 Shares 패널의 중앙에 있는 공유 목록의 끝에 표시됩니다.

CLI 절차

절차

1. `cifs status` 명령을 실행하여 CIFS가 활성화되어 있는지 확인합니다.
2. `filesys status` 명령을 실행하여 파일 시스템이 활성화되어 있는지 확인합니다.
3. `hostname` 명령을 실행하여 시스템 호스트 이름을 확인합니다.
4. CIFS 공유를 생성합니다.

   `cifs share create <share> path <path> {max-connections <max connections> | clients <clients> | users <users> | comment <comment>}`

   ```
   # cifs share create backup path /backup
   ```

5. 클라이언트에 공유 액세스 권한을 부여합니다.

   `cifs share modify <share> {max-connections <max connections> | clients <clients> | browsing {enabled | disabled} | writeable {enabled | disabled} | users <users> | comment <comment>}`

   ```
   # cifs share modify backup clients
   "srvr24.yourdomain.com,srvr24,10.24.160.116
   ```

6. 필요에 따라 공유를 보이도록 구성합니다.

   `cifs share <share> browsing enabled`

   ```
   # cifs share backup browsing enabled
   ```

7. 필요에 따라 공유를 쓰기 가능하게 지정합니다.

   `cifs share <share> writeable enabled`

   ```
   # cifs share backup writeable enabled
   ```

8. Windows 시스템에서 **시작** > **실행**을 선택하고 CIFS 공유의 호스트 이름 및 디렉토리를 입력합니다.

   \\<DDhostname>.<DDdomain.com>\<sharename>

9. CIFS 공유에 연결하는 데 문제가 있는 경우 `cifs share show` 명령을 실행하여 공유 상태를 확인합니다.

   공유가 존재하지 않거나 생성 시 철자가 잘못되면 경고: 공유 경로가 없습니다.가 표시됩니다.

   ```
   # cifs share show
   --------------- share backup ---------------

   enabled: yes
   path: /backup
   ```

10. CIFS 공유에 여전히 액세스할 수 없는 경우 모든 클라이언트 정보가 액세스 목록에 있고 모든 네트워크 연결이 작동하는지 확인하십시오.

Data Domain 시스템에서 공유 수정

공유 정보 및 접속 구성을 변경합니다.

절차

1. **Protocols** > **CIFS** > **Shares**를 선택하여 CIFS 보기의 Shares 탭으로 이동합니다.
2. Share Name 목록에서 수정할 공유 옆의 확인란을 클릭합니다.
3. **Modify**를 클릭합니다.
4. 공유 정보를 수정합니다.
   a. 설명을 변경하려면 Comment 텍스트 필드에 새 텍스트를 입력합니다.
   b. User 또는 Group 이름을 수정하려면 User/Group 목록에서 사용자 또는 그룹의 확인란을 클릭하고 **Edit**(연필 아이콘) 또는 **Delete**(X) 버튼을 클릭합니다. 사용자 또는 그룹을 추가하려면 Add(+) 버튼을 클릭하고 User/Group 대화 상자에서 Type for User or Group을 선택한 후 사용자 또는 그룹 이름을 입력합니다.
   c. 클라이언트 이름을 수정하려면 Client 목록에서 클라이언트의 확인란을 클릭하고 **Edit**(연필 아이콘) 또는 **Delete**(X) 버튼을 클릭합니다. 클라이언트를 추가하려면 Add(+) 버튼을 클릭하고 Client 대화 상자에서 이름을 추가합니다.

   참고

   모든 클라이언트가 공유를 사용할 수 있게 하려면 별표(*)를 클라이언트로 지정합니다. 사용자 이름을 하나 이상 지정하지 않는 한 클라이언트 목록의 모든 사용자가 공유에 액세스할 수 있습니다. 사용자 이름을 지정하면 나열된 이름만 공유에 액세스할 수 있습니다.

   d. **OK**를 클릭합니다.
5. Max Connections 영역의 입력란에서 한 번에 허용되는 공유에 대한 최대 접속 수를 변경합니다. 또는 접속 수에 제한을 적용하지 않으려면 Unlimited를 선택합니다.
6. **OK**를 클릭합니다.

기존 공유에서 공유 생성

기존 공유에서 공유를 생성하고 필요한 경우 새 공유를 수정합니다.

참고

기존 공유의 사용자 권한은 새 공유로 이전됩니다.

절차

1. CIFS Shares 탭에서 소스로 사용할 공유의 확인란을 클릭합니다.
2. **Create From**을 클릭합니다.
3. Data Domain 시스템에서 공유를 수정하는 방법에 대한 섹션에 설명된 대로 공유 정보를 수정합니다.

Data Domain 시스템에서 공유 해제

하나 이상의 기존 공유를 해제합니다.

절차

1. Shares 탭의 Share Name 목록에서 해제할 공유의 확인란을 클릭합니다.
2. **Disable**을 클릭합니다.
3. **Close**를 클릭합니다.

Data Domain 시스템에서 공유 설정

하나 이상의 기존 공유를 설정합니다.

절차

1. Shares 탭에서 Share Name 목록 중 사용하도록 설정하려는 공유의 확인란을 클릭합니다.
2. **Enable**을 클릭합니다.
3. **Close**를 클릭합니다.

Data Domain 시스템에서 공유 삭제

기존 공유를 하나 이상 삭제합니다.

절차

1. Shares 탭으로 이동하고 Share Name 목록에서 삭제하려는 공유의 확인란을 클릭합니다.
2. **삭제**를 클릭합니다.

   Warning 대화 상자가 나타납니다.

3. **OK**를 클릭합니다.

   공유가 제거됩니다.

MMC 관리 수행

MMC(Microsoft Management Console)를 관리에 사용합니다.

DD OS는 다음과 같은 MMC 기능을 지원합니다.

- 공유 추가 시 탐색하거나 수동 절차에 해당하는 오프라인 설정 기본값을 변경하는 경우를 제외하고 공유를 관리합니다.
- 세션을 관리 관리합니다.
- 파일을 삭제하는 경우를 제외하고 열린 파일을 관리합니다.

CIFS 클라이언트에서 Data Domain 시스템에 접속

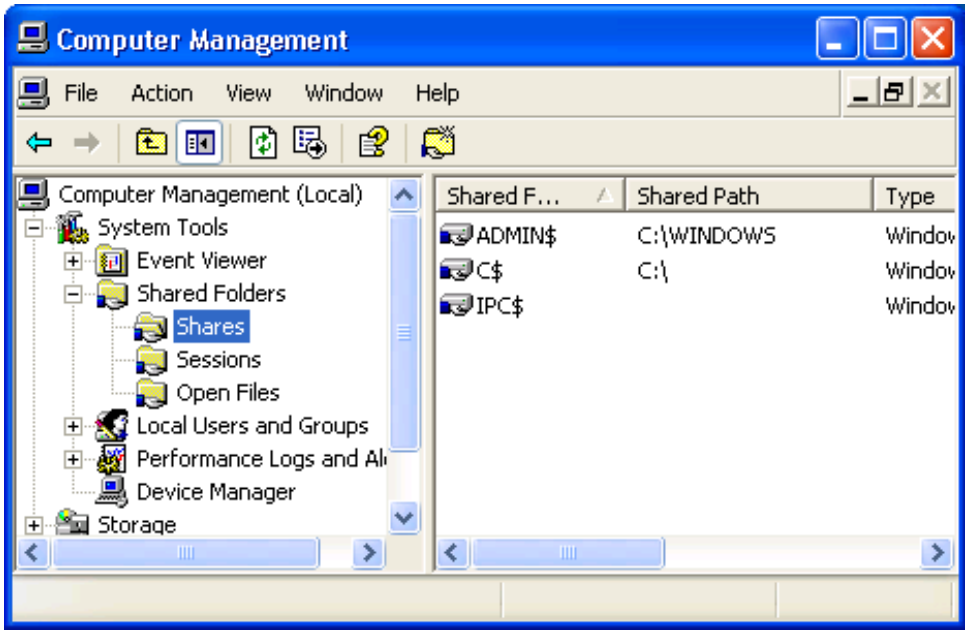
CIFS를 사용하여 Data Domain 시스템에 접속하고 읽기 전용 백업 하위 폴더를 생성합니다.

절차

1. Data Domain system CIFS 페이지에서 CIFS Status에 CIFS가 설정되어 있고 실행 중인지 확인하십시오.
2. 제어판에서 관리 도구를 열고 **컴퓨터 관리**를 선택합니다.
3. 컴퓨터 관리 대화 상자에서 **컴퓨터 관리(로컬)**를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **다른 컴퓨터에 연결**을 선택합니다.

4. 컴퓨터 선택 대화 상자에서 **다른 컴퓨터**를 선택하고 Data Domain 시스템의 이름과 IP 주소를 입력합니다.
5. 읽기 전용으로 `\backup` 하위 폴더를 생성합니다. 자세한 내용은 **/data/col1/backup** 하위 폴더를 읽기 전용으로 생성하는 방법에 대한 섹션을 참조하십시오.

그림 7 컴퓨터 관리 대화 상자



읽기 전용으로 \data\col1\backup 하위 폴더 생성

경로 및 공유 이름을 입력하고 사용 권한을 선택합니다.

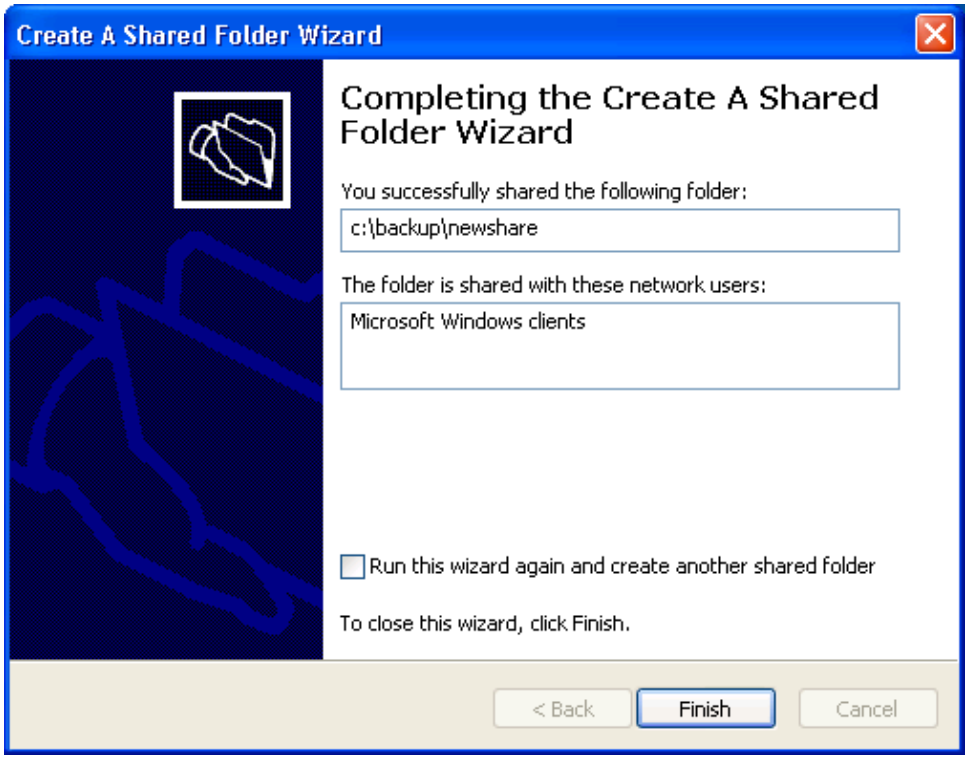
절차

1. 제어판에서 관리 도구를 열고 **컴퓨터 관리**를 선택합니다.
2. 공유 폴더 디렉토리에서 **공유**를 마우스 오른쪽 버튼으로 클릭합니다.
3. 메뉴에서 **새 파일 공유**를 선택합니다.

   공유 폴더 만들기 마법사가 열립니다. 컴퓨터 이름은 Data Domain 시스템의 이름 또는 IP 주소여야 합니다.

4. 공유할 폴더의 경로를 입력합니다. 예를 들어 `C:\data\col1\backup\newshare`를 입력합니다.
5. 공유 이름을 입력합니다. 예를 들어 **newshare**를 입력합니다. **다음**을 클릭합니다.
6. 공유 폴더 권한의 경우 선택한 관리자가 전체 액세스 권한을 갖습니다. 다른 사용자는 읽기 전용 액세스 권한을 갖습니다. **다음**을 클릭합니다.

그림 8 공유 폴더 만들기 마법사 완료



7. 완료 마법사에는 네트워크의 모든 Microsoft Windows 클라이언트와 폴더를 성공적으로 공유했다는 내용이 표시됩니다. **마침**을 클릭합니다.

   새로 생성된 공유 폴더가 컴퓨터 관리 대화 상자에 나열됩니다.

CIFS 정보 표시

공유 폴더, 세션 및 열린 파일에 대한 정보를 표시합니다.

절차

1. 제어판에서 관리 도구를 열고 **컴퓨터 관리**를 선택합니다.
2. 시스템 도구 디렉토리에서 공유 폴더(**공유**, **세션** 또는 **열린 파일**) 중 하나를 선택합니다.

   오른쪽 패널에 공유 폴더, 세션 및 열린 파일의 정보가 표시됩니다.

액세스 제어 관리

Windows 클라이언트에서 공유에 액세스하고 관리 액세스 권한을 제공하고 신뢰할 수 있는 도메인 사용자의 액세스를 허용합니다.

Windows 클라이언트에서 공유 액세스

명령줄을 사용하여 공유를 매핑합니다.

절차

- Windows 클라이언트에서 다음 DOS 명령을 사용합니다.
  `net use`*`drive`*`:`*`backup-location`*

예를 들면 다음과 같이 입력합니다.

```
# \\dd02\backup /USER:dd02\backup22
```

이 명령은 Data Domain 시스템 dd02의 백업 공유를 Windows 시스템의 H 드라이브에 매핑하고 backup22 사용자에게 `\\DD_sys\backup` 디렉토리에 대한 액세스 권한을 제공합니다.

DD OS는 SMB 변경 알림 기능을 지원합니다. 따라서 CIFS 서버가 Windows 클라이언트에 CIFS 공유 변경 사항을 자동으로 알릴 수 있게 되므로 Windows 클라이언트의 CIFS 성능이 개선되며, 클라이언트가 공유 변경 사항을 찾기 위해 Data Domain 시스템을 폴링할 필요가 없어집니다.

도메인 사용자 관리 액세스 권한 제공

명령줄을 사용해 CIFS를 추가하고 ssh 지침에 도메인 이름을 포함합니다.

절차

- 다음을 입력합니다. **adminaccess authentication add cifs**

  Data Domain 시스템에 액세스하는 SSH, Telnet 또는 FTP 명령에서는 도메인 이름, 백슬래시 및 사용자 이름을 큰따옴표로 묶어야 합니다. 예를 들면 다음과 같습니다.

  ```
  C:> ssh "domain2\djones" @dd22
  ```

도메인 사용자를 위한 Data Domain 시스템에 대한 관리 액세스 허용

명령줄을 사용하여 DD 시스템 기본 그룹 번호를 매핑한 다음 CIFS 관리 액세스를 설정합니다.

절차

1. 기본 그룹 이름과 다른 Windows 그룹 이름에 Data Domain 시스템 기본 그룹 번호를 매핑하려면
   `cifs option set "dd admin group2" ["windows`*grp-name*`"]`
   명령을 사용하십시오.

   Windows 그룹 이름은 Windows 도메인 컨트롤러에 있는 그룹(admin, user 또는 back-up operator 사용자 역할 중 하나를 기반으로 함)이며 최대 그룹 수는 50개입니다(dd admin group1부터 dd admin group50까지).

   참고

   DD OS 사용자 역할 및 Windows 그룹에 대한 설명은 Data Domain 시스템 관리에 대한 섹션을 참조하십시오.

   ---

2. 다음을 입력해 CIFS 관리 액세스를 설정합니다.

   adminaccess authentication add cifs

   - 기본 Data Domain 시스템 그룹 dd admin group1이 Windows 그룹 Domain Admins로 매핑됩니다.
   - 기본 Data Domain 시스템 그룹 dd admin group2를 Windows 도메인 컨트롤러에서 생성한 Data Domain이라는 Windows 그룹으로 매핑할 수 있습니다.
   - SSH, Telnet, FTP, HTTP 및 HTTPS를 통해 액세스가 가능합니다.

- Windows 그룹 `Data Domain`에서 Data Domain 시스템에 대한 관리 액세스를 설정한 후에는 `adminaccess` 명령을 사용해 CIFS 관리 액세스를 설정해야 합니다.

Windows에서 관리 액세스 제한

명령줄을 사용해 DD 계정이 없는 사용자의 액세스를 금지합니다.

절차

- 다음을 입력합니다. **`adminaccess authentication del cifs`**

  이 명령은 Data Domain 시스템에 계정이 없는 Windows 사용자가 Data Domain 시스템에 액세스하는 것을 금지합니다.

파일 액세스

이 섹션에는 Windows 탐색기를 사용한 DACL 및 SACL 사용 권한 설정과 ACL 등에 대한 정보가 포함되어 있습니다.

NT 액세스 제어 목록

Data Domain 시스템에서는 ACL(Access Control List)이 기본적으로 활성화되어 있습니다.

⚠ 주의

Data Domain에서는 NTFS ACL을 활성화한 후에 비활성화하지 않는 것이 좋습니다. NTFS ACL을 비활성화하기 전에 Data Domain 지원 센터에 문의하십시오.

기본 ACL 권한

ACL을 활성화할 때 CIFS 프로토콜을 통해 생성된 새 객체에 할당된 기본 권한은 상위 디렉토리의 상태에 따라 다릅니다. 다음과 같은 세 가지가 가능합니다.

- NFS 프로토콜을 통해 생성되었기 때문에 상위 디렉토리에 ACL이 없습니다.
- CIFS를 통해 생성되었거나 ACL이 명시적으로 설정되었기 때문에 상위 디렉토리에 상속 가능한 ACL이 있습니다. 상속된 ACL이 새 객체에서 설정됩니다.
- 상위 디렉토리에 ACL이 있지만 상속할 수 없습니다. 사용 권한은 다음과 같습니다.

표 106 사용 권한

유형	이름	사용 권한	적용 대상
허용	SYSTEM	전체 제어	이 폴더만
허용	CREATOR OWNER	전체 제어	이 폴더만

참고

CREATOR OWNER는 일반 사용자를 위해 파일/폴더를 생성 중인 사용자와 관리 사용자를 위한 관리자에 의해 교체됩니다.

상위 디렉토리에 ACL이 없을 경우 새 객체의 사용 권한

사용 권한은 다음과 같습니다.

- BUILTIN\Administrators:(OI)(CI)F

- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE_APPEND_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE_WRITE_DATA
- Everyone:(OI)(CI)R

이 사용 권한은 다음과 같이 보다 자세히 설명됩니다.

표 107 사용 권한 세부 정보

유형	이름	사용 권한	적용 대상
허용	Administrators	전체 제어	이 폴더, 하위 폴더 및 파일
허용	SYSTEM	전체 제어	이 폴더, 하위 폴더 및 파일
허용	CREATOR OWNER	전체 제어	하위 폴더 및 파일만
허용	Users	읽기 및 실행	이 폴더, 하위 폴더 및 파일
허용	Users	하위 폴더 생성	이 폴더 및 하위 폴더만
허용	Users	파일 생성	하위 폴더만
허용	Everyone	읽기 및 실행	이 폴더, 하위 폴더 및 파일

ACL 사용 권한 및 보안 설정
NetBackup 같은 Windows 기반 백업 및 복구 툴은 DACL 및 SACL 보호 파일을 Data Domain 시스템에 백업하고 Data Domain 시스템에서 이 파일을 복구하는 데 사용할 수 있습니다.

세분화되고 복잡한 사용 권한(DACL)
Windows 명령(예: `cacls`, `xcacls`, `xcopy` 및 `scopy`) 또는 Windows 탐색기 GUI를 사용하는 CIFS 프로토콜을 통해 파일 시스템 내에 있는 파일 또는 폴더 객체에 대해 세분화되고 복잡한 사용 권한(DACL)을 설정할 수 있습니다.

감사 ACL(SACL)
명령을 통해서나 Windows 탐색기 GUI를 사용하는 CIFS 프로토콜을 통해 파일 시스템 내에 있는 객체에 대해 감사 ACL(SACL)을 설정할 수 있습니다.

Windows 탐색기를 사용하여 DACL 사용 권한 설정

탐색기 속성 설정을 사용해 DACL 사용 권한을 선택합니다.

절차

1. 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
2. 속성 대화 상자에서 **보안** 탭을 클릭합니다.
3. 목록에서 **관리자**와 같은 그룹 또는 사용자 이름을 선택합니다. 권한이 나타납니다. 관리자를 선택한 경우에는 모든 권한이 나타납니다.
4. 특별 권한을 설정할 수 있는 **고급** 버튼을 클릭합니다.
5. ACL 고급 보안 설정 대화 상자에서 **사용 권한** 탭을 클릭합니다.
6. 목록에서 권한 항목을 선택합니다.
7. 권한 항목에 대한 자세한 내용을 보려면 항목을 선택하고 **편집**을 클릭합니다.

8. 상위 항목에서 상속 옵션을 선택하여 상위 항목의 권한이 하위 객체로 상속되도록 하고 **확인**을 클릭합니다.

Windows 탐색기를 사용해 SACL 사용 권한 설정

탐색기 속성 설정을 사용해 SACL 사용 권한을 선택합니다.

절차

1. 파일 또는 폴더를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 **속성**을 선택합니다.
2. 속성 대화 상자에서 **보안** 탭을 클릭합니다.
3. 사용 권한을 표시하는 목록에서 **관리자**와 같은 그룹 또는 사용자 이름을 선택합니다. 이 경우 해당되는 사용 권한은 모든 권한입니다.
4. 특별 권한을 설정할 수 있는 **고급** 버튼을 클릭합니다.
5. ACL 고급 보안 설정 대화 상자에서 **감사** 탭을 클릭합니다.
6. 목록에서 감사 항목을 선택합니다.
7. 특수 감사 항목의 세부 정보를 보려면 항목을 선택하고 **편집**을 클릭합니다.
8. 상위 항목에서 상속 옵션을 선택하여 상위 항목의 권한이 하위 객체로 상속되도록 하고 **확인**을 클릭합니다.

현재 소유자 보안 ID(소유자 SID) 보기 또는 변경

ACL 고급 보안 설정 대화 상자를 사용합니다.

절차

1. ACL 고급 보안 설정 대화 상자에서 **소유자** 탭을 클릭합니다.
2. 소유자를 변경하려면 소유자 변경 목록에서 이름을 선택하고 **확인**을 클릭합니다.

ID 계정 매핑 제어

ID 계정 매핑 동작은 CIFS 옵션 idmap-type이 제어합니다.

이 옵션의 값은 두 가지입니다. rid(기본값) 및 none이라는 두 개의 값이 있습니다. 옵션이 rid로 설정되어 있으면 ID-to-id 매핑이 내부에서 수행됩니다. 옵션이 none으로 설정되어 있으면 모든 CIFS 사용자가 로컬 UNIX 사용자 그룹에 속하는 "cifsuser"라는 로컬 UNIX 사용자로 매핑됩니다.

이 옵션을 관리하는 동안에는 다음 정보를 고려하십시오.

- 이 옵션을 설정하려면 CIFS를 해제해야 합니다. CIFS가 실행 중이면 CIFS 서비스를 해제하십시오.
- idmap-type은 ACL 지원이 설정된 경우에만 none으로 설정할 수 있습니다.
- idmap 유형이 변경될 때마다 올바른 파일 액세스를 위해 파일 시스템 메타데이터 변환이 필요할 수 있습니다. 변환 없이는 사용자가 데이터에 액세스하지 못할 수 있습니다. 메타데이터를 변환하려면 계약된 지원 제공업체에 문의하십시오.

CIFS 작업 모니터링

CIFS 작업 모니터링에 대한 항목입니다.

CIFS 상태 표시

CIFS 상태를 보고 CIFS 상태를 설정/해제합니다.

절차

1. DD System Manager에서 **Protocols** > **CIFS**를 선택합니다.
   - 상태는 설정되어 실행 중이거나 해제되어 있지만 CIFS 인증이 실행 중입니다.
     CIFS를 설정하려면 CIFS 서비스 설정과 관련된 섹션을 참조하고, CIFS를 해제하려면 CIFS 서비스 해제와 관련된 섹션을 참조하십시오.
   - **Connections**에는 열린 접속과 열린 파일의 수가 나열됩니다.

   표 108 접속 세부 정보

항목	설명
Open Connections	열린 CIFS 접속
Connection Limit	허용되는 최대 접속
Open Files	현재 열린 파일
Max Open Files	Data Domain 시스템의 최대 열린 파일 수

2. 자세한 접속 정보를 보려면 **Connection Details**를 클릭합니다.

   표 109 접속 세부 정보

항목	설명
Sessions	활성 CIFS 세션
Computer	세션의 DDR에 연결된 IP 주소 또는 컴퓨터 이름
User	DDR에 연결된 컴퓨터를 작동하는 사용자
Open Files	각 세션에 대해 열린 파일 수
Connection Time	접속 기간(분)
User	컴퓨터의 도메인 이름
Mode	파일 사용 권한
Locks	파일에서 잠금의 수
Files	파일 위치

CIFS 구성 표시

이 섹션에는 CIFS 구성이 표시됩니다.

인증 구성

Authentication 패널의 정보는 구성된 인증 유형에 따라 다르게 변경됩니다.

Configure 탭의 Authentication 레이블 왼쪽에 있는 Configuration 링크를 클릭합니다. **Administration** > **Access** > **Authentication** 페이지로 이동하여 Active Directory, Kerberos, 워크그룹 및 NIS 인증을 구성할 수 있습니다.

Active Directory 구성

표 110 Active Directory 구성 정보

항목	설명
Mode	Active Directory 모드가 표시됩니다.
Realm	구성된 영역이 표시됩니다.
DDNS	DDNS 서버의 상태가 표시됩니다(Enabled 또는 Disabled).
Domain Controllers	구성된 도메인 컨트롤러의 이름이 표시되거나 모든 컨트롤러가 허용될 경우 *가 표시됩니다.
Organizational Unit	구성된 조직 단위의 이름이 표시됩니다.
CIFS Server Name	구성된 CIFS 서버의 이름이 표시됩니다.
WINS Server Name	구성된 WINS 서버의 이름이 표시됩니다.
Short Domain Name	간략한 도메인 이름이 표시됩니다.

워크그룹 구성

표 111 워크그룹 구성 인증 정보

항목	설명
Mode	워크그룹 모드가 표시됩니다.
Workgroup Name	구성된 워크그룹 이름이 표시됩니다.
DDNS	DDNS 서버의 상태가 표시됩니다(Enabled 또는 Disabled).
CIFS Server Name	구성된 CIFS 서버의 이름이 표시됩니다.
WINS Server Name	구성된 WINS 서버의 이름이 표시됩니다.

공유 정보 표시

이 섹션에는 공유 정보가 표시됩니다.

구성된 공유 보기

구성된 공유 목록을 봅니다.

표 112 구성된 공유 정보

항목	설명
Share Name	공유의 이름입니다(예: share1).
Share Status	공유의 상태로 Enabled 또는 Disabled입니다.
Directory Path	공유에 대한 디렉토리 경로입니다(예: `/data/col1/backup/dir1`). 참고 col1은 소문자 L 뒤에 숫자 1을 사용한 것입니다.
Directory Path Status	디렉토리 경로의 상태입니다.

- 특정 공유에 대한 정보를 나열하려면 Filter by Share Name 입력란에 공유 이름을 입력하고 **Update**를 클릭합니다.
- 기본 목록으로 돌아가려면 **Update**를 클릭합니다.
- 공유 목록을 페이지를 이동하며 확인하려면 보기 오른쪽 맨 아래에서 **<** 및 **>** 화살표를 클릭해 앞 또는 뒤 페이지로 이동합니다. 목록의 시작으로 건너뛰려면 **|<**를 클릭하고 맨 끝으로 건너뛰려면 **>|**를 클릭합니다.
- 페이지에 나열된 공유 목록의 수를 변경하려면 **Items per Page** 드롭다운 화살표를 클릭합니다. 15, 30 또는 45개 항목 중에서 선택할 수 있습니다.

자세한 공유 정보 보기

공유 목록에서 공유 이름을 클릭하여 공유에 대한 자세한 정보를 봅니다.

표 113 공유 정보

항목	설명
Share Name	공유의 이름입니다(예: share1).
Directory Path	공유의 디렉토리 경로입니다(예: `/data/col1/backup/dir1`). 참고 col1은 소문자 L 다음에 숫자 1을 사용합니다.
Directory Path Status	DDR에 구성된 디렉토리 경로가 존재하는지 여부를 나타냅니다. 가능한 값은 Path Exists 또는 Path Does Not Exist이며 후자는 CIFS 구성이 잘못되었거나 불완전함을 나타냅니다.
Max Connections	한 번에 공유에 허용되는 최대 접속 수입니다. 기본값은 Unlimited입니다.
설명	공유가 생성되었을 때 구성된 설명입니다.
Share Status	공유의 상태로, Enabled 또는 Disabled입니다.

- Clients 영역에는 공유에 액세스하도록 구성된 클라이언트의 목록과 그 아래에 클라이언트 수가 표시됩니다.
- User/Groups 영역에는 공유에 액세스하도록 구성된 사용자나 그룹의 이름 및 유형의 목록과 그 아래에 사용자 또는 그룹 수가 표시됩니다.
- Options 영역에는 구성된 옵션의 이름과 값이 나열됩니다.

CIFS 통계 표시

명령줄을 사용해 CIFS 통계를 표시합니다.

절차

- 다음을 입력합니다. **`cifs show detailed-stats`**

  수신된 다양한 SMB 요청의 수와 이러한 요청을 처리하는 데 걸린 시간이 출력에 표시됩니다.

CIFS 문제 해결 수행

이 섹션에서는 기본적인 문제 해결 절차를 제공합니다.

참고

`cifs troubleshooting` 명령은 CIFS 사용자 및 그룹에 대한 자세한 정보를 제공합니다.

클라이언트 현재 작업 표시

명령줄을 사용해 CIFS 세션을 표시하고 파일 정보를 엽니다.

절차

- **`cifs show active`**를 입력합니다.

결과

표 114 세션

컴퓨터	사용자	열린 파일	연결 시간(초)	유휴 시간(초)
::ffff:10.25.132.84	ddve-25179109\sysadmin	1	92	0

표 115 열린 파일

사용자	모드	잠금	파일
ddve-25179109\sysadmin	1	0	C:\data\col1\backup

접속에서 열린 최대 파일 수 설정

명령줄을 사용해 동시에 열릴 수 있는 최대 파일 수를 설정합니다.

절차

- **`cifs option set max-global-open-files`** *value*를 입력합니다.

  전역으로 열린 최대 파일 수에 대한 *value*는 1부터 열릴 수 있는 최대 파일 제한 개수까지 될 수 있습니다. 최대 제한은 DDR 시스템 메모리를 바탕으로 합니다. 12GB보다 큰 시스템의 경우 열린 파일의 최대 제한은 30,000개입니다. 12GB 이하 시스템의 경우 열린 파일의 최대 제한은 10,000개입니다.

  표 116 접속 및 최대 열린 파일 제한

DDR 모델	메모리	연결 제한	열려 있는 파일의 최대 제한
DD620, DD630, DD640	8GB	300	10,000
DD640	16GB	600	30,000
DD640	20GB	600	30,000

표 116 접속 및 최대 열린 파일 제한 (계속)

DDR 모델	메모리	연결 제한	열려 있는 파일의 최대 제한
DD860	36GB	600	30,000
DD860, DD860ArT	72GB	600	30,000
	96GB	600	30,000
	128GB	600	30,000
	256GB	600	30,000

참고

시스템에는 최대 제한으로 CIFS 접속 600개와 열린 파일 250,000개가 적용됩니다. 그러나 열린 파일 수에 대한 제한이 부족하면 파일 개수를 늘릴 수 있습니다.

참고

파일 액세스 지연 시간은 디렉토리에 있는 파일 수에 영향을 받습니다. 가급적이면 디렉토리 크기를 250,000개 미만의 파일로 제한하는 것이 좋습니다. 디렉토리 크기가 이보다 크면 디렉토리에 파일을 나열하고 파일을 열거나 생성하는 것과 같은 메타데이터 작업에 대한 응답 속도가 느려질 수 있습니다.

Data Domain 시스템 클록

CIFS 액세스를 위해 Active Directory 모드를 사용할 경우 Data Domain 시스템 클록 시간은 도메인 컨트롤러와 5분 이하로 차이가 날 수 있습니다.

클록과 시간 서버는 DD System Manager의 **Administration** > **Settings** > **Time and Date Settings** 탭에서 동기화됩니다.

Windows 도메인 컨트롤러가 외부 소스에서 시간을 가져오기 때문에 NTP를 반드시 구성해야 합니다. Windows 운영 체제 버전 또는 도메인 컨트롤러에서 실행 중인 서비스 팩에 맞게 NTP를 구성하는 방법은 Microsoft 설명서를 참조하십시오.

Active Directory 인증 모드에서 Data Domain 시스템은 Windows Active Directory 도메인 컨트롤러와 클록을 주기적으로 동기화합니다.

Windows 도메인 컨트롤러에서 동기화

Windows 도메인 컨트롤러에서 명령줄을 사용해 NTP 서버와 동기화합니다.

참고

이 예는 Windows 2003 SP1에 해당됩니다. NTP 서버 이름(*ntpservername*)에 대한 도메인 서버를 대체하십시오.

절차

1. Windows 시스템에 다음과 유사한 명령을 입력합니다.

   ```
   C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-server-name C:\>w32tm /config /update C:\>w32tm /resync
   ```

2. 도메인 컨트롤러에서 NTP가 구성된 후에 시간 및 날짜 설정으로 작업하는 방법에 대한 섹션에 설명된 대로 시간 서버 동기화를 구성합니다.

NTP 서버에서 동기화

시간 및 날짜 설정 작업과 관련된 섹션에 설명된 대로 시간 서버 동기화를 구성합니다.

9장

NFS

이 장에서 다루는 내용은 다음과 같습니다.

NFS 개요

NFS 클라이언트는 Data Domain 시스템의 시스템 디렉토리나 MTree에 액세스할 수 있습니다.

- `/backup` 디렉토리는 MTree가 아닌 압축된 백업 서버 데이터에 대한 기본 대상입니다.
- 압축된 백업 서버 데이터용으로 MTree를 사용하는 경우에는 `/data/col1/backup` 경로가 루트 대상입니다.
- `/ddvar/core` 디렉토리에는 Data Domain 시스템의 핵심 파일과 로그 파일이 포함되어 있습니다. 이 영역에서 공간을 확보하려면 이전 로그와 핵심 파일을 제거해야 합니다.

참고

Data Domain 시스템에서 `/ddvar/core`는 별도의 파티션에 있습니다. `/ddvar`만 마운트하는 경우 `/ddvar` 마운트 지점에서 `/ddvar/core`로 이동할 수 없습니다.

Data Domain 시스템을 사용해 백업 및 복원 작업을 수행하는 백업 서버와 같은 클라이언트는 `/backup` 또는 `/data/col1/backup` 영역에 액세스할 수 있어야 합니다. 관리 액세스 권한이 있는 클라이언트는 `/ddvar/core` 디렉토리에 액세스하여 핵심 파일과 로그 파일을 검색할 수 있어야 합니다.

초기 Data Domain 시스템 구성의 일부로 NFS 클라이언트는 이 영역에 액세스할 수 있도록 구성되었습니다. 이 장에서는 이 설정을 수정하는 방법과 데이터 액세스를 관리하는 방법을 설명합니다.

참고

- 초기 시스템 구성에 대한 자세한 내용은 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.
- `nfs` 명령은 백업을 관리하고 NFS 클라이언트 및 Data Domain 시스템 사이를 복원하며 NFS 통계 및 상태를 표시합니다. `nfs` 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.
- Data Domain 시스템을 서버로 사용하도록 타사 클라이언트를 설정하는 방법에 대한 정보는 Data Domain 지원 웹 사이트에 제공되는 *Solaris System Tuning* 같은 관련 튜닝 가이드를 참조하십시오. Documentation > Integration Documentation 페이지의 목록에서 공급업체를 선택하고 **OK**를 클릭합니다. 목록에서 튜닝 가이드를 선택합니다.

HA 시스템과 NFS

HA 시스템은 NFS와 호환됩니다. 페일오버 시에 NFS 작업이 진행 중이더라도 나중에 작업을 다시 시작할 필요가 **없습니다**.

참고

/ddvar은 ext3 파일 시스템으로, 일반 MTree 기반 공유처럼 공유할 수 없습니다. 액티브 노드가 대기 노드로 페일오버되면 두 노드의 파일 핸들이 서로 달라지므로 /ddvar의 정보가 더 이상 유효하지 않게 됩니다. 로그 파일에 액세스하거나 시스템을 업그레이드하기 위해 /ddvar을 마운트한 경우, /ddvar을 마지막으로 마운트한 후 페일오버가 실행되었다면 /ddvar을 마운트 해제한 후 다시 마운트하십시오.

HA로 페일오버를 수행할 유효한 NFS 내보내기를 생성하려면 내보내기를 액티브 HA 노드에서 생성해야 하며 일반적으로 페일오버 네트워크 인터페이스를 통해 공유해야 합니다.

Data Domain 시스템에 대한 NFS 클라이언트 액세스 관리

이 섹션의 항목에서는 Data Domain 시스템에 대한 NFS 클라이언트 액세스를 관리하는 방법에 대해 설명합니다.

https://support.emc.com/kb/180552에서 사용할 수 있는 KB 문서, *Data Domain 및 클라이언트 OS에 대한 NFS 모범 사례*에서는 NFS용 모범 사례에 대한 추가 정보를 제공합니다.

NFS 서비스 설정

클라이언트가 NFS 프로토콜을 사용하여 시스템에 액세스할 수 있도록 NFS 서비스를 설정합니다.

절차

1. **Protocols** > **NFS**를 선택합니다.

   NFS 보기가 열리고 Exports 탭이 표시됩니다.

2. **Enable**을 클릭합니다.

NFS 서비스 해제

클라이언트가 NFS 프로토콜을 사용하여 시스템에 액세스하지 못하도록 NFS 서비스를 해제합니다.

절차

1. **Protocols** > **NFS** 탭을 선택합니다.

   NFS 보기가 열리고 Exports 탭이 표시됩니다.

2. **Disable**을 클릭합니다.

내보내기 생성

NFS 보기에 있는 Data Domain System Manager의 Create 버튼이나 구성 마법사를 사용하여 `/backup`, `/data/col1/backup`, `/ddvar`, `/ddvar/core` 영역이나 `/ddvar/ext` 영역(있는 경우)에 액세스할 수 있는 NFS 클라이언트를 지정할 수 있습니다.

Data Domain 시스템은 최대 2,048개의 내보내기를 지원하며, [2] 시스템 메모리에 따라 접속 수가 확장됩니다.

2. 이 수는 하드웨어 제한에 따라 달라질 수 있습니다.

참고

각 내보내기별로 클라이언트 액세스를 할당하고 각 내보내기별로 액세스를 제거해야 합니다. 예를 들어 클라이언트를 `/ddvar`에서 제거해도 `/data/col1/backup`에 계속 해서 액세스할 수 있습니다.

⚠ 주의

복제를 구현하는 경우 단일 대상 Data Domain 시스템은 각각에 대해 별도의 디렉토리 또는 MTree가 사용되는 한 CIFS 클라이언트와 NFS 클라이언트 모두로부터 백업을 수신할 수 있습니다. 동일한 영역에서 CIFS 및 NFS 데이터를 함께 저장하지 마십시오.

절차

1. **Protocols > NFS**를 선택합니다.

   NFS 보기가 열리고 Exports 탭이 표시됩니다.

2. **Create**를 클릭합니다.
3. Directory Path 입력란에 경로 이름을 입력합니다(예: `/data/col1/backup/dir1`).

   참고

   `col1` 소문자 L 뒤에 숫자 1을 사용한 것입니다.

4. Clients 영역에서 기존 클라이언트를 선택하거나 **+** 아이콘을 클릭하여 클라이언트를 생성합니다.

   Client 대화 상자가 표시됩니다.

   a. 입력란에 서버 이름을 입력합니다.

   정규화된 도메인 이름, 호스트 이름 또는 IP 주소를 입력할 수 있습니다. 별표(*) 하나는 와일드카드로서 모든 백업 서버가 클라이언트로 사용됨을 나타냅니다.

   참고

   `/data/col1/backup` 디렉토리에 대한 액세스 권한이 부여된 클라이언트는 전체 디렉토리에 액세스할 수 있습니다. `/data/col1/backup`의 하위 디렉토리에 대한 액세스 권한이 부여된 클라이언트는 해당 하위 디렉토리만 액세스할 수 있습니다.

   - 클라이언트는 정규화된 도메인 호스트 이름, IPv4 또는 IPv6 IP 주소, 넷마스크 또는 접두사 길이가 포함된 IPv4 주소, 접두사 길이가 포함된 IPv6 주소, `@` 접두사가 포함된 NIS 넷그룹 이름 또는 도메인 이름이 포함된 별표(*) 와일드카드(예: `*.yourcompany.com`)일 수 있습니다.
   - `/data/col1/backup`의 하위 디렉토리에 추가된 클라이언트는 해당 하위 디렉토리에만 액세스할 수 있습니다.
   - 네트워크의 모든 클라이언트에 액세스 권한을 부여하려면 클라이언트 목록으로 별표(*)를 입력합니다.

   b. 클라이언트에 해당하는 NFS 옵션의 확인란을 선택합니다.

   General:

- 읽기 전용 권한(ro)
- 1024 미만의 포트에서 접속 허용(secure)(기본값)

Anonymous UID/GID:

- UID(User Identifier) 또는 GID(Group Identifier) 0의 요청을 익명 UID/GID에 매핑(root _squash)
- 모든 사용자 요청을 익명 UID/GID에 매핑(all _squash)
- 기본 익명 UID/GID 사용

Allowed Kerberos Authentication Modes:

- 인증되지 않은 접속(sec=sys). 인증을 사용하지 않으려면 선택합니다.
- 인증된 접속(sec=krb5)

참고

무결성과 개인 정보 보호가 지원되지만, 이로 인해 성능이 상당히 저하될 수 있습니다.

c. **OK**를 클릭합니다.

5. **OK**를 클릭하여 내보내기를 생성합니다.

내보내기 수정

GUI를 사용해 디렉토리 경로, 도메인 이름 및 기타 옵션을 변경합니다.

절차

1. **Protocols** > **NFS**를 선택합니다.

   NFS 보기가 열리고 Exports 탭이 표시됩니다.

2. NFS Exports 표에서 내보내기에 해당하는 확인란을 클릭합니다.
3. **Modify**를 클릭합니다.
4. Directory Path 입력란에서 경로 이름을 수정합니다.
5. Clients 영역에서 다른 클라이언트를 선택하고 연필 모양 아이콘(수정)을 클릭하거나 **+** 아이콘을 클릭하여 클라이언트를 생성합니다.

   a. Client 입력란에 서버 이름을 입력합니다.

   정규화된 도메인 이름, 호스트 이름 또는 IP 주소를 입력할 수 있습니다. 별표(*) 하나는 와일드카드로서 모든 백업 서버가 클라이언트로 사용됨을 나타냅니다.

   참고

   `/data/col1/backup` 디렉토리에 대한 액세스 권한이 부여된 클라이언트는 전체 디렉토리에 액세스할 수 있습니다. `/data/col1/backup`의 하위 디렉토리에 대한 액세스 권한이 부여된 클라이언트는 해당 하위 디렉토리만 액세스할 수 있습니다.

   - 클라이언트는 정규화된 도메인 호스트 이름, IPv4 또는 IPv6 IP 주소, 넷마스크 또는 접두사 길이가 포함된 IPv4 주소, 접두사 길이가 포함된 IPv6 주소, `@` 접두사가 포함된 NIS 넷그룹 이름 또는 도메인 이름이 포함된 별표(*) 와일드카드(예: **`*.yourcompany.com`**)일 수 있습니다.

/data/col1/backup의 하위 디렉토리에 추가된 클라이언트는 해당 하위 디렉토리에만 액세스할 수 있습니다.

- 네트워크의 모든 클라이언트에 액세스 권한을 부여하려면 클라이언트 목록으로 별표(*)를 입력합니다.

b. 클라이언트에 해당하는 NFS 옵션의 확인란을 선택합니다.

General:

- 읽기 전용 권한(ro)
- 1024 미만의 포트에서 접속 허용(secure)(기본값)

Anonymous UID/GID:

- UID(User Identifier) 또는 GID(Group Identifier) 0의 요청을 익명 UID/GID에 매핑(root _squash)
- 모든 사용자 요청을 익명 UID/GID에 매핑(all _squash)
- 기본 익명 UID/GID 사용

Allowed Kerberos Authentication Modes:

- 인증되지 않은 접속(sec=sys). 인증을 사용하지 않으려면 선택합니다.
- 인증된 접속(sec=krb5)

참고

Integrity와 Privacy는 지원되지 않습니다.

c. **OK**를 클릭합니다.

6. **OK**를 클릭하여 내보내기를 수정합니다.

기존 내보내기에서 내보내기 생성

기존 내보내기에서 내보내기를 생성한 후 필요에 따라 수정합니다.

절차

1. NFS Exports 탭에서 소스로 사용할 내보내기의 확인란을 클릭합니다.
2. **Create From**을 클릭합니다.
3. 내보내기 수정 섹션에 있는 설명처럼 내보내기 정보를 수정합니다.

내보내기 삭제

NFS Exports 탭에서 내보내기를 삭제합니다.

절차

1. NFS Exports 탭에서 삭제할 내보내기의 확인란을 클릭합니다.
2. **Delete**를 클릭합니다.
3. **OK** 및 **Close**를 차례로 클릭하여 내보내기를 삭제합니다.

NFS 정보 표시

이 섹션의 항목에서는 DD System Manager를 사용하여 NFS 클라이언트 상태와 NFS 구성을 모니터링하는 방법에 대해 설명합니다.

NFS 상태 보기

NFS가 활성 상태인지 여부와 Kerberos의 설정 여부를 표시합니다.

절차

- **Protocols** > **NFS**를 클릭합니다.

  위쪽 패널에 NFS의 작동 상태가 표시됩니다. 예를 들어 NFS가 현재 활성 상태이고 실행 중인지 여부와 Kerberos 모드가 설정되어 있는지 여부가 표시됩니다.

  참고

  Configure를 클릭하여 **Administration** > **Access** > **Authentication** 탭을 표시하고 Kerberos 인증을 구성합니다.

NFS 내보내기 보기

Data Domain 시스템에 액세스할 수 있는 클라이언트 목록을 봅니다.

절차

1. **Protocols** > **NFS**를 클릭합니다.

   내보내기 보기에 Data Domain 시스템에 대해 구성된 NFS 내보내기 테이블과 각 내보내기의 마운트 경로, 상태 및 NFS 옵션이 표시됩니다.

2. Export in the Table를 클릭해 Exports 표 아래에 있는 Detailed Information 영역을 채웁니다.

   시스템에 내보내기의 디렉토리 경로, 구성된 옵션 및 상태 외에 클라이언트 목록이 표시됩니다.

   마운트 경로를 기준으로 정렬하려면 Filter By 입력란을 사용합니다.

   테이블을 새로 고치고 제공된 필터를 사용하려면 시스템의 **Update**를 클릭합니다.

   경로와 클라이언트 필터를 지우려면 시스템의 **Reset**을 클릭합니다.

활성 NFS 클라이언트 보기

지난 15분 동안 접속한 모든 클라이언트와 해당 마운트 경로를 표시합니다.

절차

- **Protocols** > **NFS** > **Active Clients** 탭을 선택합니다.

  Active Clients 보기에는 지난 15분 동안 접속된 모든 클라이언트와 해당 마운트 경로가 표시됩니다.

  마운트 경로와 클라이언트 이름을 기준으로 정렬하려면 Filter By 입력란을 사용합니다.

  테이블을 새로 고치고 제공된 필터를 사용하려면 시스템의 **Update**를 클릭합니다.

경로와 클라이언트 필터를 지우려면 시스템의 **Reset**을 클릭합니다.

Kerberos 도메인에 DDR 통합

DDR에 대한 도메인 이름, 호스트 이름 및 DNS 서버를 설정하십시오.

키 배포 센터(UNIX의 경우) 및 배포 센터(Windows Active Directory의 경우)로 인증 서버를 사용하도록 DDR을 설정합니다.

⚠ 주의

이 설명에 제공된 예제는 이 방식을 개발하는 데 사용되는 OS(Operating System)에만 적용됩니다. 사용 중인 OS에 맞는 명령을 사용해야 합니다.

참고

UNIX Kerberos 모드의 경우 keytab 파일이 생성된 KDC(Key Distribution Center) 서버에서 DDR로 파일을 전송해야 합니다. DDR을 한 개 이상 사용 중인 경우 DDR마다 별도의 keytab 파일이 필요합니다. keytab 파일에는 KDC 서버와 DDR 간에 공유된 암호가 포함되어 있습니다.

참고

UNIX KDC를 사용할 때 DNS 서버는 KDC 서버가 아니어도 무관하며 별도의 서버일 수 있습니다.

절차

1. DDR 명령을 사용하여 DDR에 대한 호스트 이름과 도메인 이름을 설정합니다.

   ```
   net set hostname <host>
   net set {domainname <local-domain-name>}
   ```

   참고

   호스트 이름은 DDR의 이름입니다.

2. KDC(Key Distribution Center)에서 DDR에 대한 NFS 보안 주체(노드)를 구성합니다.

   예:

   ```
   addprinc nfs/hostname@realm
   ```

   참고

   호스트 이름은 DDR의 이름입니다.

3. KDC에 보안 주체로 추가된 nfs 항목이 있는지 확인합니다.

   예:

   ```
   listprincs
   nfs/hostname@realm
   ```

4. keytab 파일에 DDR 보안 주체를 추가합니다.

   예:

   ```
   ktadd <keytab_file> nfs/hostname@realm
   ```

5. KDC에 구성된 nfs keytab 파일이 있는지 확인합니다.

   예:
   klist -k <keytab_file>

   참고

   <keytab_file>은 이전 단계에서 키를 구성하는 데 사용한 keytab 파일입니다.

6. NFS DDR에 대한 키가 생성된 위치에서 /ddvar/ 디렉토리의 DDR로 keytab 파일을 복사합니다.

   표 117 Keytab 대상

복사 시작 위치:	복사 대상 위치:
<keytab_file>(keytab 파일은 이전 단계에서 구성함)	/ddvar/

7. 다음 DDR 명령을 사용하여 DDR에서 영역을 설정합니다.

   authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdcs <IP address of server>

8. kdc-type이 UNIX이면 /ddvar/의 keytab 파일을 Kerberos 구성 파일 위치인 /ddr/etc/로 가져옵니다. 다음 DDR 명령을 사용하여 파일을 복사합니다.

   authentication kerberos keytab import

   알림

   이 단계는 kdc-type이 UNIX인 경우에만 필요합니다.

   Kerberos 설정이 완료되었습니다.

9. NFS 마운트 지점을 추가해 Kerberos를 사용하려면 nfs add 명령을 사용합니다.

   자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

10. KDC(Key Distribution Center)의 각 NFS 클라이언트에 대해 호스트, NFS 및 관련 사용자 보안 주체를 추가합니다.

    예: **listprincs**

```
host/hostname@realm
nfs/hostname@realm
root/hostname@realm
```

11. NFS 클라이언트마다 클라이언트의 keytab 파일로 해당 보안 주체를 모두 가져옵니다.

    예:
    ktadd -k <keytab_file> host/hostname@realm

    ktadd -k <keytab_file> nfs/hostname@realm

초기 구성 후 KDC 서버 추가 및 삭제

Kerberos 도메인에 DDR을 통합하고 이에 따라 키 배포 센터(UNIX의 경우) 및 배포 센터(Windows Active Directory의 경우)로 인증 서버를 사용하도록 DDR를 설정한 후에 다음 절차에 따라 KDC 서버를 추가하거나 삭제할 수 있습니다.

절차

1. Windows AD(Active Directory) 서버 또는 UNIX KDC(Key Distribution Center)에 DDR을 연결합니다.

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   예: **authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test**

   이 명령은 시스템을 krb5.test 영역에 연결하고 NFS 클라이언트에 대해 Kerberos 인증을 설정합니다.

   참고

   이 KDC에서 생성된 keytab이 DDR에 있어야만 Kerberos를 사용해 인증할 수 있습니다.

   ---

2. Kerberos 인증 구성을 확인합니다.

   authentication kerberos show config

   ```
   Home Realm:          krb5.test
   KDC List:            nfskrb-kdc.krb5.test
   KDC Type:            unix
   ```

3. 두 번째 KDC 서버를 추가합니다.

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   예: **authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test**

   참고

   이 KDC에서 생성된 keytab이 DDR에 있어야만 Kerberos를 사용해 인증할 수 있습니다.

   ---

4. 두 KDC 서버가 추가되었는지 확인합니다.

   authentication kerberos show config

   ```
   Home Realm:          krb5.test
   KDC List:            ostqa-sparc2.krb5.test, nfskrb-
   kdc.krb5.test
   KDC Type:            unix
   ```

5. Kerberos 구성 키에 대한 값을 표시합니다.

   reg show config.keberos

   ```
   config.kerberos.home_realm = krb5.test
   config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
   config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
   config.kerberos.kdc_count = 2
   config.kerberos.kdc_type = unix
   ```

6. KDC 서버를 삭제합니다.

   삭제하려는 KDC 서버를 나열하지 않고 **authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}** 명령을 사용해 KDC 서버를 삭제합니다. 예를 들어 기존 KDC 서버가 kdc1, kdc2 및 kdc3이고 영역에서 kdc2를 제거하려는 경우 다음과 같은 예를 사용할 수 있습니다.

```
authentication kerberos set realm <realm-name> kdc-type
<kdc_type> kdcs kdc1,kdc3
```

10장

NFSv4

이 장에서 다루는 내용은 다음과 같습니다.

NFSv4 소개

NFS 클라이언트는 점차 NFSv4.x를 기본 NFS 프로토콜 레벨로 사용하기 때문에 이제 클라이언트가 이전 버전과의 호환성 모드로 작동하지 않고도 Data Domain 시스템에서 NFSv4를 사용할 수 있습니다.

Data Domain 시스템에서 클라이언트는 혼합 환경에서 작동할 수 있습니다. 즉, NFSv4와 NFSv3를 통해 동일한 NFS 내보내기에 액세스할 수 있습니다.

사이트 요구 사항에 따라 NFSv4 및 NFSv3를 지원하도록 Data Domain NFS 서버를 구성할 수 있습니다. 각 NFS 내보내기를 NFSv4 클라이언트에만 사용하거나, NFSv3 클라이언트에만 사용하거나, 둘 모두에 사용할 수 있습니다.

NFSv4를 선택할지, NFSv3를 선택할지는 여러 가지 요인에 따라 달라질 수 있습니다.

- NFS 클라이언트 지원
  일부 NFS 클라이언트는 NFSv3만 지원하거나 NFSv4만 지원할 수 있으며, 하나의 버전을 사용할 때 더욱 효과적으로 작동할 수 있습니다.
- 작업 요구 사항
  기업에 따라 NFSv4 또는 NFSv3 중 하나만 사용하도록 엄격하게 표준화되어 있을 수 있습니다.
- 보안
  더 강력한 보안이 필요한 경우 NFSv4가 ACL과 확장된 소유자 및 그룹 구성을 비롯하여 NFSv3보다 더 높은 수준의 보안을 제공합니다.
- 기능 요구 사항
  바이트 범위 잠금 또는 UTF-8 파일이 필요한 경우 NFSv4를 선택해야 합니다.
- NFSv3 서브 마운트
  기존 구성에서 NFSv3 서브 마운트를 사용하는 경우 NFSv3를 선택하는 것이 적합할 수 있습니다.

Data Domain 시스템에서 사용 시 NFSv4와 NFSv3 비교

NFSv4는 NFSv3에 비해 향상된 기능을 제공합니다.

다음 표에서는 NFSv4 기능을 NFSv3 기능과 비교합니다.

표 118 NFSv4와 NFSv3 비교

기능	NFSv3	NFSv4
표준 기반 네트워크 파일 시스템	지원	지원
Kerberos 지원	지원	지원
Kerberos와 LDAP	지원	지원
할당량 보고	지원	지원
클라이언트 기반 액세스 목록을 포함한 다중 내보내기	지원	지원
ID 매핑	지원	지원
UTF-8 문자 지원	지원 안 함	지원
파일/디렉토리 기반 ACL(Access Control List)	지원 안 함	지원
확장 소유자/그룹(OWNER@)	지원 안 함	지원

표 118 NFSv4와 NFSv3 비교 (계속)

기능	NFSv3	NFSv4
파일 공유 잠금	지원 안 함	지원
바이트 범위 잠금	지원 안 함	지원
DD CIFS 통합(잠금, ACL, AD)	지원 안 함	지원
상태 저장 파일 열기 및 복구	지원 안 함	지원
글로벌 네임스페이스 및 pseudoFS	지원 안 함	지원
참조를 사용한 다중 시스템 네임스페이스	지원 안 함	지원

NFSv4 포트

NFSv4와 NFSv3를 독립적으로 활성화하거나 비활성화할 수 있습니다. 또한, NFS 버전을 다른 포트로 이동할 수 있습니다. 두 버전이 모두 동일한 포트를 사용할 필요는 없습니다.

NFSv4를 사용하는 경우 포트를 변경하기 위해 Data Domain 파일 시스템을 다시 시작할 필요가 없습니다. 그러한 경우 NFS만 다시 시작하면 됩니다.

NFSv3와 마찬가지로 NFSv4는 기본적으로 포트 2049(활성화된 경우)에서 실행됩니다.

NFSv4는 portmapper(포트 111) 또는 mountd(포트 2052)를 사용하지 않습니다.

ID 매핑 개요

NFSv4는 소유자와 그룹을 일반 외부 형식(예: `joe@example.com`)으로 식별합니다. 이러한 일반적인 형식을 ID라고 합니다.

ID는 NFS 서버에 저장되며 ID 12345 또는 ID S-123-33-667-2와 같은 내부 표현을 사용합니다. 내부 ID와 외부 ID 간의 변환을 ID 매핑이라고 합니다.

ID는 다음에 연결되어 있습니다.

- 파일 및 디렉토리 소유자
- 파일 및 디렉토리 소유자 그룹
- ACL(Access Control List) 항목

Data Domain 시스템은 NFS와 CIFS/SMB 프로토콜에 공통된 내부 형식을 사용하므로 NFS와 CIFS/SMB 간에 파일과 디렉토리를 공유할 수 있습니다. 각 프로토콜은 자체 ID 매핑을 통해 내부 형식을 고유한 외부 형식으로 변환합니다.

외부 형식

NFSv4 ID의 외부 형식은 NFSv4 표준을 따릅니다(예: NFSv4.0의 경우 RFC-7530). 또한 상호 운용성을 위해 추가 형식이 지원됩니다.

표준 ID 형식

NFSv4의 표준 외부 ID는 *identifier@domain* 형식을 갖습니다. 이 ID는 NFSv4 소유자, 소유자 그룹 및 ACE(Access Control Entry)에 사용됩니다. 도메인은 `nfs option` 명령을 사용하여 설정된 구성된 NFSv4 도메인과 일치해야 합니다.

다음 CLI 예에서는 Data Domain NFS 서버에 대해 NFSv4 도메인을 `mycorp.com`으로 설정합니다.

```
nfs option set nfs4-domain mycorp.com
```

클라이언트 NFS 도메인 설정에 대한 자세한 내용은 해당 클라이언트 관련 문서를 참조하십시오. 운영 체제에 따라 구성 파일(예: `/etc/idmapd.conf`)을 업데이트하거나 클라이언트 관리 툴을 사용해야 할 수도 있습니다.

참고

기본값을 설정하지 않으면 Data Domain 시스템의 DNS 이름을 따릅니다.

참고

파일 시스템을 자동으로 업데이트하려면 nfs4-domain에 대한 DNS 도메인을 변경한 후 다시 시작해야 합니다.

ACE 확장 ID

ACL ACE 항목에 대해 Data Domain NFS 서버는 NFSv4 RFC에서 정의된 다음과 같은 표준 NFSv4 ACE 확장 ID를 지원합니다.

- OWNER@, 파일 또는 디렉토리의 현재 소유자
- GROUP@, 파일 또는 디렉토리의 현재 소유자 그룹
- 특별 ID INTERACTIVE@, NETWORK@, DIALUP@, BATCH@, ANONYMOUS@, AUTHENTICATED@, SERVICE@.

대체 형식

상호 운용성을 허용하기 위해 Data Domain 시스템의 NFSv4 서버는 입력 및 출력에 일부 대체 ID 형식을 지원합니다.

- 숫자 ID(예: "12345")
- "S-NNN-NNN-..."으로 표시되는 Windows 호환 SID(Security Identifier)

이러한 형식의 제한 사항에 대한 자세한 내용은 입력 매핑 및 출력 매핑 섹션을 참조하십시오.

내부 ID 형식

Data Domain 파일 시스템에는 파일 시스템의 각 객체(파일 또는 디렉토리)와 함께 ID가 저장됩니다. 모든 객체는 숫자 UID(User ID) 및 GID(Group ID)를 갖습니다. 모드 비트 집합과 함께 이를 통해 기존 UNIX/Linux를 식별하고 액세스를 제어할 수 있습니다.

CIFS/SMB 프로토콜 또는 NFSv4(NFSv4 ACL이 활성화된 경우)에 의해 생성되는 객체도 확장된 SD(Security Descriptor)를 갖습니다. 각 SD에는 다음이 포함됩니다.

- 소유자 SID(Security Identifier)
- 소유자 그룹 SID
- DACL(Discretionary ACL)
- (선택 사항) SACL(System ACL)

각 SID에는 Windows SID와 비슷한 방식으로 RID(Relative ID) 및 별도의 도메인이 포함되어 있습니다. SID와 SID 매핑에 대한 자세한 내용은 자세한 내용은 NFSv4 및 CIFS 상호 운용성 섹션을 참조하십시오.

ID 매핑 시

Data Domain NFSv4 서버는 다음과 같은 경우에 매핑을 수행합니다.

- 입력 매핑
  Data Domain NFS 서버는 NFSv4 클라이언트에서 ID를 받습니다. 자세한 내용은 입력 매핑(271페이지) 섹션을 참조하십시오.
- 출력 매핑:
  Data Domain NFS 서버에서 NFSv4 클라이언트로 ID가 전송됩니다. 자세한 내용은 출력 매핑(271페이지) 섹션을 참조하십시오.
- 자격 증명 매핑
  RPC 클라이언트 자격 증명은 액세스 제어 및 기타 작업을 위해 내부 ID에 매핑됩니다. 자세한 내용은 자격 증명 매핑(272페이지) 섹션을 참조하십시오.

입력 매핑

입력 매핑은 NFSv4 클라이언트가 Data Domain NFSv4 서버로 ID를 전송하는 경우에 이루어집니다. 예를 들어 파일의 소유자 또는 소유자 그룹을 설정하는 경우에 입력 매핑이 이루어집니다. 입력 매핑은 자격 증명 매핑과 구별됩니다. 자격 증명 매핑에 대한 자세한 내용은 xxxx 섹션을 참조하십시오.

`joe@mycorp.com` 같은 표준 형식 ID는 구성된 변환 규칙에 따라 내부 UID/GID로 변환됩니다. NFSv4 ACL이 활성화된 경우 구성된 변환 규칙에 따라 SID도 생성됩니다.

숫자 ID(예: "12345")는 클라이언트에서 Kerberos 인증을 사용하지 않는 경우 해당 UID/GID로 직접 변환됩니다. Kerberos를 사용하는 경우 NFSv4 표준에서 권장하는 대로 오류가 생성됩니다. NFSv4 ACL이 활성화된 경우 변환 규칙에 따라 SID가 생성됩니다.

Windows SID(예: "S-NNN-NNN-...")는 유효성이 검사되고 직접 해당 SID로 변환됩니다. UID/GID는 변환 규칙에 따라 생성됩니다.

출력 매핑

출력 매핑은 NFSv4 서버가 NFSv4 클라이언트로 ID를 전송하는 경우에 이루어집니다. 예를 들어 서버가 파일의 소유자 또는 소유자 그룹을 반환하는 경우에 출력 매핑이 이루어집니다.

1. 구성된 경우 출력은 숫자 ID가 될 수 있습니다.
   이는 ID 매핑이 구성되지 않은 NFSv4 클라이언트(예: 일부 Linux 클라이언트)에 유용할 수 있습니다.
2. 매핑은 구성된 매핑 서비스(예: NIS 또는 Active Directory)를 사용하여 시도됩니다.
3. 매핑이 실패하고 구성이 허용된 경우 숫자 ID 또는 SID 문자열이 출력됩니다.
4. 그 외의 경우 nobody가 반환됩니다.

`nfs 옵션 nfs4-idmap-out-numeric`에 따라 출력에 대한 매핑이 구성됩니다.

- **`nfs 옵션 nfs4-idmap-out-numeric`**이 **`map-first`**로 설정된 경우 매핑이 시도됩니다. 오류 발생 시 숫자 문자열이 출력됩니다(허용된 경우). 기본값입니다.
- **`nfs 옵션 nfs4-idmap-out-numeric`**이 **`always`**로 설정된 경우 항상 숫자 문자열이 출력됩니다(허용된 경우).
- **`nfs 옵션 nfs4-idmap-out-numeric`**이 **`never`**로 설정된 경우 매핑이 시도됩니다. 오류 발생 시 **`nobody@nfs4-domain`**이 출력됩니다.
  RPC 접속에 GSS/Kerberos가 사용되는 경우 숫자 문자열이 전혀 허용되지 않고 **`nobody@nfs4-domain`**이 출력됩니다.

다음은 Data Domain NFS 서버가 항상 숫자 문자열을 출력하도록 구성하는 예입니다. Kerberos의 경우 nobody라는 이름이 반환됩니다.

```
nfs option set nfs4-idmap-out-numeric always
```

자격 증명 매핑

NFSv4 서버는 NFSv4 클라이언트에 대한 자격 증명을 제공합니다.

이러한 자격 증명은 다음과 같은 기능을 수행합니다.

- 작업에 대한 액세스 정책(예: 파일 읽기 권한) 결정
- 새 파일 및 디렉토리에 대한 기본 소유자 및 소유자 그룹 결정

클라이언트에서 전송된 자격 증명은 `john_doe@mycorp.com` 또는 시스템 자격 증명(예: `UID=1000, GID=2000`)이 될 수 있습니다. 시스템 자격 증명은 UID/GID와 보조 그룹 ID를 지정합니다.

NFSv4 ACL이 비활성화된 경우 UID/GID 및 보조 그룹 ID가 자격 증명에 사용됩니다.

NFSv4 ACL이 활성화된 경우 구성된 매핑 서비스를 사용하여 자격 증명에 대한 확장된 보안 설명자가 작성됩니다.

- 소유자, 소유자 그룹 및 보조 그룹의 SID가 SD(Security Descriptor)에 매핑되고 추가됩니다.
- 자격 증명 권한(있는 경우) SD에 추가됩니다.

NFSv4와 CIFS/SMB의 상호 운용성

NFSv4와 CIFS에서 사용하는 보안 설명자는 ID 매핑 측면에서 유사하지만 차이점이 있습니다.

최적의 상호 운용성을 보장하기 위해 다음 사항에 유의해야 합니다.

- CIFS와 NFSv4 모두에 대해 Active Directory를 구성하고 ID 매핑에 Active Directory를 사용하도록 NFS ID 매퍼를 구성해야 합니다.
- CIFS ACL을 광범위하게 사용하는 경우 NFSv4 ACL도 활성화하면 일반적으로 호환성이 향상됩니다.
  - NFSv4 ACL을 활성화하면 DACL 액세스를 평가할 때 NFSv4 자격 증명을 적절한 SID에 매핑할 수 있습니다.
- CIFS 서버는 CIFS 클라이언트에서 기본 ACL과 사용자 권한을 포함한 자격 증명을 수신합니다.
  - 반면 NFSv4 서버는 보다 제한적인 자격 증명 집합을 수신하며 ID 매퍼를 사용하여 런타임에 자격 증명을 구성합니다. 이로 인해 파일 시스템에 다른 자격 증명이 표시될 수 있습니다.

CIFS/SMB Active Directory 통합

Data Domain CIFS 서버를 사용하여 설정된 Windows Active Directory 구성을 사용하도록 Data Domain NFSv4 서버를 구성할 수 있습니다.

Data Domain 시스템은 가능하면 Active Directory를 사용하여 매핑됩니다. 이 기능은 기본적으로 비활성화되어 있지만 다음 명령을 사용하여 활성화할 수 있습니다.

```
nfs option set nfs4-idmap-active-directory enabled
```

NFSv4용 기본 DACL

NFSv4는 CIFS에서 제공되는 기본 DACL과 다른 기본 DACL(Discretionary Access Control List)을 설정합니다.

OWNER@, GROUP@ 및 EVERYONE@만 기본 NFSv4 DACL에 정의됩니다. ACL 상속을 사용하여 기본적으로 CIFS 관련 ACE를 자동으로 추가할 수 있습니다(해당하는 경우).

시스템 기본값 SID

NFSv3에서 생성된 파일 및 디렉토리와 ACL 없이 NFSv4에서 생성된 파일 및 디렉토리는 기본 UNIX 도메인이라고도 하는 기본 시스템 도메인을 사용합니다.

- 시스템 도메인의 사용자 SID는 `S-1-22-1-N` 형식을 갖습니다. 여기서 N은 UID입니다.
- 시스템 도메인의 그룹 SID는 `S-1-22-2-N` 형식을 갖습니다. 여기서 N은 GID입니다.
  예를 들어 `UID 1234`인 사용자는 소유자 SID `S-1-22-1-1234`를 갖습니다.

NFSv4 ACL 및 SID의 공통 ID

NFSv4 ACL의 EVERYONE@ 식별자와 기타 특별 ID(예: BATCH@)는 해당 CIFS SID를 사용하며 호환됩니다.

OWNER@ 및 GROUP@ ID는 CIFS에 직접적으로 대응되지 않으며, 파일 또는 디렉토리의 현재 소유자 및 현재 소유자 그룹으로 표시됩니다.

NFS 참조

참조 기능을 통해 NFSv4 클라이언트가 하나 이상의 위치에 있는 내보내기(또는 파일 시스템)에 액세스할 수 있습니다. 위치는 동일한 NFS 서버 또는 다른 NFS 서버에 있을 수 있으며 동일하거나 다른 내보내기 경로를 사용할 수 있습니다.

참조는 NFSv4 기능이기 때문에 NFSv4 마운트에만 적용됩니다.

다음을 포함하여 NFSv4 이상을 사용하는 모든 서버에 대한 참조가 가능합니다.

- NFSv4를 활성화한 상태로 NFS를 실행하는 Data Domain 시스템
- Linux 서버, NAS 어플라이언스, VNX 시스템을 비롯하여 NFSv4를 지원하는 기타 서버

참조는 Data Domain 파일 시스템의 현재 기본 경로를 사용하거나 사용하지 않고 NFS 내보내기 지점을 사용할 수 있습니다.

참조가 포함된 NFS 내보내기를 NFSv3를 통해 마운트할 수 있지만, 참조는 NFSv4 기능이므로 NFSv3 클라이언트가 리디렉션되지 않습니다. 이 특성은 내보내기를 파일 관리 레벨에서 리디렉션할 수 있도록 하므로 스케일 아웃 시스템에 유용합니다.

참조 위치

NFSv4 참조는 항상 하나 이상의 위치를 갖습니다.

이러한 위치는 다음으로 구성됩니다.

- 참조된 파일 시스템에 대한 원격 NFS 서버 경로
- 클라이언트가 원격 NFS 서버에 연결할 수 있도록 허용하는 하나 이상의 서버 네트워크 주소

일반적으로 여러 서버 주소가 동일한 위치에 연결된 경우 동일한 NFS 서버에서 해당 주소를 찾을 수 있습니다.

참조 위치 이름

NFS 내보내기 내에 있는 각 참조 위치의 이름을 지정할 수 있습니다. 해당 이름을 사용하여 참조에 액세스하고 참조를 수정 또는 삭제할 수 있습니다.

참조 이름은 다음 문자 집합의 문자를 최대 80자 포함할 수 있습니다.

- a-z
- A-Z
- 0-9
- "."
- ","
- "_"
- "-"

참고

공백이 이름에 들어 있는 경우 공백을 포함할 수 있습니다. 공백이 포함된 경우 큰따옴표로 전체 이름을 묶어야 합니다.

"."로 시작하는 이름은 Data Domain 시스템에서 자동으로 생성되도록 예약되어 있습니다. 이러한 이름을 삭제할 수 있지만 CLI 또는 SMS(System Management Services)를 사용하여 생성하거나 수정할 수는 없습니다.

참조 및 스케일 아웃 시스템

Data Domain 시스템을 스케일 아웃하는 경우 NFSv4 참조 및 위치에서 더 효과적으로 액세스를 활성화할 수 있습니다.

Data Domain 시스템은 이미 글로벌 네임스페이스를 포함할 수도 있고 포함하지 않을 수도 있기 때문에 다음 두 가지 시나리오로 NFSv4 참조를 사용하는 방식을 설명할 수 있습니다.

- Data Domain 시스템에 글로벌 네임스페이스가 포함되지 않은 경우
  - NFSv4 참조를 사용하여 글로벌 네임스페이스를 작성할 수 있습니다. 시스템 관리자가 이러한 글로벌 네임스페이스를 생성하거나, 사용자가 지능적인 SM(System Manager) 요소를 사용해 필요에 따라 참조를 작성할 수 있습니다.
- Data Domain 시스템에 글로벌 네임스페이스가 포함된 경우
  - MTree가 특정 노드에 배치된 상태로 글로벌 네임스페이스가 시스템에 포함된 경우 NFS 참조를 생성하여 해당 MTree에 대한 액세스를 스케일 아웃 시스템에 추가된 노드로 리디렉션할 수 있습니다. 이러한 참조를 생성하거나, 필요한 SM 또는 FM(File Manager) 정보를 사용할 수 있는 경우 NFS 내에서 자동으로 이 작업을 수행할 수 있습니다.
    MTree에 대한 자세한 내용은 *Data Domain Operating System 관리 가이드*를 참조하십시오.

NFSv4 및 High Availability

NFSv4를 사용하는 경우 프로토콜 내보내기(예: `/data/col1/<mtree>`)가 HA(High Availability) 설정에 미러링됩니다. 그러나 `/ddvar` 같은 구성 내보내기는 미러링되지 않습니다.

/ddvar 파일 시스템은 HA 쌍의 각 노드에 고유합니다. 따라서 /ddvar 내보내기와 연결된 클라이언트 액세스 목록이 HA 환경에서 스탠바이 노드로 미러링되지 않습니다.

액티브 노드가 스탠바이 노드로 페일오버되면 /ddvar의 정보가 더 이상 유효하지 않습니다. 원래 액티브 노드에서 /ddvar에 부여된 모든 클라이언트 사용 권한을 페일오버 후 새로운 액티브 노드에서 재생성해야 합니다.

또한 원래 액티브 노드에서 생성된 모든 추가 /ddvar 내보내기와 클라이언트(예: /ddvar/core)를 페일오버 후 새로운 액티브 노드에 추가해야 합니다.

마지막으로, 원하는 모든 /ddvar 내보내기를 클라이언트에서 마운트 해제하고 페일오버 후에 다시 마운트해야 합니다.

NFSv4 글로벌 네임스페이스

NFSv4 서버는 NFS 내보내기를 검색 가능한 경로 세트로 연결하는 가상 디렉토리 트리(일명 PseudoFS)를 제공합니다.

PseudoFS 사용 여부에 따라 NFSv4와 NFSv3가 구분되며, NFSv3의 경우 MOUNTD 보조 프로토콜을 사용합니다.

대부분의 구성에서 NFSv3 MOUNTD를 NFSv4 글로벌 네임스페이스로 변경하는 작업은 환경에 영향을 미치지 않고 수행되며 NFSv4 클라이언트와 서버에 의해 자동으로 처리됩니다.

NFSv4 글로벌 네임스페이스 및 NFSv3 서브 마운트

NFSv3 내보내기 서브 마운트를 사용하는 경우 NFSv4의 글로벌 네임스페이스 특성으로 인해 서브 마운트가 NFSv4 마운트에서 표시되지 않을 수 있습니다.

예제 1 NFSv3 기본 내보내기 및 서브 마운트 내보내기

NFSv3에 기본 내보내기와 서브 마운트 내보내기가 있는 경우 이러한 내보내기가 동일한 NFSv3 클라이언트를 사용하지만 서로 다른 액세스 수준을 가질 수 있습니다.

표 119 NFSv3 기본 내보내기 및 서브 마운트 내보내기

Export	경로	클라이언트	옵션
Mt1	/data/col1/mt1	client1.example.com	ro
Mt1-sub	/data/col1/mt1/subdir	client1.example.com	rw

앞의 표에서 NFSv3에 다음 사항이 적용됩니다.

- client1.example.com이 /data/col1/mt1에 마운트되는 경우 클라이언트가 읽기 전용 액세스 권한을 갖습니다.
- client1.example.com이 /data/col1/mt1/subdir에 마운트되는 경우 클라이언트가 읽기/쓰기 액세스 권한을 갖습니다.

NFSv4는 최상위 내보내기 경로와 관련해서 같은 방식으로 작동합니다. NFSv4의 경우, client1.example.com은 NFSv4 PseudoFS를 이동하며 최상위 내보내기 경로 /data/col1/mt1에 도달한 후에 읽기 전용 액세스 권한을 갖습니다.

그러나 내보내기가 선택되었기 때문에 서브 마운트 내보내기(Mt1-sub)는 클라이언트에 대한 PseudoFS의 일부가 아니며 읽기/쓰기 액세스 권한이 부여되지 않습니다.

Best Practice
시스템이 NFSv3 내보내기 서브 마운트를 사용하여 마운트 경로를 기준으로 클라이언트에 읽기/쓰기 액세스 권한을 부여하는 경우 이러한 서브 마운트 내보내기와 함께 NFSv4를 사용하기 전에 이를 고려해야 합니다.

NFSv4를 사용하는 각 클라이언트가 개별 PseudoFS를 갖습니다.

표 120 NFSv3 submount exports

Export	경로	클라이언트	옵션
Mt1	`/data/col1/mt1`	client1.example.com	ro
Mt1-sub	`/data/col1/mt1/subdir`	client2.example.com	rw

NFSv4 구성

기본 Data Domain 시스템 구성만 NFSv3를 활성화합니다. NFSv4를 사용하려면 먼저 NFSv4 서버를 활성화해야 합니다.

NFSv4 서버 활성화

절차

1. `nfs enable version 4`를 입력하여 NFSv4를 활성화합니다.

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. (선택 사항) NFSv3를 비활성화하려면 `nfs disable version 3`를 입력합니다.

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

사후 요구 사항

NFSv4 서버를 활성화한 후에 사이트에 맞는 추가 NFS 구성 작업을 수행해야 할 수 있습니다. 이러한 작업에는 Data Domain 시스템에 대해 다음 작업을 수행하는 것이 포함될 수 있습니다.

- NFSv4 도메인 설정
- NFSv4 ID 매핑 구성
- ACL(Access Control List) 구성

NFSv4를 포함하도록 기본 서버 설정

Data Domain NFS 명령 옵션 **`default-server-version`**은 버전을 지정하지 않고 `nfs enable` 명령을 입력하는 경우 활성화되는 NFS 버전을 제어합니다.

절차

1. `nfs option set default-server-version 3:4` 명령을 입력합니다.

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

기존 내보내기 업데이트

기존 내보내기를 업데이트하여 Data Domain 시스템에서 사용되는 NFS 버전을 변경할 수 있습니다.

절차

1. `nfs export modify all` 명령을 입력합니다.

   ```
   # nfs export modify all clients all options version=version number
   ```

   모든 기존 클라이언트가 버전 3, 4 또는 둘 다를 갖도록 NFS 버전을 적절한 문자열로 수정할 수 있습니다. 다음 예에서는 버전 3 및 4를 포함하도록 수정된 NFS를 보여 줍니다.

   ```
   #nfs export modify all clients all options version=3:4
   ```

   `nfs export` 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

Kerberos 및 NFSv4

NFSv4와 NFSv3는 모두 Kerberos 인증 메커니즘을 사용하여 사용자 자격 증명을 보호합니다.

Kerberos는 사용자 자격 증명이 NFS 패킷에서 스푸핑되지 않도록 방지하며 Data Domain 시스템으로 전송되는 동안 변조되지 않도록 보호합니다.

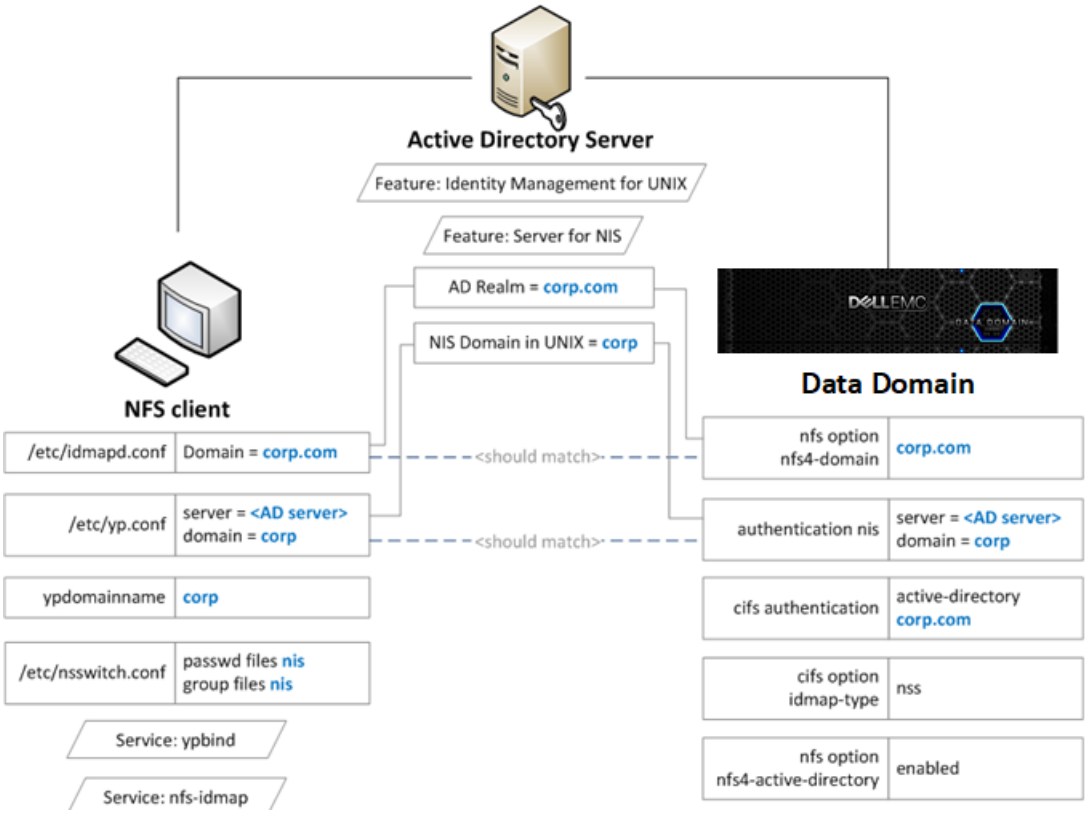
NFS 기반 Kerberos에는 다음과 같은 여러 가지 유형이 있습니다.

- Kerberos 5(**`sec=krb5`**)
  사용자 자격 증명에 Kerberos를 사용합니다.
- Kerberos 5 및 무결성(**`sec=krb5i`**)
  Kerberos를 사용하고 암호화된 체크섬을 통해 NFS 페이로드의 무결성을 검사합니다.
- Kerberos 5 및 보안(**`sec=krb5p`**)
  Kerberos 5 및 무결성을 사용하고 전체 NFS 페이로드를 암호화합니다.

참고

`krb5i`와 **`krb5p`** 모두 NFS 클라이언트와 Data Domain 시스템에 대한 추가 컴퓨팅 오버헤드로 인해 성능 저하를 일으킬 수 있습니다.

그림 9 Active Directory 구성



Kerberos를 위해 시스템을 구성할 때는 NFSv3에 사용되는 기존 명령을 사용합니다. 자세한 내용은 *Data Domain Command Reference Guide*의 nfsv3 장을 참조하십시오.

Linux 기반 KDC와 함께 Kerberos 구성

시작하기 전에

모든 시스템이 KDC(Key Distribution Center)에 액세스할 수 있는지 확인해야 합니다.

시스템이 KDC에 연결할 수 없는 경우 DNS(Domain Name System) 설정을 확인하십시오.

다음 단계를 통해 클라이언트와 Data Domain 시스템에 대한 keytab 파일을 생성할 수 있습니다.

- 1~3단계에서 Data Domain 시스템에 대한 keytab 파일을 생성합니다.
- 4~5단계에서 클라이언트에 대한 keytab 파일을 생성합니다.

절차

1. **nfs/<ddr_dns_name>@<realm>** 서비스 주체를 생성합니다.
   ```
   kadmin.local: addprinc -randkey nfs/ddr12345.<domain-name>@<domain-name>
   ```
2. **nfs/<ddr_dns_name>@<realm>**을 keytab 파일로 내보냅니다.
   ```
   kadmin.local: ktadd -k /tmp/ddr.keytab nfs/ddr12345.corp.com@CORP.COM
   ```
3. 다음 위치에서 Data Domain 시스템으로 keytab 파일을 복사합니다.

   ```
   /ddr/var/krb5.keytab
   ```

4. 클라이언트에 대한 다음 주체 중 하나를 생성하고 **keytab** 파일에 해당 주체를 내보냅니다.

```
nfs/<client_dns_name>@<REALM>
root/<client_dns_name>@<REALM>
```

5. 다음 위치에서 클라이언트로 **keytab** 파일을 복사합니다.

```
/etc/krb5.keytab
```

참고

NTP 서버를 사용하여 모든 개체에서 시간을 동기화 상태로 유지하는 것이 좋습니다.

Kerberos 인증을 사용하도록 Data Domain 시스템 구성

절차

1. `authentication` 명령을 사용하여 Data Domain 시스템에서 KDC 및 Kerberos 영역을 구성합니다.

```
# authentication kerberos set realm <영역> kdc-type unix kdcs
<kdc-server>
```

2. **keytab** 파일 가져오기:

```
# authentication kerberos keytab import
```

3. (선택 사항) 다음 명령을 입력하여 NIS 서버를 구성합니다.

```
# authentication nis servers add <server>
# authentication nis domain set <domain-name>
# authentication nis enable
# filesys restart
```

4. (선택 사항) `nfs option` 명령을 사용하여 **nfs4-domain**을 Kerberos 영역과 동일하게 만듭니다.

```
nfs option set nfs4-domain <kerberos-realm>
```

5. **sec=krb5**를 `nfs export add` 명령에 추가하여 기존 내보내기에 클라이언트를 추가합니다.

```
nfs export add <export-name> clients * options
version=4,sec=krb5
```

클라이언트 구성

절차

1. DNS 서버를 구성하고 정방향 및 역방향 조회가 작동하는지 확인합니다.
2. `/etc/krb5.conf` 구성 파일을 편집하여 KDC 및 Kerberos 영역을 구성합니다.

   사용 중인 클라이언트 운영 체제에 따라 이 단계를 수행해야 할 수 있습니다.
3. NIS 또는 다른 외부 이름 매핑 서비스를 구성합니다.

4. (선택 사항) `/etc/idmapd.conf` 파일을 편집하여 Kerberos 영역과 동일한지 확인합니다.

   사용 중인 클라이언트 운영 체제에 따라 이 단계를 수행해야 할 수 있습니다.

5. keytab 파일 **/etc/krb5.keytab**에 **nfs/** 서비스 주체 또는 **root/** 주체 항목이 포함되어 있는지 확인합니다.

```
[root@fc22 ~]# klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------
----------
3 nfs/fc22.domain-name@domain-name
```

6. **sec=krb5** 옵션을 사용하여 내보내기를 마운트합니다.

```
[root@fc22 ~]# mount ddr12345.<domain-name>:/data/col1/
mtree1 /mnt/nfs4 -o sec=krb5,vers=4
```

Active Directory 활성화

Active Directory 인증을 구성하면 Data Domain 시스템이 Windows Active Directory 영역에 포함됩니다. CIFS 클라이언트와 NFS 클라이언트는 Kerberos 인증을 사용합니다.

절차

1. `cifs set` 명령을 사용하여 Active Directory 영역에 연결합니다.

```
# cifs set authentication active-directory <영역>
```

   Kerberos는 Data Domain 시스템에서 자동으로 설정됩니다. 필요한 nfs/ 서비스 주체는 KDC에 자동으로 생성됩니다.

2. `authentication nis` 명령을 사용하여 NIS 구성:

```
# authentication nis servers add <windows-ad-server>
# authentication nis domain set <ad-realm>
# authentication nis enable
```

3. `cifs` 명령을 사용하여 ID 매핑에 NSS를 사용하도록 CIFS를 구성합니다.

```
# cifs disable
# cifs option set idmap-type nss
# cifs enable
# filesys restart
```

4. **nfs4-domain**을 Active Directory 영역과 동일하게 설정합니다.

```
# nfs option set nfs4-domain <ad-realm>
```

5. `nfs` 명령을 사용하여 NFSv4 id 매핑을 위해 Active Directory를 활성화합니다.

```
# nfs option set nfs4-idmap-active-directory enabled
```

Active Directory 구성

절차

1. Windows 서버에 AD DS(Active Directory Domain Service) 역할을 설치합니다.
2. UNIX 구성 요소에 대한 ID 관리를 설치합니다.

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adminui /all
```

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:nis /all
```

3. NIS 도메인이 서버에 구성되어 있는지 확인합니다.

```
C:\Windows\system32>nisadmin
The following are the settings on localhost

Push Interval : 1 days
Logging Mode  : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
----------------  -------------  ----------------
corp              win-ad-server  corp
```

4. NFSv4 서버에 대한 AD 사용자 및 그룹 UNIX UID/GID를 할당합니다.
   a. **Server Manager** > **Tools** > **Active Directory**로 이동합니다.
   b. AD 사용자 또는 그룹에 대해 **Properties**를 엽니다.
   c. UNIX Atributes 탭 아래에서 NIS domain, UID 및 Primary GID 필드를 작성합니다.

Active Directory에 클라이언트 구성

절차

1. NFS 클라이언트의 서비스 주체를 나타내는 새 AD 사용자를 AD 서버에 생성합니다.
2. NFS 클라이언트에 대한 **nfs/** 서비스 주체를 생성합니다.

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -
pass **** -out nfsclient.keytab
/crytp rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. (선택 사항) 클라이언트에서 **keytab** 파일을 `/etc/krb5.keytab`에 복사합니다.

   사용 중인 클라이언트 OS에 따라 이 단계를 수행해야 하는지 여부가 결정됩니다.

11장

스토리지 마이그레이션

이 장에서 다루는 내용은 다음과 같습니다.

스토리지 마이그레이션 개요

스토리지 마이그레이션을 사용하면 기존 스토리지 엔클로저를 더 높은 성능, 더 많은 용량 및 더 작은 설치 공간을 제공하는 새 엔클로저로 교체할 수 있습니다.

새 엔클로저를 설치한 후 데이터 액세스, 확장, 정리 및 복제와 같은 다른 시스템 프로세스를 지원하는 동안 이전 엔클로저의 데이터를 새 엔클로저로 마이그레이션할 수 있습니다. 스토리지 마이그레이션에는 시스템 리소스가 사용되지만 스로틀 설정을 통해 상대적으로 높거나 낮은 우선 순위를 지정하여 시스템 리소스 사용을 제어할 수 있습니다. 다른 프로세스에 더 많은 리소스를 제공하기 위해 마이그레이션을 중단한 다음 리소스 요구량이 낮아질 때 재개할 수 있습니다.

마이그레이션 중에 시스템은 소스와 대상 엔클로저의 데이터를 사용합니다. 새 데이터는 새 엔클로저에 기록됩니다. 마이그레이션되지 않은 데이터는 소스 엔클로저에서 업데이트되고 마이그레이션된 데이터는 대상 엔클로저에서 업데이트됩니다. 마이그레이션이 중단된 경우 마이그레이션된 것으로 표시되지 않은 블록에서 마이그레이션을 재개할 수 있습니다.

마이그레이션 중에는 데이터의 각 블록이 복제 및 확인되고 소스 블록 공간이 확보되고 마이그레이션된 것으로 표시되며 시스템 인덱스가 새 위치를 사용하도록 업데이트됩니다. 소스 블록으로 대상이 지정된 새 데이터는 대상 블록으로 리디렉션됩니다. 소스에서 할당되었어야 하는 모든 새 데이터 블록 할당이 대상에서 할당됩니다.

마이그레이션 복제 프로세스는 논리적 데이터 레벨이 아니라 셸프 레벨에서 수행되므로, 데이터가 저장되어 있는지 여부에 관계없이 소스 셸프의 모든 디스크 섹터가 액세스되고 복제됩니다. 따라서 스토리지 마이그레이션 유틸리티를 사용하여 논리적 데이터 공간을 축소할 수 없습니다.

참고

마이그레이션 중에는 소스 엔클로저와 대상 엔클로저 사이에 데이터 세트가 분할되므로 마이그레이션을 중단하고 소스 엔클로저의 사용만 재개할 수는 없습니다. 일단 시작한 마이그레이션은 반드시 완료되어야 합니다. 디스크 드라이브 장애와 같은 장애로 인해 마이그레이션이 중단된 경우 문제를 해결하고 마이그레이션을 재개합니다.

스토리지 마이그레이션은 마이그레이션할 데이터의 양 및 선택한 스로틀 설정에 따라 며칠에서 몇 주가 소요될 수 있습니다. 모든 데이터가 마이그레이션되면 `storage migration finalize` 명령을 사용해 수동으로 시작해야 하는 최종화 프로세스를 통해 파일 시스템이 다시 시작됩니다. 시스템이 다시 시작되는 동안 소스 엔클로저가 시스템 구성에서 제거되고 대상 엔클로저가 파일 시스템의 일부가 됩니다. 최종화 프로세스가 완료되면 소스 엔클로저를 시스템에서 제거할 수 있습니다.

스토리지 마이그레이션 후 DD OS에서 보고되는 디스크 셸프 번호가 순차적이지 않을 수 있습니다. 이것은 셸프 번호 매기기가 각 개별 디스크 셸프의 일련 번호에 연결되기 때문입니다. KB 문서 499019, *Data Domain: Storage enclosure numbering is not sequential*(https://support.emc.com)에 자세한 정보가 나와 있습니다. DD OS 버전 5.7.3.0 이상에서 KB 문서에 설명된 `enclosure show persistent-id` 명령에는 SE 액세스 권한이 아닌 관리자 액세스 권한이 필요합니다.

마이그레이션 계획 고려 사항

스토리지 마이그레이션을 시작하기 전에 다음 지침을 고려합니다.

- 스토리지 마이그레이션에는 1회 사용 라이센스가 필요하며 DD OS 5.7 이상 버전에서 지원하는 시스템 모델에서 작동합니다.

참고

스토리지 마이그레이션 작업을 여러 번 수행하려면 여러 개의 라이센스가 필요합니다. 하지만 단일 작업으로 여러 소스 엔클로저를 여러 대상 엔클로저로 마이그레이션할 수 있습니다.

- 스토리지 마이그레이션은 엔클로저 수가 아닌 용량을 기준으로 합니다. 따라서, 다음을 확인하십시오.
  - 단일 소스 엔클로저를 단일 대상 엔클로저로 마이그레이션할 수 있습니다.
  - 단일 소스 엔클로저를 여러 대상 엔클로저로 마이그레이션할 수 있습니다.
  - 여러 소스 엔클로저를 단일 대상 엔클로저로 마이그레이션할 수 있습니다.
  - 여러 소스 엔클로저를 여러 대상 엔클로저로 마이그레이션할 수 있습니다.
- 대상 엔클로저는 다음 조건에 부합해야 합니다.
  - 할당되지 않고 라이센스가 등록되지 않은 새 셸프여야 합니다.
  - DD 시스템 모델에서 지원되어야 합니다.
  - 교체하는 엔클로저만큼의 가용 용량이 포함되어 있어야 합니다.

    참고

    소스 셸프의 사용률을 결정하는 것은 불가능합니다. Data Domain 시스템은 셸프의 용량을 기반으로 모든 계산을 수행합니다.
- 새 엔클로저의 활성 계층 스토리지 용량을 지원하기 위해 DD 시스템 모델에 충분한 메모리가 있어야 합니다.
- 시스템 컨트롤러의 디스크에 대한 데이터 마이그레이션은 지원되지 않습니다.
- ⚠ 주의

  진행 중인 스토리지 마이그레이션이 완료 될 때까지 DD OS를 업그레이드하지 마십시오.
- 파일 시스템을 비활성화하거나 DD OS 업그레이드가 진행 중이거나 다른 마이그레이션이 진행 중이거나 RAID 재구성이 진행 중일 때는 스토리지 마이그레이션을 시작할 수 없습니다.

참고

스토리지 마이그레이션이 진행 중인 경우 진행 중인 마이그레이션이 완료된 후에 새로운 스토리지 마이그레이션 작업을 시작하려면 새로운 스토리지 마이그레이션 라이센스가 필요합니다. 스토리지 마이그레이션 라이센스의 존재 여부는 업그레이드 사전 점검 과정에서 보고됩니다.

- 지정된 모든 소스 엔클로저는 동일한 계층(활성 또는 아카이브)에 있어야 합니다.
- 각 소스 엔클로저에는 하나의 디스크 그룹만 포함될 수 있으며 디스크 그룹의 모든 디스크는 동일한 엔클로저에 설치되어야 합니다.
- 각 대상 엔클로저의 모든 디스크는 그 유형이 동일해야 합니다(예: 모두 SATA 또는 모두 SAS).
- 마이그레이션이 시작된 후에는 대상 엔클로저를 제거할 수 없습니다.
- 마이그레이션이 완료되고 마무리되어야 소스 엔클로저를 제거할 수 있습니다.

- 스토리지 마이그레이션 기간은 시스템 리소스(시스템 모델별로 다름), 시스템 리소스의 가용성 및 마이그레이션할 데이터 수량에 따라 다릅니다. 스토리지 마이그레이션은 완료까지 며칠 또는 몇 주가 소요될 수 있습니다.

DS60 셸프 고려 사항

DS60 고집적 셸프는 60개의 디스크를 수용할 수 있으며, 고객은 랙의 전체 공간을 사용할 수 있습니다. 드라이브는 캐비닛에서 셸프를 꺼낸 후 셸프 상단에서 액세스할 수 있습니다. 셸프는 완전히 적재된 상태에서 무게가 100kg을 넘기 때문에 DS60 셸프로 스토리지를 마이그레이션하기 전에 이 섹션의 내용을 숙지해야 합니다.

DS60 셸프로 작업할 때 다음 고려 사항에 주의하십시오.

⚠ 주의

- **랙 상단에 셸프를 적재하면 셸프가 뒤집힐 수 있습니다.**
- **바닥이 DS60 셸프의 전체 중량을 지탱할 수 있는지 확인하십시오.**
- **랙이 DS60 셸프에 충분한 전력을 공급할 수 있는지 확인하십시오.**
- **첫 번째 랙에 5개 이상의 DS60을 추가하거나 두 번째 랙에 6개 이상의 DS60을 추가하는 경우 DS60 셸프를 유지하려면 안정화 바와 사다리가 필요합니다.**

마이그레이션 상태 보기

DD System Manager에서는 두 가지 방법으로 스토리지 마이그레이션 상태를 볼 수 있습니다.

절차

1. **Hardware** > **Storage**를 선택합니다.

   Storage 영역에서 Storage Migration Status 줄을 검토합니다. 상태가 Not Licensed인 경우 스토리지 마이그레이션 기능을 사용하기 전에 라이센스를 추가해야 합니다. 스토리지 마이그레이션 라이센스가 설치된 경우 상태는 다음 중 하나일 수 있습니다. None, Starting, Migrating, Paused by User, Paused by System, Copy Completed - Pending Finalization, Finalizing, Failed during Copy 또는 Failed during Finalize

2. 스토리지 마이그레이션이 진행 중인 경우 **View Storage Migration**을 클릭하여 진행률 대화 상자를 봅니다.

   참고

   마이그레이션 상태에 전송된 블록의 백분율이 표시됩니다. 여유 블록이 많은 시스템에서는 여유 블록이 마이그레이션되지 않지만 진행률 표시에 포함됩니다. 이 경우 진행률 표시가 빠르게 상승하다가 데이터 마이그레이션이 시작되면 느려집니다.

3. 스토리지 마이그레이션이 진행 중일 때는 **Health** > **Jobs**를 선택해 상태를 볼 수도 있습니다.

마이그레이션 준비 상태 평가

마이그레이션을 시작하기 전에 시스템을 사용하여 스토리지 마이그레이션 준비 상태를 평가할 수 있습니다.

절차

1. 제품 설치 가이드에 나와 있는 지침을 사용하여 대상 엔클로저를 설치합니다.
2. **Administration** > **Licenses**를 선택하고 스토리지 마이그레이션 라이센스가 설치되어 있는지 확인합니다.
3. 스토리지 마이그레이션 라이센스가 설치되지 않은 경우 **Add Licenses**를 클릭하고 라이센스를 추가합니다.
4. **Hardware** > **Storage**를 선택하고 **Migrate Data**를 클릭합니다.
5. Select a Task 대화 상자에서 **Estimate**를 선택하고 **Next**를 클릭합니다.
6. Select Existing Enclosures 대화 상자에서 확인란을 사용해 스토리지 마이그레이션에 사용할 각 소스 엔클로저를 선택하고 **Next**를 클릭합니다.
7. Select New Enclosures 대화 상자에서 확인란을 사용해 스토리지 마이그레이션에 사용할 각 대상 엔클로저를 선택하고 **Next**를 클릭합니다.

   Add Licenses 버튼을 사용하면 새 엔클로저의 스토리지 라이센스를 현재 작업을 중단하지 않고 필요에 따라 추가할 수 있습니다.
8. Review Migration Plan 대화 상자에서 예상 마이그레이션 스케줄을 검토하고 **Next**를 클릭합니다.
9. Verify Migration Preconditions 대화 상자에서 사전 점검 결과를 검토하고 Close를 클릭합니다.

결과

사전 점검 테스트가 실패한 경우 마이그레이션을 시작하기 전에 문제를 해결합니다.

DD System Manager를 사용하여 스토리지 마이그레이션

스토리지 마이그레이션 프로세스는 시스템 준비 상태를 평가하고, 마이그레이션 시작을 확인하며, 데이터를 마이그레이션한 다음 프로세스 완료를 확인하는 단계로 구성됩니다.

절차

1. 제품 설치 가이드에 나와 있는 지침을 사용하여 대상 엔클로저를 설치합니다.
2. **Administration** > **Licenses**를 선택하고 스토리지 마이그레이션 라이센스가 설치되어 있는지 확인합니다.
3. 스토리지 마이그레이션 라이센스가 설치되지 않은 경우 **Add Licenses**를 클릭하고 라이센스를 추가합니다.
4. **Hardware** > **Storage**를 선택하고 **Migrate Data**를 클릭합니다.
5. Select a Task 대화 상자에서 **Migrate**를 선택하고 **Next**를 클릭합니다.
6. Select Existing Enclosures 대화 상자에서 확인란을 사용해 스토리지 마이그레이션에 사용할 각 소스 엔클로저를 선택하고 **Next**를 클릭합니다.
7. Select New Enclosures 대화 상자에서 확인란을 사용해 스토리지 마이그레이션에 사용할 각 대상 엔클로저를 선택하고 **Next**를 클릭합니다.

Add Licenses 버튼을 사용하면 새 엔클로저의 스토리지 라이센스를 현재 작업을 중단하지 않고 필요에 따라 추가할 수 있습니다.

8. Review Migration Plan 대화 상자에서 예상 마이그레이션 스케줄을 검토하고 **Start**를 클릭합니다.
9. Start Migration 대화 상자에서 **Start**를 클릭합니다.

   Migrate 대화 상자가 나타나고 다음 세 단계의 마이그레이션이 진행됨에 따라 대화 상자가 업데이트됩니다. Starting Migration, Migration in Progress 및 Copy Complete
10. Migrate 대화상자 제목에 Copy Complete가 표시되고 파일 시스템을 다시 시작할 수 있게 되면 **Finalize**를 클릭합니다.

    참고

    이 작업을 시작하면 파일 시스템이 다시 시작되고 10~15분 후에 완료됩니다. 이 시간 동안은 시스템을 사용할 수 없습니다.

결과

마이그레이션 최종화 작업이 완료되면 시스템이 대상 엔클로저를 사용하므로 소스 엔클로저를 제거할 수 있습니다.

스토리지 마이그레이션 대화 상자 설명

DD System Manager 대화 상자 설명에 스토리지 마이그레이션에 대한 추가 정보가 표시됩니다. 이 정보는 대화 상자의 도움말 아이콘을 클릭하여 확인할 수도 있습니다.

Select a Task 대화 상자

이 대화 상자에는 스토리지 마이그레이션 준비 상태를 평가한 후 스토리지 마이그레이션을 중지하거나, 아니면 준비 상태를 평가한 후 스토리지 마이그레이션을 시작할지를 결정하는 구성이 포함됩니다.

시스템 준비 상태를 평가하고 중지하려면 **Estimate**를 선택합니다.

시스템 평가 후 마이그레이션을 시작하려면 **Migrate**를 선택합니다. 시스템 평가 후 마이그레이션 시작 전에 스토리지 마이그레이션을 확인 또는 취소하라는 대화 상자 메시지가 표시됩니다.

Select Existing Enclosures 대화 상자

이 대화 상자에는 마이그레이션에 대한 활성 또는 보존 계층과 소스 엔클로저를 선택하는 구성이 포함됩니다.

DD Extended Retention 기능이 설치된 경우 목록 상자를 사용해 **Active Tier** 또는 **Retention Tier**를 선택합니다. DD Extended Retention이 설치되어 있지 않으면 목록 상자가 표시되지 않습니다.

Existing Enclosures 목록에는 스토리지 마이그레이션에 사용 가능한 엔클로저가 나열됩니다. 마이그레이션할 각 엔클로저의 확인란을 선택합니다. 계속할 준비가 되면 **Next**를 클릭합니다.

Select New Enclosures 대화 상자

이 대화 상자에는 마이그레이션의 대상 엔클로저를 선택하는 구성이 포함됩니다. 또한 스토리지 라이센스 상태와 **Add Licenses** 버튼도 표시됩니다.

Available Enclosures 목록에는 스토리지 마이그레이션의 대상 엔클로저로 사용 가능한 엔클로저가 나열됩니다. 원하는 대상 엔클로저의 확인란을 선택하면 됩니다.

라이센스 상태 표시줄은 시스템에 설치된 모든 스토리지 라이센스를 나타냅니다. 녹색 부분은 사용 중인 라이센스를 나타내고 투명한 부분은 라이센스가 부여된 스토리지 용량 중 대상 엔클로저에 사용할 수 있는 용량을 나타냅니다. 선택한 대상 컨트롤러를 지원하기 위해 추가 라이센스를 설치해야 하는 경우 **Add Licenses**를 클릭합니다.

계속할 준비가 되면 **Next**를 클릭합니다.

Review Migration Plan 대화 상자

이 대화 상자에는 스토리지 마이그레이션의 예상 기간이 스토리지 마이그레이션의 세 단계로 정렬되어 표시됩니다.

스토리지 마이그레이션 1단계에서는 시스템의 마이그레이션 준비 상태를 확인하는 일련의 테스트가 실행됩니다. 테스트 결과는 Verify Migration Preconditions 대화 상자에 나타납니다.

2단계에서는 소스 엔클로저의 데이터가 대상 엔클로저로 복제됩니다. 복제 작업은 시스템이 백업 클라이언트에 서비스를 계속해서 제공하는 동안 백그라운드에서 실행되므로 데이터의 양이 많은 경우 완료까지 며칠 또는 몇 주가 소요될 수 있습니다. Migration in Progress 대화 상자의 설정을 사용해 마이그레이션 우선 순위를 변경하면 마이그레이션의 속도가 빨라지거나 느려질 수 있습니다.

Copy Complete 대화 상자에서 수동으로 시작하는 3단계에서는 대상 엔클로저를 사용하도록 시스템 구성이 업데이트되고 소스 컨트롤러의 구성이 제거됩니다. 이 단계가 진행되는 동안에는 파일 시스템이 재시작되고 백업 클라이언트에서 시스템을 사용할 수 없습니다.

Verify Migration Preconditions 대화 상자

이 대화 상자에는 마이그레이션을 시작하기 전에 실행한 테스트의 결과가 표시됩니다.

테스트 시퀀스와 각 테스트에 대한 추가 정보가 다음 목록에 나열되어 있습니다.

P1. 이 시스템의 플랫폼이 지원됩니다.

이전 DD 시스템 모델은 스토리지 마이그레이션을 지원하지 않습니다.

P2. 스토리지 마이그레이션 라이센스를 사용할 수 있습니다.

스토리지 마이그레이션 라이센스가 있어야 합니다.

P3. 현재 실행 중인 다른 마이그레이션이 없습니다.

다른 스토리지 마이그레이션을 시작하려면 이전 스토리지 마이그레이션을 완료해야 합니다.

P4. 현재 마이그레이션 요청이 중단된 마이그레이션 요청과 동일합니다.

중단된 마이그레이션을 재개하고 완료하십시오.

P5. 기존 엔클로저에 있는 디스크 그룹 레이아웃을 확인합니다.

스토리지 마이그레이션을 수행하려면 각 소스 엔클로저에 디스크 그룹이 하나만 있어야 하며 해당 그룹의 모든 디스크가 소스 엔클로저에 있어야 합니다.

P6. 최종 시스템 용량을 확인합니다.

마이그레이션이 완료되고 소스 엔클로저를 제거한 후의 총 시스템 용량이 DD 시스템에서 지원하는 용량을 초과하지 않아야 합니다.

P7. 교체용 엔클로저의 용량을 확인합니다.

대상 엔클로저의 가용 용량이 소스 엔클로저의 가용 용량보다 커야 합니다.

P8. 소스 엔클로저가 동일한 활성 계층 또는 보존 유닛에 있습니다.

활성 계층 또는 보존 계층에서의 스토리지 마이그레이션이 지원됩니다. 두 계층에서 동시에 스토리지 마이그레이션을 수행할 수는 없습니다.

P9. 소스 엔클로저가 본체에 있는 엔클로저가 아닙니다.

시스템 컨트롤러는 CLI에서 엔클로저로 나열되지만 시스템 컨트롤러에 설치된 디스크의 경우 스토리지 마이그레이션이 지원되지 않습니다.

P10. 교체용 엔클로저를 스토리지에 추가할 수 있습니다.

각 대상 엔클로저의 모든 디스크는 그 유형이 동일해야 합니다(예: 모두 SATA 또는 모두 SAS).

P11. 소스 컨트롤러에 재구성 중인 RAID가 없습니다.

RAID 재구성이 진행 중인 동안에는 스토리지 마이그레이션을 시작할 수 없습니다.

P12. 소스 셸프가 지원되는 계층에 속합니다.

소스 디스크 엔클로저는 마이그레이션 대상에서 지원되는 계층의 일부여야 합니다.

마이그레이션 진행률 대화 상자

이 일련의 대화 상자는 스토리지 마이그레이션 상태 및 각 단계에서 적용되는 제어를 제공합니다.

Migrate - Starting Migration
첫 번째 단계의 진행률이 진행 표시줄에 표시되며 이 단계에서 사용할 수 있는 제어는 없습니다.

Migrate - Migration in Progress
두 번째 단계에서는 소스 엔클로저의 데이터가 대상 엔클로저로 복제되며 진행 표시줄에 진행률이 표시됩니다. 복제 작업이 며칠에서 몇 주까지 걸릴 수 있으므로 마이그레이션 중에 사용되는 리소스를 관리하고 다른 프로세스에 리소스가 필요할 경우 마이그레이션을 중지하는 제어를 사용할 수 있습니다.

Pause를 클릭하여 마이그레이션을 중지하고 나중에 **Resume**을 클릭하여 마이그레이션을 계속할 수 있습니다.

Low, **Medium** 및 **High** 버튼은 스토리지 마이그레이션 리소스 요구량에 대한 스로틀 설정을 정의합니다. 스로틀 설정을 낮게 설정하면 스토리지 마이그레이션의 리소스 우선 순위가 낮아지므로 마이그레이션 속도가 저하되지만 시스템 리소스를 적게 사용합니다. 이와 반대로, 스로틀 설정을 높게 설정하면 스토리지 마이그레이션의 우선 순위가 높아져 마이그레이션 속도가 빨라지지만 시스템 리소스를 더 많이 사용합니다. 중간으로 설정하면 중간 우선 순위가 선택됩니다.

마이그레이션 기간 동안 이 대화 상자를 열어 둘 필요는 없습니다. 이 대화 상자를 닫은 후 마이그레이션 상태를 확인하려면 **Hardware** > **Storage**를 선택하고 마이그레이션 상태를 보면 됩니다. Hardware/Storage 페이지에서 이 대화 상자로 돌아오려면 **Manage Migration**을 클릭합니다. **Health** > **Jobs**를 선택하여 마이그레이션 진행률을 볼 수도 있습니다.

Migrate - Copy Complete
복제가 완료되면 **Finalize**를 클릭할 때까지 마이그레이션 프로세스가 대기 상태를 유지합니다. 10~15분 정도 소요되는 이 최종 단계에서는 파일 시스템이 재시작되고 시스템을 사용할 수 없재습니다. 이 단계는 유지 보수 기간이나 시스템 활동이 적은 기간에 시작하는 것이 좋습니다.

CLI를 사용하여 스토리지 마이그레이션

마이그레이션에는 소스 DG에 포맷된 블록 세트(예: 소스 블록 세트)의 할당된 모든 블록을 대상 DG에 포맷된 블록 세트(예: 대상 블록 세트)로 이동하는 작업이 필요합니다. 할당된 모든 블록을 소스 블록 세트에서 이동한 후에는 파일 시스템에서 이러한 블록 세트를 제거하고 스토리지 계층에서 블록 세트의 디스크를 제거하며 DDR에서 물리적 디스크 및 엔클로저를 제거할 수 있습니다.

참고

스토리지 마이그레이션을 위한 새 엔클로저를 준비하는 작업은 스토리지 마이그레이션 프로세스를 통해 관리됩니다. 엔클로저를 추가하는 방식으로 대상 엔클로저를 준비하지 마십시오. 예를 들어 `filesys expand` 명령은 엔클로저를 추가할 때 사용할 수 있지만 이 명령을 사용하여 추가된 엔클로저는 스토리지 마이그레이션 대상으로 사용될 수 없습니다.

DS60 디스크 셸프에는 각각 15개의 디스크로 구성된 4개의 디스크 팩이 포함되어 있습니다. DS60 셸프가 마이그레이션 소스 또는 대상인 경우 디스크 팩은 ***엔클로저*:*팩*** 형식으로 참조됩니다. 이 예제에서는 소스가 엔클로저 7, 팩 2(7:2)이고 대상이 엔클로저 7, 팩 4(7:4)입니다.

절차

1. 제품 설치 가이드에 나와 있는 지침을 사용하여 대상 엔클로저를 설치합니다.
2. 스토리지 마이그레이션 기능 라이센스가 설치되어 있는지 확인합니다.

   ```
   # elicense show
   ```
3. 라이센스가 설치되지 않은 경우 e-라이센스를 업데이트하여 스토리지 마이그레이션 기능 라이센스를 추가합니다.

   ```
   # elicense update
   ```
4. 소스와 대상 디스크의 디스크 상태를 봅니다.

   ```
   # disk show state
   ```

   소스 디스크는 **active** 상태에 있어야 하고 대상 디스크는 **unknown** 상태에 있어야 합니다.
5. **storage migration precheck** 명령을 실행하여 시스템의 마이그레이션 준비 상태를 확인합니다.

   ```
   # storage migration precheck source-enclosures 7:2 destination-
   enclosures 7:4
   ```
6. 마이그레이션 스로틀 설정을 봅니다.

   ```
   storage migration option show throttle
   ```
7. 시스템이 준비되면 스토리지 마이그레이션을 시작합니다.

   ```
   # storage migration start source-enclosures 7:2 destination-
   enclosures 7:4
   ```
8. 선택적으로, 마이그레이션 중에 소스 및 대상 디스크의 디스크 상태를 봅니다.

```
# disk show state
```

마이그레이션 중에 소스 디스크는 **migrating** 상태에 있어야 하고 대상 디스크는 **destination** 상태에 있어야 합니다.

9. 필요에 따라 마이그레이션 상태를 검토합니다.

```
# storage migration status
```

10. 소스와 대상 디스크의 디스크 상태를 봅니다.

```
# disk show state
```

마이그레이션 중에 소스 디스크는 **migrating** 상태에 있어야 하고 대상 디스크는 **destination** 상태에 있어야 합니다.

11. 마이그레이션이 완료되면 대상 엔클로저를 사용하도록 구성을 업데이트합니다.

참고

이 작업을 시작하면 파일 시스템이 다시 시작되고 10~15분 후에 완료됩니다. 이 시간 동안은 시스템을 사용할 수 없습니다.

```
storage migration finalize
```

12. 각 소스 엔클로저에서 모든 데이터를 제거하려는 경우 지금 데이터를 제거합니다.

```
storage sanitize start enclosure <enclosure-id>[:<pack-id>]
```

참고

storage sanitize 명령은 인증된 데이터 삭제 방식이 아닙니다. Data Domain에서는 공인 데이터 삭제를 서비스로 제공합니다. 자세한 내용은 Data Domain 영업 담당자에게 문의하십시오.

13. 소스와 대상 디스크의 디스크 상태를 봅니다.

```
# disk show state
```

마이그레이션 후 소스 디스크는 **unknown** 상태에 있어야 하고 대상 디스크는 **active** 상태에 있어야 합니다.

결과

마이그레이션 최종화 작업이 완료되면 시스템이 대상 스토리지를 사용하므로 소스 스토리지를 제거할 수 있습니다.

CLI 스토리지 마이그레이션 예

elicense show

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

elicense update

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
```

```
## Feature           Count   Mode              Expiration Date
-- -----------       -----  ---------------   ---------------
1  REPLICATION       1      permanent (int)   n/a
2  VTL               1      permanent (int)   n/a
3  Storage Migration 1      permanent (int)
-- -----------       -----  ---------------   ---------------
** This will replace all existing Data Domain licenses on the system with the above EMC ELMS
licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

disk show state

그림 10 `disk show state`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
-------------   ----------------------------------------------
1                .  .  .  .
2                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7               |--------|--------|--------|--------|
                | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)   |U  U  U |.  .  s |U  U  U |U  U  U |
     D(37-48)   |U  U  U |.  .  . |U  U  U |U  U  U |
     C(25-36)   |U  U  U |.  .  . |U  U  U |U  U  U |
     B(13-24)   |U  U  U |.  .  . |U  U  U |U  U  U |
     A( 1-12)   |U  U  U |.  .  . |U  U  U |U  U  U |
                |--------|--------|--------|--------|
-------------   ----------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

storage migration precheck

```
#storage migration precheck  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

      1 "Verifying platform support.....................................................PASS"
      2 "Verifying valid storage migration license exists...............................PASS"
      3 "Verifying no other migration is running........................................PASS"
      4 "Verifying request matches interrupted migration................................PASS"
      5 "Verifying data layout on the source shelves....................................PASS"
      6 "Verifying final system capacity................................................PASS"
      7 "Verifying destination capacity.................................................PASS"
      8 "Verifying source shelves belong to same tier...................................PASS"
      9 "Verifying enclosure 1 is not used as source....................................PASS"
     10 "Verifying destination shelves are addable to storage..........................PASS"
     11 "Verifying no RAID reconstruction is going on in source shelves................PASS"
```

```
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min
```

storage migration show history

그림 11 `storage migration show history`

```
# storage migration show history
Id   Source      Source Enclosure   Dest        Dest Enclosure    Status     Start Time                 End Time
     Enclosure*  Serial No.         Enclosure*  Serial No.
--   ----------  ----------------   ----------  ---------------   ---------  -------------------------  -------------------------
2    9:0         SHU952400106A23    7:0         SHU9524084G055B   Finalized  Sat Aug  8 11:59:37 2015   Mon Aug 10 11:10:11 2015
1    9:0         SHU952400106A23    7:0         SHU9524084G055B   Finalized  Thu Aug  6 16:39:55 2015   Fri Aug  7 10:28:07 2015
                                    8:0         SHU9524084G04LR
--   ----------  ----------------   ----------  ---------------   ---------  -------------------------  -------------------------
(*) Enclosure ids at migration start time.
```

storage migration start

```
#storage migration start  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

  Expected time to migrate data: 84 hrs 40 min

**   Storage migration once started cannot be aborted.
     Existing data on the destination shelves will be overwritten.
        Do you want to continue with the migration? (yes|no) [no]: yes

Performing migration pre-check:
      1 Verifying platform support.....................................................PASS
      2 Verifying valid storage migration license exists...............................PASS
      3 Verifying no other migration is running.......................................PASS
      4 Verifying request matches interrupted migration...............................PASS
      5 Verifying data layout on the source shelves...................................PASS
      6 Verifying final system capacity...............................................PASS
      7 Verifying destination capacity................................................PASS
      8 Verifying source shelves belong to same tier..................................PASS
      9 Verifying enclosure 1 is not used as source...................................PASS
     10 Verifying destination shelves are addable to storage..........................PASS
     11 Verifying no RAID reconstruction is going on in source shelves................PASS

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.
Space reservation may add up to an hour or more based on system resources.

Storage migration process initiated.
Check storage migration status to monitor progress.
```

storage migration status

그림 12 `storage migration status`

```
# storage migration status
Id   Source          Destination     State       Percent    Estimated Time to Complete   Current Throttle
     Enclosure(s)    Enclosure(s)                Complete                                Setting
--   ------------    ------------    ---------   --------   --------------------------   ----------------
5    7:2             7:4             migrating   45%        30 hrs 18 mins               high
--   ------------    ------------    ---------   --------   --------------------------   ----------------
```

disk show state, 마이그레이션 진행 중

그림 13 `disk show state, migration in progress`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ---------------------------------------------
1                 .  .  .  .
2                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                 v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)    |U  U  U |m  m  s |U  U  U |s  d  d |
     D(37-48)    |U  U  U |m  m  m |U  U  U |d  d  d |
     C(25-36)    |U  U  U |m  m  m |U  U  U |d  d  d |
     B(13-24)    |U  U  U |m  m  m |U  U  U |d  d  d |
     A( 1-12)    |U  U  U |m  m  m |U  U  U |d  d  d |
                 |--------|--------|--------|--------|
--------------   ---------------------------------------------

Legend   State               Count
------   -----------------   -----
.        In Use Disks        4
s        Spare Disks         2
v        Available Disks     15
U        Unknown Disks       90
m        Migrating Disks     14
d        Destination Disks   14
```

storage migration finalize

그림 14 `storage migration finalize`

```
# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
        Do you want to continue? (yes|no) [no]: yes

Performing migration finalization pre-check:
(P1)    Verifying storage migration is ready for finalization....PASS
(P2)    Verifying there are no foreign disks.....................PASS
(P3)    Verifying data layout on the source shelves..............PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait..........
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....................
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.
```

disk show state, 마이그레이션 완료

그림 15 `disk show state, migration complete`

```
# disk show state
Enclosure         Disk
  Row(disk-id)     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ------------------------------------------------
1                  .  .  .  .
2                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)    |U  U  U |U  U  U |U  U  U |s  .  . |
      D(37-48)    |U  U  U |U  U  U |U  U  U |.  .  . |
      C(25-36)    |U  U  U |U  U  U |U  U  U |.  .  . |
      B(13-24)    |U  U  U |U  U  U |U  U  U |.  .  . |
      A( 1-12)    |U  U  U |U  U  U |U  U  U |.  .  . |
                  |--------|--------|--------|--------|
--------------   ------------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

참고

현재 스토리지 마이그레이션은 액티브 노드에서만 지원됩니다. HA 클러스터의 대기 노드에서는 스토리지 마이그레이션이 지원되지 않습니다.

12장

플래시 기반 메타데이터

이 장에서 다루는 내용은 다음과 같습니다.

MDoF(Metadata on Flash) 개요

MDoF는 플래시 기술을 사용하여 파일 시스템 메타데이터에 대한 캐시를 생성합니다. SSD 캐시는 지연 시간이 짧고 IOPS(Input/Output Per Second)가 높아 메타데이터 및 데이터 액세스 시간이 단축됩니다.

참고

필요한 최소 소프트웨어 버전은 DD OS 6.0입니다.

SSD에 파일 시스템 메타데이터를 캐싱하면 기존 워크로드와 랜덤 워크로드 모두 입출력 성능이 향상됩니다.

기존 워크로드의 경우 HDD에서 SSD로 메타데이터에 대한 랜덤 액세스를 오프로드하면 하드 드라이브가 스트리밍 쓰기 및 읽기 요청을 수용할 수 있습니다.

랜덤 워크로드의 경우 SSD 캐시가 짧은 지연 시간으로 메타데이터 작업을 수행하므로 HDD는 캐시 요청 대신 데이터 요청을 처리할 수 있습니다.

SSD의 읽기 캐시는 자주 액세스하는 데이터를 캐싱하여 랜덤 읽기 성능을 향상시킵니다. NVRAM에 데이터를 쓰는 작업과 지연 시간이 짧은 메타데이터 작업을 결합하면 NVRAM을 빠르게 소모시켜 랜덤 쓰기 지연 시간을 향상시킬 수 있습니다. 캐시가 없어도 파일 시스템 작업이 수행되지만 파일 시스템 성능이 저하됩니다.

캐시 계층을 처음 생성할 때는 파일 시스템이 실행된 후에 캐시 계층을 추가하는 경우에만 파일 시스템의 재시작이 필요합니다. 캐시 계층 디스크와 함께 제공되는 새로운 시스템의 경우 파일 시스템을 활성화하기 전에 캐시 계층을 처음 생성할 때 파일 시스템의 재시작이 필요 없습니다. 파일 시스템을 비활성화했다가 다시 활성화할 필요가 없이, 실행 중인 시스템에 캐시를 더 추가할 수 있습니다.

참고

DD OS 5.7에서 DD OS 6.0으로 업그레이드된 DD9500 시스템은 캐시 계층을 처음 생성한 경우 파일 시스템을 한 번 다시 시작해야 합니다.

SSD와 관련된 한 가지 특수 조건은 남은 스페어 블록 수가 0에 가까워지면 SSD가 읽기 전용 상태가 된다는 것입니다. 읽기 전용 조건이 발생하면 DD OS는 드라이브를 읽기 전용 캐시로 처리하고 알림을 전송합니다.

MDoF는 다음과 같은 Data Domain 시스템에서 지원됩니다.

- DD6300
- DD6800
- DD9300
- DD9500
- DD9800
- 16TB 이상 용량 구성(DD VE의 경우 SSD 캐시 계층)의 DD VE 인스턴스(DD3300 시스템 포함)

MDoF 라이선스 및 용량

MDoF 기능을 사용하려면 ELMS를 통해 활성화된 라이선스가 필요합니다. SSD Cache 라이선스는 기본적으로 활성화되지 않습니다.

다음 표에서는 시스템별 SSD 용량 라이선스 및 SSD 용량에 대해 설명합니다.

표 121 시스템별 SSD 용량 라이선스

모델	메모리	SSD 수	SSD 용량
DD6300	48GB(기본)	1	800GB
	96GB(확장)	2	1600GB
DD6800	192GB(기본)	2	1600GB
	192GB(확장)	4	3200GB
DD9300	192GB(기본)	5	4000GB
	384GB(확장)	8	6400GB
DD9500	256GB(기본)	8	6400GB
	512GB(확장)	15	12000GB
DD9800	256GB(기본)	8	6400GB
	768GB(확장)	15	12000GB

DD VE를 위한 SSD 캐시 계층

DD VE 인스턴스 및 DD3300 시스템에는 SSD 캐시 계층에 대한 라이선스가 필요하지 않습니다. 지원되는 최대 SSD 용량은 Active Tier 용량의 1%입니다.

다음 표에서는 시스템별 SSD 용량 라이선스 및 SSD 용량에 대해 설명합니다.

표 122 DD VE 및 DD3300 SSD 용량

용량 구성	최대 SSD 용량
DD VE 16TB	160GB
DD VE 32TB	320GB
DD VE 48TB	480GB
DD VE 64TB	640GB
DD VE 96TB	960 GB
DD3300 8TB	160GB
DD3300 16TB	160GB
DD3300 32TB	320GB

SSD 캐시 계층

SSD 캐시 계층은 파일 시스템에 대한 SSD 캐시 스토리지를 제공합니다. 파일 시스템은 사용자의 능동적 개입 없이 SSD 캐시 계층에서 필요한 스토리지를 가져옵니다.

MDoF SSD 캐시 계층 - 시스템 관리

SSD 캐시에 대한 다음 고려 사항에 유의하십시오.

- SSD가 컨트롤러 내에서 구축되면 해당 SSD는 내부 루트 드라이브로 간주됩니다. SSD는 `storage show all` 명령 출력에서 엔클로저 1로 표시됩니다.

- HDD를 관리하는 것과 동일한 방식으로 `disk` 명령을 사용하여 SSD를 관리합니다.
- `storage add` 명령을 실행하여 개별 SSD 또는 SSD 엔클로저를 SSD 캐시 계층에 추가합니다.
- SSD 캐시 계층 공간은 관리할 필요가 없습니다. 파일 시스템은 SSD 캐시 계층에서 필요한 스토리지를 가져와 클라이언트 간에서 공유합니다.
- `filesys create` 명령은 시스템에서 SSD를 사용할 수 있는 경우 SSD 볼륨을 생성합니다.

  참고

  SSD가 나중에 시스템에 추가되는 경우 시스템에서 자동으로 SSD 볼륨을 생성하고 파일 시스템에 알려야 합니다. SSD Cache Manager는 등록된 클라이언트에 알림을 보내 캐시 객체를 생성하게 합니다.

- SSD 볼륨에 활성 드라이브가 하나만 있는 경우 활성 드라이브가 시스템에서 제거되면 마지막으로 오프라인 상태가 된 드라이브가 다시 온라인 상태가 됩니다.

다음 섹션에서는 Data Domain System Manager 및 DD OS CLI에서 SSD 캐시 계층을 관리하는 방법에 대해 설명합니다.

SSD 캐시 계층 관리

스토리지 구성 기능을 사용하면 SSD 캐시 계층에서 스토리지를 추가하고 제거할 수 있습니다.

절차

1. **Hardware** > **Storage** > **Overview**를 선택합니다.
2. **Cache Tier** 대화 상자를 확장합니다.
3. **Configure**를 클릭합니다.

   활성 계층에 추가할 수 있는 최대 스토리지 양은 사용하는 DD 컨트롤러에 따라 다릅니다.

   참고

   라이선스가 부여된 용량 표시줄에 설치된 엔클로저에 대한 라이선스가 부여된 용량(사용된 용량 및 남은 용량)의 부분이 표시됩니다.

4. 추가할 셸프의 확인란을 선택합니다.
5. **Add to Tier** 버튼을 클릭합니다.
6. **OK**를 클릭하여 스토리지를 추가합니다.

   참고

   추가된 셸프를 제거하려면 Tier Configuration 목록에서 **Remove from Configuration**과 **OK**를 차례로 클릭합니다.

CLI 절차

캐시 계층 SSD가 본체에 설치되는 경우:

a. 캐시 계층에 SSD를 추가합니다.

```
#  storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done
```

```
Disk 1.13 successfully added to the cache tier.


Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

b. 새로 추가된 SSD의 상태를 확인합니다.

```
# disk show state
Enclosure   Disk
             1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------   ---------------------------------------------
1            .  .  .  .  s  .  .  s  s  s  s  s  v  v
2            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
---------   ---------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      6
s        Spare Disks       6
v        Available Disks   2
U        Unknown Disks     30
------   ---------------   -----
Total 44 disks
```

캐시 계층 SSD가 외부 셸프에 설치되는 경우:

a. 시스템이 SSD 셸프를 인식하는지 확인합니다. 아래 예에서는 SSD 셸프가 엔클로저 2입니다.

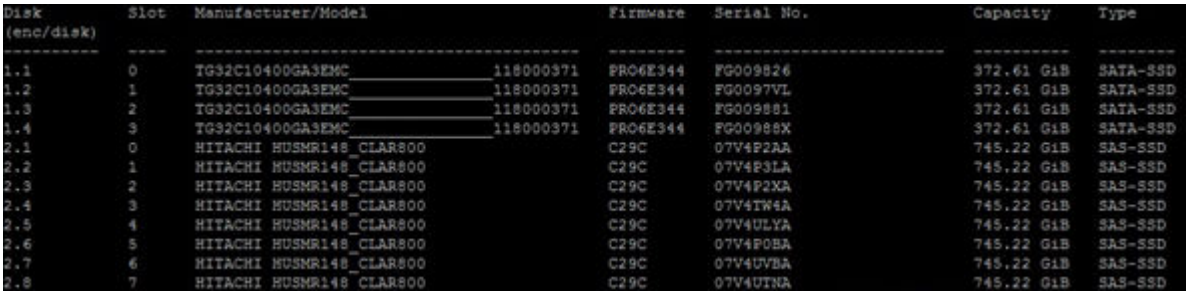
```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ---------------------------------------------
1            .  .  .  .
2            U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   ---------------------------------------------

Legend   State                Count
------   ------------------   -----
.        In Use Disks         32
v        Available Disks      182
U        Unknown Disks        8
-        Not Installed Disks  7
------   ------------------ -----
Total 222 disks
```

b. SSD 셸프의 셸프 ID를 식별합니다. SSD는 `Type` 열에 `SAS-SSD` 또는 `SATA-SSD`로 표시됩니다.

```
#  disk show hardware
```

그림 16



Disk (enc/disk)	Slot	Manufacturer/Model	Firmware	Serial No.	Capacity	Type
1.1	0	TG32C10400GA3EMC_____118000371	PRO6E344	FG009826	372.61 GiB	SATA-SSD
1.2	1	TG32C10400GA3EMC_____118000371	PRO6E344	FG0097VL	372.61 GiB	SATA-SSD
1.3	2	TG32C10400GA3EMC_____118000371	PRO6E344	FG009881	372.61 GiB	SATA-SSD
1.4	3	TG32C10400GA3EMC_____118000371	PRO6E344	FG00988X	372.61 GiB	SATA-SSD
2.1	0	HITACHI HUSMR148_CLAR800	C29C	07V4P2AA	745.22 GiB	SAS-SSD
2.2	1	HITACHI HUSMR148_CLAR800	C29C	07V4P3LA	745.22 GiB	SAS-SSD
2.3	2	HITACHI HUSMR148_CLAR800	C29C	07V4P2XA	745.22 GiB	SAS-SSD
2.4	3	HITACHI HUSMR148_CLAR800	C29C	07V4IW4A	745.22 GiB	SAS-SSD
2.5	4	HITACHI HUSMR148_CLAR800	C29C	07V4ULYA	745.22 GiB	SAS-SSD
2.6	5	HITACHI HUSMR148_CLAR800	C29C	07V4P0BA	745.22 GiB	SAS-SSD
2.7	6	HITACHI HUSMR148_CLAR800	C29C	07V4UVBA	745.22 GiB	SAS-SSD
2.8	7	HITACHI HUSMR148_CLAR800	C29C	07V4UTNA	745.22 GiB	SAS-SSD

c. 캐시 계층에 SSD 셸프를 추가합니다.

```
#  storage add enclosure 2 tier cache

Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2
successfully added to the cache tier.

Updating system information...done

Successfully added: 2  done
```

d. 새로 추가된 SSD의 상태를 확인합니다.

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    -----------------------------------------------
1            .  .  .  .
2            .  .  .  .  .  .  .  .  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60)  |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48)  |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36)  |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24)  |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12)  |v  v  v |v  v  v |v  v  v |v  v  v |
             |--------|--------|--------|--------|
11            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------    -----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

캐시 계층에서 컨트롤러 탑재 SSD를 제거하려면 다음을 수행합니다.

```
# storage remove disk 1.13

Removing disk 1.13...done
```

```
Updating system information...done

Disk 1.13 successfully removed.
```

시스템에서 SSD 셸프를 제거하려면 다음을 수행합니다.

```
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

SSD 알림

SSD 캐시 계층에 관련된 알림은 세 가지가 있습니다.

SSD 캐시 계층 알림은 다음과 같습니다.

- 라이센스 등록
  파일 시스템이 활성화되어 있고 라이센스가 허용하는 것보다 적은 물리적 캐시 용량이 구성되어 있으면 현재 SSD 용량 및 용량 라이센스에 대한 알림이 생성됩니다. 이 알림은 경고 알림으로 분류됩니다. 캐시가 없어도 파일 시스템 작업이 수행되지만 파일 시스템 성능이 저하됩니다. 파일 시스템을 비활성화했다가 다시 활성화할 필요가 없이, 실행 중인 시스템에 캐시를 더 추가할 수 있습니다.
- 읽기 전용 구성
  남은 스페어 블록 수가 0에 가까워지면 SSD가 읽기 전용 상태가 됩니다. 읽기 전용 조건이 발생하면 DD OS는 드라이브를 읽기 전용 캐시로 처리합니다.

  SSD가 읽기 전용 상태이고 교체가 필요한 경우 `EVT-STORAGE-00001` 알림이 표시됩니다.
- SSD EOL
  SSD의 수명이 끝나면 SSD 셸프 내의 SSD 위치를 식별하는 하드웨어 장애 알림이 생성됩니다. 이 알림은 중요 알림으로 분류됩니다.

  EOL 카운터가 98에 도달하면 `EVT-STORAGE-00016` 알림이 표시됩니다. EOL 카운터가 99에 도달하면 드라이브가 사전 예방 차원에서 장애 처리됩니다.

13장

SCSI 타겟

이 장에는 다음과 같은 내용이 포함됩니다.

SCSI Target 개요

SCSI(Small Computer System Interface) Target은 모든 SCSI 서비스 및 전송을 위한 통합 관리 데몬입니다. SCSI Target은 DD VTL(Virtual Tape Library), DD Boost over FC(Fibre Channel) 및 vDisk/ProtectPoint Block Services와 DD 시스템에 타겟 LUN(Logical Unit Number)이 있는 모든 서비스를 지원합니다.

SCSI Target 서비스 및 전송

SCSI Target 데몬은 FC 포트가 있거나 DD VTL의 라이센스가 등록된 경우에 시작됩니다. 모든 SCSI Target *서비스* 및 *전송*을 위한 통합 관리를 제공합니다.

- *서비스*는 DD VTL(테이프 드라이브 및 체인저), DD Boost over FC(프로세서 디바이스) 또는 vDisk(가상 디스크 디바이스)와 같이 DD 시스템에 타겟 LUN이 있고 SCSI Target 명령을 사용하는 모든 서비스를 말합니다.
- *전송*을 통해 *디바이스*가 *이니시에이터*에 표시될 수 있습니다.
- *이니시에이터*는 FC 프로토콜을 사용하여 데이터를 읽고 쓰기 위해 시스템에 접속하는 백업 클라이언트입니다. 특정 이니시에이터는 DD Boost over FC, vDisk 또는 DD VTL을 지원하지만 3가지 모두를 지원하지는 않습니다.
- *디바이스*는 물리적 포트를 통해 SAN(Storage Area Network)에 표시됩니다. 호스트 이니시에이터는 SAN을 통해 DD 시스템과 통신합니다.
- *액세스 그룹*은 디바이스와 이니시에이터 사이의 액세스 권한을 관리합니다.
- *엔드포인트*는 이니시에이터가 접속하는 DD 시스템에 있는 논리 타겟입니다. 엔드포인트의 비활성화, 활성화 또는 이름 변경이 가능합니다. 엔드포인트를 삭제하려면 연결된 전송 하드웨어가 더 이상 존재하지 않아야 합니다. 새로운 전송 접속이 발생하면 엔드포인트가 자동으로 검색 및 생성됩니다. 엔드포인트에는 포트 토폴로지, FCP2-RETRY 상태, WWPN 및 WWNN과 같은 속성이 있습니다.
- *NPIV*(N-Port ID Virtualization)는 여러 엔드포인트에서 단일의 물리적 포트를 공유할 수 있도록 하는 Fibre Channel 기능입니다. NPIV는 하드웨어 요구 사항을 완화하고 페일오버 기능을 제공합니다.
- DD OS 6.0에서는 사용자가 페일오버를 위한 보조 시스템 주소의 시퀀스를 지정할 수 있습니다. 예를 들어 시스템이 0a, 0b, 1a, 1b를 지정하고 사용자가 1b, 1a, 0a, 0b를 지정한 경우 사용자 지정 시퀀스가 페일오버에 사용됩니다. `scsitarget endpoint show detailed` 명령은 사용자가 지정한 시퀀스를 표시합니다.

다음 예외 사항을 참고하십시오.

- DD Boost는 FC와 IP 클라이언트에 동시에 서비스를 제공할 수 있지만 두 전송이 동일한 이니시에이터를 공유할 수는 없습니다.
- 액세스 그룹당 하나의 이니시에이터만 있어야 합니다. 각 액세스 그룹에는 하나의 유형(DD VTL, vDisk/ProtectPoint Block Services 또는 DD Boost over FC)이 할당됩니다.

SCSI Target 아키텍처 - 지원되는 아키텍처 및 지원되지 않는 아키텍처

SCSI Target은 다음 아키텍처를 지원합니다.

- **서로 다른 이니시에이터에서 DD VTL과 DD Boost over FC 사용:** 2개의 서로 다른 이니시에이터(동일하거나 다른 클라이언트에 있는 이니시에이터)에서 동일하거나 다른 DD 시스템 타겟 엔드포인트를 통해 DD VTL 및 DD Boost over FC를 사용하여 DD 시스템에 액세스할 수 있습니다.
- **한 이니시에이터에서 DD VTL과 DD Boost over FC를 사용하여 2개의 서로 다른 DD 시스템에 액세스:** 모든 서비스를 사용하여 단일 이니시에이터에서 2개의 서로 다른 DD 시스템에 액세스할 수 있습니다.

SCSI Target은 다음 아키텍처를 지원하지 않습니다.

- **한 이니시에이터에서 DD VTL과 DD Boost over FC를 사용하여 동일한 DD 시스템에 액세스:** 동일한 이니시에이터에서는 서로 다른 서비스를 통해 동일한 DD 시스템에 액세스할 수 없습니다.

씬 프로토콜

씬 프로토콜은 기본 프로토콜이 SCSI 명령에 응답할 수 없을 때 해당 명령에 응답하는 VDisk 및 DD VTL에 대한 경량 데몬입니다. 여러 프로토콜을 사용하는 Fibre Channel 환경에서 씬 프로토콜을 다음을 수행합니다.

- 이니시에이터 멈춤 방지
- 불필요한 이니시에이터 중단 방지
- 이니시에이터 디바이스가 사라지지 않도록 방지
- 대기 모드 지원
- 빠른 검색과 사전 검색이 가능한 디바이스 지원
- 프로토콜 HA 동작 개선
- 빠른 레지스트리 액세스 불필요

DD Boost 및 scscitarget 명령(CLI)에 대한 자세한 정보

DD System Manager를 통해 DD Boost를 사용하는 방법에 대한 자세한 내용은 이 문서의 관련 장을 참조하십시오. DD Boost에 대한 다른 정보 유형은 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

이 장에서는 DD System Manager를 통해 SCSI Target을 사용하는 방법을 중점적으로 설명합니다. 기본 작업에 익숙해진 후에는 *Data Domain Operating System 명령 참조 가이드*의 `scscitarget` 명령을 사용하여 더 많은 고급 관리 작업을 수행할 수 있습니다.

DD VTL 트래픽이 많은 경우 그룹의 SCSI Target 또는 vdisk 디바이스 하나 이상에 대한 사용 중인 엔드포인트 목록을 기본 및 보조 엔드포인트 목록으로 전환하는 `scsitarget group use` 명령을 실행하지 마십시오.

Fibre Channel 보기

Fibre Channel 보기에는 Fibre Channel 및/또는 NPIV가 사용하도록 설정되었는지 여부에 대한 현재 상태가 표시됩니다. 또한 Resources와 Access Groups라는 두 가지 탭이 표시됩니다. 리소스에는 포트, 엔드포인트 및 이니시에이터가 포함됩니다. 액세스 그룹에는 이니시에이터 WWPN(Worldwide Port Name) 또는 별칭의 컬렉션과 이들이 액세스할 수 있는 드라이브 및 체인저가 저장됩니다.

NPIV 활성화

NPIV(N_Port ID Virtualization)는 여러 엔드포인트에서 단일의 물리적 포트를 공유할 수 있도록 하는 Fibre Channel 기능입니다. NPIV는 하드웨어 요구 사항을 완화하고 엔드포인트 페일오버/페일백 기능을 제공합니다. NPIV는 기본적으로 구성되지 않으므로 활성화해야 합니다.

참고

NPIV는 HA 구성에서 기본적으로 활성화됩니다.

NPIV는 간소화된 다중 시스템 통합 기능을 제공합니다.

- NPIV는 하나의 HBA 물리적 포트를 여러 WWPN을 사용하여 Fibre Channel Fabric에 등록할 수 있도록 하는 ANSI T11 표준입니다.

- 가상 포트와 물리적 포트는 포트 속성이 동일하며 정확히 같은 방식으로 동작합니다.
- 엔드포인트와 포트 간에는 여러 엔드포인트가 동일한 물리적 포트를 공유하는 m:1의 관계가 존재할 수 있습니다.

특히 NPIV를 활성화하면 다음 기능을 사용할 수 있습니다.

- 여러 엔드포인트를 각각 가상(NPIV) 포트를 사용하여 단일 물리적 포트에 연결할 수 있습니다. 기본 포트는 물리적 포트에 대한 자리 표시자이며 엔드포인트에 연결되지 않습니다.
- NPIV를 사용하는 경우 엔드포인트 페일오버/페일백이 자동으로 활성화됩니다.

참고

NPIV를 활성화한 후에는 각 엔드포인트에서 "Secondary System Address"를 지정해야 합니다. 그렇지 않으면 엔드포인트 페일오버가 실행되지 않습니다.

- 여러 DD 시스템을 단일 DD 시스템으로 통합해도 단일 DD 시스템의 HBA의 수는 동일하게 유지됩니다.
- 엔드포인트 페일오버는 포트가 온라인에서 오프라인으로 전환되는 것을 FC-SSM이 감지하면 트리거됩니다. 물리적 포트가 scsitarget을 활성화하기 전에 오프라인 상태이다가 scsitarget을 활성화한 후에도 계속 오프라인 상태인 경우 FC-SSM이 포트 오프라인 이벤트를 생성하지 않으므로 엔드포인트 페일오버를 실행할 수 없습니다. 포트가 다시 온라인 상태가 되고 자동 페일백이 활성화되어 있는 경우 해당 포트를 기본 포트로 사용하는 페일오버된 엔드포인트가 모두 해당 기본 포트로 페일백됩니다.

Data Domain HA 기능을 실행하려면 페일오버 프로세스를 진행하는 동안 NPIV가 HA 쌍의 노드 간에 WWN을 이동해야 합니다.

참고

NPIV를 활성화하려면 다음 조건이 충족되어야 합니다.

- DD 시스템이 DD OS 5.7을 실행해야 합니다.
- 모든 포트는 4Gb, 8Gb 및 16Gb Fibre Channel HBA 및 SLIC에 접속해야 합니다.
- DD 시스템 ID가 유효해야 합니다. 즉, 0이 아니어야 합니다.

또한 포트 토폴로지 및 포트 이름을 검토하여 NPIV 활성화가 가능한지가 확인됩니다.

- *모든* 포트에 대한 토폴로지가 loop-preferred인 경우 NPIV가 허용됩니다.
- *일부* 포트에 대한 토폴로지가 loop-preferred인 경우 NPIV가 허용됩니다. 그러나 loop-only인 포트에 대해서는 NPIV를 비활성화하거나 loop-preferred로 토폴로지를 재구성해야 NPIV가 제대로 기능합니다.
- 모든 포트의 토폴로지가 loop-preferred가 *아닌* 경우 NPIV가 허용되지 *않습니다*.
- 액세스 그룹에 포트 이름이 표시되는 경우 포트 이름이 연결된 엔드포인트 이름으로 대체됩니다.

절차

1. **Hardware** > **Fibre Channel**을 선택합니다.
2. NPIV: Disabled 옆에서 **Enable**을 선택합니다.
3. Enable NPIV 대화 상자에서 NPIV를 활성화하려면 모든 Fibre Channel 포트를 비활성화해야 한다는 내용의 경고가 표시됩니다. 이 작업을 확인하려면 **Yes**를 선택합니다.

CLI 절차

a. (글로벌) NPIV가 활성화되어 있는지 확인합니다.

```
# scsitarget transport option show npiv
SCSI Target Transport Options
Option   Value
------   --------
npiv     disabled
------   --------
```

b. NPIV가 비활성화되어 있는 경우 활성화합니다. 먼저 모든 포트를 비활성화해야 합니다.

```
# scsitarget port disable all
All ports successfully disabled.
# scsitarget transport option set npiv enabled
Enabling FiberChannel NPIV mode may require SAN zoning to
be changed to configure both base port and NPIV WWPNs.
Any FiberChannel port names used in the access groups will
be converted to their corresponding endpoint names in order
to prevent ambiguity.
    Do you want to continue? (yes|no) [no]:
```

c. 비활성화된 포트를 다시 활성화합니다.

```
# scsitarget port enable all
All ports successfully enabled.
```

d. 물리적 포트의 NPIV 설정이 “auto”로 구성되어 있는지 확인합니다.

```
# scsitarget port show detailed 0a
System Address:     0a
Enabled:            Yes
Status:             Online
Transport:          FibreChannel
Operational Status: Normal
FC NPIV:            Enabled (auto)
.
.
.
```

e. 선택한 운영 및 보조 포트를 사용하여 새 엔드포인트를 생성합니다.

```
# scsitarget endpoint add test0a0b system-address 0aprimary-
system-address 0a secondary-system-address 0b
```

엔드포인트가 기본적으로 비활성화되어 있으므로 활성화합니다.

```
# scsitarget endpoint enable test0a0b
```

그런 다음 엔드포인트 정보를 표시합니다.

```
# scsitarget endpoint show detailed test0a0b
Endpoint:                 test0a0b
Current System Address:   0b
Primary System Address:   0a
Secondary System Address: 0b
Enabled:                  Yes
Status:                   Online
Transport:                FibreChannel
FC WWNN:                  50:02:18:80:08:a0:00:91
FC WWPN:                  50:02:18:84:08:b6:00:91
```

f. 새로 생성된 엔드포인트의 자동 생성된 WWPN에 호스트 시스템을 조닝(Zoning)합니다.

g. DD VTL, vDisk 또는 DFC(DD Boost over Fibre Channel) 디바이스를 생성하고 이 디바이스를 호스트 시스템에서 사용할 수 있는지 확인합니다.

h. 호스트에서 선택한 DD 디바이스에 액세스(읽기 및/또는 쓰기)할 수 있는지 확인합니다.

i. “secondary” 옵션으로 엔드포인트 페일오버를 테스트하여 엔드포인트가 SSA(Secondary System Address)로 이동하는지 확인합니다.

```
# scsitarget endpoint use test0a0b secondary
```

j. 여전히 호스트에서 선택한 DD 디바이스에 액세스(읽기 및/또는 쓰기)할 수 있는지 확인합니다. “primary” 옵션으로 페일백을 테스트하여 엔드포인트가 다시 PSA(Primary System Address)로 돌아가는지 확인합니다.

```
# scsitarget endpoint use test0a0b primary
```

k. 여전히 호스트에서 선택한 DD 디바이스에 액세스(읽기 및/또는 쓰기)할 수 있는지 확인합니다.

NPIV 해제

NPIV를 해제하려면 여러 엔드포인트가 연결된 포트가 없어야 합니다.

참고

NPIV는 HA 구성에 필요합니다. 기본적으로 설정되며, 해제할 수 없습니다.

절차

1. **Hardware** > **Fibre Channel**을 선택합니다.
2. NPIV: Enabled 옆에서 **Disable**을 선택합니다.
3. Disable NPIV 대화 상자에서 구성 수정에 대한 메시지를 검토하고 준비가 되면 **OK**를 선택합니다.

Resources 탭

Hardware > **Fibre Channel** > **Resources** 탭에는 포트, 엔드포인트 및 이니시에이터에 대한 정보가 표시됩니다.

표 123 포트

항목	설명
System Address	포트의 시스템 주소입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Enabled	포트 작동 상태로, Enabled 또는 Disabled입니다.
NPIV	NPIV 상태로, Enabled 또는 Disabled입니다.
Link Status	링크 상태로, Online 또는 Offline으로 표시되며 포트의 작동 여부 및 트래픽 처리 가능 여부를 나타냅니다.
Operation Status	작업 상태로, Normal 또는 Marginal입니다.
# of Endpoints	이 포트에 연결된 엔드포인트의 수입니다.

표 124 엔드포인트

항목	설명
Name	엔드포인트의 이름입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
System Address	엔드포인트의 시스템 주소입니다.
Enabled	포트 작동 상태로, Enabled 또는 Disabled가 있습니다.
Link Status	Online 또는 Offline으로, 포트가 작동 중이고 트래픽을 처리할 수 있는지 여부를 나타냅니다.

표 125 이니시에이터

항목	설명
Name	이니시에이터의 이름입니다.
Service	이니시에이터가 지원하는 서비스로, DD VTL, DD Boost 또는 vDisk입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Vendor Name	이니시에이터의 모델입니다.
Online Endpoints	이 이니시에이터에 표시된 엔드포인트입니다. 이니시에이터를 사용할 수 없는 경우 `none` 또는 `offline`이 표시됩니다.

포트 구성

시작 시 포트가 검색되고 검색된 각 포트에 대해 단일의 엔드포인트가 자동으로 생성됩니다.

기본 포트의 속성은 NPIV가 설정되었는지 여부에 따라 다릅니다.

- 비 NPIV 모드에서 포트는 엔드포인트와 동일한 속성을 사용합니다. 즉, 기본 포트 및 엔드포인트의 WWPN이 동일합니다.
- NPIV 모드에서 기본 포트 속성은 기본값에서 파생됩니다. 즉, NPIV 모드를 지속적으로 전환할 수 있도록 기본 포트에 대한 새 WWPN이 생성되고 유지됩니다. 또한 NPIV 모드에서는 포트 하나로 여러 엔드포인트를 지원할 수 있습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **Ports** 아래에서 포트를 선택한 다음 **Modify**(연필 모양)를 선택합니다.

3. Configure Port 대화 상자에서 이 포트의 NPIV를 자동으로 설정 또는 해제할지를 선택합니다.
4. Topology의 경우 Loop Preferred, Loop Only, Point to Point 또는 Default를 선택합니다.
5. Speed의 경우 1, 2, 4, 8 또는 16Gbps를 선택하거나 auto를 선택합니다.
6. **OK**를 선택합니다.

포트 설정

포트를 사용하려면 먼저 사용하도록 설정해야 합니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Ports** > **Enable**을 선택합니다. 모든 포트가 이미 설정된 경우 해당 결과에 대한 메시지가 표시됩니다.
3. Enable Ports 대화 상자의 목록에서 포트를 하나 이상 선택하고 **Next**를 선택합니다.
4. 확인 후 **Next**를 선택하여 작업을 완료합니다.

포트 해제

포트를 단순히 해제하거나 포트의 모든 엔드포인트를 하나 이상의 다른 포트로 페일오버할 수 있습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Ports** > **Disable**을 선택합니다.
3. Disable Endpoints 대화 상자의 목록에서 포트를 하나 이상 선택하고 **Next**를 선택합니다.
4. 확인 대화 상자에서 포트를 단순히 해제하거나 포트의 모든 엔드포인트를 다른 포트로 페일오버하도록 선택할 수 있습니다.

엔드포인트 추가

엔드포인트는 기본 가상 포트에 매핑되는 가상 객체입니다. 비 NPIV 모드(HA 구성에서는 사용할 수 없음)에서는 물리적 포트 하나당 한 개의 엔드포인트만 허용되며 엔드포인트를 Fabric으로 구성할 때는 기본 포트가 사용됩니다. NPIV가 활성화된 경우 가상(NPIV) 포트를 사용하여 여러 엔드포인트를 물리적 포트 하나에 연결할 수 있으며 엔드포인트 페일오버/페일백이 활성화됩니다.

참고

HA 구성에서는 비 NPIV 모드를 사용할 수 없습니다. NPIV는 기본적으로 활성화되며 비활성화할 수 없습니다.

참고

NPIV 모드에서 엔드포인트에는 다음이 적용됩니다.

- 운영 시스템 주소가 있습니다.
- 0개 이상의 보조 시스템 주소가 있을 수 있습니다.
- 포트 장애 시 대체 시스템 주소로 페일오버될 수 있지만 여유가 없는 포트로의 페일오버는 지원되지 않습니다.
- 포트가 온라인으로 돌아오면 원래의 운영 포트를 사용하도록 페일백될 수 있습니다.

참고

NPIV를 사용할 때는 각 엔드포인트에 하나의 프로토콜(즉, DD VTL Fibre Channel, DD Boost-over-Fibre Channel 또는 vDisk Fibre Channel)만 사용하는 것이 좋습니다. 페일오버 구성의 경우 보조 엔드포인트도 운영 엔드포인트와 동일한 프로토콜을 사용하도록 구성해야 합니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **Endpoints** 아래에서 **Add**(+ 기호)를 선택합니다.
3. Add Endpoint 대화 상자에서 엔드포인트의 이름(1~128자)을 입력합니다. 이 필드는 비어 있거나 "all"이라는 단어일 수 없으며 별표(*), 물음표(?), 슬래시 또는 백슬래시(/, \), 오른쪽 또는 왼쪽 괄호[(,)]를 포함할 수 없습니다.
4. Endpoint Status로는 Enabled 또는 Disabled를 선택합니다.
5. NPIV가 활성화된 경우 드롭다운 목록에서 운영 시스템 주소를 선택합니다. 운영 시스템 주소는 보조 시스템 주소와 달라야 합니다.
6. NPIV가 활성화된 경우 보조 시스템 주소로 페일오버하려면 보조 시스템 주소 옆의 해당하는 상자를 선택합니다.
7. **OK**를 선택합니다.

엔드포인트 구성

엔드포인트를 추가한 후 Configure Endpoint 대화 상자에서 엔드포인트를 수정할 수 있습니다.

참고

NPIV를 사용할 때는 각 엔드포인트에 하나의 프로토콜(즉, DD VTL Fibre Channel, DD Boost-over-Fibre Channel 또는 vDisk Fibre Channel)만 사용하는 것이 좋습니다. 페일오버 구성의 경우 보조 엔드포인트도 운영 엔드포인트와 동일한 프로토콜을 사용하도록 구성해야 합니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **Endpoints** 아래에서 엔드포인트를 선택한 다음 **Modify**(연필 모양)를 선택합니다.
3. Configure Endpoint 대화 상자에서 엔드포인트의 이름(1자~128자)을 입력합니다. 이 필드는 비어 있거나 "all"이라는 단어일 수 없으며 별표(*), 물음표(?), 슬래시 또는 백슬래시(/, \), 오른쪽 또는 왼쪽 괄호[(,)]를 포함할 수 없습니다.

4. Endpoint Status로는 Enabled 또는 Disabled를 선택합니다.
5. 드롭다운 목록에서 운영 시스템 주소를 선택합니다. 운영 시스템 주소는 보조 시스템 주소와 달라야 합니다.
6. 보조 시스템 주소로 페일오버하려면 보조 시스템 주소 옆의 해당하는 상자를 선택합니다.
7. **OK**를 선택합니다.

엔드포인트의 시스템 주소 수정

`scsitarget endpoint modify` 명령 옵션을 사용하여 SCSI Target 엔드포인트의 활성 시스템 주소를 수정할 수 있습니다. 컨트롤러 업그레이드 후 또는 컨트롤러 HBA(Host Bus Adapter)가 이동된 경우 등 엔드포인트가 더 이상 존재하지 않는 시스템 주소와 연결되어 있는 경우에 유용합니다. 엔드포인트의 시스템 주소가 수정되면 WWPN(Worldwide Port Name) 및 WWNN(Worldwide Node Name)을 포함하는 엔드포인트의 모든 속성(있는 경우)이 보존되고 새 시스템 주소와 함께 사용됩니다.

다음 예에서는 엔드포인트 ep-1이 시스템 주소 5a에 할당되었지만 이 시스템 주소가 더 이상 유효하지 않습니다. 새 컨트롤러 HBA가 시스템 주소10a에 추가되었습니다. SCSI Target 서브시스템은 새로 검색된 시스템 주소에 대해 자동으로 새 엔드포인트 ep-new를 생성했습니다. 단일 엔드포인트만 지정된 시스템 주소와 연결할 수 있기 때문에 ep-new를 삭제한 후 ep-1을 시스템 주소 10a에 할당해야 합니다.

참고

WWPN 및 WWNN이 다른 시스템 주소로 이동했기 때문에 SAN 환경에 따라 수정된 엔드포인트를 온라인 상태로 만드는 데 어느 정도 시간이 걸릴 수 있습니다. 새 구성을 반영하려면 SAN 조닝(Zoning)도 업데이트해야 합니다.

절차

1. 모든 엔드포인트를 표시해 변경할 엔드포인트를 확인합니다.

   ```
   # scsitarget endpoint show list
   ```

2. 모든 엔드포인트를 사용하지 않도록 설정합니다.

   ```
   # scsitarget endpoint disable all
   ```

3. 불필요한 새 엔드포인트 ep-new를 삭제합니다.

   ```
   # scsitarget endpoint del ep-new
   ```

4. 사용하고자 하는 엔드포인트 ep-1을 새 시스템 주소 10a를 할당해 수정합니다.

   ```
   # scsitarget endpoint modify ep-1 system-address 10a
   ```

5. 모든 엔드포인트를 설정합니다.

   ```
   # scsitarget endpoint enable all
   ```

엔드포인트 설정

비 NPIV 모드에서 엔드포인트를 설정하면 현재 포트가 해제된 경우에만 포트가 설정됩니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Endpoints** > **Enable**을 선택합니다. 모든 엔드포인트가 이미 설정된 경우 이 결과에 대한 메시지가 표시됩니다.

3. Enable Endpoints 대화 상자의 목록에서 엔드포인트를 하나 이상 선택하고 **Next**를 선택합니다.
4. 확인 후 **Next**를 선택하여 작업을 완료합니다.

엔드포인트 해제

포트를 사용하는 모든 엔드포인트를 해제하지 않는 한, 즉 비 NPIV 모드에서는 엔드포인트를 해제해도 연결된 포트가 해제되지 않습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Endpoints** > **Disable**을 선택합니다.
3. Disable Endpoints 대화 상자의 목록에서 엔드포인트를 하나 이상 선택하고 **Next**를 선택합니다. 엔드포인트가 사용 중인 경우 엔드포인트를 해제하면 시스템이 중단될 수 있다는 경고가 표시됩니다.
4. **Next**를 선택하여 작업을 완료합니다.

엔드포인트 삭제

기본 하드웨어를 더 이상 사용할 수 없는 경우 엔드포인트를 삭제할 수 있습니다. 그러나 기본 하드웨어가 여전히 존재하거나 사용할 수 있게 되는 경우에는 하드웨어에 대한 새 엔드포인트가 자동으로 검색되고 기본값을 바탕으로 구성됩니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Endpoints** > **Delete**를 선택합니다.
3. Disable Endpoints 대화 상자의 목록에서 엔드포인트를 하나 이상 선택하고 **Next**를 선택합니다. 엔드포인트가 사용 중인 경우 엔드포인트를 삭제하면 시스템이 중단될 수 있다는 경고가 표시됩니다.
4. **Next**를 선택하여 작업을 완료합니다.

이니시에이터 추가

FC(Fibre Channel) 프로토콜을 사용하여 데이터를 읽고 쓰기 위해 시스템에 접속하는 백업 클라이언트로 사용할 이니시에이터를 추가합니다. 특정 이니시에이터는 FC 기반 DD Boost 또는 DD VTL을 지원하지만 둘 모두를 지원하지는 않습니다. 하나의 DD 시스템에 최대 1,024개의 이니시에이터를 구성할 수 있습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. Initiators 아래에서 Add(+ 기호)를 선택합니다.
3. Add Initiator 대화 상자에서 포트의 고유한 WWPN을 지정된 형식으로 입력합니다.
4. 이니시에이터의 이름을 입력합니다.
5. Address Method를 선택합니다. **Auto**는 표준 주소 지정에 사용되고 **VSA**(Volume Set Addressing)는 주로 가상 버스, 타겟 및 LUN의 주소 지정에 사용됩니다.
6. **OK**를 선택합니다.

CLI 절차

```
# scsitarget group add My_Group initiator My_Initiator
```

이니시에이터 수정 또는 삭제

이니시에이터를 삭제하려면 이니시에이터가 오프라인 상태이고 어떤 그룹에도 연결되어 있지 않아야 합니다. 그렇지 않은 경우에는 오류 메시지가 나타나고 이니시에이터가 삭제되지 않습니다. 액세스 그룹을 삭제하기 전에 액세스 그룹의 모든 이니시에이터를 삭제해야 합니다. 이니시에이터가 표시되는 상태로 남는 경우 자동으로 다시 검색될 수 있습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. Initiators에서 이니시에이터 중 하나를 선택합니다. 이니시에이터를 삭제하려면 Delete(X) 버튼을 선택합니다. 이니시에이터를 수정하려면 연필 모양의 Modify 버튼을 선택하여 Modify Initiator 대화 상자를 표시합니다.
3. 이니시에이터의 Name 및/또는 Address Method[**Auto**가 표준 주소 지정에 사용되고 **VSA**(Volume Set Addressing)가 가상 버스, 타겟 및 LUN의 주소 지정에 주로 사용됨]를 변경합니다.
4. **OK**를 선택합니다.

이니시에이터 별칭 설정에 대한 권장 사항 - CLI만 해당
구성 프로세스 중에 발생할 수 있는 혼란과 사용자 오류를 줄일 수 있도록 이니시에이터 별칭을 설정하는 것이 좋습니다.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group    Status   WWNN                     WWPN                     Port
---------  -------  -------  -----------------------  -----------------------  ---
NewVTL     aussie1  Online   20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
                    Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
---------  ------------------  --------------
NewVTL                              auto
---------  ------------------  --------------
```

고정 주소(루프 ID) 설정

일부 백업 소프트웨어를 사용하려면 모든 전용 루프 타겟에 다른 노드와 충돌하지 않는 고정 주소(루프 ID)가 있어야 합니다. 루프 ID의 범위는 0-125입니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Set Loop ID**를 선택합니다.
3. Set Loop ID 대화 상자에서 루프 ID(0-125)를 입력하고 **OK**를 선택합니다.

페일오버 옵션 설정

NPIV가 활성화된 경우 자동 페일오버 및 페일백에 대한 옵션을 설정할 수 있습니다.

다음은 Fibre Channel 포트 페일오버에 대한 애플리케이션별 예상 동작입니다.

- Fibre Channel 엔드포인트가 페일오버되면 DD Boost over Fibre Channel이 사용자 개입 없이 계속해서 작동됩니다.
- DD VTL Fibre Channel 엔드포인트가 페일오버되면 DD VTL Fibre Channel이 사용자 개입 없이 계속해서 작동됩니다. 영향을 받은 Fibre Channel 엔드포인트를 사용하여 이니시에이터에서 검색을 수행해야 합니다. 즉, DD VTL 디바이스의 운영 체제를 검색하고 구성해야 합니다. 활성 백업 및 복구 작업을 다시 시작해야 합니다.

- Fibre Channel 엔드포인트가 페일오버되면 vDisk Fibre Channel이 사용자 개입 없이 계속해서 작동됩니다.

관리자에 의해 모든 포트가 비활성화된 후 다시 활성화된 경우 포트가 활성화된 순서가 지정되지 않으므로 자동 페일백이 보장되지 않습니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources**를 선택합니다.
2. **More Tasks** > **Set Failover Options**를 선택합니다.
3. Set Failover Options 대화 상자에서 페일오버 및 페일백 지연을 초 단위로 입력하고 자동 페일백 활성화 여부를 선택한 다음 **OK**를 선택합니다.

Access Groups 탭

Hardware > **Fibre Channel** > **Access Groups** 탭은 DD Boost 및 DD VTL 액세스 그룹에 대한 정보를 제공합니다. *View DD Boost Groups* 또는 *View VTL Groups* 링크를 선택하면 DD Boost 또는 DD VTL 페이지로 이동됩니다.

표 126 액세스 그룹

항목	설명
Group Name	액세스 그룹의 이름입니다.
Service	이 액세스 그룹에 대한 서비스입니다(DD Boost 또는 DD VTL).
Endpoints	이 액세스 그룹과 연결된 엔드포인트입니다.
Initiators	이 액세스 그룹과 연결된 이니시에이터입니다.
Number of Devices	이 액세스 그룹과 연결된 디바이스의 수입니다.

FC 링크 모니터링의 DD OS 버전별 차이

DD OS 릴리즈에 따라 FC(Fibre Channel) 링크 모니터링을 처리하는 방법이 다릅니다.

DD OS 5.3 이상
포트 모니터링에서 시스템 시작 시 FC 포트를 감지하며, 포트가 활성화되어 있고 오프라인 상태인 경우 알림을 생성합니다. 알림을 지우려면 `scsitarget port` 명령을 사용하여 사용하지 않는 포트를 비활성화하십시오.

DD OS 5.1~5.3
포트가 오프라인 상태인 경우 링크가 다운되었다는 알림이 생성됩니다. 이 알림은 관리되므로 지워질 때까지 활성 상태로 유지되며, DD VTL FC 포트가 온라인 상태이거나 비활성화되면 지워집니다. 포트를 사용하고 있지 않은 경우 모니터링할 필요가 없으면 포트를 비활성화하십시오.

DD OS 5.0~5.1
포트가 오프라인 상태인 경우 링크가 다운되었다는 알림이 생성됩니다. 이 알림은 관리되지 않으므로 활성 상태로 유지되지 않으며 현재 알림 목록에 나타나지 않습니다. 포트가 온라인 상태이면 링크가 연결되어 있다는 알림이 생성됩니다. 포트를 사용하고 있지 않은 경우 모니터링할 필요가 없으면 포트를 비활성화하십시오.

DD OS 4.9~5.0
FC 포트가 모니터링할 DD VTL 그룹에 포함되어야 합니다.

14장

DD Boost 작업

이 장에는 다음과 같은 내용이 포함됩니다.

Data Domain Boost 정보

DD Boost(Data Domain Boost)는 백업 및 엔터프라이즈 애플리케이션과의 고급 통합 기능을 제공하여 성능 및 사용 편의성을 개선합니다. DD Boost는 데이터 중복 제거 프로세스의 일부를 백업 서버 또는 애플리케이션 클라이언트에 분산하여 클라이언트 측에서 데이터 중복 제거를 수행할 수 있게 함으로써 백업 및 복구의 속도와 효율을 높입니다.

DD Boost는 선택적으로 사용할 수 있는 제품으로, Data Domain 시스템에 사용하려면 별도의 라이센스가 필요합니다. Data Domain 시스템용 DD Boost 소프트웨어 라이센스 키는 Data Domain에서 직접 구매할 수 있습니다.

참고

특별 라이센스인 BLOCK-SERVICES-PROTECTPOINT가 있으면 클라이언트에서 ProtectPoint 블록 서비스를 통해 DD Boost 라이센스 없이 DD Boost 기능을 사용할 수 있습니다. DD Boost를 ProtectPoint 클라이언트에서만 활성화한 경우, 즉 BLOCK-SERVICES-PROTECTPOINT 라이센스만 설치한 경우 DD Boost가 ProtectPoint에 대해서만 활성화된 것으로 라이센스 상태에 표시됩니다.

DD Boost에는 백업 서버에서 실행되는 구성 요소와 Data Domain 시스템에서 실행되는 구성 요소가 있습니다.

- NetWorker 백업 애플리케이션, Avamar 백업 애플리케이션 및 기타 DD Boost 파트너 백업 애플리케이션의 컨텍스트에서 백업 서버에서 실행되는 구성 요소(DD Boost 라이브러리)는 특정 백업 애플리케이션에 통합됩니다.
- Symantec 백업 애플리케이션(NetBackup 및 Backup Exec)과 Oracle RMAN 플러그인의 컨텍스트에서는 각 미디어 서버에 설치된 해당 버전의 DD Boost 플러그인을 다운로드해야 합니다. DD Boost 플러그인에는 Data Domain 시스템에서 실행 중인 DD Boost 서버와 통합하기 위한 DD Boost 라이브러리가 포함됩니다.

백업 애플리케이션(예: Avamar, NetWorker, NetBackup 또는 Backup Exec)은 백업 및 복제가 언제 발생하는지 제어하는 정책을 설정합니다. 관리자는 하나의 콘솔에서 백업, 복제 및 복구를 관리하며, 효율적인 WAN Replicator 소프트웨어를 포함하여 DD Boost의 모든 기능을 사용할 수 있습니다. 이 애플리케이션은 카탈로그의 모든 파일(데이터 모음)뿐 아니라 Data Domain 시스템에서 생성된 파일도 관리합니다.

Data Domain 시스템에서 사용자가 생성하는 스토리지 유닛은 DD Boost 프로토콜을 사용하는 백업 애플리케이션에 노출됩니다. Symantec 애플리케이션의 경우 스토리지 유닛이 디스크 풀로 표시됩니다. NetWorker의 경우 스토리지 유닛은 LSU(Logical Storage Unit)로 표시됩니다. 스토리지 유닛은 MTree이기 때문에 MTree 할당량 설정을 지원합니다. 스토리지 유닛을 대신해 MTree를 생성하지 마십시오.

이 장에는 설치 지침이 포함되어 있지 않으므로 설치하려는 제품의 설명서를 참조하십시오. 예를 들어 Symantec 백업 애플리케이션(NetBackup 및 Backup Exec)을 사용해 DD Boost를 설정하는 방법에 대한 내용은 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오. 기타 애플리케이션을 사용해 DD Boost를 설정하는 방법에 대한 내용은 애플리케이션별 설명서를 참조하십시오.

Data Domain 시스템에서 DD Boost를 구성하고 관리하는 방법에 대한 추가 정보는 *OpenStorage용 Data Domain Boost 관리 가이드*(NetBackup 및 Backup Exec의 경우) 및 *Domain Boost for Partner Integration Administration Guide*(그 외 백업 애플리케이션의 경우)에서 확인할 수 있습니다.

DD System Manager를 사용한 DD Boost 관리

DD System Manager에서 DD Boost 보기에 액세스합니다.

절차

1. **Data Management** > **File System**을 선택합니다. 파일 시스템 상태를 확인하여 파일 시스템이 활성화되고 실행 중인지 확인합니다.
2. **Protocols** > **DD Boost**를 선택합니다.

   라이센스가 없는 상태에서 DD Boost 페이지로 이동하면 Status에 DD Boost의 라이센스가 등록되지 않았다는 메시지가 나타납니다. **Add License**를 클릭하고 Add License Key 대화 상자에 유효한 라이센스를 입력합니다.

   참고

   특별 라이센스인 BLOCK-SERVICES-PROTECTPOINT가 있으면 클라이언트에서 ProtectPoint 블록 서비스를 통해 DD Boost 라이센스 없이 DD Boost 기능을 사용할 수 있습니다. DD Boost를 ProtectPoint 클라이언트에서만 활성화한 경우(BLOCK-SERVICES-PROTECTPOINT 라이센스만 설치한 경우) DD Boost가 ProtectPoint에 대해서만 활성화된 것으로 라이센스 상태에 표시됩니다.

   DD Boost 탭(Settings, Active Connections, IP Network, Fibre Channel 및 Storage Units)을 사용해 DD Boost를 관리합니다.

DD Boost 사용자 이름 지정

DD Boost 사용자는 DD OS 사용자이기도 합니다. DD Boost 사용자 이름을 지정하려면 기존 DD OS 사용자 이름을 선택하거나, 새로운 DD OS 사용자 이름을 생성하고 이 이름을 DD Boost 사용자로 지정합니다.

백업 애플리케이션은 DD Boost 사용자 이름 및 암호를 사용하여 Data Domain 시스템에 접속합니다. 이 시스템에 접속하는 각 백업 서버에서 이러한 자격 증명을 구성해야 합니다. Data Domain 시스템에서는 여러 DD Boost 사용자를 지원합니다. Symantec NetBackup 및 Backup Exec를 사용하여 DD Boost를 설정하는 방법에 대한 자세한 내용은 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오. 다른 애플리케이션을 통해 DD Boost를 설정하는 방법에 대한 자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide* 및 애플리케이션별 설명서를 참조하십시오.

절차

1. **Protocols** > **DD Boost**를 선택합니다.
2. Users with DD Boost Access 목록 위에서 **Add(+)**를 선택합니다.

   Add User 대화 상자가 나타납니다.

3. 기존 사용자를 선택하려면 드롭다운 목록에서 사용자 이름을 선택합니다.

   가능하면 관리 역할 권한이 *none*으로 설정되어 있는 사용자 이름을 선택하십시오.

4. 새 사용자를 생성하고 선택하려면 **Create a new Local User**를 선택하고 다음을 수행합니다.

   a. User 필드에 새 사용자 이름을 입력합니다.

      사용자가 백업 애플리케이션에서 Data Domain 시스템에 접속하도록 구성되어야 합니다.

b. 해당 필드에 암호를 두 번 입력합니다.

5. **Add**를 클릭합니다.

DD Boost 사용자 암호 변경

DD Boost 사용자 암호를 변경합니다.

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. Users with DD Boost Access 목록에서 사용자를 선택합니다.
3. DD Boost 사용자 목록 위에서 연필 모양의 **편집** 버튼을 클릭합니다.

   Change Password 대화 상자가 나타납니다.

4. 해당 상자에 암호를 두 번 입력합니다.
5. **Change**를 클릭합니다.

DD Boost 사용자 이름 제거

DD Boost 액세스 목록에서 사용자를 제거합니다.

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. Users with DD Boost Access 목록에서 제거해야 하는 사용자를 선택합니다.
3. DD Boost 사용자 목록 위에서 **Remove**(X)를 클릭합니다.

   Remove User 대화 상자가 나타납니다.

4. **Remove**를 클릭합니다.

   제거 후에도 DD OS 액세스 목록에는 사용자가 남아 있습니다.

DD Boost 설정

DD Boost Settings 탭을 사용해 DD Boost를 설정하고 DD Boost 사용자를 선택하거나 추가합니다.

절차

1. **Protocols** > **DD Boost**를 선택합니다.
2. DD Boost Status 영역에서 **Enable**을 클릭합니다.

   Enable DD Boost 대화 상자가 표시됩니다.

3. 메뉴에서 기존 사용자 이름을 선택하거나 이름, 암호 및 역할을 제공하여 새 사용자를 추가합니다.

Kerberos 구성

DD Boost Settings 탭을 사용하여 Kerberos를 구성할 수 있습니다.

절차

1. **Protocols > DD Boost > Settings**를 선택합니다.
2. Kerberos Mode status 영역에서 **Configure**를 클릭합니다.

   Administration > Access 아래에 Authentication 탭이 표시됩니다.

참고

System Manager의 **Administration > Access** 아래에서 Authentication으로 직접 이동하여 Kerberos를 활성화할 수도 있습니다.

3. Active Directory/Kerberos Authentication에서 **Configure**를 클릭합니다.

   Active Directory/Kerberos Authentication 대화 상자가 표시됩니다.
   사용할 Kerberos KDC(Key Distribution Center) 유형을 선택합니다.

   - **Disabled**

     참고

     Disabled를 선택하면 NFS 클라이언트가 Kerberos 인증을 사용하지 않게 됩니다. CIFS 클라이언트에서는 워크그룹 인증이 사용됩니다.

   - **Windows/Active Directory**

     참고

     Active Directory 인증에 대한 영역 이름, 사용자 이름 및 암호를 입력합니다.

   - **Unix**

     a. 세 KDC 서버 중 하나의 영역 이름, IP 주소/호스트 이름을 입력합니다.

     b. KDC 서버 중 하나에서 keytab 파일을 업로드합니다.

DD Boost 해제

DD Boost를 해제하면 백업 서버에 대한 모든 활성 접속이 끊깁니다. DD Boost를 해제하거나 제거하면 DD Boost FC 서비스도 해제됩니다.

시작하기 전에

해제하기 전에 백업 애플리케이션에서 실행 중인 작업이 없는지 확인하십시오.

참고

두 Data Domain 복원 사이에서 DD Boost에 의해 시작된 파일 복제는 취소되지 않습니다.

절차

1. **Protocols** > **DD Boost**를 선택합니다.
2. DD Boost Status 영역에서 **Disable**을 클릭합니다.
3. Disable DD Boost 확인 대화 상자에서 **OK**를 클릭합니다.

DD Boost 스토리지 유닛 보기

Storage Units 탭에 액세스하여 DD Boost 스토리지 유닛을 보고 관리합니다.

DD Boost Storage Unit 탭:

- 스토리지 유닛이 나열되고 각 스토리지 유닛에 대한 다음 정보가 제공됩니다.

표 127 스토리지 유닛 정보

항목	설명
Storage Unit	스토리지 유닛의 이름입니다.
User	스토리지 유닛을 소유하는 DD Boost 사용자입니다.
Quota Hard Limit	사용된 고정적 제한 할당량의 비율입니다.
Last 24 hr Pre-Comp	백업 애플리케이션에서 지난 24시간 동안 기록된 원시 데이터의 양입니다.
Last 24 hr Post-Comp	지난 24시간 동안 압축 후 사용된 스토리지의 양입니다.
Last 24 hr Comp Ratio	지난 24시간 동안의 압축률입니다.
Weekly Avg Post-Comp	지난 5주 동안 사용된 압축된 스토리지의 평균 양입니다.
Last Week Post-Comp	지난 7일 동안 사용된 압축된 스토리지의 평균 양입니다.
Weekly Avg Comp Ratio	지난 5주 동안의 평균 압축률입니다.
Last Week Comp Ratio	지난 7일 동안의 평균 압축률입니다.

- 스토리지 유닛을 생성, 수정 및 삭제할 수 있습니다.
- 목록에서 선택한 스토리지 유닛에 대한 관련 4개의 탭인 Storage Unit, Space Usage, Daily Written 및 Data Movement가 표시됩니다.

  참고

  Data Movement 탭은 선택 사항인 Data Domain Extended Retention(이전의 DD Archiver) 또는 Data Domain Cloud Tier(DD Cloud Tier) 라이선스가 설치되어 있는 경우에만 사용할 수 있습니다.

- **View DD Boost Replications** 링크를 클릭하면 **Replication** > **On-Demand** > **File Replication**으로 이동됩니다.

  참고

  DD Boost가 File Replication 탭 이외의 탭을 표시하려면 DD Replicator 라이선스가 필요합니다.

스토리지 유닛 생성

Data Domain 시스템에서 최소 하나의 스토리지 유닛을 생성해야 하며, DD Boost 사용자에게 해당 스토리지 유닛을 할당해야 합니다. Storage Units 탭을 사용해 스토리지 유닛을 생성합니다.

각 스토리지 유닛은 `/data/col1` 디렉토리의 최상위 하위 디렉토리로, 스토리지 유닛 간에 계층 구조가 존재하지 않습니다.

절차

1. **Protocols** > **DD Boost** > **Storage Units**를 선택합니다.
2. **Create**(+)를 클릭합니다.

   Create Storage Unit 대화 상자가 나타납니다.

3. Name 상자에 스토리지 유닛 이름을 입력합니다.

   각 스토리지 유닛 이름은 고유해야 합니다. 스토리지 유닛 이름은 50자까지 가능합니다. 다음 문자를 사용할 수 있습니다.

- 알파벳 대문자 및 소문자: A-Z, a-z
- 숫자: 0-9
- 공백

  참고

  스토리지 유닛 이름에 공백이 있는 경우 스토리지 유닛 이름을 큰따옴표(")로 묶어야 합니다.

- 쉼표(,)
- 마침표(.): 이름 앞에 붙지 않아야 합니다.
- 느낌표(!)
- 번호 기호(#)
- 달러 기호($)
- 퍼센트 기호(%)
- 더하기 기호(+)
- at 기호(@)
- 등호 기호(=)
- 앰퍼샌드(&)
- 세미콜론(;)
- 괄호[()]
- 대괄호([])
- 중괄호({})
- 캐럿(^)
- 물결표(~)
- 아포스트로피(기울지 않은 작은따옴표)
- 기울어진 작은따옴표(')
- 빼기 기호(-)
- 밑줄(_)

4. 드롭다운 목록에서 사용자를 선택해 이 스토리지 유닛에 액세스할 수 있는 기존 사용자 이름을 선택합니다.

   가능하면 관리 역할 권한이 *none*으로 설정되어 있는 사용자 이름을 선택하십시오.

5. 이 스토리지 유닛에 액세스할 수 있는 새 사용자 이름을 생성하고 선택하려면 **Create a new Local User**를 선택하고 다음을 수행합니다.

   a. User 상자에 새 사용자 이름을 입력합니다.

      사용자가 백업 애플리케이션에서 Data Domain 시스템에 접속하도록 구성되어야 합니다.

   b. 해당 상자에 암호를 두 번 입력합니다.

6. 스토리지 유닛이 공간을 지나치게 많이 사용하지 못하도록 스토리지 공간 제한을 설정하려면 유동적 또는 고정적 제한 할당량 설정을 입력하거나 두 가지 제한을 모두 입력합니다. 유동적 제한을 입력하면 스토리지 유닛 크기가 제한을 초과

할 경우 알림이 전송되지만 데이터를 여전히 여기에 기록할 수 있습니다. 고정적 제한에 도달했을 때에는 스토리지 유닛에 데이터를 기록할 수 없습니다.

참고

할당량 제한은 압축 전 값입니다. 할당량 제한을 설정하려면 **Set to Specific Value**를 선택하고 값을 입력하십시오. 측정 단위를 MiB, GiB, TiB 또는 PiB 중에서 선택하십시오.

참고

유동적 제한과 고정적 제한을 모두 설정할 경우 할당량의 유동적 제한이 할당량의 고정적 제한을 초과할 수 없습니다.

7. **Create**를 클릭합니다.
8. Data Domain Boost를 사용하는 각 시스템에 대해 위의 단계를 반복합니다.

스토리지 유닛 정보 보기

DD Boost Storage Units 탭에서 스토리지 유닛을 선택하고 선택한 스토리지 유닛에 대한 Storage Unit, Space Usage, Daily Written 및 Data Movement 탭에 액세스할 수 있습니다.

Storage Unit 탭

Storage Unit 탭에는 Summary 및 Quota 패널에서 선택한 스토리지 유닛에 대한 자세한 정보가 표시됩니다. Snapshot 패널에서는 스냅샷 세부 정보가 표시되고 새 스냅샷과 스케줄을 생성할 수 있으며 **Data Management** > **Snapshots** 탭에 대한 링크를 제공합니다.

- Summary 패널에는 선택한 스토리지 유닛에 대해 요약된 정보가 표시됩니다.

  표 128 Summary 패널

Summary 항목	설명
Total Files	스토리지 유닛에 있는 파일 이미지의 총 개수입니다. 로그 파일에 다운로드할 수 있는 압축 세부 정보를 보려면 Download Compression Details 링크를 클릭하십시오. 생성을 완료하는 데는 몇 분 정도 걸릴 수 있습니다. 완료된 후에 Download를 클릭하십시오.
Full Path	`/data/col1/filename`
Status	R: 읽기, W: 쓰기, Q: 할당량이 정의됨
Pre-Comp Used	이미 사용한 압축 전 스토리지의 용량입니다.

- Quota 패널에는 선택한 스토리지 유닛에 대한 할당량 정보가 표시됩니다.

  표 129 Quota 패널

Quota 항목	설명
Quota Enforcement	활성화 또는 비활성화입니다. Quota를 클릭하면 할당량을 구성할 수 있는 **Data Management** > **Quota** 탭으로 이동합니다.
Pre-Comp Soft Limit	스토리지 유닛에 대해 설정된 가변 할당량(soft quota)의 현재 값입니다.

표 129 Quota 패널 (계속)

Quota 항목	설명
Pre-Comp Hard Limit	스토리지 유닛에 대해 설정된 고정 할당량(hard quota)의 현재 값입니다.
Quota Summary	사용한 고정적 제한의 비율입니다.

탭에 표시된 압축 전 유동적 및 고정적 제한을 수정하려면

1. Quota 패널에서 **Quota** 링크를 클릭합니다.
2. Configure Quota 대화 상자에서 가변 할당량(soft quota) 및 고정 할당량(hard quota)의 값을 입력하고 MiB, GiB, TiB 또는 PiB 중에서 선택하십시오. **OK**를 클릭합니다.

- Snapshots
  Snapshots 패널에는 스토리지 유닛의 스냅샷에 대한 정보가 표시됩니다.

표 130 Snapshots 패널

항목	설명
Total Snapshots	이 MTree에 대해 생성된 스냅샷의 총 개수입니다. MTree마다 총 750개의 스냅샷을 생성할 수 있습니다.
Expired	이 MTree에서 삭제하기 위해 표시해 두었지만 아직 정리 작업을 통해 제거하지 않은 스냅샷의 개수입니다.
Unexpired	유지하기 위해 표시해 둔 이 MTree에 있는 스냅샷의 개수입니다.
Oldest Snapshot	이 MTree에 대해 가장 오래된 스냅샷의 날짜입니다.
Newest Snapshot	이 MTree에 대해 가장 최신 스냅샷의 날짜입니다.
Next Scheduled	다음으로 예약된 스냅샷의 날짜입니다.
Assigned Snapshot Schedules	이 MTree에 할당된 스냅샷 스케줄의 이름입니다.

Snapshots 패널에서 다음을 수행할 수 있습니다.

- 선택한 스토리지 유닛에 스냅샷 스케줄을 할당합니다. **Assign Schedules**를 클릭합니다. 스케줄의 확인란을 선택하고 **OK** 및 **Close**를 차례로 클릭합니다.
- 새 스케줄을 생성합니다. **Assign Snapshot Schedules** > **Create Snapshot Schedule**을 클릭합니다. 새 스케줄의 이름을 입력합니다.

참고

스냅샷 이름은 문자, 숫자, _, -, %d(달의 숫자 일: 01~31), %a(약식 요일 이름), %m(연 기준 숫자 형식 월: 01~12), %b(약식 월 이름), %y(연도, 2자리), %Y(연도, 4자리), %H(시: 00~23) 및 %M(분: 00~59)으로만 구성될 수 있으며, 그 뒤에 대화 상자에 표시된 패턴이 와야 합니다. 새 패턴을 입력하고 **Validate Pattern & Update Sample**을 클릭합니다. **Next**를 클릭합니다.

- 달력에서 해당 날짜를 클릭하거나 해당 월의 마지막 날을 클릭해 매주, 매일(또는 선택한 날짜), 매달 지정된 날짜 중에서 스케줄을 실행할 시기를 선택합니다. **Next**를 클릭합니다.
- 스케줄을 실행할 날짜의 시간을 입력합니다. At Specific Times 또는 In Intervals를 선택합니다. 특정 시간을 선택할 경우 목록에서 시간을 선택합니다. 추가(+) 버튼을 클릭해 시간을 추가합니다(24시간 형식). 간격의 경우 In Intervals를 선택하고 시작 및 종료 시간과 8시간에 한 번처럼 빈도(Every)를 설정합니다. **Next**를 클릭합니다.
- 스냅샷의 보존 기간을 일, 월 또는 년 단위로 입력합니다. **Next**를 클릭합니다.
- 구성 요약을 검토합니다. 값을 편집하려면 **Back**을 클릭합니다. 스케줄을 생성하려면 **Finish**를 클릭합니다.

- Snapshots 링크를 클릭하면 **Data Management** > **Snapshots** 탭으로 이동합니다.

Space Usage 탭

Space Usage 탭 그래프에는 시간에 따른 스토리지 유닛의 데이터 사용량이 시각적으로 표시됩니다.

- 그래프 선 위의 특정 시점을 클릭하여 해당 시점의 데이터를 보여 주는 상자를 표시합니다.
- 그래프 하단의 **Print**를 클릭하여 표준 Print 대화 상자를 엽니다.
- **Show in new window**를 클릭하여 그래프를 새 브라우저 창에 표시합니다.

두 가지 유형의 그래프 데이터인 사용된 논리적 공간(압축 전)과 사용된 물리적 용량(압축 후)이 표시됩니다.

Daily Written 탭

Daily Written 보기에는 7일에서 120일 사이에서 선택 가능한 특정 기간 동안 매일 시스템에 기록된 데이터를 시각적으로 보여 주는 그래프가 표시됩니다. 데이터 양은 압축 전 및 압축 후 양을 비교하여 시간별로 표시됩니다.

Data Movement 탭

DD Extended Retention 라이선스가 활성화된 경우 DD Extended Retention 스토리지 영역으로 이동한 디스크 공간의 용량을 표시하는 Daily Written 그래프와 같은 형식의 그래프입니다.

스토리지 유닛 수정

Modify Storage Unit 대화 상자를 사용해 스토리지 유닛의 이름을 바꾸고 다른 기존 사용자를 선택하고 새 사용자를 생성 및 선택하고 할당량 설정을 편집합니다.

절차

1. **Protocols** > **DD Boost** > **Storage Units**를 선택합니다.
2. Storage Unit 목록에서 수정할 스토리지 유닛을 선택합니다.

3. 연필 모양 아이콘을 클릭합니다.

   Modify Storage Unit 대화 상자가 나타납니다.

4. 스토리지 유닛의 이름을 바꾸려면 **Name** 필드의 텍스트를 편집합니다.
5. 다른 기존 사용자를 선택하려면 드롭다운 목록에서 사용자 이름을 선택합니다.

   가능하면 관리 역할 권한이 *none*으로 설정되어 있는 사용자 이름을 선택하십시오.

6. 새 사용자를 생성하고 선택하려면 **Create a new Local User**를 선택하고 다음을 수행합니다.

   a. User 상자에 새 사용자 이름을 입력합니다.

      사용자가 백업 애플리케이션에서 Data Domain 시스템에 접속하도록 구성되어야 합니다.

   b. 해당 상자에 암호를 두 번 입력합니다.

7. 필요에 따라 할당량 설정을 편집합니다.

   스토리지 유닛이 공간을 지나치게 많이 사용하지 못하도록 스토리지 공간 제한을 설정하려면 유동적 또는 고정적 제한 할당량 설정을 입력하거나 두 가지 제한을 모두 입력합니다. 유동적 제한을 입력하면 스토리지 유닛 크기가 제한을 초과할 경우 알림이 전송되지만 데이터를 여전히 여기에 기록할 수 있습니다. 고정적 제한에 도달했을 때에는 스토리지 유닛에 데이터를 기록할 수 없습니다.

   참고

   할당량 제한은 압축 전 값입니다. 할당량 제한을 설정하려면 **Set to Specific Value**를 선택하고 값을 입력하십시오. 측정 단위를 MiB, GiB, TiB 또는 PiB 중에서 선택하십시오.

   참고

   유동적 제한과 고정적 제한을 모두 설정할 경우 할당량의 유동적 제한이 할당량의 고정적 제한을 초과할 수 없습니다.

8. **Modify**를 클릭합니다.

스토리지 유닛 이름 바꾸기

Modify Storage Unit 대화 상자를 사용해 스토리지 유닛의 이름을 바꿉니다.

스토리지 유닛의 이름을 바꾸면 스토리지 유닛의 이름이 변경되고 다음은 유지됩니다.

- 사용자 이름 소유권
- 스트림 제한 구성
- 용량 할당량 구성 및 보고된 물리적 크기
- 로컬 Data Domain 시스템의 AIR 연결

절차

1. **Protocols** > **DD Boost** > **Storage Units**로 이동합니다.
2. Storage Unit 목록에서 이름을 바꿀 스토리지 유닛을 선택합니다.
3. 연필 모양 아이콘을 클릭합니다.

Modify Storage Unit 대화 상자가 나타납니다.

4. **Name** 필드의 텍스트를 편집합니다.
5. **Modify**를 클릭합니다.

스토리지 유닛 삭제

Storage Units 탭을 사용해 Data Domain 시스템에서 스토리지 유닛을 삭제합니다. 스토리지 유닛을 삭제하면 스토리지 유닛과 해당 스토리지 유닛에 포함된 모든 이미지가 Data Domain 시스템에서 제거됩니다.

절차

1. **Protocols** > **DD Boost** > **Storage Units**를 선택합니다.
2. 목록에서 삭제할 스토리지 유닛을 선택합니다.
3. **Delete**(X) 버튼을 클릭합니다.
4. **OK**를 클릭합니다.

결과

Data Domain 시스템에서 스토리지 유닛이 제거됩니다. 해당 백업 애플리케이션 카탈로그 항목도 수동으로 제거해야 합니다.

스토리지 유닛 삭제 취소

Storage Units 탭을 사용해 스토리지 유닛을 삭제를 취소합니다.

스토리지 유닛의 삭제를 취소하면 이전에 삭제한 스토리지 유닛이 다음을 포함하여 복구됩니다.

- 사용자 이름 소유권
- 스트림 제한 구성
- 용량 할당량 구성 및 보고된 물리적 크기
- 로컬 Data Domain 시스템의 AIR 연결

참고

삭제된 스토리지 유닛은 다음 `filesys clean` 명령을 실행하기 전까지 사용할 수 있습니다.

절차

1. **Protocols** > **DD Boost** > **Storage Units** > **More Tasks** > **Undelete Storage Unit...**을 선택합니다.
2. Undelete Storage Units 대화 상자에서 삭제를 취소할 스토리지 유닛을 선택합니다.
3. **OK**를 클릭합니다.

DD Boost 옵션 선택

Set DD Boost Options 대화 상자를 사용해 분산 세그먼트 처리, 가상 신세틱, 파일 복제를 위한 저대역폭 최적화, 파일 복제 암호화 및 파일 복제 네트워크 기본 설정(IPv4 또는 IPv6)에 대한 설정을 지정합니다.

절차

1. DD Boost 옵션 설정을 표시하려면 **Protocols** > **DD Boost** > **Settings** > **Advanced Options**를 선택합니다.
2. 설정을 변경하려면 **More Tasks** > **Set Options**를 선택합니다.

   Set DD Boost Options 대화 상자가 나타납니다.

3. 활성화할 옵션을 선택합니다.
4. 비활성화할 옵션을 선택 취소합니다.

   File Replication Network Preference 옵션을 선택 취소하려면 다른 옵션을 선택합니다.

5. DD Boost 보안 옵션을 설정합니다.

   a. **Authentication Mode**를 선택합니다.

   - None
   - Two-way
   - Two-way Password

   b. **Encryption Strength**를 선택합니다.

   - None
   - Medium
   - High

   Data Domain 시스템은 글로벌 인증 모드 및 암호화 강도를 클라이언트별 인증 모드 및 암호화 강도와 비교하여 효과적인 인증 모드 및 인증 암호화 강도를 계산합니다. 시스템은 한 항목의 가장 높은 인증 모드와 다른 항목의 가장 높은 암호화 설정을 사용하는 것이 아닙니다. 효과적인 인증 모드 및 암호화 강도는 가장 높은 인증 모드를 제공하는 단일 항목에서 제공됩니다.
6. **OK**를 클릭합니다.

참고

`ddboost option` 명령을 통해 분산된 세그먼트 처리를 관리할 수도 있습니다. 이 명령은 *Data Domain Operating System 명령 참조 가이드*에 자세히 설명되어 있습니다.

분산된 세그먼트 처리

분산된 세그먼트 처리는 미디어 서버와 Data Domain 시스템 간의 중복 데이터 전송을 제거하여 거의 모든 경우에 백업 처리량을 증가시킵니다.

`ddboost option` 명령을 통해 분산된 세그먼트 처리를 관리할 수 있습니다. 이 명령은 *Data Domain Operating System 명령 참조 가이드*에 자세히 설명되어 있습니다.

참고

분산된 세그먼트 처리는 Data Domain Extended Retention(이전의 Data Domain Archiver) 구성에서 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

가상 신세틱(Virtual Synthetic)

가상 신세틱 전체(synthetic full) 백업은 전체 신세틱 백업 또는 전체 백업과 같은 최신 전체 백업과 모든 후속 증분 백업을 합성한 것입니다. 가상 신세틱(Virtual Synthetic)은 기본적으로 설정되어 있습니다.

저대역폭 최적화

대역폭이 낮은 네트워크(WAN)를 통해 파일 복제를 사용하는 경우 저대역폭 최적화를 통해 복제 속도를 높일 수 있습니다. 이 기능은 데이터를 전송하는 동안 추가 압축을 제공합니다. 대역폭이 낮은 압축은 복제 라이센스가 설치된 Data Domain 시스템에서 사용할 수 있습니다.

기본적으로 비활성화되어 있는 저대역폭 최적화는 총 대역폭이 6Mbps 미만인 네트워크에서 사용하도록 설계되었습니다. 파일 시스템 쓰기 성능을 극대화해야 하는 작업에는 이 옵션을 사용하지 마십시오.

참고

`ddboost file-replication` 명령을 통해 저대역폭 최적화를 관리할 수도 있습니다. 이 명령은 *Data Domain Operating System 명령 참조 가이드*에 자세히 설명되어 있습니다.

파일 복제 암호화

DD Boost 파일 복제 암호화 옵션을 활성화하여 데이터 복제 스트림을 암호화할 수 있습니다.

참고

저장된 데이터 옵션이 없는 시스템에서 DD Boost 파일 복제 암호화를 사용하는 경우 소스 시스템과 대상 시스템 모두에서 on으로 설정되어야 합니다.

관리되는 파일 복제 TCP 포트 설정

DD Boost의 관리되는 파일 복제의 경우 소스 및 타겟 Data Domain 시스템 모두에서 동일한 글로벌 수신 포트를 사용합니다. 수신 포트를 설정하려면 `replication option` 명령을 *Data Domain Operating Sysem 명령 참조 가이드*에 설명된 대로 사용합니다.

파일 복제 네트워크 기본 설정

이 옵션을 사용해 DD Boost 파일 복제에 대한 기본 네트워크 유형을 IPv4 또는 IPv6로 설정합니다.

DD Boost 인증서 관리

호스트 인증서를 사용하면 연결을 설정할 때 DD Boost 클라이언트 프로그램에서 시스템의 ID를 확인할 수 있습니다. CA 인증서는 시스템에서 신뢰해야 하는 인증 기관을 식별합니다. 이 섹션의 항목에서는 DD Boost에 대한 호스트 및 CA 인증서를 관리하는 방법에 대해 설명합니다.

DD Boost의 호스트 인증서 추가

호스트 인증서를 시스템에 추가합니다. DD OS는 DD Boost용으로 하나의 호스트 인증서를 지원합니다.

절차

1. 호스트 인증서를 아직 요청하지 않은 경우 신뢰하는 인증 기관에 요청하십시오.
2. 호스트 인증서를 받은 후 DD Service Manager를 실행하는 컴퓨터로 복사하거나 이동합니다.
3. 호스트 인증서를 추가할 시스템에서 DD System Manager를 시작합니다.

   참고

   DD System Manager는 DD System Manager를 실행하는 관리 시스템에서만 인증서 관리를 지원합니다.

4. **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**를 선택합니다.

   참고

   관리 대상 시스템에서 원격으로 인증서를 관리하려고 하면 DD System Manager의 인증서 관리 대화 상자 맨 위에 정보 메시지가 표시됩니다. 시스템의 인증서를 관리하려면 해당 시스템에서 DD System Manager를 시작해야 합니다.

5. Host Certificate 영역에서 **Add**를 클릭합니다.
6. .p12 파일로 호스트 인증서를 추가하려면 다음을 수행합니다.
   a. **I want to upload the certificate as a .p12 file**을 선택합니다.
   b. **Password** 입력란에 암호를 입력합니다.
   c. **Browse**를 클릭하고 시스템에 업로드할 호스트 인증서 파일을 선택합니다.
   d. **Add**를 클릭합니다.
7. .pem 파일로 호스트 인증서를 추가하려면 다음을 수행합니다.
   a. **I want to upload the public key as a .pem file and use a generated private key**를 선택합니다.
   b. **Browse**를 클릭하고 시스템에 업로드할 호스트 인증서 파일을 선택합니다.
   c. **Add**를 클릭합니다.

DD Boost의 CA 인증서 추가

신뢰할 수 있는 CA의 인증서를 시스템에 추가합니다. DD OS는 신뢰할 수 있는 CA의 여러 인증서를 지원합니다.

절차

1. 신뢰할 수 있는 CA의 인증서를 가져옵니다.
2. 신뢰할 수 있는 CA 인증서를 DD Service Manager를 실행하는 컴퓨터로 복사하거나 이동합니다.
3. CA 인증서를 추가할 시스템에서 DD System Manager를 시작합니다.

   참고

   DD System Manager는 DD System Manager를 실행하는 관리 시스템에서만 인증서 관리를 지원합니다.

4. **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**를 선택합니다.

참고

관리 대상 시스템에서 원격으로 인증서를 관리하려고 하면 DD System Manager의 인증서 관리 대화 상자 맨 위에 정보 메시지가 표시됩니다. 시스템의 인증서를 관리하려면 해당 시스템에서 DD System Manager를 시작해야 합니다.

5. CA Certificate 영역에서 **Add**를 클릭합니다.

   Add CA Certificate for DD Boost 대화 상자가 나타납니다.

6. .pem 파일로 CA 인증서를 추가하려면 다음을 수행합니다.
   a. **I want to upload the certificate as a .pem file**을 선택합니다.
   b. **Browse**를 클릭하고 시스템에 업로드할 호스트 인증서 파일을 선택한 다음 **Open**을 클릭합니다.
   c. **Add**를 클릭합니다.
7. 복사 및 붙여넣기를 사용해 CA 인증서를 추가하려면 다음을 수행합니다.
   a. 사용하는 운영 체제의 컨트롤을 사용하여 인증서 텍스트를 클립보드에 복사합니다.
   b. **I want to copy and paste the certificate text**를 선택합니다.
   c. 인증서 텍스트를 복사 및 붙여넣기 선택 아래의 상자에 붙여 넣습니다.
   d. **Add**를 클릭합니다.

DD Boost 클라이언트 액세스 및 암호화 관리

DD Boost Settings 탭을 사용해 Data Domain 시스템과 DD Boost의 연결을 설정할 수 있는 특정 클라이언트 또는 클라이언트 집합을 구성하고 클라이언트의 암호화 사용 여부를 구성합니다. 기본적으로 시스템은 암호화 없이 모든 클라이언트의 액세스를 허용하도록 구성됩니다.

참고

전송 중 암호화를 설정하면 시스템 성능에 영향을 미칩니다.

참고

DD Boost는 MITM(Man-In-The-Middle) 공격으로부터 시스템을 보호하기 위한 글로벌 인증 및 암호화 옵션을 제공합니다. Data Domain 시스템에서 GUI 또는 CLI 명령을 사용하여 인증 및 암호화 설정을 지정합니다. 자세한 내용은 *Data Domain Boost for OpenStorage 3.4 관리 가이드* 및 DD Boost 클라이언트 추가(336페이지) 또는 *Data Domain 6.1 명령 참조 가이드*를 참조하십시오.

DD Boost 클라이언트 추가

허용되는 DD Boost 클라이언트를 생성하고 클라이언트의 암호화 사용 여부를 지정합니다.

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. Allowed Clients 섹션에서 **Create (+)**를 클릭합니다.

   Add Allowed Client 대화 상자가 나타납니다.

3. 클라이언트의 호스트 이름을 입력합니다.

   정규화된 도메인 이름(예: host1.emc.com) 또는 와일드카드가 포함된 호스트 이름(예: *.emc.com)을 입력할 수 있습니다.

4. Encryption Strength를 선택합니다.

   옵션은 None(암호화 없음), Medium(AES128-SHA1) 또는 High(AES256-SHA1)입니다.

5. Authentication Mode를 선택합니다.

   옵션은 One Way, Two Way, Two Way Password 또는 Anonymous입니다.

6. **OK**를 클릭합니다.

DD Boost 클라이언트 수정

허용되는 DD Boost 클라이언트의 이름, 암호화 강도 및 인증 모드를 변경합니다.

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. Allowed Clients 목록에서 수정할 클라이언트를 선택합니다.
3. 연필 아이콘으로 표시되는 **Edit** 버튼을 클릭합니다.

   Modify Allowed Client 대화 상자가 나타납니다.

4. 클라이언트 이름을 변경하려면 Client 텍스트를 편집합니다.
5. 암호화 강도를 변경하려면 옵션을 선택합니다.

   옵션은 None(암호화 없음), Medium(AES128-SHA1) 또는 High(AES256-SHA1)입니다.

6. 인증 모드를 변경하려면 옵션을 선택합니다.

   옵션은 One Way, Two Way 또는 Anonymous입니다.

7. **OK**를 클릭합니다.

DD Boost 클라이언트 제거

허용되는 DD Boost 클라이언트를 삭제합니다.

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. 목록에서 클라이언트를 선택합니다.
3. **Delete(X)** 버튼을 클릭합니다.

   Delete Allowed Clients 대화 상자가 나타납니다.

4. 클라이언트 이름을 확인하고 선택합니다. **OK**를 클릭합니다.

인터페이스 그룹 정보

이 기능을 사용하면 여러 이더넷 링크를 하나의 그룹으로 결합해 Data Domain 시스템의 한 인터페이스만 백업 애플리케이션에 등록할 수 있습니다. DD Boost 라이브러리는

Data Domain 시스템과 협상하여 데이터를 전송할 최상의 인터페이스를 확보합니다. 로드 밸런싱은 Data Domain 시스템에 더 높은 물리적 처리량을 제공합니다.

인터페이스 그룹을 구성하면 Data Domain 시스템 내에 여러 IP 주소를 하나의 그룹으로 지정하여 구성한 전용 네트워크가 생성됩니다. 클라이언트는 단일 그룹에 할당되고 그룹 인터페이스는 로드 밸런싱을 사용하여 데이터 전송 성능 및 신뢰성을 개선합니다.

예를 들어 Symantec NetBackup 환경에서 미디어 서버 클라이언트는 단일 공용 네트워크 IP 주소를 사용하여 Data Domain 시스템에 액세스합니다. Data Domain 시스템과의 모든 통신은 NetBackup 서버에서 구성된 이 관리되는 IP 접속을 통해 시작됩니다.

인터페이스 그룹이 구성된 경우, Data Domain 시스템이 미디어 서버 클라이언트에서 데이터를 수신하면 데이터 전송이 로드 밸런싱되어 그룹의 모든 인터페이스에 분산되므로 특히 여러 1GigE 접속을 사용하는 고객의 경우 입출력 처리량이 향상됩니다.

데이터 전송은 인터페이스에서 미완료된 접속 수에 따라 로드 밸런싱됩니다. 백업 및 복구 작업의 접속만 로드 밸런싱됩니다. 그룹의 인터페이스에서 미완료된 접속 수에 대한 자세한 정보를 보려면 Active Connections를 확인하십시오.

그룹의 인터페이스에 장애가 발생하는 경우 해당 인터페이스로 전송 중인 모든 작업이 정상적으로 작동하는 링크(백업 애플리케이션에 알려지지 않음)에서 자동으로 재개됩니다. 장애 후의 모든 후속 작업도 그룹의 정상적인 인터페이스로 라우팅됩니다. 그룹이 비활성화되어 있거나 대체 인터페이스에서 복구 시도가 실패하는 경우 관리되는 IP가 복구에 사용됩니다. 한 그룹에서 장애가 발생해도 다른 그룹의 인터페이스가 사용되지 않습니다.

인터페이스 그룹을 관리할 때는 다음 정보를 고려하십시오.

- IP 주소가 Data Domain 시스템에서 구성되어야 하고 해당 인터페이스가 활성화되어야 합니다. 인터페이스 구성을 확인하려면 **Hardware** > **Ethernet** > **Interfaces** 페이지를 선택하고 여유 포트를 확인합니다. 인터페이스의 IP 주소 구성에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*의 `net` 장 또는 *Data Domain Operating System 초기 구성 가이드*를 참조하십시오.
- `ifgroup` 명령을 사용해 인터페이스 그룹을 관리할 수 있습니다. 이러한 명령은 *Data Domain Operating System 명령 참조 가이드*에 자세히 설명되어 있습니다.
- 인터페이스 그룹은 IPv4 기능과 동일한 IPv6 기능을 제공하여 정적 IPv6 주소를 완벽하게 지원합니다. 동시 IPv4 및 IPv6 클라이언트 접속이 허용됩니다. IPv6를 통해 연결된 클라이언트에는 IPv6 ifgroup 인터페이스만 표시됩니다. IPv4를 통해 연결된 클라이언트에는 IPv4 ifgroup 인터페이스만 표시됩니다. 개별 ifgroup에는 IPv4 주소만 모두 포함되거나 IPv6 주소만 모두 포함됩니다. 자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.
- 구성된 인터페이스는 Activities 페이지의 아래쪽에 있는 Active Connections에 나열됩니다.

참고

HA 시스템에 인터페이스 그룹을 사용하는 방법에 대한 자세한 내용은 HA 시스템에서 DD Boost 사용(350페이지)에서 참조하십시오.

뒤에 나오는 항목에서는 인터페이스 그룹을 관리하는 방법에 대해 설명합니다.

인터페이스

IFGROUP은 물리적 인터페이스와 가상 인터페이스를 지원합니다.

IFGROUP 인터페이스는 단일 IFGROUP *<group-name>*의 구성원이며 다음으로 구성될 수 있습니다.

- 물리적 인터페이스. 예: `eth0a`
- 링크 페일오버 또는 Link Aggregation을 위해 생성된 가상 인터페이스. 예: `veth1`
- 가상 별칭 인터페이스. 예: `eth0a:2` 또는 `veth1:2`
- 가상 VLAN 인터페이스. 예: `eth0a.1` 또는 `veth1.1`
- 네트워크 오류 시 페일오버를 수행할 수 있도록 IFGROUP *<group-name>* 내의 모든 인터페이스는 고유한 인터페이스(이더넷, 가상 이더넷)에 위치해야 합니다.

IFGROUP은 IPv4와 동일한 기능을 IPv6에 제공하여 정적 IPv6 주소를 완벽하게 지원합니다. 동시 IPv4 및 IPv6 클라이언트 접속이 허용됩니다. IPv6를 통해 연결된 클라이언트에는 IPv6 IFGROUP 인터페이스만 표시됩니다. IPv4를 통해 연결된 클라이언트에는 IPv4 IFGROUP 인터페이스만 표시됩니다. 개별 IFGROUP에는 IPv4 주소만 모두 포함되거나 IPv6 주소만 모두 포함됩니다.

자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

인터페이스 적용

IFGROUP을 사용하면 전용 네트워크 연결을 적용하여 네트워크 오류가 발생한 후 실패한 작업이 공용 네트워크에 다시 연결되는 것을 방지할 수 있습니다.

인터페이스 적용을 활성화하면 실패한 작업이 대체 전용 네트워크 IP 주소에서만 재시도됩니다. 인터페이스 적용은 IFGROUP 인터페이스를 사용하는 클라이언트에서만 제공됩니다.

인터페이스 적용은 기본적으로 꺼져 있습니다(FALSE). 인터페이스 적용을 활성화하려면 시스템 레지스트리에 다음 설정을 추가해야 합니다.

```
system.ENFORCE_IFGROUP_RW=TRUE
```

레지스트리에 이 설정을 입력한 후 `filesys restart`를 수행해야 설정이 적용됩니다.

자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

클라이언트

IFGROUP은 클라이언트에 대한 다양한 명명 형식을 지원합니다. 클라이언트 선택은 지정된 우선 순위에 따릅니다.

IFGROUP 클라이언트는 단일 ifgroup *<group-name>*의 구성원이며 다음으로 구성될 수 있습니다.

- FQDN(Fully Qualified Domain Name)(예: ddboost.datadomain.com)
- 부분 호스트. 이를 통해 호스트 이름의 처음 *n*개 문자에 대한 검색을 수행할 수 있습니다. 예를 들어 n=3일 경우 유효한 형식은 `rtp_.*emc.com` 및 `dur_.*emc.com` 입니다. *n*(1-5)의 5개 값이 지원됩니다.
- 와일드카드(예: `*.datadomain.com` 또는 "*")
- 클라이언트의 단축 이름(예: ddboost)
- 클라이언트 공용 IP 범위(예: 128.5.20.0/24)

클라이언트는 쓰기 또는 읽기 처리 전에 서버에서 IFGROUP IP 주소를 요청합니다. 클라이언트 IFGROUP 연결을 선택하기 위해 다음 우선 순위에 따라 클라이언트 정보가 평가됩니다.

1. 연결된 Data Domain 시스템의 IP 주소. 클라이언트와 Data Domain 시스템 사이에 이미 활성 연결이 있고 이 연결이 IFGROUP의 인터페이스에 존재하는 경우 클라이언트에서 IFGROUP 인터페이스를 사용할 수 있습니다.

2. 연결된 클라이언트 IP 범위. 클라이언트 소스 IP에 대한 IP 마스크 검사가 수행됩니다. 클라이언트 소스 IP 주소가 IFGROUP 클라이언트 목록의 마스크와 일치할 경우 클라이언트에서 IFGROUP 인터페이스를 사용할 수 있습니다.
   - IPv4의 경우 네트워크에 따라 5가지 범위 마스크를 선택할 수 있습니다.
   - IPv6의 경우 고정 마스크 /64, /112 및 /128을 사용할 수 있습니다.

   이 호스트 범위 검사는 다수의 클라이언트가 포함되는 개별 VLAN에 고유한 부분 호스트 이름(도메인)이 없는 경우에 유용합니다.
3. 클라이언트 이름: `abc-11.d1.com`
4. 클라이언트 도메인 이름: `*.d1.com`
5. 모든 클라이언트: `*`

자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide*를 참조하십시오.

인터페이스 그룹 생성

IP Network 탭을 사용해 인터페이스 그룹을 생성하고 인터페이스 및 클라이언트를 그룹에 추가합니다.

인터페이스 그룹이 여러 개 있으면 다음을 수행할 수 있으므로 DD Boost의 효율이 향상됩니다.

- DD Boost를 구성해 그룹으로 구성된 특정 인터페이스를 사용합니다.
- 해당 인터페이스 그룹 중 하나에 클라이언트를 할당합니다.
- DD Boost 클라이언트를 사용할 경우 어떤 인터페이스가 활성 상태인지 모니터링합니다.

먼저 인터페이스 그룹을 생성한 뒤 새 미디어 서버를 사용할 수 있게 되면 클라이언트를 인터페이스 그룹에 추가합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Interface Groups 섹션에서 Add(+)를 클릭합니다.
3. 인터페이스 그룹 이름을 입력합니다.
4. 하나 이상의 인터페이스를 선택합니다. 최대 32개의 인터페이스를 구성할 수 있습니다.

   참고

   별칭 구성에 따라 일부 인터페이스는 같은 그룹의 다른 인터페이스와 물리적 인터페이스를 공유할 경우 선택할 수 없을 수도 있습니다. 페일오버 복구를 위해서는 그룹 내의 각 인터페이스가 다른 물리적 인터페이스에 있어야 하기 때문입니다.
5. **OK**를 클릭합니다.
6. Configured Clients 섹션에서 Add(+)를 클릭합니다.
7. 정규화된 클라이언트 이름 또는 **`*.mydomain.com`**을 입력합니다.

참고

* 클라이언트는 처음에 기본 그룹에서 사용할 수 있습니다. * 클라이언트는 단일 ifgroup의 구성원만 될 수 있습니다.

8. 이전에 구성된 인터페이스 그룹을 선택하고 **OK**를 클릭합니다.

인터페이스 그룹 설정 및 해제

IP Network 탭을 사용해 인터페이스 그룹을 설정 및 해제합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Interface Groups 섹션의 목록에서 인터페이스 그룹을 선택합니다.

참고

인터페이스 그룹에 클라이언트와 인터페이스가 모두 할당되어 있지 않은 경우 인터페이스 그룹을 설정할 수 없습니다.

3. **Edit**(연필 모양)를 클릭합니다.
4. **Enabled**를 클릭하여 인터페이스 그룹을 설정합니다. 해제하려면 확인란의 선택을 취소합니다.
5. **OK**를 클릭합니다.

인터페이스 그룹의 이름 및 인터페이스 수정

IP Network 탭을 사용해 인터페이스 그룹의 이름을 변경하고 그룹에 연결된 인터페이스를 변경합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Interface Groups 섹션의 목록에서 인터페이스 그룹을 선택합니다.
3. **Edit**(연필 모양) 버튼을 클릭합니다.
4. 이름을 다시 입력해 이름을 수정합니다.

   그룹 이름은 길이가 1 - 24자여야 하며 문자, 숫자, 밑줄 및 대시만 포함할 수 있습니다. 다른 그룹 이름과 동일할 수 없으며 “default”, “yes”, “no” 또는 “all”이 될 수 없습니다.

5. 인터페이스 목록에서 클라이언트 인터페이스를 선택하거나 선택을 취소합니다.

참고

그룹에서 모든 인터페이스를 제거하면 자동으로 비활성화됩니다.

6. **OK**를 클릭합니다.

인터페이스 그룹 삭제

IP Network 탭을 사용해 인터페이스 그룹을 삭제합니다. 인터페이스 그룹을 삭제하면 그룹에 연결된 모든 인터페이스와 클라이언트가 삭제됩니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Interface Groups 섹션의 목록에서 인터페이스 그룹을 선택합니다. 기본 그룹은 삭제할 수 없습니다.
3. Delete(**X**) 버튼을 클릭합니다.
4. 삭제를 확인합니다.

인터페이스 그룹에 클라이언트 추가

IP Network 탭을 사용해 인터페이스 그룹에 클라이언트를 추가합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Clients 섹션에서 추가(**+**) 버튼을 클릭합니다.
3. 클라이언트의 이름을 입력합니다.

   클라이언트 이름은 고유해야 하며 다음으로 구성될 수 있습니다.

   - **FQDN**
   - ***.domain**
   - 클라이언트 공용 IP 범위:
     - IPv4의 경우 `xx.xx.xx.0/24`는 연결하는 IP에 대해 24비트 마스크를 제공합니다. /24는 IFGROUP 액세스에 대해 클라이언트 소스 IP 주소를 평가할 때 마스킹되는 비트를 나타냅니다.
     - IPv6의 경우 `xxxx::0/112`는 연결하는 IP에 대해 112비트 마스크를 제공합니다. /112는 IFGROUP 액세스에 대해 클라이언트 소스 IP 주소를 평가할 때 마스킹되는 비트를 나타냅니다.

   클라이언트 이름은 최대 128자입니다.
4. 이전에 구성된 인터페이스 그룹을 선택하고 **OK**를 클릭합니다.

클라이언트의 이름 또는 인터페이스 그룹 수정

IP Network 탭을 사용해 클라이언트의 이름 또는 인터페이스 그룹을 변경합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Clients 섹션에서 클라이언트를 선택합니다.
3. **Edit**(연필 모양) 버튼을 클릭합니다.
4. 새 클라이언트 이름을 입력합니다.

   클라이언트 이름은 고유해야 하며 다음으로 구성될 수 있습니다.

   - **FQDN**
   - ***.domain**
   - 클라이언트 공용 IP 범위:
     - IPv4의 경우 `xx.xx.xx.0/24`는 연결하는 IP에 대해 24비트 마스크를 제공합니다. /24는 IFGROUP 액세스에 대해 클라이언트 소스 IP 주소를 평가할 때 마스킹되는 비트를 나타냅니다.

- IPv6의 경우 `xxxx::0/112`는 연결하는 IP에 대해 112비트 마스크를 제공합니다. /112는 IFGROUP 액세스에 대해 클라이언트 소스 IP 주소를 평가할 때 마스킹되는 비트를 나타냅니다.

클라이언트 이름은 최대 128자입니다.

5. 메뉴에서 새 인터페이스 그룹을 선택합니다.

참고

클라이언트가 없는 이전 인터페이스 그룹은 비활성화됩니다.

6. **OK**를 클릭합니다.

인터페이스 그룹에서 클라이언트 삭제

IP Network 탭을 사용해 인터페이스 그룹에서 클라이언트를 삭제합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Clients 섹션에서 클라이언트를 선택합니다.
3. Delete(**X**) 버튼을 클릭합니다.

참고

클라이언트가 속한 인터페이스 그룹에 다른 클라이언트가 없으면 인터페이스 그룹이 해제됩니다.

4. 삭제를 확인합니다.

MFR(Managed File Replication)을 위한 인터페이스 그룹 사용

인터페이스 그룹을 사용하여 DD Boost MFR에 사용되는 인터페이스를 제어하고 복제 접속에 사용할 특정 네트워크를 지정하고 대역폭과 안정성이 높은 여러 네트워크 인터페이스를 활용해 페일오버 조건을 충족할 수 있습니다. IPv4 또는 IPv6, 별칭 IP/VLAN IP 및 LACP/페일오버 집계 등의 모든 Data Domain IP 유형이 지원됩니다.

참고

복제에 사용되는 인터페이스 그룹은 앞서 설명한 인터페이스 그룹과 다르며 DD Boost MFR(Managed File Replication)용으로만 지원됩니다. MFR에 대한 인터페이스 그룹 사용에 대한 자세한 내용은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

인터페이스 그룹을 사용하지 않고 복제를 구성하려면 여러 단계를 수행해야 합니다.

1. 타겟 Data Domain 시스템에 대한 소스 Data Domain 시스템의 `/etc/hosts` 파일에 항목을 추가하고 전용 LAN 네트워크 인터페이스 중 하나를 대상 IP 주소로 하드 코딩합니다.
2. 소스 Data Domain 시스템의 경로를 타겟 Data Domain 시스템에 추가하여 소스 Data Domain 시스템의 물리 또는 가상 포트를 원격 대상 IP 주소에 지정합니다.
3. 네트워크를 통해 Data Domain 시스템 간의 모든 스위치에 LACP를 구성하여 로드 밸런싱 및 페일오버를 지원합니다.
4. 여러 애플리케이션에서 서로 다른 타겟 Data Domain 시스템 이름을 사용하여 `/etc/hosts` 파일에서 이름 지정 충돌이 발생하지 않도록 합니다.

복제에 인터페이스 그룹을 사용하면 DD OS System Manager 또는 DD OS CLI 명령을 통해 이 구성을 간소화할 수 있습니다. 인터페이스 그룹을 사용하여 복제 경로를 구성하면 다음을 수행할 수 있습니다.

- 호스트 이름이 확인된 IP 주소를 다른 전용 Data Domain 시스템 IP 주소를 사용하여 공용 네트워크로부터 리디렉션합니다.
- 구성된 선택 기준을 바탕으로 인터페이스 그룹을 식별하여 타겟 Data Domain 시스템에서 모든 인터페이스에 접속할 수 있는 단일의 인터페이스 그룹을 제공합니다.
- 그룹에 속하는 인터페이스 목록에서 양호한 상태의 전용 네트워크 인터페이스를 선택합니다.
- 동일한 전용 네트워크 내의 여러 Data Domain 인터페이스에 로드 밸런싱을 제공합니다.
- 인터페이스 그룹의 인터페이스 복구를 위한 페일오버 인터페이스를 제공합니다.
- 소스 Data Domain 시스템에 구성된 경우 호스트 페일오버를 제공합니다.
- NAT(Network Address Translation) 사용

파일 복제를 위한 인터페이스 그룹 일치를 결정하는 선택 순서는 다음과 같습니다.

1. 로컬 MTree(스토리지 유닛) 경로 및 특정 원격 Data Domain 호스트 이름
2. 원격 Data Domain 호스트 이름이 포함된 로컬 MTree(스토리지 유닛) 경로
3. 특정 Data Domain 호스트 이름이 포함된 MTree(스토리지 유닛) 경로

동일한 MTree는 MTree의 Data Domain 호스트 이름이 다를 경우에만 여러 인터페이스 그룹에 나타날 수 있습니다. 동일한 Data Domain 호스트 이름은 MTree 경로가 다를 경우에만 여러 인터페이스 그룹에 나타날 수 있습니다. 원격 호스트 이름은 FQDN(예: dd890-1.emc.com)이어야 합니다.

인터페이스 그룹 선택은 소스 Data Domain 시스템과 타겟 Data Domain 시스템에서 서로에게 미치는 영향 없이 로컬로 수행됩니다. WAN 복제 네트워크의 경우 소스 IP 주소가 원격 IP 주소의 게이트웨이에 해당하므로 원격 인터페이스 그룹만 구성하면 됩니다.

인터페이스 그룹에 복제 경로 추가

IP Network 탭을 사용해 인터페이스 그룹에 복제 경로를 추가합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Replication Paths 섹션에서 추가(**+**) 버튼을 클릭합니다.
3. **MTree** 및/또는 **Remote Host**에 대한 값을 입력합니다.
4. 이전에 구성된 인터페이스 그룹을 선택하고 **OK**를 클릭합니다.

인터페이스 그룹에 대한 복제 경로 수정

IP Network 탭을 사용해 인터페이스 그룹에 대한 복제 경로를 수정합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Replication Paths 섹션에서 복제 경로를 선택합니다.
3. **Edit**(연필 모양) 버튼을 클릭합니다.
4. **MTree**, **Remote Host** 또는 **Interface Group**에 대한 일부 또는 전체 값을 수정합니다.
5. **OK**를 클릭합니다.

인터페이스 그룹에 대한 복제 경로 삭제

IP Network 탭을 사용해 인터페이스 그룹에 대한 복제 경로를 삭제합니다.

절차

1. **Protocols** > **DD Boost** > **IP Network**를 선택합니다.
2. Configured Replication Paths 섹션에서 복제 경로를 선택합니다.
3. Delete(**X**) 버튼을 클릭합니다.
4. Delete Replication Path(s) 대화 상자에서 **OK**를 클릭합니다.

DD Boost 제거

이 옵션은 스토리지 유닛에 포함된 모든 데이터(이미지)를 영구적으로 제거할 때 사용합니다. DD Boost를 해제하거나 제거하면 DD Boost FC 서비스도 해제됩니다. 관리 사용자만 DD Boost를 제거할 수 있습니다.

절차

1. 해당하는 백업 애플리케이션 카탈로그 항목을 수동으로 제거합니다(만료시킵니다).

   참고

   여러 백업 애플리케이션이 동일한 Data Domain 시스템을 사용하는 경우에는 각 애플리케이션의 카탈로그에서 모든 항목을 제거하십시오.

2. **Protocols** > **DD Boost** > **More Tasks** > **Destroy DD Boost...**를 선택합니다.
3. 메시지가 표시되면 관리자 자격 증명을 입력합니다.
4. **OK**를 클릭합니다.

DD Boost-over-Fibre Channel 구성

DD OS 이전 버전에서는 DD Boost 라이브러리와 Data Domain 시스템 간의 모든 통신이 IP 네트워킹을 통해 수행되었습니다. 이제 DD OS에서는 DD Boost 라이브러리와 Data Domain 시스템 간의 통신을 위한 대체 전송 메커니즘으로 Fibre Channel을 제공합니다.

참고

Windows, Linux, HP-UX(64비트 Itanium 아키텍처), AIX 및 Solaris 클라이언트 환경이 지원됩니다.

DD Boost 사용자 활성화

Data Domain 시스템에 DD Boost-over-FC 서비스를 구성하기 전에 한 명 이상의 DD Boost 사용자를 추가하고 DD Boost를 활성화해야 합니다.

시작하기 전에

- DD System Manager에 로그인합니다. 지침은 “DD System Manager 로그인 및 로그아웃”을 참조하십시오.

  CLI 절차

  ```
  login as: sysadmin
  Data Domain OS 5.7.x.x-12345
  ```

```
Using keyboard-interactive authentication.
Password:
```

- CLI를 사용하는 경우 SCSI 타겟 데몬이 활성화되었는지 확인하십시오.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

참고

DD System Manager를 사용하는 경우 SCSI 타겟 데몬은 DD Boost-over-FC 서비스를 활성화(이 절차의 마지막)할 때 자동으로 활성화됩니다.

- DD Boost 라이센스가 설치되어 있는지 확인합니다. DD System Manager에서 **Protocols** > **DD Boost** > **Settings**를 선택합니다. Status에 DD Boost 라이센스가 없는 것으로 표시될 경우 **Add License**를 클릭하고 Add License Key 대화 상자에 유효한 라이센스를 입력합니다.

  CLI 절차

```
# license show
```

```
# license add license-code
```

절차

1. **Protocols** > **DD Boost** > **Settings**를 선택합니다.
2. Users with DD Boost Access 섹션에서 하나 이상의 DD Boost 사용자 이름을 지정합니다.

   DD Boost 사용자는 DD OS 사용자이기도 합니다. DD Boost 사용자 이름을 지정할 때 기존 DD OS 사용자 이름을 선택하거나, 새로운 DD OS 사용자 이름을 생성하고 이 이름을 DD Boost 사용자로 지정할 수 있습니다. 이 릴리즈는 여러 DD Boost 사용자를 지원합니다. 자세한 지침은 “DD Boost 사용자 이름 지정”을 참조하십시오.

   CLI 절차

```
# user add username [password password]
```

```
# ddboost set user-name exampleuser
```

3. **Enable**을 클릭하여 DD Boost를 활성화합니다.

   CLI 절차

```
# ddboost enable
Starting DDBOOST, please wait..............
DDBOOST is enabled.
```

결과

이제 Data Domain 시스템에 DD Boost-over-FC 서비스를 구성할 수 있습니다.

DD Boost 구성

사용자를 추가하고 DD Boost를 활성화한 후에는 Fibre Channel 옵션을 활성화하고 DD Boost Fibre Channel 서버 이름을 지정해야 합니다. 사용하는 애플리케이션에 따라 하나 이상의 스토리지 유닛을 생성하고 DD Boost API/플러그인을 Data Domain 시스템에 액세스할 미디어 서버에 설치해야 할 수 있습니다.

절차

1. **Protocols** > **DD Boost** > **Fibre Channel**을 선택합니다.
2. **Enable**을 클릭하여 Fibre Channel 전송을 활성화합니다.

   CLI 절차

   ```
   # ddboost option set fc enabled
   Please wait...
   DD Boost option "FC" set to enabled.
   ```

3. DD Boost Fibre Channel 서버 이름을 기본값(호스트 이름)에서 변경하려면 **Edit**를 클릭하고 새 서버 이름을 입력한 다음 **OK**를 클릭합니다.

   CLI 절차

   ```
   # ddboost fc dfc-server-name set DFC-ddbeta2
   DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
   Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
   ```

4. **Protocols** > **DD Boost** > **Storage Units**를 선택해 스토리지 유닛을 생성합니다(애플리케이션에서 이미 생성되지 않은 경우).

   Data Domain 시스템에서 최소 하나의 스토리지 유닛을 생성해야 하며, DD Boost 사용자에게 해당 스토리지 유닛을 할당해야 합니다. 자세한 지침은 “스토리지 유닛 생성”을 참조하십시오.

   CLI 절차

   ```
   # ddboost storage-unit create storage_unit_name-su
   ```

5. DD Boost API/플러그인을 설치합니다(애플리케이션에 따라 필요한 경우).

   Data Domain 시스템에 액세스해야 하는 NetBackup 미디어 서버에 DD Boost OpenStorage 플러그인 소프트웨어가 설치되어 있어야 합니다. 이 플러그인에는 Data Domain 시스템과 통합되는 필수 DD Boost 라이브러리가 포함되어 있습니다. 자세한 설치 및 구성 지침은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

결과

이제 접속 구성을 확인하고 액세스 그룹을 생성할 수 있습니다.

접속 구성 확인 및 액세스 그룹 생성

Hardware > **Fibre Channel** > **Resources**로 이동해 액세스 지점의 이니시에이터 및 엔드포인트를 관리합니다. **Protocols** > **DD Boost** > **Fibre Channel**로 이동해 DD Boost-over-FC 액세스 그룹을 생성하고 관리합니다.

참고

백업 또는 복원 작업이 실행 중인 동안 Data Domain 시스템의 액세스 그룹을 변경하지 마십시오. 실행 중인 작업이 실패할 수 있습니다. 작업 실행 중 액세스 그룹 변경으로 인한 영향은 백업 소프트웨어와 호스트 구성의 조합에 따라 달라집니다.

절차

1. **Hardware** > **Fibre Channel** > **Resources** > **Initiators**를 선택하여 이니시에이터가 있는 확인합니다.

구성 프로세스 중의 혼란을 줄이려면 이니시에이터에 별칭을 할당하는 것이 좋습니다.

CLI 절차

```
# scsitarget initiator show list
Initiator      System Address                 Group   Service
------------   -----------------------   ----------   -------
initiator-1    21:00:00:24:ff:31:b7:16         n/a       n/a
initiator-2    21:00:00:24:ff:31:b8:32         n/a       n/a
initiator-3    25:00:00:21:88:00:73:ee         n/a       n/a
initiator-4    50:06:01:6d:3c:e0:68:14         n/a       n/a
initiator-5    50:06:01:6a:46:e0:55:9a         n/a       n/a
initiator-6    21:00:00:24:ff:31:b7:17         n/a       n/a
initiator-7    21:00:00:24:ff:31:b8:33         n/a       n/a
initiator-8    25:10:00:21:88:00:73:ee         n/a       n/a
initiator-9    50:06:01:6c:3c:e0:68:14         n/a       n/a
initiator-10   50:06:01:6b:46:e0:55:9a         n/a       n/a
tsm6_p23       21:00:00:24:ff:31:ce:f8   SetUp_Test       VTL
------------   -----------------------   ----------   -------
```

2. 이니시에이터에 별칭을 할당하려면 이니시에이터 하나를 선택하고 연필 모양의 편집 아이콘을 클릭합니다. Modify Initiator 대화 상자의 Name 필드에 별칭을 입력하고 **OK**를 클릭합니다.

   CLI 절차

   ```
   # scsitarget initiator rename initiator-1 initiator-renamed
   Initiator 'initiator-1' successfully renamed.
   ```

   ```
   # scsitarget initiator show list
   Initiator           System Address                 Group
   Service
   -----------------   -----------------------   ----------
   -------
   initiator-2         21:00:00:24:ff:31:b8:32          n/a
   n/a
   initiator-renamed   21:00:00:24:ff:31:b7:16          n/a
   n/a
   -----------------   -----------------------   ----------
   -------
   ```

3. Resources 탭에서 엔드포인트가 있고 설정되어 있는지 확인합니다.

   CLI 절차

   ```
   # scsitarget endpoint show list
   -------------   --------------   ------------   -------   ------
   endpoint-fc-0   5a               FibreChannel   Yes       Online
   endpoint-fc-1   5b               FibreChannel   Yes       Online
   -------------   --------------   ------------   -------   ------
   ```

4. **Protocols** > **DD Boost** > **Fibre Channel**로 이동합니다.
5. DD Boost Access Groups 영역에서 **+** 아이콘을 클릭해 액세스 그룹을 추가합니다.
6. 액세스 그룹의 고유한 이름을 입력합니다. 중복 이름은 지원되지 않습니다.

   CLI 절차

   ```
   # ddboost fc group create test-dfc-group
   DDBoost FC Group "test-dfc-group" successfully created.
   ```

7. 하나 이상의 이니시에이터를 선택합니다. 필요에 따라 새 이름을 입력해 이니시에이터 이름을 바꿉니다. **Next**를 클릭합니다.

   CLI 절차

   ```
   #ddboost fc group add test-dfc-group initiator initiator-5
   Initiator(s) "initiator-5" added to group "test-dfc-group".
   ```

이니시에이터는 Fibre Channel 프로토콜을 사용하여 데이터를 읽고 쓰기 위해 시스템에 접속하는 백업 클라이언트에 연결된 HBA에 있는 포트입니다. WWPN은 미디어 서버에 있는 Fibre Channel 포트의 고유한 월드 와이드 포트 이름(Worldwide Port Name)입니다.

8. 그룹에서 사용할 DD Boost 디바이스의 수를 지정합니다. 이 수는 이니시에이터가 검색할 수 있는 디바이스를 결정하므로 Data Domain 시스템에 대한 입출력 경로의 수가 됩니다. 기본값은 1이고 최소값은 1이며 최대값은 64입니다.

   CLI 절차

   ```
   # ddboost fc group modify Test device-set count 5
   Added 3 devices.
   ```

   여러 클라이언트에 대해 권장되는 값은 *Data Domain Boost for OpenStorage 관리 가이드*를 참조하십시오.

9. 엔드포인트 목록에서 all, none 또는 select 그룹에 포함할 엔드포인트를 선택합니다. **Next**를 클릭합니다.

   CLI 절차

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpoint allsecondary-endpoint all
   Device 'ddboost-dev8' successfully added to group.
   ```

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpointendpoint-fc-1 secondary-endpoint fc-port-0
   Device 'ddboost-dev8' is already in group 'Test'.
   ```

   HBA에 연결된 FC 포트를 통해 LUN을 제공하는 경우 포트를 운영, 보조 또는 없음으로 지정할 수 있습니다. LUN 집합에 대한 운영 포트는 현재 이러한 LUN을 Fabric에 알리는 포트입니다. 보조 포트는 운영 경로에 장애가 발생할 경우 LUN 세트를 브로드캐스팅하는 포트로 수동 조작이 필요합니다. 없음 설정은 선택한 LUN을 알리지 않으려는 경우 사용됩니다. LUN 표시는 SAN 토폴로지에 따라 다릅니다.

10. Summary를 검토하고 필요한 경우 수정합니다. **Finish**를 클릭하여 액세스 그룹을 생성합니다. 생성된 액세스 그룹이 DD Boost Access Groups 목록에 표시됩니다.

    CLI 절차

    ```
    # scsitarget group show detailed
    ```

참고

기존 액세스 그룹의 설정을 변경하려면 목록에서 액세스 그룹을 선택하고 수정(연필 모양) 아이콘을 클릭합니다.

액세스 그룹 삭제

Fibre Channel 탭을 사용해 액세스 그룹을 삭제합니다.

절차

1. **Protocols** > **DD Boost** > **Fibre Channel**을 선택합니다.
2. DD Boost Access Groups 목록에서 삭제할 그룹을 선택합니다.

참고

이니시에이터가 할당된 그룹은 삭제할 수 없습니다. 그룹을 편집해 이니시에이터를 먼저 제거합니다.

3. Delete(**X**) 버튼을 클릭합니다.

HA 시스템에서 DD Boost 사용

HA는 DD Boost를 사용하는 모든 애플리케이션에 대해 원활한 페일오버를 지원합니다. 즉, 수동 작업 백업 또는 복구 작업 사용자의 수작업 없이도 모든 백업 또는 복구 작업이 계속 실행됩니다. MFR(Managed File Replication), DSP(Distributed Segment Processing), 파일 복제 및 DIG(Dynamic Interface Group)을 비롯한 다른 모든 DD Boost 사용자 시나리오도 HA 시스템에서 지원됩니다.

HA 시스템에서 DD Boost를 사용하는 것과 관련하여 다음과 같은 특별한 고려 사항을 유의하십시오.

- HA 지원 Data Domain 시스템에서 DD 서버를 페일오버하는 데에는 10분이 채 걸리지 않습니다. 그러나 DD Boost 애플리케이션 복구 작업은 DD 서버 페일오버가 완료되어야 시작할 수 있기 때문에 DD Boost 애플리케이션을 복구하는 데 이보다 오래 걸릴 수 있습니다. 또한 애플리케이션에서 Boost 라이브러리를 호출할 때까지 Boost 애플리케이션 복구를 시작할 수 없습니다.
- HA 시스템에서 DD Boost를 사용하려면 Boost 애플리케이션이 Boost HA 라이브러리를 사용 중이어야 합니다. HA Boost 라이브러리 이외의 라이브러리를 사용하는 애플리케이션은 원활하게 페일오버되지 않습니다.
- MFR은 소스 시스템과 대상 시스템이 모두 HA를 지원하는 경우에 원활하게 페일오버됩니다. 부분적인 HA 구성(소스 또는 대상 시스템 중 하나만 활성화된 경우)에서는 HA를 지원하는 시스템에 장애가 발생한 경우에 MFR이 지원됩니다. 자세한 내용은 *DD Boost for OpenStorage 관리 가이드* 또는 *DD Boost for Partner Integration Administration Guide*를 참조하십시오.
- 액티브 Data Domain 시스템과 대기 Data Domain 시스템 간의 직접 상호 연결과 관련한 IP 주소는 동적 인터페이스 그룹에 포함하면 안 됩니다.
- DD Boost 클라이언트는 부동 IP 주소를 사용하도록 구성해야 합니다.

DD Boost 탭 정보

DD System Manager의 DD Boost 탭 사용 방법을 학습합니다.

설정

Settings 탭을 사용해 DD Boost를 설정하거나 해제하고 클라이언트 및 사용자를 선택하고 고급 옵션을 지정합니다.

Settings 탭에는 DD Boost 상태(Enabled 또는 Disabled)가 표시됩니다. **Status** 버튼을 사용해 **Enabled** 또는 **Disabled** 사이를 전환합니다.

Allowed Clients 아래에서 시스템에 대한 액세스 권한을 가질 클라이언트를 선택합니다. 클라이언트 목록을 관리하려면 **Add**, **Modify** 및 **Delete** 버튼을 사용합니다.

Users with DD Boost Access 아래에서 DD Boost에 대한 액세스 권한을 가질 사용자를 선택합니다. 사용자 목록을 관리하려면 **Add**, **Change Password** 및 **Remove** 버튼을 사용합니다.

Advanced Options를 확장하여 설정된 고급 옵션을 확인합니다. 이러한 옵션을 재설정하려면 **More Tasks** > **Set Options**로 이동합니다.

Active Connections

Active Connections 탭을 사용해 클라이언트, 인터페이스 및 아웃바운드 파일에 대한 정보를 봅니다.

표 131 접속된 클라이언트 정보

항목	설명
Client	접속된 클라이언트의 이름입니다.
Idle	클라이언트가 유휴 상태이면 Yes이고 아니면 No입니다.
Plug-In Version	설치된 DD Boost 플러그인 버전입니다(예: 2.2.1.1).
OS 버전	설치된 운영 체제 버전입니다(예: Linux 2.6.1 7-1.2142_FC4smp x86_64).
Application Version	설치된 백업 애플리케이션 버전입니다(예: NetBackup 6.5.6).
암호화됨	접속이 암호화되면 Yes이고 아니면 No입니다.
DSP	접속이 DSP(Distributed Segment Processing)를 사용하고 있는지 여부입니다.
Transport	사용 중인 전송의 유형으로 IPv4, IPv6, FC(Fibre Channel) 등입니다.

표 132 구성된 인터페이스 접속 정보

항목	설명
인터페이스	인터페이스의 IP 주소입니다.
Interface Group	다음 중 하나를 선택합니다. • 인터페이스 그룹의 이름입니다. • 속한 그룹이 없는 경우 None입니다.
백업	활성 백업 접속의 수입니다.
복구	활성 복원 접속의 수입니다.
복제	활성 복제 접속의 수입니다.
신세틱	신세틱(Synthetic) 백업의 수입니다.
Total	인터페이스에 대한 총 접속 수입니다.

표 133 아웃바운드 파일 복제 정보

아웃바운드 파일 항목	설명
File Name	나가는 이미지 파일의 이름입니다.
Target Host	파일을 수신하는 호스트의 이름입니다.
Logical Bytes to Transfer	전송할 논리적 바이트의 수입니다.

표 133 아웃바운드 파일 복제 정보 (계속)

아웃바운드 파일 항목	설명
Logical Bytes Transferred	이미 전송된 논리적 바이트의 수입니다.
Low Bandwidth Optimization	이미 전송된 저대역폭 바이트의 수입니다.

IP 네트워크

IP Network 탭에는 구성된 인터페이스 그룹이 나열됩니다. 세부 정보에는 그룹이 설정되어 있는지 여부와 구성된 클라이언트 인터페이스가 포함됩니다. 관리자는 Interface Group 메뉴를 사용하여 인터페이스 그룹과 연결된 클라이언트를 볼 수 있습니다.

Fibre Channel

Fibre Channel 탭에는 구성된 DD Boost 액세스 그룹이 나열됩니다. Fibre Channel 탭에서 액세스 그룹을 생성 및 삭제하고 DD Boost 액세스 그룹에 대한 이니시에이터, 디바이스 및 엔드포인트를 구성할 수 있습니다.

Storage Units

Storage Units 탭을 사용하여 스토리지 유닛을 보고, 생성하고, 수정하고, 삭제합니다.

표 134 Storage Units 탭

항목	설명
Storage Units	
DD Boost 복제 보기	DD Boost 복제 컨텍스트를 봅니다.
Storage Unit	스토리지 유닛의 이름입니다.
User	스토리지 유닛과 연결된 사용자 이름입니다.
Quota Hard Limit	스토리지 유닛에 대해 설정된 하드 할당량입니다.
Last 24hr Pre-Comp	압축 전에 지난 24시간 동안 스토리지 유닛에 기록된 데이터의 양입니다.
Last 24hr Post-Comp	압축 후에 지난 24시간 동안 스토리지 유닛에 기록된 데이터의 양입니다.
Last 24hr Comp Ratio	지난 24시간 동안 스토리지 유닛에 기록된 데이터의 압축률입니다.
Weekly Avg Post-Comp	압축 후에 매주 스토리지 유닛에 기록되는 평균 데이터 양입니다.
Last Week Post-Comp	압축 후에 지난주 동안 스토리지 유닛에 기록된 데이터의 양입니다.
Weekly Avg Comp Ratio	매주 스토리지 유닛에 기록되는 데이터의 평균 압축률입니다.
Last Week Comp Ratio	지난주 동안 스토리지 유닛에 기록된 데이터의 압축률입니다.

스토리지 유닛을 선택하여 자세한 정보를 봅니다. 자세한 정보는 다음 3개의 탭에서 확인할 수 있습니다.

- Storage Unit 탭

  표 135 Storage unit details: Storage Unit 탭

항목	설명
Total Files	스토리지 유닛에 있는 파일 이미지의 총 개수입니다.
Full Path	스토리지 유닛의 전체 경로입니다.
Status	스토리지 유닛의 현재 상태입니다(여러 상태의 조합이 지원됨). 상태는 다음 중 하나일 수 있습니다. ■ D - 삭제됨 ■ RO - 읽기 전용 ■ RW - 읽기/쓰기 ■ RD - 복제 대상 ■ RLE - DD Retention Lock 활성화됨 ■ RLD - DD Retention Lock 비활성화됨
Pre-Comp Used	이미 사용한 압축 전 스토리지의 용량입니다.
Used (Post-Comp)	스토리지 유닛의 파일을 압축한 이후의 총 크기입니다.
Compression	파일에 적용된 압축률입니다.
Schedules	스토리지 유닛에 할당된 물리적 용량 측정 스케줄의 횟수입니다.
Submitted Measurements	스토리지 유닛의 물리적 용량을 측정한 횟수입니다.
Quota Enforcement	Quota를 클릭하여 Data Management Quota 페이지로 이동하면 MTree에서 사용하는 고정 및 가변 할당량 값/비율이 나열됩니다.
Pre-Comp Soft Limit	스토리지 유닛에 대해 설정된 가변 할당량(soft quota)의 현재 값입니다.
Pre-Comp Hard Limit	스토리지 유닛에 대해 설정된 고정 할당량(hard quota)의 현재 값입니다.
Quota Summary	사용한 고정적 제한의 비율입니다.
Total Snapshots	스토리지 유닛의 총 스냅샷 수입니다.
Expired	스토리지 유닛의 만료된 스냅샷 수입니다.
Unexpired	스토리지 유닛의 만료되지 않은 스냅샷 수입니다.
Oldest Snapshot	스토리지 유닛의 가장 오래된 스냅샷입니다.
Newest Snapshot	스토리지 유닛의 가장 최신 스냅샷입니다.
Next Scheduled	다음으로 예약된 스토리지 유닛 스냅샷입니다.
Assigned Snapshot Schedules	스토리지 유닛에 할당된 스냅샷 스케줄입니다.

- Space Usage 탭: 사용된 압축 전 바이트, 사용된 압축 후 바이트, 압축 계수를 보여주는 그래프를 표시합니다.

- Daily Written 탭: 기록된 압축 전 바이트, 기록된 압축 후 바이트, 총 압축 계수를 보여 주는 그래프를 표시합니다.

15장

DD VTL(Virtual Tape Library)

이 장에는 다음과 같은 내용이 포함됩니다.

DD VTL(Virtual Tape Library) 개요

DD VTL(Data Domain Virtual Tape Library)은 물리적 테이프의 사용을 에뮬레이트하는 디스크 기반 백업 시스템입니다. 물리적 테이프 라이브러리와 거의 동일한 기능을 사용해 백업 애플리케이션이 DD 시스템 스토리지에 연결되고 관리할 수 있도록 합니다.

가상 테이프 드라이브는 물리적 테이프 드라이브와 같은 방법으로 백업 소프트웨어에서 액세스할 수 있습니다. DD VTL에서 이 드라이브를 생성하면 백업 소프트웨어에 SCSI 테이프 드라이브로 나타납니다. DD VTL 자체는 백업 소프트웨어에 표준 드라이버 인터페이스를 통해 액세스되는 SCSI 로봇 디바이스로 나타납니다. 그러나 미디어 체인저 및 백업 이미지의 이동은 DD VTL로 구성된 DD 시스템이 아닌 백업 소프트웨어에 의해 관리됩니다.

다음 용어는 DD VTL과 함께 사용할 경우 특별한 의미를 갖습니다.

- *라이브러리(Library)*: 라이브러리는 물리적 테이프 라이브러리를 드라이브, 체인저, CAP(Cartridge Access Port) 및 슬롯(카트리지 슬롯)으로 에뮬레이트합니다.
- *테이프*: 테이프는 파일로 표시됩니다. 볼트(Vault)에서 라이브러리로 테이프를 가져올 수 있습니다. 라이브러리에서 볼트(Vault)로 테이프를 내보낼 수 있습니다. 드라이브, 슬롯 및 CAP의 라이브러리 내에서 테이프를 이동할 수 있습니다.
- *풀*: 풀은 파일 시스템의 디렉토리로 매핑되는 테이프 모음입니다. 풀은 테이프를 대상으로 복제하는 데 사용됩니다. 기본적으로 풀은 생성될 때 디렉토리 풀로 지정하지 않으면 MTree 풀로 생성됩니다. 디렉토리 기반 풀을 MTree 기반 풀로 변환해 MTree의 보다 유용한 기능을 활용할 수 있습니다.
- *볼트*: 볼트(Vault)에는 라이브러리에서 사용되지 않는 테이프가 들어 있습니다. 테이프는 라이브러리 또는 볼트(Vault)에 상주합니다.

DD VTL은 특정 백업 소프트웨어와 하드웨어 구성을 사용해 테스트를 거쳤으며 해당 구성을 통해 지원됩니다. 자세한 내용은 온라인 지원 사이트의 해당 *Backup Compatibility Guide*를 참조하십시오.

DD VTL은 테이프 라이브러리 및 파일 시스템(NFS/CIFS/DD Boost) 인터페이스의 동시 사용을 지원합니다.

DR(Disaster Recovery)이 필요할 경우 DD Replicator를 사용하여 풀과 테이프를 원격 DD 시스템에 복제할 수 있습니다.

테이프의 데이터가 수정되지 않도록 보호하기 위해 DD Retention Lock Governance 소프트웨어를 사용해 테이프를 잠글 수 있습니다.

참고

현재 16Gb/s의 경우 Data Domain에서는 Fabric 및 포인트 투 포인트 토폴로지를 지원합니다. 다른 토폴로지는 문제가 발생합니다.

KB 문서 *Data Domain: https://support.emc.com/kb/180591*에 제공되는 VTL 모범 사례 가이드에서는 DD VTL 모범 사례에 대한 추가 정보를 제공합니다.

DD VTL 계획

DD VTL(Virtual Tape Library) 기능에는 적절한 라이센스 등록, 인터페이스 카드, 사용자 사용 권한과 같은 특정 요구 사항이 있습니다. 여기에 이러한 요구 사항과 세부 정보 및 권장 사항이 함께 나열되어 있습니다.

- 적절한 DD VTL 라이센스.

  - DD VTL은 라이센스가 부여된 기능이며 NDMP(Network Data Management Protocol) over IP(Internet Protocol) 또는 DD VTL directly over FC(Fibre Channel)를 사용해야 합니다.
  - IBM i 시스템의 경우 추가 라이센스(I/OS 라이센스)가 필요합니다.
  - DD System Manager를 통해 DD VTL 라이센스를 추가하면 DD VTL 기능이 자동으로 비활성화되고 활성화됩니다.
- 설치된 FC 인터페이스 카드 또는 NDMP를 사용하도록 구성된 DD VTL
  - 백업 서버와 DD 시스템 간의 DD VTL 통신이 FC 인터페이스를 통해 수행되는 경우 DD 시스템에 FC 인터페이스 카드가 설치되어 있어야 합니다. FC 인터페이스 카드가 DD 시스템에서 제거되거나 변경될 때마다 해당 카드와 연결된 모든 DD VTL 구성을 업데이트해야 합니다.
  - 백업 서버와 DD 시스템 간의 DD VTL 통신이 NDMP를 통해 수행되는 경우 FC 인터페이스 카드가 필요하지 않습니다. 그러나 TapeServer 액세스 그룹을 구성해야 합니다. 또한 NDMP를 사용하는 경우 모든 이니시에이터 및 포트 기능이 적용되지 않습니다.
  - NDMP 클라이언트가 DD 시스템으로 정보를 보낼 수 있도록 net filter를 구성해야 합니다. **net filter add operation allow clients *<client-IP-address>*** 명령을 실행하여 NDMP 클라이언트에 대한 액세스를 허용합니다.
    - 보안을 강화하려면 **net filter add operation allow clients *<client-IP-address>* interfaces *<DD-interface-IP-address>*** 명령을 실행합니다.
    - 다른 모든 net filter 규칙보다 먼저 이 규칙을 적용하려면 **seq-id 1** 옵션을 추가합니다.
- 백업 소프트웨어 최소 레코드(블록) 크기
  - 가능하면 64KiB 이상의 최소 레코드(블록) 크기를 사용하도록 백업 소프트웨어를 설정하십시오. 일반적으로 크기가 클수록 성능이 빨라지고 데이터 압축이 향상됩니다.
  - 백업 애플리케이션에 따라, 초기 구성 후 이 크기를 변경하면 원래 크기로 기록된 데이터를 읽지 못하게 될 수도 있습니다.
- 시스템에 대한 적절한 사용자 액세스
  - 기본적인 테이프 작업 및 모니터링에는 사용자 로그인만 필요합니다.
  - DD VTL 서비스를 활성화 및 구성하고 다른 구성 작업을 수행하려면 sysadmin 로그인이 필요합니다.

DD VTL 제한

DD VTL을 설정하거나 사용하기 전에 크기, 슬롯 등에 대한 다음 제한을 검토하십시오.

- 입출력 크기 – DD VTL을 사용하는 모든 DD 시스템에 대해 최대로 지원되는 입출력 크기는 1MB입니다.
- 라이브러리 – DD VTL은 시스템당 최대 64개의 라이브러리를 지원합니다(각 DD 시스템에서 DD VTL 인스턴스 64개에 해당함).
- 이니시에이터 – DD VTL은 DD 시스템당 최대 1,024개의 이니시에이터 또는 WWPN(World-Wide Port Name)을 지원합니다.
- 테이프 드라이브 – 테이프 드라이브에 대한 정보는 다음 섹션에 제공됩니다.
- 데이터 스트림 – 데이터 스트림에 대한 정보는 다음 표에 표시됩니다.

표 136 Data Domain 시스템에 전송되는 데이터 스트림

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD140, DD160, DD610	4GB 또는 6GB/0.5GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8GB/0.5GB 또는 1GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16GB 또는 20GB/1GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36GB/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72GB[b]/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 또는 64GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885

표 136 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD9800	256/768GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8TB	8GB/512MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16TB	16GB/512MB 또는 24GB/1GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32TB	24GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48TB	36GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64TB	48GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96TB	64GB/2GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4TB	12GB(가상 메모리)/512MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32TB	46GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

표 136 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

a. DirRepl, OptDup, MTreeRepl 스트림
b. Data Domain Extended Retention 소프트웨어 옵션은 확장(최대) 메모리를 지원하는 이러한 디바이스에서만 사용할 수 있습니다.

- 슬롯 – DD VTL은 최대 다음과 같은 수의 슬롯을 지원합니다.
  - 라이브러리당 32,000개
  - DD 시스템당 64,000개

  슬롯 수를 드라이브 수와 같거나 그보다 더 많게 유지하기 위해 DD 시스템에서 슬롯을 자동으로 추가합니다.

  참고

  일부 디바이스 드라이버(예: IBM AIX Atape 디바이스 드라이버)의 라이브러리 구성에는 특정 드라이브/슬롯 제한이 적용됩니다. 이는 DD 시스템이 지원하는 슬롯 수보다 작을 수 있습니다. 이 제한은 백업 애플리케이션과 이러한 애플리케이션에서 사용하는 드라이브에 영향을 미칠 수 있습니다.
- CAP(Cartridge Access Port) – DD VTL은 최대 다음과 같은 수의 CAP를 지원합니다.
  - 라이브러리당 100개
  - DD 시스템당 1,000개

DD VTL에서 지원되는 드라이브 수

DD VTL에 의해 지원되는 최대 드라이브 수는 CPU 코어의 수와 DD 시스템에 설치된 메모리(해당되는 경우 RAM과 NVRAM 모두)의 양에 따라 다릅니다.

참고

각 모델에 대해 CPU 코어와 메모리의 많은 조합이 있고 지원되는 드라이브의 수는 특정 모델 그 자체가 아니라 *오로지* CPU 코어와 메모리에 따라서만 결정되기 때문에, 이 표에는 모델 번호가 나와 있지 않습니다.

표 137 DD VTL에서 지원되는 드라이브 수

CPU 코어 수	RAM(GB)	NVRAM(GB)	지원되는 최대 드라이브 수
32 미만	4 이하	해당 없음	64
	4 이상, 최대 38	해당 없음	128
	38 이상, 최대 128	해당 없음	256
	128 이상	해당 없음	540
32~39	최대 128	4 미만	270
	최대 128	4 이상	540
	128 이상	해당 없음	540
40~59	해당 없음	해당 없음	540
60개 이상	해당 없음	해당 없음	1080

테이프 바코드

테이프를 생성할 때는 고유한 *바코드*를 할당해야 합니다. 바코드를 중복할 경우 예측할 수 없는 동작이 발생할 수 있으니 절대 중복하지 마십시오. 각 바코드는 8자로 구성됩니다. 첫 여섯 자리는 숫자 또는 대문자(0-9, A-Z)이고 마지막 두 자리는 지원되는 테이프 유형에 대한 테이프 코드입니다. 다음 표를 참조하십시오.

참고

DD VTL 바코드는 8자로 구성되지만 체인저 유형에 따라 6자 또는 8자가 백업 애플리케이션으로 전송될 수 있습니다.

표 138 테이프 유형별 테이프 코드

테이프 유형	기본 용량(달리 명시하지 않는 한)	테이프 코드
LTO-1	100GiB	L1
LTO-1	50GiB(비기본값)	LA[a]
LTO-1	30GiB(비기본값)	LB
LTO-1	10GiB(비기본값)	LC
LTO-2	200GiB	L2
LTO-3	400GiB	L3
LTO-4	800GiB	L4
LTO-5(기본값)	1.5TiB	L5

a. TSM의 경우 LA 코드가 무시되면 L2 테이프 코드를 사용합니다.

테이프 라이브러리가 여러 개인 경우 "L" 바로 전의 6번째 자리에 숫자가 있으면 바코드가 자동으로 증가합니다. 오버플로우가 발생하는 경우(9 -> 0) 번호 지정이 왼쪽으로 한 위치 이동합니다. 증가할 다음 자리에 문자가 있으면 증가가 중지됩니다. 몇 가지 샘플 바코드와 각 바코드가 증가하는 방식은 다음과 같습니다.

- 000000L1은 100GiB 용량의 테이프를 생성하고 최대 100,000개의 테이프(000000~99999)를 허용할 수 있습니다.
- AA0000LA는 50GiB 용량의 테이프를 생성하고 최대 10,000개의 테이프(0000~9999)를 허용할 수 있습니다.
- AAAA00LB는 30GiB 용량의 테이프를 생성하고 최대 100개의 테이프(00~99)를 허용할 수 있습니다.
- AAAAAALC는 10GiB 용량의 테이프를 하나 생성합니다. 이 이름으로는 테이프를 하나만 생성할 수 있습니다.
- AAA350L1은 100GiB 용량의 테이프를 생성하고 최대 650개의 테이프(350~999)를 허용할 수 있습니다.
- 000AAALA는 50GiB 용량의 테이프를 하나 생성합니다. 이 이름으로는 테이프를 하나만 생성할 수 있습니다.
- 5M7Q3KLB는 30GiB 용량의 테이프를 하나 생성합니다. 이 이름으로는 테이프를 하나만 생성할 수 있습니다.

LTO 테이프 드라이브 호환성

서로 다른 세대의 LTO(Linear Tape-Open) 기술이 설정에 포함될 수 있습니다. 이러한 세대 간 호환성이 표 형식으로 제공됩니다.

이 표에 사용된 약어의 의미는 다음과 같습니다.

- RW = 읽기 및 쓰기 호환
- R = 읽기 전용 호환
- — = 호환되지 않음

표 139 LTO 테이프 드라이브 호환성

테이프 형식	LTO-5 드라이브	LTO-4 드라이브	LTO-3 드라이브	LTO-2 드라이브	LTO-1 드라이브
LTO-5 테이프	RW	—	—	—	—
LTO-4 테이프	RW	RW	—	—	—
LTO-3 테이프	R	RW	RW	—	—
LTO-2 테이프	—	R	RW	RW	—
LTO-1 테이프	—	—	R	RW	RW

DD VTL 설정

간단한 DD VTL을 설정하려면 구성 마법사를 사용합니다. 구성 마법사는 *시작* 장에 설명되어 있습니다.

*Data Domain Operating System 초기 구성 가이드*에서 유사한 설명서를 확인할 수 있습니다.

그러고 나서 다음 항목을 계속 진행해 DD VTL을 활성화하고, 라이브러리를 생성하고, 테이프를 생성해 가져오십시오.

참고

배포 환경에 AS400 시스템이 DD VTL 클라이언트로 포함될 경우 Data Domain 시스템과 AS400 클라이언트 시스템 간에 DD VTL 관계를 구성하기 전에 DD VTL 기본 옵션 구성(365페이지) 항목을 참조하여 VTL 체인저 및 드라이브에 대한 일련 번호 접두사를 구성합니다.

HA 시스템과 DD VTL

HA 시스템은 DD VTL과 호환되지만 페일오버 시에 DD VTL 작업이 진행 중인 경우 페일오버가 완료된 후 작업을 수동으로 재시작해야 합니다.

HA 환경에서 DD VTL을 사용하기 위한 HBA, 스위치, 펌웨어 및 드라이버 요구 사항에 대한 자세한 내용은 *Data Domain Operating System Backup Compatibility Guide*를 참조하십시오.

클라우드에 DD VTL 테이프 저장

DD VTL은 DD Cloud Tier 스토리지에 VTL 볼팅을 저장할 수 있도록 지원합니다. 이 기능을 사용하려면 Data Domain 시스템이 지원되는 Cloud Tier 구성이고 VTL 라이센스 이외에 Cloud Tier 라이센스를 가져야 합니다.

DD VTL이 볼팅에 클라우드 스토리지를 사용하도록 구성하기 전에 DD Cloud Tier 스토리지를 구성하고 라이센스를 등록합니다. DD Cloud Tier 요구 사항과 DD Cloud Tier를 구성하는 방법에 대한 자세한 내용은 DD Cloud Tier(467페이지)에 나와 있습니다.

VTL의 FC 및 네트워크 인터페이스 요구 사항은 클라우드 기반과 로컬 볼팅 스토리지에서 모두 동일합니다. 볼팅에 클라우드 스토리지를 사용하기 위해 DD VTL에 특별한 구성은 필요 없습니다. DD VTL을 구성하는 경우 클라우드 스토리지를 볼팅 위치로 선택합니다. 그러나 클라우드 기반 볼팅을 사용하는 경우 클라우드 기반 볼팅에 고유한 몇 가지 데이터 관리 옵션이 있습니다. 자세한 내용은 클라우드 기반 볼팅 작업(383페이지)에 나와 있습니다.

DD VTL 관리

DD System Manager(Data Domain System Manager) 또는 DD OS(Data Domain Operating System) CLI(Command Line Interface)를 사용하여 DD VTL을 관리할 수 있습니다. 로그인 후 DD VTL 프로세스의 상태를 확인하고 라이선스 정보를 확인하고 옵션을 검토 및 구성할 수 있습니다.

로그인

GUI(Graphical User Interface)를 사용하여 DD VTL(Virtual Tape Library)을 관리하려면 DD System Manager에 로그인합니다.

CLI 절차

CLI에서 로그인할 수도 있습니다.

```
login as: sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```

SCSI 타겟 데몬 활성화(CLI 전용)

CLI에서 로그인하는 경우 scsitarget 데몬(Fibre Channel 서비스)을 활성화해야 합니다. 이 데몬은 DD System Manager에서 DD VTL 또는 DD Boost-FC 활성화를 선택하는 동안 활성화됩니다. CLI에서는 이러한 프로세스를 개별적으로 활성화해야 합니다.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

DD VTL에 액세스

DD System Manager 왼쪽의 메뉴에서 **Protocols** > **VTL**을 선택합니다.

상태

Virtual Tape Libraries > **VTL Service** 영역의 맨 위에 DD VTL 프로세스의 상태가 표시됩니다(예: **Enabled: Running**). 상태의 첫 번째 부분에는 **Enabled**(켜짐) 또는 **Disabled**(꺼짐)가 표시됩니다. 두 번째 부분에는 다음 프로세스 상태 중 하나가 표시됩니다.

표 140 DD VTL 프로세스 상태

상태	설명
Running	DD VTL 프로세스가 활성화되어 있고 활성입니다(녹색으로 표시됨).
Starting	DD VTL 프로세스가 시작되는 중입니다.
Stopping	DD VTL 프로세스가 종료되는 중입니다.
Stopped	DD VTL 프로세스가 비활성화되어 있습니다(빨간색으로 표시됨).

표 140 DD VTL 프로세스 상태 (계속)

상태	설명
Timing out	DD VTL 프로세스가 충돌하여 자동 재시작을 시도하는 중입니다.
Stuck	자동 재시작이 여러 차례 실패한 후, DD VTL 프로세스를 정상적으로 종료할 수 없어 프로세스 중지를 시도하고 있습니다.

DD VTL 라이선스

VTL License 줄에는 DD VTL 라이선스가 적용되었는지 여부가 표시됩니다. Unlicensed라고 표시되어 있으면 **Add License**를 선택합니다. Add License Key 대화 상자에 라이선스 키를 입력합니다. **Next**와 **OK**를 차례로 선택합니다.

참고

모든 라이선스 정보는 출고 시 구성 프로세스 중에 입력되지만 DD VTL을 나중에 구매한 경우 해당 시기에 DD VTL 라이선스 키가 제공되지 않았을 수 있습니다.

CLI 절차

CLI에서 DD VTL 라이선스가 설치되어 있는지도 확인할 수 있습니다.

```
# elicense show
## License Key                    Feature
--    -------------------        -----------
1     DEFA-EFCD-FCDE-CDEF        Replication
2     EFCD-FCDE-CDEF-DEFA        VTL
--    -------------------        -----------
```

라이선스가 없는 경우 각 유닛에 제공된 설명서(빠른 설치 카드)에서 구매한 라이선스를 확인할 수 있습니다. 라이선스 키를 입력하려면 다음 명령 중 하나를 입력합니다.

```
# license add <license-code>
```

```
# elicense update <license-file>
```

I/OS License(IBM i 사용자용)

IBM i 사용자의 경우 I/OS License 줄에서 I/OS 라이선스 적용 여부를 확인할 수 있습니다. Unlicensed라고 표시되어 있으면 **Add License**를 선택합니다. 유효한 I/OS 라이선스를 다음 형식 중 하나로 입력해야 합니다. **xxxx-xxxx-xxxx-xxxx** 또는 **xxxx-xxxx-xxxx-xxxx-xxxx** I/OS 라이선스는 IBM i 시스템에서 사용할 라이브러리와 드라이브를 생성하기 전에 설치해야 합니다. **Next**와 **OK**를 차례로 선택합니다.

DD VTL 활성화

DD VTL을 활성화하면 Data Domain HBA의 WWN이 고객 Fabric에 브로드캐스팅되고 모든 라이브러리 및 라이브러리 드라이브가 활성화됩니다. 변경 제어 프로세스 형태의 포워딩 계획이 필요한 경우 이 프로세스를 활성화하여 조닝(Zoning)을 용이하게 해야 합니다.

절차

1. DD VTL 라이센스가 있고 파일 시스템이 활성화되어 있는지 확인합니다.
2. **Virtual Tape Libraries** > **VTL Service**를 선택합니다.
3. Status 영역 오른쪽에서 **Enable**을 선택합니다.
4. Enable Service 대화 상자에서 **OK**를 선택합니다.
5. DD VTL이 활성화되면 Status가 녹색 **Enabled: Running**으로 바뀝니다. 또한 구성된 DD VTL 옵션이 Option Defaults 영역에 표시됩니다.

CLI 절차

```
# vtl enable Starting VTL, please wait ... VTL is enabled.
```

DD VTL 비활성화

DD VTL을 비활성화하면 모든 라이브러리가 닫히고 DD VTL 프로세스가 종료됩니다.

절차

1. **Virtual Tape Libraries** > **VTL Service**를 선택합니다.
2. Status 영역 오른쪽에서 **Disable**을 선택합니다.
3. Disable Service 대화 상자에서 **OK**를 선택합니다.
4. DD VTL을 비활성화하면 Status가 빨간색으로 **Disabled: Stopped**로 바뀝니다.

CLI 절차

```
# vtl disable
```

DD VTL 옵션 기본값

VTL Service 페이지의 Option Default 영역에 기본 DD VTL 옵션(auto-eject, auto-offline 및 barcode-length)에 대한 현재 설정이 표시됩니다.

사용하는 DD VTL의 현재 기본 옵션은 **Virtual Tape Libraries** > **VTL Service** 영역에 표시됩니다. 이러한 값을 변경하려면 **Configure**를 선택합니다.

표 141 옵션 기본값

항목	설명
Property	구성된 옵션을 나열합니다. • auto-eject • auto-offline • barcode-length
Value	구성된 각 옵션에 대한 값을 제공합니다. • auto-eject: 기본값(disabled), enabled 또는 disabled • auto-offline: 기본값(disabled), enabled 또는 disabled • barcode-length: 기본값(8), 6 또는 8

DD VTL 기본 옵션 구성

DD VTL 기본 옵션은 라이선스를 추가할 때, 라이브러리를 생성할 때 또는 그 후에 언제든지 구성할 수 있습니다.

참고

DD VTL에는 기본적으로 글로벌 옵션이 할당되며 이러한 옵션은 수동으로 업데이트 방법을 변경하지 않는 한 글로벌 옵션이 변경될 때마다 업데이트됩니다.

절차

1. **Virtual Tape Libraries** > **VTL Service**를 선택합니다.
2. Option Defaults 영역에서 **Configure**를 선택합니다. Configure Default Options 대화 상자에서 기본 옵션의 일부 또는 전체를 변경합니다.

표 142 DD VTL 기본 옵션

옵션	값	참고
auto-eject	기본값(disabled), enable 또는 disable	자동 꺼내기를 활성화하면 다음 경우를 제외하고 CAP(Cartridge Access Port)에 삽입된 테이프가 자동으로 가상 볼트(Vault)로 이동합니다. • 테이프가 볼트(Vault)에서 제공된 경우에는 테이프가 CAP에 그대로 있습니다. • 값 0(false)으로 `ALLOW_MEDIUM_REMOVAL` 명령을 라이브러리에 대해 실행하여 CAP에서 외부로 미디어를 제거하지 못하게 하는 경우.
auto-offline	기본값(disabled), enable 또는 disable	자동 오프라인을 활성화하면 테이프 이동 작업이 수행되기 전에 드라이브가 자동으로 오프라인으로 전환됩니다.
barcode-length	기본값(8), 6 또는 8[L180, RESTORER-L180 및 DDVTL 체인저 모델의 경우 자동으로 6으로 설정됨]	DD VTL 바코드는 8자로 구성되지만 체인저 유형에 따라 6자 또는 8자가 백업 애플리케이션으로 전송될 수 있습니다.

3. **OK**를 선택합니다.
4. 이러한 서비스 옵션을 모두 비활성화하려면 **Reset to Factory**를 선택합니다. 그러면 값이 즉시 출고 기본값으로 재설정됩니다.

사후 요구 사항

DD VTL 환경에 AS400이 DD VTL 클라이언트로서 포함되어 있는 경우 DD VTL 환경에 AS400을 추가하기 전에 일련 번호 접두사에 대한 DD VTL 옵션을 수동으로 구성합니다. 이 작업은 DD VTL을 사용하는 Data Domain 시스템이 여러 개 있는 경우 일련 번호 중복을 피하는 데 필요합니다. 일련 번호 접두사 값은 다음과 같아야 합니다.

- 환경의 Data Domain 시스템에 동일한 접두사 번호를 갖는 DD VTL이 없도록 고유한 6자리 값으로 지정해야 합니다.
- 0으로 끝나지 않아야 합니다.

Data Domain 도메인 시스템의 배포 및 DD VTL의 구성 동안 이 값을 1번만 구성합니다. 향후 시스템에서 DD OS를 업그레이드해도 계속 유지됩니다. 이 값을 설정하기 위해 DD VTL 서비스를 다시 시작할 필요가 없습니다. 이 값을 설정한 후 생성된 모든 DD VTL 라이브러리는 일련 번호에 대해 새 접두사를 사용합니다.

`CLI equivalent`

```
# vtl option set serial-number-prefix value
# vtl option show serial-number-prefix
```

라이브러리 작업

라이브러리는 물리적 테이프 라이브러리를 드라이브, 체인저, CAP(Cartridge Access Port) 및 슬롯(카트리지 슬롯)으로 에뮬레이트합니다. **Virtual Tape Libraries** > **VTL Service** > **Libraries**를 선택하면 구성된 모든 라이브러리에 대한 자세한 정보가 표시됩니다.

표 143 라이브러리 정보

항목	설명
Name	구성된 라이브러리의 이름입니다.
Drives	라이브러리에서 구성된 드라이브의 개수입니다.
Slots	라이브러리에서 구성된 슬롯의 개수입니다.
CAPs	라이브러리에서 구성된 CAP(Cartridge Access Port)의 개수입니다.

More Tasks 메뉴에서 라이브러리를 생성 및 삭제하고 테이프를 검색할 수 있습니다.

라이브러리 생성

DD VTL은 시스템당 최대 64개의 라이브러리를 지원합니다(각 DD 시스템에서 64개의 동시 활성 VTL(Virtual Tape Library) 인스턴스에 해당).

시작하기 전에

배포 환경에 AS400 시스템이 DD VTL 클라이언트로 포함될 경우 DD VTL 라이브러리를 생성하고 Data Domain 시스템과 AS400 클라이언트 시스템 간에 DD VTL 관계를 구성하기 전에 DD VTL 기본 옵션 구성(365페이지) 항목을 참조하여 VTL 체인저 및 드라이브에 대한 일련 번호 접두사를 구성합니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries**를 선택합니다.
2. **More Tasks** > **Library** > **Create**를 선택합니다.
3. Create Library 대화 상자에서 다음 정보를 입력합니다.

표 144 Create Library 대화 상자

필드	사용자 입력
Library Name	1~32자의 영숫자로 이름을 입력합니다.
Number of Drives	드라이브의 개수를 1~98개로 입력합니다(참고 참조). 생성할 드라이브 수는 라이브러리에 기록될 데이터 스트림의 수에 해당합니다. 참고 DD VTL에 의해 지원되는 최대 드라이브 수는 CPU 코어의 수와 DD 시스템에 설치된 메모리(해당되는 경우 RAM과 NVRAM 모두)의 양에 따라 다릅니다.

표 144 Create Library 대화 상자 (계속)

필드	사용자 입력
Drive Model	드롭다운 목록에서 원하는 모델을 선택합니다. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5(기본값) • HP-LTO-3 • HP-LTO-4 드라이브 유형 또는 미디어 유형을 동일한 라이브러리에 혼합하지 마십시오. 백업 작업에서 예기치 않은 결과 및/또는 오류가 발생할 수 있습니다.
Number of Slots	라이브러리에 있는 슬롯의 개수를 입력합니다. 다음은 몇 가지 고려 사항입니다. • 슬롯 수는 드라이브 수보다 많거나 동일해야 합니다. • 개별 라이브러리당 최대 슬롯 개수는 32,000개입니다. • 시스템당 최대 슬롯 개수는 64,000개입니다. • 테이프가 DD VTL에 유지되고 볼트(Vault)로 내보내지지 않도록 충분한 수의 슬롯을 확보하십시오. 그렇게 해야 DD VTL을 재구성할 필요가 없고 관리 부담이 줄어듭니다. • 슬롯 수별로 라이선스가 부여되는 애플리케이션을 고려하십시오. 예를 들어 DD580의 표준 100GB 카트리지의 경우 슬롯 5000개를 구성할 수 있습니다. 이 수는 최대 500TB를 수용하는 데 충분합니다(적절하게 압축 가능한 데이터를 가정).
Number of CAPs	(선택 사항) CAP(Cartridge Access Port)의 개수를 입력합니다. • 라이브러리당 최대 CAP는 100개입니다. • 시스템당 최대 CAP는 1,000개입니다. 지침은 온라인 지원 사이트에서 특정 백업 소프트웨어 애플리케이션 설명서를 확인하십시오.
Changer Model Name	드롭다운 목록에서 원하는 모델을 선택합니다. • L180(기본값) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL 지침은 온라인 지원 사이트에서 특정 백업 소프트웨어 애플리케이션 설명서를 확인하십시오. 지원되는 소프트웨어에 대한 에뮬

표 144 Create Library 대화 상자 (계속)

필드	사용자 입력
	레이트된 라이브러리 호환성을 확인하려면 또한 DD VTL 지원 매트릭스를 참조하십시오.
옵션	
auto-eject	기본값(disabled), enable, disable
auto-offline	기본값(disabled), enable, disable
barcode-length	기본값(8), 6, 8[L180, RESTORER-L180 및 DDVTL 체인저 모델의 경우 자동으로 6으로 설정됨]

4. **OK**를 선택합니다.

   Create Library Status 대화 상자에 **Completed**라고 표시되면 **OK**를 선택합니다.

   새 라이브러리가 VTL Service 트리의 Libraries 아이콘 아래에 나타나고, 구성한 옵션이 라이브러리 아래에 아이콘으로 표시됩니다. 라이브러리를 선택하면 정보 패널에 라이브러리의 세부 정보가 표시됩니다.

   VTL 및 드라이브에 대한 액세스는 액세스 그룹을 통해 관리됩니다.

CLI 절차

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL'
to view it.

# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

라이브러리 삭제

테이프가 라이브러리 내의 드라이브에 있고 해당 라이브러리가 삭제된 경우 테이프가 볼트(Vault)로 옮겨집니다. 그러나 테이프의 풀은 변경되지 않습니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries**를 선택합니다.
2. **More Tasks** > **Library** > **Delete**를 선택합니다.
3. Delete Libraries 대화 상자에서 삭제할 항목의 확인란을 선택하거나 확인합니다.
   - 각 라이브러리의 이름 또는
   - 모든 라이브러리를 삭제할 경우 라이브러리 이름
4. **Next**를 선택합니다.
5. 삭제할 라이브러리를 확인하고 confirmation 대화 상자에서 **Submit**을 선택합니다.
6. Delete Libraries Status 대화 상자에 `Completed`라고 표시되면 **Close**를 선택합니다. 선택한 라이브러리가 DD VTL에서 삭제됩니다.

CLI 절차

```
# vtl del OldVTL
```

테이프 검색

위치, 풀 및/또는 바코드 등 다양한 조건을 사용해 테이프를 검색할 수 있습니다.

절차

1. **Virtual Tape Libraries** 또는 **Pools**를 선택합니다.
2. 라이브러리, 볼트(Valult), 풀 등 검색할 영역을 선택합니다.
3. **More Tasks** > **Tapes** > **Search**를 선택합니다.
4. Search Tapes 대화 상자에 찾으려는 테이프에 대한 정보를 입력합니다.

표 145 Search Tapes 대화 상자

필드	사용자 입력
Location	위치를 지정하거나 기본값(All)을 사용합니다.
Pool	테이프를 검색할 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 되돌립니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.

5. **Search**를 선택합니다.

선택한 라이브러리 작업

Virtual Tape Libraries > **VTL Service** > **Libraries** > *library*를 선택하면 선택한 라이브러리에 대한 자세한 정보가 표시됩니다.

표 146 디바이스

항목	설명
Device	드라이브, 슬롯 및 CAP(Cartridge Access Port)와 같은 라이브러리의 요소입니다.
Loaded	미디어가 로드된 디바이스의 수입니다.
Empty	미디어가 로드되지 않은 디바이스의 수입니다.
Total	로드된 디바이스와 빈 디바이스의 총 수입니다.

표 147 옵션

속성	값
auto-eject	enabled 또는 disabled
auto-offline	enabled 또는 disabled
barcode-length	6 또는 8

표 148 테이프

항목	설명
Pool	테이프가 있는 풀의 이름입니다.
Tape Count	해당 풀의 테이프 수입니다.
Capacity	해당 풀에 있는 테이프의 구성된 총 데이터 용량으로, GiB(기비바이트, 기가바이트(GB)의 2진 표기법) 단위로 표시됩니다.
Used	해당 풀의 가상 테이프에서 사용된 공간의 양입니다.
Average Compression	해당 풀에 있는 테이프의 데이터에 적용된 평균 압축 양입니다.

More Tasks 메뉴에서 라이브러리 옵션 삭제, 이름 변경 또는 설정을 수행하거나 테이프 생성, 삭제, 가져오기, 내보내기를 수행하거나 슬롯 및 CAP을 추가 또는 삭제할 수 있습니다.

테이프 생성

테이프는 라이브러리 또는 풀에서 생성할 수 있습니다. 풀에서 시작한 경우 먼저 시스템이 테이프를 생성한 후 라이브러리로 가져옵니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* 또는 **Vault** 또는 **Pools** > **Pools >** *pool*을 선택합니다.
2. **More Tasks** > **Tapes** > **Create**를 선택합니다.
3. Create Tapes 대화 상자에 테이프에 대한 다음 정보를 입력합니다.

   표 149 Create Tapes 대화 상자

필드	사용자 입력
Library(라이브러리에서 시작한 경우)	드롭다운 메뉴를 사용할 수 있는 경우 라이브러리를 선택하고 기본 선택 항목을 비워 둡니다.
풀 이름	드롭다운 목록에서 테이프가 상주하게 될 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
테이프 수	라이브러리의 경우 1~20개를 선택합니다. 풀의 경우 1~100,000개를 선택하거나 기본값(20)을 사용합니다. 지원되는 테이프 개수는 제한되지 않지만 한 번에 100,000개가 넘는 테이프를 생성할 수 없습니다.
Starting Barcode	초기 바코드 번호를 입력합니다(형식 A99000LA 사용).
Tape Capacity	(선택 사항) 각 테이프에 대한 GiB를 1 - 4000 사이로 지정합니다. 이 설정은 바코드 용량 설정을 재정의합니다. 디스크 공간을 보다 효율적으로 사용하려면 100GiB 이하를 사용합니다.

4. **OK**를 선택하고 **Close**를 선택합니다.

CLI 절차

```
 # vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool ...
added 5 tape(s)...
```

참고

테이프 볼륨 이름은 10진수 형식으로 자동 증가되어야 합니다.

테이프 삭제

라이브러리 또는 풀에서 테이프를 삭제할 수 있습니다. 라이브러리에서 시작한 경우 먼저 시스템이 테이프를 내보낸 후 삭제합니다. 테이프는 라이브러리가 아닌 볼트(Vault)에 있어야 합니다. 복제 대상 DD 시스템에서는 테이프 삭제가 허용되지 않습니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* 또는 **Vault** 또는 **Pools** > **Pools >** *pool*을 선택합니다.
2. **More Tasks** > **Tapes** > **Delete**를 선택합니다.
3. Delete Tapes 대화 상자에서 삭제할 테이프에 대한 검색 정보를 입력하고 **Search**를 선택합니다.

표 150 Delete Tapes 대화 상자

필드	사용자 입력
Location	드롭다운 목록이 있는 경우 라이브러리를 선택하거나 기본 **Vault** 선택을 사용합니다.
Pool	테이프를 검색할 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 검색합니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.
Select all pages	검색 쿼리에 의해 반환된 모든 테이프를 선택하려면 **Select All Pages** 확인란을 선택합니다.
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

4. 삭제해야 하는 테이프의 확인란 또는 머리글 열의 확인란을 선택해 모든 테이프를 삭제하고 **Next**를 선택합니다.
5. 확인 창에서 **Submit**을 선택하고 **Close**를 선택합니다.

참고

테이프가 제거된 후에 테이프에 사용된 물리 디스크 공간은 파일 시스템 정리 작업 이후까지 재확보되지 않습니다.

CLI 절차

```
# vtl tape del barcode [count count] [pool pool]
```

예:

```
# vtl tape del A00000L1
```

참고

범위를 사용할 수 있지만 범위에 누락된 테이프가 있는 경우 작업이 중지됩니다.

테이프 가져오기

*테이프 가져오기*는 기존 테이프가 볼트(Vault)에서 라이브러리 슬롯, 드라이브 또는 CAP(Cartridge Access Port)로 이동함을 의미합니다.

한 번에 가져올 수 있는 테이프 수는 라이브러리의 빈 슬롯 수로 제한됩니다. 즉, 현재 비어 있는 슬롯 수보다 많은 테이프를 가져올 수 없습니다.

라이브러리의 사용 가능한 슬롯을 보려면 스택 메뉴에서 라이브러리를 선택합니다. 라이브러리에 대한 정보 패널의 Empty 열에 사용 가능한 슬롯 수가 표시됩니다.

- 테이프가 드라이브에 있고 테이프 출처가 슬롯으로 알려진 경우 슬롯이 예약됩니다.
- 테이프가 드라이브에 있고 테이프 출처가 알려지지 않은 경우(슬롯 또는 CAP) 슬롯이 예약됩니다.
- 테이프가 드라이브에 있고 테이프 출처가 CAP로 알려진 경우 슬롯이 예약되지 않습니다. 테이프가 드라이브에서 제거되면 CAP로 돌아갑니다.
- 테이프를 드라이브로 이동하려면 뒤에 나오는 테이프 이동에 대한 섹션을 참조하십시오.

절차

1. 단계 a 또는 b를 사용해 테이프를 가져올 수 있습니다.
   a. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다. 그런 다음 **More Tasks** > **Tapes** > **Import**를 선택합니다. Import Tapes 대화 상자에서 가져올 테이프에 대한 검색 정보를 입력하고 **Search**를 선택합니다.

표 151 Import Tapes 대화 상자

필드	사용자 입력
Location	드롭다운 목록이 있는 경우 목록에서 테이프 위치를 선택하거나 기본값인 **Vault**를 사용합니다.
Pool	테이프를 검색할 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 되돌립니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Destination > Device를 선택합니다.	테이프를 가져올 대상 장치를 선택합니다. 가능한 값은 드라이브, CAP 및 슬롯입니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.

표 151 Import Tapes 대화 상자 (계속)

필드	사용자 입력
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

이전 조건에 따라, 가져올 테이프를 선택할 수 있는 기본 테이프 세트가 검색됩니다. 풀, 바코드 또는 개수가 변경되는 경우에는 Search를 선택하여 선택할 수 있는 테이프 세트를 업데이트합니다.

b. **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library* > **Changer** > **Drives** > *drive* > **Tapes**를 선택합니다. 다음 항목 옆의 확인란을 선택하여 가져올 테이프를 선택합니다.

- 개별 테이프 또는
- 현재 페이지의 모든 테이프를 선택하려면 **Barcode** 열 또는
- 검색 쿼리에 의해 반환된 모든 테이프를 선택하려면 **Select all pages** 확인란

Location에 Vault라고 표시되는 테이프만 가져올 수 있습니다.

Import from Vault를 선택합니다. 이 버튼은 기본적으로 해제되어 있으며 선택한 테이프가 모두 Vault에서 제공된 경우에만 설정됩니다.

2. Import Tapes의 라이브러리 보기에서 요약 정보 및 테이프 목록을 확인하고 **OK**를 선택합니다.
3. 상태 창에서 **Close**를 선택합니다.

CLI 절차

```
# vtl tape show pool VTL_Pool
Processing tapes....
Barcode  Pool     Location State    Size    Used (%)            Comp ModTime
-------- -------- -------- ----- ------- --------------- ---- -------------------
A00000L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
-------- -------- -------- ----- ------- --------------- ---- -------------------
VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x
```

테이프 내보내기

*테이프 내보내기*는 슬롯, 드라이브 또는 CAP(Cartridge Access Port)에서 테이프를 제거하여 볼트(Vault)로 보냅니다.

절차

1. 단계 a 또는 b를 사용해 테이프를 내보낼 수 있습니다.

   a. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다. 그런 다음 **More Tasks** > **Tapes** > **Export**를 선택합니다. Export Tapes 대화 상자에서 내보낼 테이프에 대한 검색 정보를 입력하고 **Search**를 선택합니다.

   표 152 Export Tapes 대화 상자

필드	사용자 입력
Location	드롭다운 목록에서 테이프가 있는 라이브러리의 이름을 선택하거나 선택된 라이브러리를 사용합니다.
Pool	테이프를 검색할 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 되돌립니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.
Select all pages	검색 쿼리에 의해 반환된 모든 테이프를 선택하려면 **Select All Pages** 확인란을 선택합니다.
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

   b. **Virtual Tape Libraries** > **VTL Service** > **Libraries***> library***> Changer** > **Drives >** *drive* **> Tapes**를 선택합니다. 다음 항목 옆의 확인란을 선택하여 내보낼 테이프를 선택합니다.

   - 개별 테이프 또는
   - 현재 페이지의 모든 테이프를 선택하려면 **Barcode** 열 또는
   - 검색 쿼리에 의해 반환된 모든 테이프를 선택하려면 **Select all pages** 확인란

   Location 열에서 라이브러리 이름이 있는 테이프만 내보낼 수 있습니다.

   Export from Library를 선택합니다. 이 버튼은 기본적으로 해제되어 있으며 선택한 테이프가 모두 Location 열에 라이브러리 이름이 있는 경우에만 설정됩니다.

2. Export Tapes의 라이브러리 보기에서 요약 정보 및 테이프 목록을 확인하고 **OK**를 선택합니다.
3. 상태 창에서 **Close**를 선택합니다.

CLI 절차

```
# vtl export NewVTL cap address 1 count 4
... exported 4 tape(s)...
```

라이브러리 내에서 디바이스 간 테이프 이동

라이브러리 내의 물리적 디바이스 간에 테이프를 이동하여 물리적 테이프 라이브러리에 대한 백업 소프트웨어 절차(라이브러리의 테이프를 슬롯에서 드라이브로, 슬롯에서 CAP로, CAP에서 드라이브로 이동하고 그 반대로도 이동)와 유사한 효과를 얻을 수 있습니다. 물리적 테이프 라이브러리에서 백업 소프트웨어는 라이브러리 외부로 테이프를 이동하지 않습니다. 따라서 대상 라이브러리가 변경될 수 없으며 설명을 위해서만 표시됩니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***library***를 선택합니다.

   라이브러리에서 시작될 때 Tapes 패널에서 디바이스 간에만 테이프를 이동할 수 있습니다.

2. **More Tasks** > **Tapes** > **Move**를 선택합니다.

   라이브러리에서 시작될 때 Tapes 패널에서 디바이스 간에만 테이프를 이동할 수 있습니다.

3. Move Tape 대화 상자에서 이동할 테이프에 대한 검색 정보를 입력하고 **Search**를 선택합니다.

   표 153 Move Tape 대화 상자

필드	사용자 입력
Location	위치는 변경할 수 없습니다.
Pool	풀을 선택합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 되돌립니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

4. 검색 결과 목록에서 이동할 테이프를 선택합니다.
5. 다음 중 하나를 수행합니다.
   a. Device 목록에서 디바이스(예: 슬롯, 드라이브 또는 CAP)를 선택하고 두 번째 및 이후 테이프의 순차적 번호를 사용하여 시작 주소를 입력합니다. 이동할 각 테이프에 대해 지정된 주소가 사용되는 경우 사용 가능한 다음 주소가 사용됩니다.
   b. 드라이브의 테이프가 원래 슬롯에서 제공되었고 해당 슬롯으로 돌아가려는 경우나 테이프가 사용 가능한 다음 슬롯으로 이동하려는 경우 주소를 비워 둡니다.

6. **Next**를 선택합니다.
7. Move Tape 대화 상자에서 요약 정보와 테이프 목록을 확인하고 **Submit**를 선택합니다.
8. 상태 창에서 **Close**를 선택합니다.

슬롯 추가

구성된 라이브러리의 슬롯을 추가하여 스토리지 요소의 수를 변경할 수 있습니다.

참고

일부 백업 애플리케이션은 슬롯이 DD VTL에 추가된 것을 자동으로 인식하지 않습니다. 이러한 유형의 변경을 인식하도록 애플리케이션을 구성하는 방법에 대한 자세한 내용은 애플리케이션 설명서를 참조하십시오.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다.
2. **More Tasks** > **Slots** > **Add**를 선택합니다.
3. Add Slots 대화 상자의 Number of Slots에 추가할 슬롯 수를 입력합니다. 라이브러리의 총 슬롯 수는 32,000개를 초과할 수 없고, 시스템에 있는 모든 라이브러리의 총 슬롯 수는 64,000개를 초과할 수 없습니다.
4. 상태가 `Completed`로 표시되면 **OK**와 **Close**를 선택합니다.

슬롯 삭제

구성된 라이브러리에서 슬롯을 삭제하여 스토리지 요소의 수를 변경할 수 있습니다.

참고

일부 백업 애플리케이션은 슬롯이 DD VTL에서 삭제된 것을 자동으로 인식하지 않습니다. 이러한 유형의 변경을 인식하도록 애플리케이션을 구성하는 방법에 대한 자세한 내용은 애플리케이션 설명서를 참조하십시오.

절차

1. 삭제할 슬롯에 카트리지가 포함된 경우 해당 카트리지를 볼트(Vault)로 이동합니다. 커밋되지 않은 빈 슬롯만 삭제됩니다.
2. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다.
3. **More Tasks** > **Slots** > **Delete**를 선택합니다.
4. Delete Slots 대화 상자의 Number of Slots에 삭제할 슬롯 수를 입력합니다.
5. 상태가 `Completed`로 표시되면 **OK**와 **Close**를 선택합니다.

CAP 추가

구성된 라이브러리에서 CAP(Cartridge Access Port)를 추가하여 스토리지 요소의 수를 변경할 수 있습니다.

참고

CAP는 제한된 수의 백업 애플리케이션에서 사용됩니다. CAP가 지원되는지 확인하려면 애플리케이션 설명서를 참조하십시오.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다.
2. **More Tasks** > **CAPs** > **Add**를 선택합니다.
3. Add CAPs 대화 상자의 Number of CAPs에 추가할 CAP 수를 입력합니다. CAP는 라이브러리당 1개~100개, 시스템당 1개~1,000개를 추가할 수 있습니다.
4. 상태가 `Completed`로 표시되면 **OK**와 **Close**를 선택합니다.

CAP 삭제

구성된 라이브러리에서 CAP(Cartridge Access Port)를 삭제해 스토리지 요소의 개수를 변경할 수 있습니다.

참고

일부 백업 애플리케이션은 CAP가 DD VTL에서 삭제되었음을 자동으로 인식하지 못합니다. 이러한 유형의 변경을 인식하도록 애플리케이션을 구성하는 방법에 대한 자세한 내용은 애플리케이션 설명서를 참조하십시오.

절차

1. 삭제하려는 CAP에 카트리지가 포함되어 있으면 해당 카트리지를 볼트(Vault)로 이동합니다. 그렇지 않으면 자동으로 이동됩니다.
2. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*를 선택합니다.
3. **More Tasks** > **CAPs** > **Delete**를 선택합니다.
4. Delete CAPs 대화 상자에 삭제할 CAP 개수를 입력합니다. CAP는 라이브러리당 최대 100개 또는 시스템당 최대 1,000개를 삭제할 수 있습니다.
5. 상태가 `Completed`로 표시되면 **OK**와 **Close**를 선택합니다.

체인저 정보 보기

체인저는 DD VTL당 하나만 존재할 수 있습니다. 선택하는 체인저 모델은 특정 구성에 따라 다릅니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries**를 선택합니다.
2. 특정 라이브러리를 선택합니다.
3. 확장되지 않을 경우 왼쪽에 있는 더하기 기호(+)를 선택해 라이브러리를 열고 체인저 요소를 선택하면 다음과 같은 정보를 제공하는 Changer information 패널이 표시됩니다.

표 154 Changer information 패널

항목	설명
Vendor	체인저를 제조한 공급업체의 이름
Product	모델 이름
Revision	개정 버전 수준
Serial Number	체인저 일련 번호

드라이브 작업

Virtual Tape Libraries > **VTL Service** > **Libraries** > *library* >**Drives**를 선택하면 선택한 라이브러리의 모든 드라이브에 대한 자세한 정보가 표시됩니다.

표 155 Drives information 패널

열	설명
드라이브	이름별 드라이브의 목록입니다. 이름은 "Drive #"이고 #은 1과 드라이브 목록의 드라이브 위치 또는 주소를 나타내는 n 사이의 번호입니다.
공급업체	드라이브의 제조업체 또는 공급업체입니다(예: IBM).
제품	드라이브의 제품 이름입니다(예: ULTRIUM-TD5).
개정 버전	드라이브 제품의 개정 버전 번호입니다.
일련 번호	드라이브 제품의 일련 번호입니다.
상태	드라이브가 Empty, Open, Locked 또는 Loaded 중 어떤 상태인지 보여 줍니다. 드라이브가 Locked 또는 Loaded 상태가 되려면 테이프가 있어야 합니다.
테이프	드라이브에 있는 테이프(있는 경우)의 바코드입니다.
풀	드라이브에 있는 테이프(있는 경우)의 풀입니다.

Tape and library drivers – 드라이브로 작업하려면 IBM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (default), HP-LTO-3 또는 HP-LTO-4 드라이브 및 StorageTek L180(기본값), RESTORER-L180, IBM TS3500, I2000, I6000 또는 DDVTL 라이브러리를 지원하는 백업 소프트웨어 공급업체가 제공한 테이프와 라이브러리 드라이버를 사용해야 합니다. 자세한 내용은 공급업체의 *애플리케이션 호환성 매트릭스 및 통합 가이드*를 참조하십시오. 드라이브를 구성할 때 사용 중인 플랫폼에 의해 결정되는 백업 데이터 스트림의 제한 사항에 대해서도 유의하십시오.

LTO drive capacities – DD 시스템에서 LTO 드라이브를 가상 드라이브로 취급하기 때문에 각 드라이브 유형에 대한 최대 용량을 4TiB(4,000GiB)로 설정할 수 있습니다. 각 LTO 드라이브 유형의 기본 용량은 다음과 같습니다.

- LTO-1 드라이브: 100GiB
- LTO-2 드라이브: 200GiB
- LTO-3 드라이브: 400GiB
- LTO-4 드라이브: 800GiB
- LTO-5 드라이브: 1.5TiB

Migrating LTO-1 tapes – 기존 LTO-1 유형 VTL에서 지원되는 다른 LTO 유형 테이프 및 드라이브를 포함하는 VTL로 테이프를 마이그레이션할 수 있습니다. 마이그레이션 옵션은 각 백업 애플리케이션마다 다르므로 사용 중인 애플리케이션에 맞는 LTO 테이프 마이그레이션 가이드의 지침을 따르십시오. 적절한 가이드를 찾으려면 온라인 지원 사이트로 이동해 검색 입력란에 **LTO Tape Migration for VTL**을 입력하십시오.

Tape full: Early warning – 남은 테이프 공간이 99.9%보다 크지만 100%보다 작을 정도로 거의 가득 차 있으면 경고가 표시됩니다. 애플리케이션은 테이프 끝이 100% 용량에 도달할 때까지 계속해서 기록합니다. 하지만 마지막으로 기록한 내용은 복구할 수 없습니다.

More Tasks 메뉴에서 드라이브를 생성하거나 삭제할 수 있습니다.

드라이브 생성

특정 DD VTL에서 지원되는 최대 드라이브 수를 확인하려면 *DD VTL에서 지원되는 드라이브 수* 섹션을 참조하십시오.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library***>** **Changer** > **Drives**를 선택합니다.
2. **More Tasks** > **Drives** > **Create**를 선택합니다.
3. Create Drive 대화 상자에서 다음 정보를 입력합니다.

   표 156 Create Drive 대화 상자

필드	사용자 입력
Location	라이브러리 이름을 선택하거나 선택된 이름을 그대로 둡니다.
Number of Drives	이 장의 앞부분에 있는 *DD VTL에서 지원되는 드라이브 수* 섹션의 표를 참조합니다.
Model Name	드롭다운 목록에서 모델을 선택합니다. 다른 드라이브가 이미 있는 경우 이 옵션은 비활성화되며 기존 드라이브 유형을 사용해야 합니다. 동일한 라이브러리에서 드라이브 유형을 혼합할 수 없습니다. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5(기본값) • HP-LTO-3 • HP-LTO-4

4. **OK**를 선택하고 상태가 `Completed`로 표시되면 **OK**를 선택합니다.

   추가된 드라이브가 Drives 목록에 나타납니다.

드라이브 삭제

드라이브를 삭제하려면 먼저 비워 두어야 합니다.

절차

1. 삭제하려는 드라이브에 테이프가 있으면 테이프를 제거합니다.
2. **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library***>** **Changer** > **Drives**를 선택합니다.
3. **More Tasks** > **Drives** > **Delete**를 선택합니다.
4. Delete Drives 대화 상자에서 삭제할 드라이브의 확인란을 선택하거나 **Drive** 확인란을 선택해 모든 드라이브를 삭제합니다.
5. **Next**를 선택하고 삭제할 드라이브를 올바로 선택했는지 확인한 후 **Submit**을 선택합니다.
6. Delete Drive Status 대화 상자에 `Completed`가 표시되면 **Close**를 선택합니다.

Drives 목록에서 드라이브가 제거됩니다.

선택한 드라이브 작업

Virtual Tape Libraries > **VTL Service** > **Libraries** > *library*> **Drives** >*drive*를 선택하면 선택한 드라이브에 대한 자세한 정보가 표시됩니다.

표 157 Drive 탭

열	설명
Drive	이름별 드라이브의 목록입니다. 이름은 “Drive #”이고 #은 1과 드라이브 목록의 드라이브 위치 또는 주소를 나타내는 n 사이의 번호입니다.
Vendor	드라이브의 제조업체 또는 공급업체입니다(예: IBM).
Product	드라이브의 제품 이름입니다(예: ULTRIUM-TD5).
Revision	드라이브 제품의 개정 버전 번호입니다.
Serial Number	드라이브 제품의 일련 번호입니다.
Status	드라이브가 Empty, Open, Locked 또는 Loaded 중 어떤 상태인지 보여 줍니다. 드라이브가 Locked 또는 Loaded 상태가 되려면 테이프가 있어야 합니다.
Tape	드라이브에 있는 테이프(있는 경우)의 바코드입니다.
Pool	드라이브에 있는 테이프(있는 경우)의 풀입니다.

표 158 Statistics 탭

열	설명
Endpoint	엔드포인트의 특정 이름입니다.
Ops/s	초당 작업 수입니다.
Read KiB/s	초당 읽기 속도(KiB)입니다.
Write KiB/s	초당 쓰기 속도(KiB)입니다.

More Tasks 메뉴에서 드라이브를 삭제하거나 새로 고침을 수행할 수 있습니다.

테이프 작업

테이프는 파일로 표시됩니다. 볼트(Vault)에서 라이브러리로 테이프를 가져올 수 있습니다. 라이브러리에서 볼트(Vault)로 테이프를 내보낼 수 있습니다. 드라이브, 슬롯(카트리지 슬롯) 및 CAP(Cartridge Access Port)의 라이브러리 내에서 테이프를 이동할 수 있습니다.

테이프가 생성되면 볼트(Vault)에 배치됩니다. 볼트(Vault)에 추가된 테이프는 가져오거나 내보내거나 이동하거나 검색 또는 제거할 수 있습니다.

Virtual Tape Libraries > **VTL Service** > **Libraries** > *library* >**Tapes**를 선택하면 선택한 라이브러리의 모든 테이프에 대한 자세한 정보가 표시됩니다.

표 159 테이프 설명

항목	설명
Barcode	테이프의 고유한 바코드입니다.
Pool	테이프를 보유하고 있는 풀의 이름입니다. 기본 풀은 사용자가 생성한 풀에 할당이 취소된 모든 테이프를 보유하고 있습니다.
Location	테이프의 위치이며 라이브러리(드라이브, CAP 또는 슬롯 번호) 또는 가상 볼트(Vault)에 있습니다.
State	테이프의 상태입니다. • RW – 읽기-쓰기 가능 • RL – Retention Lock 설정 • RO – 읽기만 가능 • WP – 쓰기 금지 • RD – 복제 대상
Capacity	테이프의 총 용량입니다.
Used	테이프에서 사용된 공간의 용량입니다.
Compression	테이프의 데이터에서 수행된 압축의 용량입니다.
Last Modified	테이프의 정보를 마지막으로 변경한 날짜입니다. 기간 기반의 정책에 대한 시스템에서 사용된 수정 시간은 DD System Manager의 테이프 정보 섹션에 표시된 마지막으로 수정한 날짜와 다를 수 있습니다.
Locked Until	DD Retention Lock 기한을 설정한 경우 설정된 시간이 표시됩니다. Retention Lock이 없으면 이 값은 `Not specified`입니다.

정보 패널에서는 볼트(Vault)에서 테이프를 가져오거나, 라이브러리에 테이프를 내보내거나, 테이프의 상태를 설정하거나, 테이프를 생성 또는 삭제할 수 있습니다.

More Tasks 메뉴에서 테이프를 이동할 수 있습니다.

테이프의 쓰기 또는 Retention Lock 상태 변경

테이프의 쓰기 또는 Retention Lock 상태를 변경하기 전에 테이프를 생성하고 가져와야 합니다. DD VTL 테이프는 표준 Data Domain Retention Lock 정책을 따릅니다. 테이프의 보존 기간이 만료된 후에는 테이프에 쓰거나 테이프를 변경할 수 없습니다. 하지만 삭제할 수는 있습니다.

절차

1. **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***library*** > **Tapes**를 선택합니다.
2. 목록에서 수정할 테이프를 선택하고 **Set State**(목록 위)를 선택합니다.
3. Set Tape State 대화 상자에서 **Read-Writeable**, **Write-Protected** 또는 **Retention-Lock**을 선택합니다.
4. 상태가 Retention-Lock이면 다음 중 하나를 수행합니다.
   - 지정된 일, 주, 월, 년 단위로 테이프의 만료 날짜를 입력합니다.
   - 달력 아이콘을 선택하고 달력에서 날짜를 선택합니다. Retention-Lock이 선택한 날짜 정오에 만료됩니다.

5. **Next**를 선택하고 **Submit**을 선택해 상태를 변경합니다.

볼트(Vault) 작업

볼트(Vault)에는 라이브러리에서 사용되지 않는 테이프가 들어 있습니다. 테이프는 라이브러리 또는 볼트(Vault)에 상주합니다.

Virtual Tape Libraries > **VTL Service** > **Vault**를 선택하면 볼트(Vault)에 있는 기본 풀과 다른 모든 기존 풀에 대한 자세한 정보가 표시됩니다.

DD Cloud Tier 및 DD VTL을 사용하는 시스템에는 클라우드 스토리지에 볼팅을 저장하는 옵션이 있습니다.

표 160 풀 요약

항목	설명
Pool Count	VTL 풀의 수입니다.
Tape Count	풀의 테이프 수입니다.
크기	풀에 있는 공간의 총 용량입니다.
Logical Used	풀에서 사용된 공간의 용량입니다.
압축	풀의 평균 압축 양입니다.

Protection Distribution 창에는 다음과 같은 정보가 표시됩니다.

참고

이 표는 Data Domain 시스템에서 DD Cloud Tier가 활성화된 경우에만 나타납니다.

표 161 Protection Distribution

항목	설명
Storage type	Vault 또는 Cloud입니다.
클라우드 공급업체	DD Cloud Tier에 테이프가 있는 시스템의 경우 각 클라우드 공급업체에 대한 열이 있습니다.
Logical Used	풀에서 사용된 공간의 용량입니다.
Pool Count	VTL 풀의 수입니다.
Tape Count	풀의 테이프 수입니다.

More Tasks 메뉴에서 볼트(Vault)의 테이프를 생성, 삭제 및 검색할 수 있습니다.

클라우드 기반 볼팅 작업

DD VTL은 DD Cloud Tier 스토리지에 볼팅(vaulting)이 저장되는 구성에 고유한 여러 매개 변수를 지원합니다.

클라우드 기반 볼팅 스토리지를 사용하는 경우 다음과 같은 작업을 수행할 수 있습니다.

- 지정된 VTL 풀에 대한 데이터 이동 정책 및 클라우드 유닛 정보 구성. **vtl pool modify *<pool-name>* data-movement-policy {user-managed | age-**

threshold *<days>* | none} to-tier {cloud} cloud-unit *<cloud-unit-name>* 명령을 실행합니다.
사용 가능한 데이터 이동 정책은 다음과 같습니다.

- User-managed: 관리자는 풀에 이 정책을 설정하여 Cloud Tier로 마이그레이션할 테이프를 풀에서 수동으로 선택할 수 있습니다. 테이프를 선택한 후 첫 번째 데이터 이동 작업에서 해당 테이프가 Cloud Tier로 마이그레이션됩니다.
- Age-threshold: 관리자는 풀에 이 정책을 설정하여 DD VTL이 테이프 사용 기간에 따라 Cloud Tier로 마이그레이션할 테이프를 풀에서 자동으로 선택하도록 할 수 있습니다. 테이프는 사용 기간 임계값을 충족한 후 6시간 이내에 마이그레이션하도록 선택되며 테이프 선택 후 첫 번째 데이터 이동 작업에서 마이그레이션됩니다.

- Cloud Tier로 마이그레이션할 특정 테이프 선택. **vtl tape select-for-move barcode *<barcode>* [count *<count>*] pool *<pool>* to-tier {cloud}** 명령을 실행합니다.
- Cloud Tier로 마이그레이션할 특정 테이프 선택 해제. **vtl tape deselect-for-move barcode *<barcode>* [count *<count>*] pool *<pool>* to-tier {cloud}** 명령을 실행합니다.
- Cloud Tier에서 테이프 리콜. **vtl tape recall start barcode *<barcode>* [count *<count>*] pool *<pool>*** 명령을 실행합니다.
  리콜 후 테이프는 로컬 DD VTL 볼팅에 상주하며 액세스를 위해 라이브러리로 가져와야 합니다.

참고

테이프의 현재 위치를 확인하려면 언제든지 `vtl tape show` 명령을 실행합니다. 테이프를 Cloud Tier 내/외부로 이동한 경우 1시간 이내에 테이프 위치가 업데이트됩니다.

데이터 이동을 위한 VTL 풀 준비

VTL 풀에 대한 데이터 이동 정책을 설정하여 로컬 볼트에서 DD Cloud Tier로의 VTL 데이터 마이그레이션을 관리합니다.

VTL의 데이터 이동은 테이프 볼륨 레벨에서 이루어집니다. 개별 테이프 볼륨 또는 테이프 볼륨 컬렉션을 Cloud Tier로 이동할 수 있지만 볼팅(vaulting) 위치에서만 가능합니다. 다른 VTL 요소의 테이프는 이동할 수 없습니다.

참고

기본 VTL 풀 및 볼팅, `/data/col1/backup` 디렉토리 또는 기존 라이브러리 구성은 테이프를 클라우드로 이동하는 데 사용할 수 없습니다.

절차

1. **Protocols** > **DD VTL**을 선택합니다.
2. 풀 목록을 확장하고 DD Cloud Tier로의 마이그레이션을 활성화할 풀을 선택합니다.
3. **Cloud Data Movement** 창의 **Cloud Data Movement Policy**에서 **Create**를 클릭합니다.
4. **Policy** 드롭다운 목록에서 데이터 이동 정책을 선택합니다.
   - **Age of tapes in days**
   - **Manual selection**

5. 데이터 이동 정책 세부 정보를 설정합니다.
   - **Age of tapes in days**에서 수명 임계값(이 기간이 지나면 테이프가 DD Cloud Tier로 마이그레이션됨)을 선택하고 대상 클라우드 유닛을 지정합니다.
   - **Manual selection**의 경우 대상 클라우드 유닛을 지정합니다.
6. **Create**를 클릭합니다.

참고

데이터 이동 정책을 생성한 후 **Edit** 및 **Clear** 버튼을 사용하여 데이터 이동 정책을 수정하거나 삭제할 수 있습니다.

CLI 절차

절차

1. 데이터 이동 정책을 user-managed 또는 age-threshold로 설정

참고

VTL 풀과 클라우드 유닛은 대/소문자를 구분하며 대/소문자가 정확하지 않을 경우 명령이 실패합니다.

- 데이터 이동 정책을 user-managed로 설정하려면 다음 명령을 실행합니다.
  ```
  vtl pool modify cloud-vtl-pool data-movement-policy
  user-managed to-tier cloud cloud-unit ecs-unit1
  ```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".
```

- 데이터 이동 정책을 age-threshold로 설정하려면 다음 명령을 실행합니다.

  참고

  최소값은 14일이고 최대값은 182,250일입니다.

  ```
  vtl pool modify cloud-vtl-pool data-movement-policy age-
  threshold 14 to-tier cloud cloud-unit ecs-unit1
  ```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-
vtl-pool".
```

2. VTL 풀에 대한 데이터 이동 정책을 확인합니다.

   다음 명령을 실행합니다.
   ```
   vtl pool show all
   ```

```
VTL Pools
Pool                    Status   Tapes   Size (GiB)   Used (GiB)   Comp   Cloud Unit
Cloud Policy
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
cloud-vtl-pool          RW          50          250           41    45x   ecs-unit1
user-managed
Default                 RW           0            0            0     0x   -
none
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
8080 tapes in 5 pools
```

```
RO  : Read Only
RD  : Replication Destination
BCM : Backwards-Compatibility
```

3. VTL 풀 MTree에 대한 정책이 `app-managed`인지 확인합니다.

   다음 명령을 실행합니다.
   `data-movement policy show all`

```
Mtree                       Target(Tier/Unit Name)   Policy        Value
--------------------------  -----------------------  ------------  -------
/data/col1/cloud-vtl-pool   Cloud/ecs-unit1           app-managed   enabled
--------------------------  -----------------------  ------------  -------
```

백업 애플리케이션 인벤토리에서 테이프 제거

백업 애플리케이션을 사용하여 클라우드로 이동할 테이프 볼륨이 백업 애플리케이션 요구 사항에 따라 표시되고 인벤토리가 작성되었는지 확인합니다.

데이터 이동을 위한 테이프 볼륨을 선택합니다.

DD Cloud Tier로의 마이그레이션(즉시 또는 다음에 예약된 데이터 마이그레이션)을 위한 테이프를 수동으로 선택하거나, 마이그레이션 스케줄에서 테이프를 수동으로 제거합니다.

시작하기 전에

백업 애플리케이션이 클라우드 스토리지로 이동하는 볼륨의 상태 변경을 인식하는지 확인합니다. 백업 애플리케이션에 필요한 단계를 완료하여 최신 볼륨 상태를 반영하도록 인벤토리를 새로 고칩니다.

테이프가 볼트에 없는 경우 DD Cloud Tier로 마이그레이션할 수 없습니다.

절차

1. **Protocols** > **DD VTL**을 선택합니다.
2. 풀 목록을 확장하고 DD Cloud Tier로 테이프를 마이그레이션하도록 구성된 풀을 선택합니다.
3. 풀 창에서 **Tape** 탭을 클릭합니다.
4. DD Cloud Tier로의 마이그레이션을 위한 테이프를 선택합니다.
5. **Select for Cloud Move**를 클릭하여 다음에 예약된 마이그레이션에 테이프를 마이그레이션하거나, **Move to Cloud Now**를 클릭하여 즉시 테이프를 마이그레이션합니다.

   참고

   데이터 이동 정책이 테이프 수명에 기반하는 경우 Data Domain 시스템에서 자동으로 마이그레이션할 테이프가 선택되기 때문에 **Select for Cloud Move**를 사용할 수 없습니다.

6. 확인 대화 상자에서 **Yes**를 클릭합니다.

데이터 이동을 위한 테이프 볼륨 선택 취소

DD Cloud Tier로 마이그레이션하도록 선택된 테이프를 마이그레이션 스케줄에서 제거할 수 있습니다.

절차

1. **Protocols** > **DD VTL**을 선택합니다.

2. 풀 목록을 확장하고 DD Cloud Tier로 테이프를 마이그레이션하도록 구성된 풀을 선택합니다.
3. 풀 창에서 **Tape** 탭을 클릭합니다.
4. DD Cloud Tier로의 마이그레이션을 위한 테이프를 선택합니다.
5. **Unselect Cloud Move**를 클릭하여 테이프를 마이그레이션 스케줄에서 제거합니다.
6. 확인 대화 상자에서 **Yes**를 클릭합니다.

CLI 절차

절차

1. 이동할 테이프 볼륨의 슬롯 위치를 파악합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape show cloud-vtl
   ```

```
Processing tapes....
Barcode    Pool             Location            State    Size           Used (%)
Comp   Modification Time
--------   --------------   -----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1    RW      5 GiB   5.0 GiB (99.07%)
205x   2017/05/05 10:43:43
T00002L3   cloud-vtl-pool   cloud-vtl slot 2    RW      5 GiB   5.0 GiB (99.07%)
36x   2017/05/05 10:45:10
T00003L3   cloud-vtl-pool   cloud-vtl slot 3    RW      5 GiB   5.0 GiB (99.07%)
73x   2017/05/05 10:45:26
```

2. DD VTL에서 테이프를 내보낼 슬롯의 숫자 값을 지정합니다.

   다음 명령을 실행합니다.
   ```
   vtl export cloud-vtl-pool slot 1 count 1
   ```

3. 테이프가 볼팅에 있는지 확인합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape show vault
   ```

4. 데이터 이동을 위한 테이프를 선택합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape select-for-move barcode T00001L3 count 1 pool
   cloud-vtl-pool to-tier cloud
   ```

   참고

   데이터 이동 정책이 **age-threshold**인 경우 **15~20**분 후에 데이터 이동이 자동으로 수행됩니다.

5. 다음 데이터 이동 작업 중 클라우드 스토리지로 이동하도록 예약된 테이프의 목록을 봅니다. 이동하도록 선택된 테이프의 위치 열에 `(S)`가 표시됩니다.

   다음 명령을 실행합니다.
   ```
   vtl tape show vault
   ```

```
Processing tapes.....
Barcode    Pool               Location    State      Size          Used (%)    Comp
Modification Time
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
T00003L3   cloud-vtl-pool     vault (S)   RW        5 GiB   5.0 GiB (99.07%)    63x
2017/05/05 10:43:43
T00006L3   cloud-vtl-pool     ecs-unit1   n/a       5 GiB   5.0 GiB (99.07%)    62x
```

데이터 이동을 위한 테이프 볼륨을 선택합니다.

```
2017/05/05 10:45:49
--------   -----------------   ---------   ------   ------   ----------------   ----
-------------------
* RD : Replication Destination
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4024
Total pools:               3
Total size of tapes:       40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression:       9.7x
```

6. 데이터 이동 정책이 **user-managed**인 경우 데이터 이동 작업을 시작합니다.

   다음 명령을 실행합니다.
   ```
   data-movement start
   ```

7. 데이터 이동 작업의 상태를 확인합니다.

   다음 명령을 실행합니다.
   ```
   data-movement watch
   ```

8. 테이프 볼륨이 클라우드 스토리지에 성공적으로 이동하는지 확인합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape show all cloud-unit ecs-unit1
   ```

```
Processing tapes.....
Barcode  Pool           Location  State  Size         Used (%) Comp Modification Time
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
T00001L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  62x 2017/05/05 10:45:49
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4
Total pools:               2
Total size of tapes:       16 GiB
Total space used by tapes: 14.9 GiB
Average Compression:       59.5x
```

클라우드에 저장된 데이터 복구

클라이언트가 복구를 위해 백업 애플리케이션 서버에서 데이터를 요청하는 경우 백업 애플리케이션은 클라우드 유닛에서 필요한 볼륨을 요청하는 알림 또는 메시지를 생성해야 합니다.

백업 애플리케이션에 볼륨 유무를 알리기 전에 볼륨을 클라우드에서 리콜하고 **Data Domain VTL** 라이브러리에 체크인해야 합니다.

참고

백업 애플리케이션이 클라우드 스토리지로 이동하는 볼륨의 상태 변경을 인식하는지 확인합니다. 백업 애플리케이션에 필요한 단계를 완료하여 최신 볼륨 상태를 반영하도록 인벤토리를 새로 고칩니다.

클라우드 스토리지에서 테이프 볼륨을 수동으로 리콜

DD Cloud Tier에서 로컬 VTL 볼트로 테이프를 리콜합니다.

절차

1. **Protocols** > **DD VTL**을 선택합니다.
2. 풀 목록을 확장하고 DD Cloud Tier로 테이프를 마이그레이션하도록 구성된 풀을 선택합니다.
3. 풀 창에서 **Tape** 탭을 클릭합니다.
4. 클라우드 유닛에 위치한 하나 이상의 테이프를 선택합니다.
5. **Recall Cloud Tapes**를 클릭하여 DD Cloud Tier에서 테이프를 리콜합니다.

결과

다음번 예약된 데이터 마이그레이션 후 클라우드 유닛에서 볼트로 테이프가 리콜됩니다. 볼트에서 라이브러리로 테이프를 반환할 수 있습니다.

CLI 절차

절차

1. 데이터를 복구하는 데 필요한 볼륨을 식별합니다.
2. 볼팅(vaulting)에서 테이프 볼륨을 리콜합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
   ```
3. 리콜 작업이 시작되었는지 확인합니다.

   다음 명령을 실행합니다.
   ```
   data-movement status
   ```
4. 리콜 작업이 성공적으로 완료되었는지 확인합니다.

   다음 명령을 실행합니다.
   ```
   vtl tape show all barcode T00001L3
   ```

```
Processing tapes....
Barcode    Pool             Location           State    Size           Used (%)
Comp   Modification Time
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1   RW      5 GiB   5.0 GiB (99.07%)
239x   2017/05/05 10:41:41
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     1
Total pools:               1
Total size of tapes:       5 GiB
Total space used by tapes: 5.0 GiB
Average Compression:       239.1x
```

5. 파일 위치를 확인합니다.

   다음 명령을 실행합니다.

```
filesys report generate file-location path /data/col1/
cloud-vtl-pool
```

```
filesys report generate file-location path /data/col1/cloud-vtl-pool
-------------------------------      --------------------------
File Name                            Location(Unit Name)
-------------------------------      --------------------------
/data/col1/cloud-vtl-pool/.vtl_pool     Active
/data/col1/cloud-vtl-pool/.vtc/T00001L3 Active
-----------------------------------------------------------------
```

6. DD VTL에 리콜된 테이프를 가져옵니다.

   다음 명령을 실행합니다.
   ```
   vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-
   vtl-pool element slot
   ```

```
imported 1 tape(s)...sysadmin@ddbeta70# vtl tape show cloud-vtlProcessing tapes.....
```

7. 백업 애플리케이션 인벤토리로 볼륨을 체크인합니다.
8. 백업 애플리케이션을 통해 데이터를 복구합니다.
9. 복구가 완료되면 백업 애플리케이션 인벤토리에서 테이프 볼륨을 확인합니다.
10. Data Domain VTL에서 Data Domain Vault로 테이프 볼륨을 내보냅니다.
11. 클라우드 유닛으로 테이프를 다시 이동합니다.

액세스 그룹 작업

*액세스 그룹*에는 이니시에이터 WWPN(Worldwide Port Name) 또는 별칭의 컬렉션과 이들이 액세스할 수 있는 드라이브 및 체인저가 저장됩니다. *TapeServer*라는 DD VTL 기본 그룹을 사용하여 NDMP(Network Data Management Protocol) 기반 백업 애플리케이션을 지원할 디바이스를 추가할 수 있습니다.

액세스 그룹 구성에서 일반 백업 애플리케이션의 이니시에이터가 동일한 액세스 그룹의 디바이스에서 데이터를 읽고 쓰도록 설정할 수 있습니다.

액세스 그룹을 사용하면 클라이언트가 시스템에서 선택된 LUN(미디어 체인저 또는 가상 테이프 드라이브)에만 액세스할 수 있습니다. 액세스 그룹에 대해 설정된 클라이언트는 해당 액세스 그룹의 디바이스에만 액세스할 수 있습니다.

백업 또는 복구 작업이 실행 중인 동안 DD 시스템의 액세스 그룹을 변경하지 마십시오. 실행 중인 작업이 실패할 수 있습니다. 작업 실행 중 액세스 그룹 변경으로 인한 영향은 백업 소프트웨어와 호스트 구성의 조합에 따라 달라집니다.

Access Groups > **Groups**를 선택하면 모든 액세스 그룹에 대한 다음 정보가 표시됩니다.

표 162 액세스 그룹 정보

항목	설명
Group Name	그룹의 이름입니다.
Initiators	그룹에 있는 이니시에이터의 수입니다.
Devices	그룹에 있는 디바이스의 수입니다.

View All Access Groups를 선택하는 경우 Fibre Channel 보기가 나타납니다.

More Tasks 메뉴에서 그룹을 생성하거나 삭제할 수 있습니다.

액세스 그룹 생성

액세스 그룹은 디바이스와 이니시에이터 사이의 액세스 권한을 관리합니다. NDMP를 사용하지 않는 경우 기본 TapeServer 액세스 그룹을 사용하지 마십시오.

절차

1. **Access Groups** > **Groups**를 선택합니다.
2. **More Tasks** > **Group** > **Create**를 선택합니다.
3. Create Access Group 대화 상자에서 1-128자 사이의 이름을 입력하고 **Next**를 선택합니다.
4. 디바이스를 추가하고 **Next**를 선택합니다.
5. 요약을 검토하고 필요에 따라 **Finish** 또는 **Back**을 선택합니다.

   CLI 절차

   ```
   # vtl group create My_Group
   ```

액세스 그룹 디바이스 추가

액세스 그룹 구성에서 일반 백업 애플리케이션의 이니시에이터가 동일한 액세스 그룹의 디바이스에서 데이터를 읽고 쓰도록 설정할 수 있습니다.

절차

1. **Access Groups** > **Groups**를 선택합니다. 특정 *group*을 선택할 수도 있습니다.
2. **More Tasks** > **Group** > **Create** 또는 **Group** > **Configure**를 선택합니다.
3. Create or Modify Access Group 대화 상자에서 **Group Name**을 입력하거나 필요한 경우 수정합니다. 이 필드는 필수 항목입니다.
4. 액세스 그룹에 대한 이니시에이터를 구성하려면 이니시에이터 옆의 확인란을 선택합니다. 나중에 이니시에이터를 그룹에 추가할 수 있습니다.
5. **Next**를 선택합니다.
6. Devices 화면에서 추가 버튼(**+**)을 선택하여 Add Devices 대화 상자를 표시합니다.
   a. 올바른 라이브러리가 Library Name 드롭다운 목록에서 선택되어 있는지 확인하거나 다른 라이브러리를 선택합니다.
   b. Device 영역에서 그룹에 포함할 디바이스(체인저 및 드라이브)의 확인란을 선택합니다.
   c. 필요에 따라 LUN Start Address 입력란에서 시작 LUN을 지정합니다.

      이는 DD 시스템에서 이니시에이터에 반환하는 LUN입니다. 각 디바이스는 라이브러리와 디바이스 이름으로 고유하게 식별됩니다. 예를 들어 Library 1에 drive 1이 있고 Library 2에 drive 1이 있을 수 있습니다. 따라서 LUN은 라이브러리와 디바이스 이름으로 식별되는 디바이스와 연결됩니다.

      FC HBA/SLIC에 연결된 FC 포트를 통해 LUN을 제공하는 경우 포트를 운영, 보조 또는 없음으로 지정할 수 있습니다. LUN 세트에 대한 운영 포트는 현재 이러한 LUN을 Fabric에 알리는 포트입니다. 보조 포트는 운영 경로에 장애가 발생할 경우 LUN 세트를 브로드캐스팅하는 포트로 수동 조작이 필요합니다. 없음 설정은 선택한 LUN을 알리지 않으려는 경우 사용됩니다. LUN 제공은 해당하는 SAN 토폴로지에 따라 다릅니다.

      액세스 그룹의 이니시에이터는 해당 그룹에 추가된 LUN 디바이스와 상호 작용합니다.

액세스 그룹을 생성할 때 허용되는 최대 LUN은 16,383개입니다.

LUN은 개별 그룹에 한 번만 사용할 수 있으며, 동일한 LUN을 여러 그룹에서 사용할 수 있습니다.

일부 이니시에이터(클라이언트)에는 타겟 LUN 번호 지정에 대한 특정 규칙이 있습니다. 예를 들어 LUN 0을 요구하거나 연속 LUN을 요구할 수 있습니다. 이러한 규칙을 따르지 않는 경우 이니시에이터가 DD VTL 타겟 포트에 할당된 LUN의 일부 또는 전체에 액세스하지 못할 수 있습니다.

이니시에이터 설명서에서 특별한 규칙을 확인하고 필요한 경우 규칙을 따르도록 DD VTL 타겟 포트에서 디바이스 LUN을 수정합니다. 예를 들어 이니시에이터가 LUN 0이 DD VTL 타겟 포트에 할당되도록 요구하는 경우, 포트에 할당된 디바이스의 LUN을 확인하고 LUN 0에 할당된 디바이스가 없으면 디바이스가 LUN 0에 할당되도록 디바이스의 LUN을 변경합니다.

d. Primary and Secondary Endpoints 영역에서 선택한 디바이스가 표시될 포트를 결정하는 옵션을 선택합니다. 지정된 포트에 대해 다음 조건이 적용됩니다.

- all – 선택한 디바이스가 모든 포트에서 표시됩니다.
- none – 선택한 디바이스가 어떠한 포트에서도 표시되지 않습니다.
- select – 선택한 디바이스가 선택된 포트에서 표시됩니다. 적절한 포트의 확인란을 선택합니다.
  운영 포트만 선택된 경우 선택한 디바이스가 운영 포트에서만 표시됩니다.

  보조 포트만 선택된 경우 선택한 디바이스가 보조 포트에서만 표시됩니다. 운영 포트를 사용할 수 없게 되면 보조 포트를 사용할 수 있습니다.

보조 포트로의 전환은 자동 작업이 아닙니다. 운영 포트를 사용할 수 없게 되는 경우 수동으로 DD VTL 디바이스를 보조 포트로 전환해야 합니다.

포트 목록은 물리적 포트 번호의 목록입니다. 포트 번호는 PCI 슬롯을 나타내고 문자는 PCI 카드의 포트를 나타냅니다. 1a, 1b 또는 2a, 2b 등을 예로 들 수 있습니다.

드라이브는 구성한 모든 포트에서 동일한 LUN과 함께 나타납니다.

e. **OK**를 선택합니다.

새 그룹이 표시되는 Devices 대화 상자로 돌아갑니다. 디바이스를 더 추가하려면 위의 5개 하위 단계를 반복합니다.

7. **Next**를 선택합니다.
8. `Completed` 상태 메시지가 표시되면 **Close**를 선택합니다.

CLI 절차

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all#
vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all#
vtl group add SetUp_Test vtl SetUp_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1

# vtl group show Setup_Test
Group: SetUp_Test

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
tsm6_p23          21:00:00:24:ff:31:ce:f8
---------------   ----------------------
```

```
Devices:
Device Name          LUN   Primary Ports   Secondary Ports    In-use Ports
-----------------    ---   -------------   ---------------   -------------
SetUp_Test changer     0             all               all             all
SetUp_Test drive 1     1             all               all             all
SetUp_Test drive 2     2              5a                5b              5a
SetUp_Test drive 3     3   endpoint-fc-0     endpoint-fc-1   endpoint-fc-0
-----------------    ---   -------------   ---------------   -------------
```

액세스 그룹 디바이스 수정 또는 삭제

액세스 그룹의 디바이스를 수정하거나 액세스 그룹에서 디바이스를 삭제해야 할 수 있습니다.

절차

1. **Protocols** > **VTL** > **Access Groups** > **Groups**> *group*을 선택합니다.
2. **More Tasks** > **Group** > **Configure**를 선택합니다.
3. Modify Access Group 대화 상자에서 **Group Name**을 입력하거나 수정합니다. 이 필드는 필수 항목입니다.
4. 액세스 그룹에 대한 이니시에이터를 구성하려면 이니시에이터 옆의 확인란을 선택합니다. 나중에 이니시에이터를 그룹에 추가할 수 있습니다.
5. **Next**를 선택합니다.
6. 디바이스를 선택하고 연필 모양의 편집 아이콘을 선택하여 Modify Devices 대화 상자를 표시합니다. 그런 다음 a~e단계를 수행합니다. 디바이스를 삭제하려면 X 모양의 삭제 아이콘을 선택하고 e단계로 건너뜁니다.
   a. 올바른 라이브러리가 Library 드롭다운 목록에서 선택되어 있는지 확인하거나 다른 라이브러리를 선택합니다.
   b. Devices to Modify 영역에서 수정할 디바이스(체인저 및 드라이브)의 확인란을 선택합니다.
   c. 필요에 따라 LUN Start Address 상자에서 시작 LUN(Logical Unit Number)을 수정합니다.

      이는 DD 시스템에서 이니시에이터에 반환하는 LUN입니다. 각 디바이스는 라이브러리와 디바이스 이름으로 고유하게 식별됩니다. 예를 들어 Library 1에 drive 1이 있고 Library 2에 drive 1이 있을 수 있습니다. 따라서 LUN은 라이브러리와 디바이스 이름으로 식별되는 디바이스와 연결됩니다.

      액세스 그룹의 이니시에이터는 해당 그룹에 추가된 LUN 디바이스와 상호 작용합니다.

      액세스 그룹을 생성할 때 허용되는 최대 LUN은 16,383개입니다.

      LUN은 개별 그룹에 한 번만 사용할 수 있으며, 동일한 LUN을 여러 그룹에서 사용할 수 있습니다.

      일부 이니시에이터(클라이언트)에는 타겟 LUN 번호 지정에 대한 특정 규칙이 있습니다. 예를 들어 LUN 0을 요구하거나 연속 LUN을 요구할 수 있습니다. 이러한 규칙을 따르지 않는 경우 이니시에이터가 DD VTL 타겟 포트에 할당된 LUN의 일부 또는 전체에 액세스하지 못할 수 있습니다.

      이니시에이터 설명서에서 특별한 규칙을 확인하고 필요한 경우 규칙을 따르도록 DD VTL 타겟 포트에서 디바이스 LUN을 수정합니다. 예를 들어 이니시에이터가 LUN 0이 DD VTL 타겟 포트에 할당되도록 요구하는 경우, 포트에 할당된 디바이스의 LUN을 확인하고 LUN 0에 할당된 디바이스가 없으면 디바이스가 LUN 0에 할당되도록 디바이스의 LUN을 변경합니다.

d. Primary and Secondary Ports 영역에서 선택한 디바이스가 표시되는 포트를 결정하는 옵션을 변경합니다. 지정된 포트에 대해 다음 조건이 적용됩니다.

- all – 선택한 디바이스가 모든 포트에서 표시됩니다.
- none – 선택한 디바이스가 어떠한 포트에서도 표시되지 않습니다.
- select – 선택한 디바이스가 선택된 포트에서 표시됩니다. 디바이스가 표시될 포트의 확인란을 선택합니다.
  운영 포트만 선택된 경우 선택한 디바이스가 운영 포트에서만 표시됩니다.

  보조 포트만 선택된 경우 선택한 디바이스가 보조 포트에서만 표시됩니다. 운영 포트를 사용할 수 없게 되면 보조 포트를 사용할 수 있습니다.

보조 포트로의 전환은 자동 작업이 아닙니다. 운영 포트를 사용할 수 없게 되는 경우 수동으로 DD VTL 디바이스를 보조 포트로 전환해야 합니다.

포트 목록은 물리적 포트 번호의 목록입니다. 포트 번호는 PCI 슬롯을 나타내고 문자는 PCI 카드의 포트를 나타냅니다. 1a, 1b 또는 2a, 2b 등을 예로 들 수 있습니다.

드라이브는 구성한 모든 포트에서 동일한 LUN과 함께 나타납니다.

e. **OK**를 선택합니다.

액세스 그룹 삭제

액세스 그룹을 삭제하기 전에 액세스 그룹에 있는 모든 이니시에이터 및 LUN을 제거해야 합니다.

절차

1. 모든 이니시에이터와 LUN을 그룹에서 제거합니다.
2. **Access Groups** > **Groups**를 선택합니다.
3. **More Tasks** > **Group** > **Delete**를 선택합니다.
4. Delete Group 대화 상자에서 제거할 그룹의 확인란을 선택하고 **Next**를 선택합니다.
5. 그룹 확인 대화 상자에서 삭제를 확인하고 **Submit**을 선택합니다.
6. Delete Groups Status에 `Completed`가 표시되면 **Close**를 선택합니다.

CLI 절차

```
# scsitarget group destroy My_Group
```

선택된 액세스 그룹 작업

Access Groups > **Groups** > *group*을 선택하여 선택된 액세스 그룹에 대한 다음 정보를 표시합니다.

표 163 LUNs 탭

항목	설명
LUN	디바이스 주소 – 최대 숫자는 16383입니다. 그룹 내에서 LUN을 한 번만 사용할 수 있지만 동일한 LUN을 다른 그룹 내에서

표 163 LUNs 탭 (계속)

항목	설명
	다시 사용할 수 있습니다. 그룹에 추가된 DD VTL 디바이스는 연속 LUN을 사용해야 합니다.
Library	LUN과 연결된 라이브러리의 이름입니다.
Device	체인저와 드라이브입니다.
In-Use Endpoints	현재 사용 중인 엔드포인트 세트로, primary 또는 secondary입니다.
Primary Endpoints	백업 애플리케이션에서 사용하는 초기(또는 기본) 엔드포인트입니다. 이 엔드포인트에서 장애가 발생할 경우 보조 엔드포인트가 사용될 수 있습니다(사용 가능한 경우).
Secondary Endpoints	운영 엔드포인트에서 장애가 발생하는 경우 사용할 페일오버 엔드포인트 세트입니다.

표 164 Initiators 탭

항목	설명
Name	이니시에이터의 이름으로, 이니시에이터에 할당된 별칭 또는 WWPN입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, Fibre Channel 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.

More Tasks 메뉴에서 선택된 그룹을 구성하거나 사용 중인 엔드포인트를 설정할 수 있습니다.

디바이스의 엔드포인트 선택

엔드포인트는 디바이스를 이니시에이터에 연결하므로 디바이스를 연결하기 전에 이 프로세스를 사용하여 엔드포인트를 설정하십시오.

절차

1. **Access Groups** > **Groups**> *group*을 선택합니다.
2. **More Tasks** > **Endpoints** > **Set In-Use**를 선택합니다.
3. Set in-Use Endpoints 대화 상자에서 특정 디바이스만 선택하거나 **Devices**를 선택하여 목록의 모든 디바이스를 선택합니다.
4. 엔드포인트가 운영 엔드포인트인지 아니면 보조 엔드포인트인지를 나타냅니다.
5. **OK**를 선택합니다.

NDMP 디바이스 TapeServer 그룹 구성

DD VTL TapeServer 그룹에는 NDMP(Network Data Management Protocol) 기반 백업 애플리케이션과 상호 작용하고 FC(Fibre Channel) 대신 IP(Internet Protocol)를 통해 제어 정보와 데이터 스트림을 보내는 테이프 드라이브가 포함되어 있습니다. NDMP TapeServer에서 사용하는 디바이스는 DD VTL 그룹 TapeServer에 포함되어야 하며 *오직* NDMP TapeServer에서만 사용할 수 있습니다.

절차

1. 테이프 드라이브를 새 라이브러리나 기존 라이브러리(이 예에서는 “dd990-16”)에 추가합니다.
2. 라이브러리의 슬롯과 CAP를 생성합니다.
3. 라이브러리(이 예에서는 “dd990-16”)에 생성된 디바이스를 TapeServer 액세스 그룹에 추가합니다.
4. 명령줄에서 다음을 입력하여 NDMP 데몬을 활성화합니다.

```
# ndmpd enable
Starting NDMP daemon, please wait.............
NDMP daemon is enabled.
```

5. NDMP 데몬이 TapeServer 그룹의 디바이스를 인식하는지 확인합니다.

```
# ndmpd show devicenames
NDMP Device          Virtual Name       Vendor   Product       Serial Number
-----------------    ----------------   ------   -----------   -------------
/dev/dd_ch_c0t0l0    dd990-16 changer   STK      L180          6290820000
/dev/dd_st_c0t1l0    dd990-16 drive 1   IBM      ULTRIUM-TD3   6290820001
/dev/dd_st_c0t2l0    dd990-16 drive 2   IBM      ULTRIUM-TD3   6290820002
/dev/dd_st_c0t3l0    dd990-16 drive 3   IBM      ULTRIUM-TD3   6290820003
/dev/dd_st_c0t4l0    dd990-16 drive 4   IBM      ULTRIUM-TD3   6290820004
-----------------    ----------------   ------   -----------   -------------
```

6. 다음 명령을 사용하여 NDMP 사용자(이 예에서는 ndmp)를 추가합니다.

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. ndmp 사용자가 올바르게 추가되었는지 확인합니다.

```
# ndmpd user show
ndmp
```

8. NDMP 구성을 표시합니다.

```
# ndmpd option show all
Name              Value
--------------    --------
authentication    text
debug             disabled
port              10000
preferred-ip
--------------    --------
```

9. 보안 강화를 위해 MD5 암호화를 사용하도록 기본 사용자 암호 인증을 변경하고 변경 내용을 확인합니다(인증 값이 text에서 md5로 변경됨).

```
# ndmpd option set authentication md5# ndmpd option show all
Name              Value
--------------    --------
authentication    md5
debug             disabled
port              10000
preferred-ip
--------------    --------
```

결과

이제 NDMP가 구성되었으며 TapeServer 액세스 그룹이 디바이스 구성을 표시합니다. 전체 명령 세트와 옵션을 보려면 *Data Domain Operating System 명령 참조 가이드*의 ndmpd 장을 참조하십시오.

리소스 관련 작업

Resources > **Resources** 를 선택하면 이니시에이터 및 엔드포인트에 대한 정보가 표시됩니다. *이니시에이터*는 FC(Fibre Channel) 프로토콜을 사용하여 데이터를 읽고 쓰

기 위해 시스템에 접속하는 백업 클라이언트입니다. 특정 이니시에이터는 FC 기반 DD Boost 또는 DD VTL을 지원하지만 둘 모두를 지원하지는 않습니다. *엔드포인트*는 이니시에이터가 연결하는 DD 시스템에 있는 논리 타겟입니다.

표 165 Initiators 탭

항목	설명
Name	이니시에이터의 이름으로, 이니시에이터에 할당된 별칭 또는 WWPN입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Online Endpoints	포트가 이니시에이터에 표시되는 그룹 이름입니다. 이니시에이터를 사용할 수 없는 경우 `None` 또는 `Offline`이 표시됩니다.

표 166 Endpoints 탭

항목	설명
Name	엔드포인트의 특정 이름입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
System Address	엔드포인트에 대한 시스템 주소입니다.
Enabled	HBA(Host Bus Adapter) 포트의 작동 상태로, `Yes`(활성화) 또는 `No`(비활성화)입니다.
Status	DD VTL 링크 상태로, `Online`(트래픽을 처리할 수 있음) 또는 `Offline`입니다.

Configure Resources

Configure Resources를 선택하면 엔드포인트와 이니시에이터를 구성할 수 있는 Fibre Channel 영역으로 이동됩니다.

이니시에이터 작업

Resources > **Resources** > **Initiators**를 선택하면 이니시에이터에 대한 정보가 표시됩니다. *이니시에이터*는 DD 시스템 인터페이스와 연동하는 클라이언트 시스템 FC HBA(Fibre Channel Host Bus Adapter) WWPN(Worldwide Port Name)입니다. *이니시에이터 이름*은 간편하게 사용하기 위한 클라이언트 WWPN의 별칭입니다.

이니시에이터로 매핑된 클라이언트는 액세스 그룹이 추가되기 전에 DD 시스템의 데이터에 액세스할 수 없습니다.

이니시에이터나 클라이언트에 대한 액세스 그룹이 추가된 후 클라이언트는 해당 액세스 그룹의 디바이스만 액세스할 수 있습니다. 하나의 클라이언트에 여러 디바이스에 대한 액세스 그룹이 있을 수 있습니다.

하나의 액세스 그룹에 여러 개의 이니시에이터가 포함될 수 있지만 각 이니시에이터는 하나의 액세스 그룹에만 존재할 수 있습니다.

참고

하나의 DD 시스템에 최대 1,024개의 이니시에이터를 구성할 수 있습니다.

표 167 이니시에이터 정보

항목	설명
Name	이니시에이터의 이름입니다.
Group	이니시에이터와 연결된 그룹입니다.
Online Endpoints	이니시에이터에 표시된 엔드포인트입니다. 이니시에이터를 사용할 수 없는 경우 `none` 또는 `offline`이 표시됩니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Vendor Name	이니시에이터 공급업체의 이름입니다.

Configure Initiators를 선택하면 엔드포인트와 이니시에이터를 구성할 수 있는 Fibre Channel 영역으로 이동됩니다.

CLI 절차

```
# vtl initiator show
Initiator  Group      Status  WWNN                    WWPN                    Port
---------  ---------  ------  ----------------------  ----------------------  ----
tsm6_p1    tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8 10b
---------  ---------  ------  ----------------------  ----------------------  ----

Initiator  Symbolic Port Name                          Address Method
---------  ------------------------------------------  --------------
tsm6_p1    QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
---------  ------------------------------------------  --------------
```

엔드포인트 작업

Resources > **Resources** > **Endpoints**를 선택하면 엔드포인트 하드웨어 및 접속 구성에 대한 정보가 표시됩니다.

표 168 Hardware 탭

항목	설명
System Address	엔드포인트의 시스템 주소입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.

표 168 Hardware 탭 (계속)

항목	설명
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Enabled	HBA(Host Bus Adapter) 포트의 작동 상태로, `Yes`(사용) 또는 `No`(사용 안 함)입니다.
NPIV	이 엔드포인트의 NPIV 상태로, Enabled 또는 Disabled입니다.
링크 상태	이 엔드포인트의 링크 상태로, Online 또는 Offline입니다.
Operation Status	이 엔드포인트의 작동 상태로, Normal 또는 Marginal입니다.
# of Endpoints	이 엔드포인트에 연결된 엔드포인트의 수입니다.

표 169 Endpoints 탭

항목	설명
Name	엔드포인트의 특정 이름입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, FC(Fibre Channel) 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
System Address	엔드포인트의 시스템 주소입니다.
Enabled	HBA(Host Bus Adapter) 포트의 작동 상태로, `Yes`(사용) 또는 `No`(사용 안 함)입니다.
링크 상태	이 엔드포인트의 링크 상태로, Online 또는 Offline입니다.

Configure Endpoints

Configure Endpoints를 선택하면 엔드포인트에 대한 위의 정보를 변경할 수 있는 Fibre Channel 영역으로 이동됩니다.

CLI 절차

```
# scsitarget endpoint show list
Endpoint       System Address  Transport     Enabled  Status
--------       --------------  ---------     -------  ------
endpoint-fc-0  5a              FibreChannel  Yes      Online
endpoint-fc-1  5b              FibreChannel  Yes      Online
```

선택된 엔드포인트 작업

Resources > **Resources** > **Endpoints** > *endpoint*를 선택하면 엔드포인트 하드웨어, 접속 구성 및 통계에 대한 정보가 표시됩니다.

표 170 Hardware 탭

항목	설명
System Address	엔드포인트의 시스템 주소입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, Fibre Channel 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
Enabled	HBA(Host Bus Adapter) 포트의 작동 상태로, `Yes`(사용) 또는 `No`(사용 안 함)입니다.
NPIV	이 엔드포인트의 NPIV 상태로, Enabled 또는 Disabled입니다.
LInk Status	이 엔드포인트의 링크 상태로, Online 또는 Offline입니다.
Operation Status	이 엔드포인트의 작동 상태로, Normal 또는 Marginal입니다.
# of Endpoints	이 엔드포인트에 연결된 엔드포인트의 수입니다.

표 171 Summary 탭

항목	설명
Name	엔드포인트의 특정 이름입니다.
WWPN	고유한 WWPN(Worldwide Port Name)으로, Fibre Channel 포트의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
WWNN	고유한 WWNN(Worldwide Node Name)으로, FC 노드의 64비트 식별자(4비트 *NAA(Network Address Authority)* 식별자 + 60비트 값)입니다.
System Address	엔드포인트의 시스템 주소입니다.
Enabled	HBA(Host Bus Adapter) 포트의 작동 상태로, `Yes`(사용) 또는 `No`(사용 안 함)입니다.
LInk Status	이 엔드포인트의 링크 상태로, Online 또는 Offline입니다.

표 172 Statistics 탭

항목	설명
Endpoint	엔드포인트의 특정 이름입니다.
Library	엔드포인트가 포함된 라이브러리의 이름입니다.
Device	디바이스 수입니다.
Ops/s	초당 작업 수입니다.
Read KiB/s	초당 읽기 속도(KiB)입니다.
Write KiB/s	초당 쓰기 속도(KiB)입니다.

표 173 Detailed Statistics 탭

항목	설명
Endpoint	엔드포인트의 특정 이름입니다.
# of Control Commands	제어 명령의 수입니다.
# of Read Commands	읽기 명령의 수입니다.
# of Write Commands	쓰기 명령의 수입니다.
In (MiB)	쓴 MiB(MB의 2진 표기법)의 수입니다.
Out (MiB)	읽은 MiB의 수입니다.
# of Error Protocol	오류 프로토콜의 수입니다.
# of Link Fail	링크 장애의 수입니다.
# of Invalid Crc	잘못된 CRC(Cyclic Redundancy Check)의 수입니다.
# of Invalid TxWord	잘못된 tx(전송) 단어의 수입니다.
# of Lip	LIP(Loop Initialization Primitive)의 수입니다.
# of Loss Signal	손실된 신호나 접속의 수입니다.
# of Loss Sync	동기화가 손실된 신호나 접속의 수입니다.

풀 작업

Pools > **Pools**를 선택하면 기본 풀과 다른 모든 기존 풀에 대한 자세한 정보가 표시됩니다. *풀*은 파일 시스템의 디렉토리로 매핑되는 테이프 모음입니다. 풀은 테이프를 대상으로 복제하는 데 사용됩니다. 디렉토리 기반 풀을 MTree 기반 풀로 변환해 MTree의 보다 유용한 기능을 활용할 수 있습니다.

풀에 대한 다음 사항에 유의하십시오.

- 풀의 유형은 MTree(권장) 또는 이전 버전과 호환되는 디렉토리일 수 있습니다.
- 풀은 개별 테이프가 있는 위치에 관계없이 복제될 수 있습니다. 테이프는 볼트(Vault) 또는 라이브러리(슬롯, CAP 또는 드라이브)에 있을 수 있습니다.
- 한 풀에서 다른 풀로 테이프를 복제하고 이동할 수 있습니다.
- 풀은 백업 소프트웨어에서 액세스할 수 없습니다.
- 풀을 복제할 때 복제 대상에서 DD VTL 구성 또는 라이선스가 필요하지 않습니다.
- 고유 바코드를 사용하여 테이프를 생성해야 합니다. 바코드가 중복되면 백업 애플리케이션에서 예측할 수 없는 동작이 발생할 수 있으며 사용자에게 혼란을 줄 수 있습니다.
- DD 시스템의 서로 다른 두 풀에 있는 두 테이프가 동일한 이름을 사용할 수 있으며, 이 경우 두 테이프 중 하나를 다른 테이프의 풀로 이동할 수 없습니다. 마찬가지로 복제 대상으로 전송된 풀의 이름은 대상에서 고유해야 합니다.

표 174 Pools 탭

항목	설명
Name	풀의 이름입니다.

표 174 Pools 탭 (계속)

항목	설명
Type	Directory 또는 MTree 풀입니다.
Status	풀의 상태입니다.
Tape Count	풀의 테이프 수입니다.
Size	풀에 있는 테이프의 구성된 총 데이터 용량으로, GiB(기비바이트, 기가바이트(GB)의 2진 표기법) 단위로 표시됩니다.
Physical Used	풀의 가상 테이프에서 사용된 공간의 양입니다.
Compression	풀에 있는 테이프의 데이터에 적용된 평균 압축 양입니다.
Cloud Unit	DD VTL 풀이 데이터를 마이그레이션하는 클라우드 유닛의 이름입니다.
Cloud Data Movement Policy	DD Cloud Tier 스토리지로의 DD VTL 데이터 마이그레이션을 제어하는 데이터 이동 정책입니다.

표 175 Replication 탭

항목	설명
Name	풀의 이름입니다.
Configured	이 풀에 대해 복제가 구성되었는지 여부로, yes 또는 no입니다.
Remote Source	풀이 다른 DD 시스템에서 복제된 경우에만 항목이 포함됩니다.
Remote Destination	풀을 다른 DD 시스템으로 복제한 경우에만 항목이 포함됩니다.

More Tasks 메뉴에서 풀을 생성하고 삭제할 수 있으며 테이프를 검색할 수 있습니다.

풀 생성

설정에 필요한 경우(예: 5.2 이전 DD OS 시스템을 통한 복제) 이전 버전과 호환되는 풀을 생성할 수 있습니다.

절차

1. **Pools** > **Pools**를 선택합니다.
2. **More Tasks** > **Pool** > **Create**를 선택합니다.
3. Create Pool 대화 상자에 풀 이름을 입력합니다. 다음 사항을 유의하십시오.
   - “all, ”“vault” 또는 “summary”는 사용할 수 없습니다.
   - 풀 이름에는 처음이나 끝에 공백 또는 마침표가 올 수 없습니다.
   - 풀 이름은 대/소문자를 구분합니다.
4. 디렉토리 풀을 생성하려는 경우(이전 버전의 DD System Manager와 호환됨) “Create a directory backwards compatibility mode pool” 옵션을 선택합니다.“ ” 단, MTree 풀을 사용할 경우 얻을 수 있는 이점에는 다음과 같은 사항이 포함됩니다.

- 개별 스냅샷 및 스케줄 스냅샷 만들기
- Retention Lock 적용
- 개별 보존 정책 설정
- 압축 정보 얻기
- 보존 계층에 데이터 마이그레이션 정책 적용
- 고정적 및 유동적 제한을 설정해 스토리지 공간 사용 정책(할당량 지원) 수립

5. **OK**를 선택해 Create Pool Status 대화 상자를 표시합니다.
6. Create Pool Status 대화 상자에 `Completed`라고 표시되면 **Close**를 선택합니다. Pools 하위 트리에 풀이 추가되고 여기에 가상 테이프를 추가할 수 있습니다.

CLI 절차

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

풀 삭제

풀을 삭제하려면 먼저 풀에 포함된 테이프를 모두 삭제해야 합니다. 풀에 대해 복제가 구성된 경우 복제 페어도 삭제해야 합니다. 풀 삭제는 MTree의 이름을 바꾸고 MTree를 삭제하는 것에 해당하며, 이 작업은 다음 정리 프로세스에서 수행됩니다.

절차

1. **Pools** > **Pools** > ***pool***을 선택합니다.
2. **More Tasks** > **Pool** > **Delete**를 선택합니다.
3. Delete Pools 대화 상자에서 삭제할 항목의 확인란을 선택합니다.
   - 각 풀의 이름 또는
   - 모든 풀을 삭제하려는 경우에는 **Pool Names**
4. 확인 대화 상자에서 **Submit**을 선택합니다.
5. Delete Pool Status 대화 상자에 `Completed`가 표시되면 **Close**를 선택합니다.

   풀이 Pools 하위 트리에서 제거됩니다.

선택한 풀 작업

Virtual Tape Libraries > **VTL Service** > **Vault** > *pool* 및 **Pools** > **Pools** > *pool* 모두 선택한 풀의 세부 정보를 제공합니다. 풀 "Default"는 항상 존재합니다.

Pool 탭

표 176 요약

항목	설명
Convert to MTree Pool	Directory 풀을 MTree 풀로 변환하려면 이 버튼을 선택합니다.
유형	Directory 또는 MTree 풀입니다.
Tape Count	풀의 테이프 수입니다.

표 176 요약 (계속)

항목	설명
Capacity	풀에 있는 테이프의 구성된 총 데이터 용량으로 GiB 단위(Gibibyte: GB(Gigabyte)의 2진 표기법)로 표시됩니다.
Logical Used	풀의 가상 테이프에서 사용된 공간의 양입니다.
Compression	풀에 있는 테이프의 데이터에 적용된 평균 압축 양입니다.

표 177 Pool 탭: Cloud Data Movement - Protection Distribution

항목	설명
Pool type (%)	VTL 풀 및 클라우드(해당하는 경우)이며 데이터의 현재 비율이 괄호 안에 표시됩니다.
이름	로컬 VTL 풀 또는 클라우드 공급업체의 이름입니다.
Logical Used	풀의 가상 테이프에서 사용된 공간의 양입니다.
Tape Count	풀의 테이프 수입니다.

표 178 Pool 탭: Cloud Data Movement - Cloud Data Movement Policy

항목	설명
Policy	테이프 수명(일) 또는 수동 선택 항목입니다.
Older Than	수명 기반 데이터 이동 정책의 수명 임계값입니다.
Cloud Unit	대상 클라우드 유닛입니다.

Tape 탭

표 179 테이프 컨트롤

항목	설명
생성	새 테이프를 생성합니다.
Delete	선택한 테이프를 삭제합니다.
Copy	테이프의 복제본을 만듭니다.
Move between Pool	선택된 테이프를 다른 풀로 이동합니다.
Select for Cloud Move[a]	선택된 테이프를 DD Cloud Tier로 마이그레이션하도록 예약합니다.
Unselect from Cloud Move[a]	선택된 테이프를 DD Cloud Tier로 마이그레이션하는 스케줄에서 제거합니다.
Recall Cloud Tapes	선택된 테이프를 DD Cloud Tier에서 리콜합니다.
Move to Cloud Now	다음번 예약된 마이그레이션까지 기다리지 않고 선택된 테이프를 DD Cloud Tier로 마이그레이션합니다.

a. 이 옵션은 데이터 이동 정책이 수동 선택에 대해 구성된 경우에만 사용할 수 있습니다.

표 180 테이프 정보

항목	설명
Barcode	테이프 바코드입니다.
Size	테이프의 최대 크기입니다.
Physical Used	테이프에서 사용된 물리적 스토리지 용량입니다.
압축	테이프에 대한 압축률입니다.
Location	테이프의 위치입니다.
수정 시간	테이프가 마지막으로 수정된 시간입니다.
Recall Time	테이프가 리콜된 마지막 시간입니다.

Replication 탭

표 181 복제

항목	설명
Name	풀의 이름입니다.
Configured	이 풀에 대해 복제가 구성되었는지 여부로, yes 또는 no입니다.
Remote Source	풀이 다른 DD 시스템에서 복제된 경우에만 항목이 포함됩니다.
Remote Destination	풀을 다른 DD 시스템으로 복제한 경우에만 항목이 포함됩니다.

오른쪽 맨 위에 있는 **Replication Detail** 버튼을 선택해 선택한 풀에 대한 Replication Information 패널로 이동할 수도 있습니다.

Virtual Tape Libraries 또는 Pools 영역의 More Tasks 메뉴에서 풀의 테이프를 생성, 삭제, 이동, 복제 또는 검색할 수 있습니다.

Pools 영역의 More Tasks 메뉴에서는 풀의 이름을 변경하거나 삭제할 수도 있습니다.

MTree 풀로 디렉토리 풀 변환

MTree 풀에는 디렉토리 풀보다 많은 장점이 있습니다. 자세한 내용은 *풀 생성* 섹션을 참조하십시오.

절차

1. 다음과 같은 사전 요구 사항이 충족되었는지 확인합니다.
   - 소스 및 대상 풀이 동기화되어 양쪽의 데이터와 테이프 수가 그대로 유지되어야 합니다.
   - 디렉토리 풀이 복제 소스 또는 대상이 아니어야 합니다.
   - 파일 시스템이 꽉 차지 않아야 합니다.
   - 파일 시스템이 허용되는 최대 MTree 수(100)에 도달하지 않아야 합니다.
   - 동일한 이름의 MTree가 이미 있지 않아야 합니다.
   - 디렉토리 풀이 여러 시스템에 복제되는 경우 복제하는 시스템이 관리하는 시스템에 알려져야 합니다.

- 디렉토리 풀이 오래된 DD OS로 복제되는 경우(예: DD OS 5.5에서 DD OS 5.4로) 이를 변환할 수 없습니다. 해결 방법은 다음과 같습니다.
  - 두 번째 DD 시스템에 디렉토리 풀을 복제합니다.
  - 두 번째 DD 시스템에서 세 번째 DD 시스템으로 디렉토리 풀을 복제합니다.
  - 관리하는 DD 시스템의 Data Domain 네트워크에서 두 번째 및 세 번째 DD 시스템을 제거합니다.
  - DD OS 5.5를 실행하는 시스템의 Pools 하위 메뉴에서 **Pools**와 디렉토리 풀을 선택합니다. Pools 탭에서 **Convert to MTree Pool**을 선택합니다.

2. 변환할 디렉토리 풀이 강조 표시된 상태에서 **Convert to MTree Pool**을 선택합니다.
3. Convert to MTree Pool 대화 상자에서 **OK**를 선택합니다.
4. 변환은 다음과 같은 방식으로 복제에 영향을 미칩니다.
   - DD VTL은 변환 중에 복제된 시스템에서 일시적으로 비활성화됩니다.
   - 대상 데이터가 대상 시스템의 새로운 풀에 복제되어 새로운 복제가 초기화되고 동기화될 때까지 데이터를 유지합니다. 이후에 **CONVERTED-*pool***이라는 이 일시적으로 복제된 풀을 안전하게 삭제할 수 있습니다. 여기서 *pool*은 업그레이드된 풀의 이름(또는 풀 이름이 긴 경우 첫 18자)입니다. 이는 DD OS 5.4.1.0 이상에만 적용됩니다.
   - 타겟 복제 디렉토리가 MTree 형식으로 변환됩니다. 이는 DD OS 5.2 이상에만 적용됩니다.
   - 복제 페어가 풀 변환 전에 분리되고 오류가 없는 경우 이후에 다시 설정됩니다.
   - MTree 풀 변환과 연관된 시스템에서는 DD Retention Lock을 활성화할 수 없습니다.

풀 간 테이프 이동

테이프가 볼트(Vault)에 상주하는 경우 테이프를 풀 간에 이동해 복제 작업을 수용할 수 있습니다. 예를 들어 기본 풀에서 모든 테이프가 생성된다면 풀이 필요하지만 나중에 테이프 그룹 복제를 위해 독립적인 그룹이 필요할 수 있습니다. 명명된 풀을 생성하고 테이프 그룹을 새 풀로 재구성할 수 있습니다.

참고

디렉토리 복제 소스인 테이프 풀에서 테이프를 이동할 수 없습니다. 해결 방법으로 다음과 같이 할 수 있습니다.

- 새 풀에 테이프를 복제한 후 이전 풀에서 테이프를 삭제합니다.
- 디렉토리 복제 소스에 해당하는 테이프 풀에서 테이프를 이동할 수 있는 MTree 풀을 사용합니다.

절차

1. 풀이 강조 표시된 상태에서 **More Tasks** > **Tapes** > **Move**를 선택합니다.

   풀에서 시작할 경우 Tapes Panel에서는 풀 사이에서만 테이프를 이동할 수 있습니다.

2. Move Tape 대화 상자에서 이동할 테이프를 검색할 정보를 입력하고 **Search**를 선택합니다.

표 182 Move Tapes 대화 상자

필드	사용자 입력
Location	위치는 변경할 수 없습니다.
Pool	테이프가 상주하는 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 Default 풀을 사용합니다.
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 가져옵니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	반환할 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

3. 검색 결과 목록에서 이동할 테이프를 선택합니다.
4. Select Destination: Location 목록에서 테이프를 이동할 풀의 위치를 선택합니다. 이 옵션은 (명명된) Pool 보기에서 시작한 경우에만 사용할 수 있습니다.
5. **Next**를 선택합니다.
6. Move Tapes 보기에서 요약 정보와 테이프 목록을 확인하고 **Submit**을 선택합니다.
7. 상태 창에서 **Close**를 선택합니다.

풀 간 테이프 복제

복제 작업을 지원하기 위해 테이프를 풀 사이에서 복제하거나 볼트(Vault)에서 풀로 복제할 수 있습니다. 이 옵션은 (명명된) Pool 보기에서 시작한 경우에만 사용할 수 있습니다.

절차

1. 풀이 강조 표시된 상태에서 **More Tasks** > **Tapes** > **Copy**를 선택합니다.
2. Copy Tapes Between Pools 대화 상자에서 복제할 테이프의 확인란을 선택하거나 복제할 테이프 검색을 위한 정보를 입력하고 **Search**를 선택합니다.

표 183 Copy Tapes Between Pools 대화 상자

필드	사용자 입력
Location	테이프를 찾을 위치로 라이브러리 또는 **Vault**를 선택합니다. 풀(Pools 메뉴 아래)에 테이프가 항상 표시되기는 하지만 기술적으로 라이브러리나 볼트(Vault) 둘 다가 아니라 둘 중 하나에만 있으며, 두 개의 라이브러리에 동시에 있지 않습니다. Import/Export 옵션을 사용해 볼트(Vault)와 라이브러리 사이에서 테이프를 이동합니다.
Pool	풀 사이에서 테이프를 복제하려면 테이프가 현재 상주하는 풀의 이름을 선택합니다. 풀이 생성되지 않았다면 **Default** 풀을 사용합니다.

표 183 Copy Tapes Between Pools 대화 상자 (계속)

필드	사용자 입력
Barcode	고유한 바코드를 지정하거나 기본값(*)을 사용해 테이프 그룹을 가져옵니다. 바코드에는 와일드카드 ? 및 *가 허용됩니다. 여기서 ?는 단일 문자, *는 0자 이상의 문자와 일치합니다.
Count	가져올 최대 테이프 수를 입력합니다. 이 필드를 비워 두면 바코드 기본값(*)이 사용됩니다.
Tapes Per Page	페이지당 표시할 테이프의 최대 개수를 선택합니다. 가능한 값은 15, 30 및 45입니다.
Items Selected	여러 페이지에서 선택한 테이프의 수를 표시합니다. 테이프를 선택할 때마다 자동으로 업데이트됩니다.

3. 검색 결과 목록에서 복제할 테이프를 선택합니다.
4. Select Destination: Pool 목록에서 테이프를 복제할 풀을 선택합니다. 바코드가 일치하는 테이프가 대상 풀에 이미 있는 경우 오류가 표시되고 복제가 중단됩니다.
5. **Next**를 선택합니다.
6. Copy Tapes Between Pools 대화 상자에서 요약 정보와 테이프 목록을 확인하고 **Submit**을 선택합니다.
7. Copy Tapes Between Pools Status 창에서 **Close**를 선택합니다.

풀 이름 바꾸기

라이브러리에 어떠한 테이프도 없는 경우에만 풀의 이름을 바꿀 수 있습니다.

절차

1. **Pools** > **Pools** > ***pool***을 선택합니다.
2. **More Tasks** > **Pool** > **Rename**을 선택합니다.
3. Rename Pool 대화 상자에 새 풀 이름을 입력합니다. 다음과 같은 사항을 주의해야 합니다.
   - “all, ”“vault” 또는 “summary”는 사용할 수 없습니다.
   - 풀 이름에는 처음이나 끝에 공백 또는 마침표가 올 수 없습니다.
   - 풀 이름은 대/소문자를 구분합니다.
4. **OK**를 선택해 Rename Pool Status 대화 상자를 표시합니다.
5. Rename Pool Status 대화 상자에 `Completed`가 표시되면 **OK**를 선택합니다.

   Pools 및 Virtual Tape Libraries 영역의 Pools 하위 트리에 풀의 이름이 변경되어 표시됩니다.

16장

DD Replicator

이 장에서 다루는 내용은 다음과 같습니다.

DD Replicator 개요

DD Replicator(Data Domain Replicator)는 DR(Disaster Recovery)과 멀티 사이트 백업 및 아카이브 통합을 위해 자동화되고 네트워크 효율성이 뛰어나며 암호화된 정책 기반의 복제 기능을 제공합니다. DD Replicator는 WAN(Wide Area Network)을 통해 압축 및 중복 제거된 데이터만 비동기식으로 복제합니다.

DD Replicator는 *로컬* 중복 제거 및 *사이트 간* 중복 제거라는 두 가지 레벨의 데이터 중복 제거를 수행하여 대역폭 요구량을 크게 줄입니다. 로컬 데이터 중복 제거는 WAN을 통해 복제될 고유한 세그먼트를 결정합니다. 더욱이 사이트 간 데이터 중복 제거는 여러 사이트의 데이터를 동일한 대상 시스템으로 복제할 때 대역폭 요구량을 한층 더 단축합니다. 사이트 간 데이터 중복 제거 기능 덕분에, 다른 사이트로부터 이미 전송되었거나 로컬 백업 또는 아카이빙을 통해 이미 생성된 중복 세그먼트는 다시 복제되지 않습니다. 따라서 모든 사이트에서 네트워크 효율성이 개선되고 일일 네트워크 대역폭 요구량이 최대 99% 줄어들어 네트워크 기반 복제 작업의 속도, 신뢰성 및 경제성이 강화됩니다.

DD Replicator는 광범위한 재해 복구 요구 사항을 충족할 수 있도록 전체 시스템 미러링, 양방향, 다대일, 일대다, 다단계(Cascaded) 등의 유연한 복제 토폴로지를 제공합니다. 또한 사용자는 DD 시스템에서 데이터를 전부 복제하거나 일부만 선택하여 복제할 수 있습니다. DD Replicator는 표준 SSL(Secure Socket Layer) 프로토콜을 사용하여 DD 시스템 간에 복제되는 데이터를 암호화함으로써 보안 수준을 강화합니다.

DD Replicator는 성능 및 지원되는 팬인(Fan-in) 비율을 확장하여 대규모 엔터프라이즈 환경을 원활하게 지원할 수 있습니다.

DD Replicator를 시작하기 전에 다음의 일반적인 요구 사항을 참고하십시오.

- DD Replicator는 라이센스가 등록된 제품입니다. 라이센스를 구매하려면 Data Domain 영업 담당자에게 문의하십시오.
- 보통 서로 두 개의 릴리즈 내에 있는 시스템 사이에서만 복제할 수 있습니다(예: 5.6부터 6.0까지). 그러나 이례적인 릴리즈 번호 지정으로 인해 예외가 발생할 수 있으므로 *복제 버전 호환성* 섹션의 표를 검토하거나 Data Domain 영업 담당자에게 문의하십시오.
- 현재 버전의 DD System Manager에서 DD Replicator를 관리하고 모니터링할 수 없는 경우 *Data Domain Operating System 명령 참조 가이드*에 설명된 `replication` 명령을 사용하십시오.

복제 구성을 위한 사전 요구 사항

복제를 구성하기 전에 다음 사전 요구 사항을 검토하여 초기 데이터 전송 시간을 최소화하고 데이터 덮어쓰기 등을 방지하십시오.

- **Contexts** – 다음 표에 있는 복제 스트림 수를 검토하여 사용하는 DD 시스템의 최대 컨텍스트 수를 결정합니다.

  표 184 Data Domain 시스템에 전송되는 데이터 스트림

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD140, DD160, DD610	4GB 또는 6GB/0.5GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8GB/0.5GB 또는 1GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16GB 또는 20GB/1GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36GB/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72GB[b]/1GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 또는 64GB/2GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270

표 184 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD4500	192GB[b]/4GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 또는 256GB[b]/4GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768GB	1885	300	540	1,080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8TB	8GB/512MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16TB	16GB/512MB 또는 24GB/1GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32TB	24GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48TB	36GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64TB	48GB/1GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96TB	64GB/2GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4TB	12GB(가상 메모리)/512MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30

표 184 Data Domain 시스템에 전송되는 데이터 스트림 (계속)

모델	RAM/NVRAM	백업 쓰기 스트림	백업 읽기 스트림	복제[a] 소스 스트림	복제[a] 대상 스트림	혼합
DD3300 8TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16TB	32GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32TB	46GB(가상 메모리)/1,536GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl 스트림
b. Data Domain Extended Retention 소프트웨어 옵션은 확장(최대) 메모리를 지원하는 이러한 디바이스에서만 사용할 수 있습니다.

- **Compatibility** – 서로 다른 버전의 DD OS를 실행하는 DD 시스템을 사용 중인 경우 다음 섹션인 복제 버전 호환성을 검토하십시오.
- **Initial Replication** – 소스에 데이터가 많이 있으면 초기 복제 작업이 몇 시간 정도 걸릴 수 있습니다. 고속의 지연 시간이 낮은 링크를 통해 두 DD 시스템을 동일한 위치에 배치하는 것이 좋습니다. 첫 번째 복제 후에는 새 데이터만 전송되므로 의도한 위치로 시스템을 이동할 수 있습니다.
- **Bandwidth Delay Settings** – 소스와 대상의 대역폭 지연 설정은 동일해야 합니다. 이러한 튜닝 제어는 TCP(Transmission Control Protocol) 버퍼 크기를 제어하여 지연 시간이 높은 링크보다 우수한 복제 성능을 제공합니다. 소스 시스템에서는 확인을 기다리는 동안 대상으로 충분한 데이터를 보낼 수 있습니다.
- **Only One Context for Directories/Subdirectories** – 디렉토리(및 하위 디렉토리)는 한 번에 하나의 컨텍스트에만 포함될 수 있으니 소스 디렉토리의 하위 디렉토리가 다른 디렉토리 복제 컨텍스트에 사용되지 않는지 확인하십시오.
- **Adequate Storage** – 대상에는 최소한 소스와 *동일한 양의 공간*이 있어야 합니다.
- **Destination Empty for Directory Replication** – 디렉토리 복제를 위해서는 대상 디렉토리가 덮어써질 것에 대비해 대상 디렉토리가 비어 있거나 더는 필요하지 않은 컨텐츠여야 합니다.
- **Security** – DD OS에서는 이더넷 연결을 통한 안전한 복제를 구성할 수 있도록 포트 3009가 열려 있어야 합니다.

복제 버전 호환성

서로 다른 버전의 DD OS에서 실행되는 DD 시스템을 소스 또는 대상으로 사용하려면 다음 표에서 단일 노드, DD Extended Retention, DD Retention Lock, MTree, 디렉토리, 컬렉션, 델타(저대역폭 최적화) 및 다단계(Cascaded) 복제에 대한 호환성 정보를 참조하십시오.

일반 정보:

- DD Boost 또는 OST의 지원되는 구성은 *Data Domain Boost for Partner Integration Administration Guide* 또는 *OpenStorage용 Data Domain Boost 관리 가이드*에서 "최적화된 복제 버전 호환성"을 참조하십시오.
- MTree 복제 및 디렉토리 복제를 동시에 사용하여 동일한 데이터를 복제할 수 없습니다.

- 지원되는 모든 복제 구성에 대해 복구 절차를 사용할 수 있습니다.
- 컬렉션 복제가 지원되는 경우 파일 마이그레이션도 지원됩니다.
- DD OS 5.2.x를 실행하는 소스 DD 시스템과 DD OS 5.4.x 또는 DD OS 5.5.x를 실행하는 대상 DD 시스템 간의 MTree 복제에서 소스 MTree에 DD Retention Lock Governance가 활성화된 경우 MTree 복제가 지원되지 않습니다
- DD OS 6.0을 실행하는 소스 DD 시스템에서 이전 버전의 DD OS를 실행하는 타겟 DD 시스템으로의 MTree 복제인 경우 복제 프로세스는 대상 DD 시스템에 있는 이전 버전의 DD OS에 따라 동작합니다. 대상 DD 시스템에서 복구 작업이나 다단계 복제가 수행되면 가상 신세틱이 적용되지 않습니다.
- 다단계(Cascaded) 구성의 경우 최대 홉 수는 2(즉, DD 시스템 3대)입니다. D2M(Directory-to-MTree) 마이그레이션은 최대 두 개의 이전 릴리스까지 이전 버전과의 호환성을 지원합니다. D2M(Directory-to-MTree) 마이그레이션에 대한 자세한 내용은 D2M(Directory-to-MTree) 복제 마이그레이션(445페이지) 섹션을 참조하십시오.
- 일대다, 다대일 및 다단계 복제는 이 그림과 같이 최대 3개의 연속 DD OS 릴리스 제품군을 지원합니다.

그림 17 유효한 복제 구성

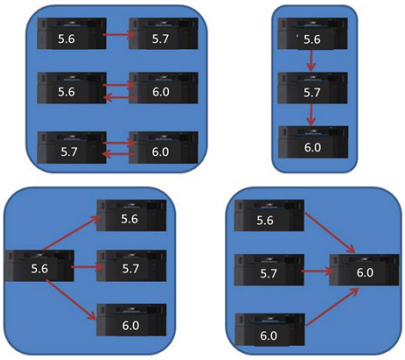


표 설명:

- 각 DD OS 릴리스에는 해당 제품군의 모든 릴리스가 포함됩니다. 예를 들어 DD OS 5.7에는 5.7.1, 5.7.x, 6.0 등이 포함됩니다.
- c = 컬렉션 복제
- dir = 디렉토리 복제
- m = MTree 복제
- del = 델타(저대역폭 최적화) 복제
- dest = 대상
- src = 소스
- NA = 해당 없음

표 185 구성: 단일 노드에서 단일 노드로

src/ dest	5.0(dest)	5.1(dest)	5.2(dest)	5.3(dest)	5.4(dest)	5.5(dest)	5.6(dest)	5.7(dest)	6.0(dest)	6.1(dest)	6.2 (dest)
5.0(src)	c, dir, del	dir, del	dir, del	NA	NA	NA	NA	NA	NA	NA	NA
5.1(src)	dir, del	c, dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	NA	NA	NA	NA	NA	NA
5.2(src)	dir, del	dir, del, m[a]	c, dir, del, m[b]	dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA	NA
5.3(src)	NA	dir, del, m[a]	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA	NA
5.4(src)	NA	dir, del, m[a]	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA
5.5(src)	NA	NA	dir, del, m	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA
5.6(src)	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA
5.7(src)	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA
6.0(src)	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m
6.1(src)	NA	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m

a. DD VTL의 경우 MTree 복제가 지원되지 않습니다.
b. 컬렉션 복제는 규정 준수 데이터에 대해서만 지원됩니다.

표 186 구성: DD Extended Retention에서 DD Extended Retention으로

src/ dest	5.0(dest)	5.1(dest)	5.2(dest)	5.3(dest)	5.4(dest)	5.5(dest)	5.6(dest)	5.7(dest)	6.0(dest)	6.1(dest)	6.2 (dest)
5.0(src)	c	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1(src)	NA	c	m[a]	m[b]	m[b]	NA	NA	NA	NA	NA	NA
5.2(src)	NA	m[a]	c, m[a]	m[a]	m[a]	m[a]	NA	NA	NA	NA	NA
5.3(src)	NA	m[c]	m[c]	c, m	m	m	NA	NA	NA		NA
5.4(src)	NA	m[c]	m[c]	m	c, m	m	m	NA	NA	NA	NA
5.5(src)	NA	NA	m[c]	m	m	c, m	m	m	NA	NA	NA
5.6(src)	NA	NA	NA	NA	m	m	c, m	m	m		NA
5.7(src)	NA	NA	NA	NA	NA	m	m	c, m	m	m	NA

표 186 구성: DD Extended Retention에서 DD Extended Retention으로 (계속)

src/ dest	5.0(dest)	5.1(dest)	5.2(dest)	5.3(dest)	5.4(dest)	5.5(dest)	5.6(dest)	5.7(dest)	6.0(dest)	6.1(dest)	6.2 (dest)
6.0(src)	NA	NA	NA	NA	NA	NA	m	m	c, m	m	m
6.1(src)	NA	NA	NA	NA	NA	NA	NA	m	m	c, m	m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	m	m	c, m

a. 이 구성의 소스 또는 대상에서는 MTree 복제를 통한 파일 마이그레이션이 지원되지 않습니다.
b. 이 구성의 소스에서는 MTree 복제를 통한 파일 마이그레이션이 지원되지 않습니다.
c. 이 구성의 대상에서는 MTree 복제를 통한 파일 마이그레이션이 지원되지 않습니다.

표 187 구성: 단일 노드에서 DD Extended Retention으로

src/ dest	5.0(dest)	5.1(dest)	5.2(dest)	5.3(dest)	5.4(dest)	5.5(dest)	5.6(dest)	5.7(dest)	6.0(dest)	6.1(dest)	6.2 (dest)
5.0(src)	dir	dir	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1(src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	NA	NA	NA	NA	NA	NA
5.2(src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	NA	NA	NA	NA	NA
5.3(src)	NA	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	NA	NA	NA	NA	NA
5.4(src)	NA	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	dir, m	NA	NA	NA	NA
5.5(src)	NA	NA	dir, m[a]	dir, m	dir, m	dir, m	dir, m	dir, m	NA	NA	NA
5.6(src)	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m	NA	NA
5.7(src)	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m	NA
6.0(src)	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m
6.1(src)	NA	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m

a. 이 구성에서는 파일 마이그레이션이 지원되지 않습니다.

복제 유형

일반적으로 복제는 백업 시스템에서 데이터를 받는 *소스* DD 시스템과 하나 이상의 *대상* DD 시스템으로 구성됩니다. 각 DD 시스템은 복제 컨텍스트의 소스 및/또는 대상이 될 수 있습니다. 각 DD 시스템은 복제 도중에도 정상적인 백업 및 복구 기능을 수행할 수 있습니다.

각 복제 유형은 기존 디렉토리 또는 소스의 MTree과 연결된 *컨텍스트*를 설정합니다. 컨텍스트가 설정되면 복제된 컨텍스트가 대상에 생성됩니다. 컨텍스트는 항상 활성 상태인 복제 페어를 설정하고 소스에 기록되는 모든 데이터는 기회가 생기는 대로 대상에 복제됩니다. 복제 컨텍스트에 구성된 경로는 절대 참조이며 경로가 구성된 시스템에 따라 변경되지 않습니다.

Data Domain 시스템에서 디렉토리, 컬렉션 또는 MTree 복제를 설정할 수 있습니다.

- *디렉토리 복제* 방식은 개별 디렉토리 수준에서의 복제를 지원합니다.
- *컬렉션 복제* 방식은 소스의 전체 데이터 저장소를 복제한 다음 대상에 전송하며 복제된 볼륨은 읽기 전용입니다.
- *MTree 복제* 방식은 전체 MTree(고급 관리를 지원하는 가상 파일 구조)를 복제합니다. 미디어 풀도 복제할 수 있으며 기본적으로 MTree가 생성된 후 복제됩니다(DD OS 5.3 기준). 미디어 풀은 이전 버전과의 호환성 모드에서도 생성될 수 있으며 복제 시 디렉토리 복제 컨텍스트가 됩니다.

모든 복제 유형에 대해 다음 요구 사항을 참고하십시오.

- 대상 Data Domain 시스템에는 최소한 소스 디렉토리의 예상 최대 크기 이상의 가용 스토리지 용량이 있어야 합니다. 대상 Data Domain 시스템의 네트워크 대역폭과 디스크 공간이 복제 소스의 모든 트래픽을 처리하기에 충분한지 확인하십시오.

- 파일 시스템을 활성화할 수 있어야 하며 복제 유형에 따라 복제 초기화의 일부로 활성화되기도 합니다.
- 소스는 반드시 존재해야 합니다.
- 대상은 존재할 수 없습니다.
- 대상은 컨텍스트가 작성되고 초기화될 때 생성됩니다.
- 복제가 시작된 후에는 대상의 소유권과 사용 권한이 항상 소스와 동일하게 맞춰집니다.
- 복제 명령 옵션에서 특정 복제 페어는 항상 대상을 통해 식별됩니다.
- 두 시스템에는 각 시스템에서 파트너의 호스트 이름을 확인할 수 있도록 IP 네트워크를 통해 식별 가능한 활성 상태의 라우트가 있어야 합니다.

복제 유형은 특정 요구 사항에 따라 선택할 수 있습니다. 다음 섹션에서는 이 세 가지 유형의 복제에 대한 기능 및 설명을 제공하고 DD Boost에서 사용하는 관리되는 파일 복제를 간략히 소개합니다.

관리되는 파일 복제

DD Boost에서 사용되는 *관리되는 파일 복제*는 백업 소프트웨어에서 관리하고 제어하는 복제의 유형입니다.

관리되는 파일 복제를 사용하면 백업 소프트웨어의 요청 시 백업 이미지가 한 DD 시스템에서 다른 DD 시스템으로 한 번에 하나씩 직접 전송됩니다.

백업 소프트웨어는 모든 복제본을 추적하기 때문에 복제 상태 및 여러 복제본을 사용한 복구 작업을 손쉽게 모니터링할 수 있습니다.

관리되는 파일 복제는 전체 시스템 미러링, 양방향, 다대일, 일대다 및 다중 구간(Cascaded) 등의 유연한 복제 토폴로지를 제공하므로 효율적인 사이트 간 데이터 중복 제거가 가능합니다.

관리되는 파일 복제에 대한 몇 가지 추가 고려 사항은 다음과 같습니다.

- 복제 컨텍스트를 구성하지 않아도 됩니다.
- 사용자의 개입 없이 수명주기 정책을 통해 복제 정보가 제어됩니다.
- DD Boost에서 필요에 따라 즉시 컨텍스트를 작성하고 분할합니다.

자세한 내용은 *Data Domain Operating System 명령 참조 가이드*에서 `ddboost file-replication` 명령을 참조하십시오.

디렉토리 복제

*디렉토리 복제*는 복제 소스로 구성된 DD 파일 시스템 디렉토리 내의 중복 제거된 데이터를 다른 시스템에서 복제 대상으로 구성된 디렉토리로 전송합니다.

디렉토리 복제를 사용하면 DD 시스템 하나가 동시에 한 복제 컨텍스트에서는 소스이고 다른 복제 컨텍스트에서는 대상일 수 있습니다. 또한 데이터를 복제하는 동안에도 DD 시스템이 백업 및 아카이브 애플리케이션에서 데이터를 수신할 수 있습니다.

디렉토리 복제에서는 관리 파일 복제(DD Boost에서 사용되는 유형)와 같은 유연한 네트워크 구축 토폴로지와 사이트 간 중복 제거 효과가 있을 수 있습니다.

디렉토리 복제를 사용할 때 추가로 다음과 같은 몇 가지 사항을 고려하십시오.

- 동일한 디렉토리 내에 CIFS와 NFS 데이터를 함께 저장하지 마십시오. 단일 대상 DD 시스템은 CIFS 및 NFS에 대해 별도의 디렉토리가 사용되는 한 CIFS 클라이언트와 NFS 클라이언트 모두에서 백업을 수신할 수 있습니다.

- 모든 디렉토리는 하나의 컨텍스트에만 존재할 수 있습니다. 상위 디렉토리의 하위 디렉토리가 이미 복제 중인 경우 상위 디렉토리를 복제 컨텍스트에 사용할 수 없습니다.
- 파일 또는 테이프를 디렉토리 복제 소스 디렉토리 *안 또는 밖*으로 이름을 바꾸거나 이동할 수 *없습니다*. 디렉토리 복제 소스 디렉토리 *안*에서 파일이나 테이프의 이름을 바꿀 수는 *있습니다*.
- 대상 DD 시스템에는 최소한 소스 디렉토리의 예상 최대 크기 즉, 압축 후 크기 이상의 가용 스토리지 용량이 있어야 합니다.
- 복제가 초기화되면 대상 디렉토리가 자동으로 생성됩니다.
- 복제가 시작된 후에는 대상 디렉토리의 소유권과 사용 권한이 항상 소스 디렉토리와 동일하게 유지됩니다. 컨텍스트가 존재하는 동안에는 대상 디렉토리가 읽기 전용 상태로 유지되고 소스 디렉토리의 데이터만 수신할 수 있습니다.
- 어느 시점에든 전역 압축 방식의 차이로 인해 소스와 대상 디렉토리의 크기가 달라질 수 있습니다.

폴더 생성 권장 사항

디렉토리 복제는 `/data/col1/backup` 아래의 개별 하위 디렉토리 레벨에서 데이터를 복제합니다.

세분화된 데이터 분리를 제공하려면 호스트 시스템에서 **/backup Mtree** 내에 다른 디렉토리(DirA, DirB 등)를 생성해야 합니다. 각 디렉토리는 사용자 환경에 기반해야 하며 이러한 디렉토리를 다른 위치로 복제해야 합니다. 전체 **/backup MTree**를 복제하는 대신 **/data/col1/backup/**(예: **/data/col1/backup/DirC**) 아래의 각 하위 디렉토리에 복제 컨텍스트를 설정합니다. 3중으로 사용하는 이유는 다음과 같습니다.

- DirA가 한 사이트로 이동하고 DirB는 다른 사이트로 이동할 수 있으므로 대상 위치를 제어할 수 있습니다.
- 이 수준의 세분화에서는 관리, 모니터링 및 장애 격리가 가능합니다. 각 복제 컨텍스트를 일시 중지, 중지, 제거 또는 보고할 수 있습니다.
- 단일 컨텍스트에서는 성능이 제한됩니다. 여러 컨텍스트를 생성하면 집계 복제 성능을 개선할 수 있습니다.
- 일반적인 권장 사항으로 여러 복제 스트림에 복제 로드를 분산하려면 약 **5~10**개의 컨텍스트가 필요할 수 있습니다. 컨텍스트 수는 사이트 설계 및 해당 위치의 데이터 볼륨 및 구성을 바탕으로 검증되어야 합니다.

참고

권장 컨텍스트 수는 설계에 따라 결정되는 문제이며 일부 경우 복제 최적화를 위해 데이터 분리를 선택할 때 이러한 분리가 미칠 수 있는 영향을 고려해야 합니다. 일반적으로 데이터는 데이터를 복제하는 방식에 대해 최적화되는 것이 아니라 데이터가 저장되는 방식에 대해 최적화됩니다. 따라서 백업 환경을 변경할 때는 이 점에 유의하십시오.

MTree 복제

*MTree 복제*는 DD 시스템 간에 **MTree**를 복제할 때 사용됩니다. 소스에 스냅샷이 정기적으로 생성되며, 디렉토리 복제에 사용된 것과 동일한 사이트 간 데이터 중복 제거 메커니즘을 활용하여 스냅샷 간의 차이점이 대상으로 전송됩니다. 이에 따라 대상의 데이터가 항상 파일 정합성이 보장되는 소스의 시점 복제본이 됩니다. 또한 데이터 변동의 복제도 줄어들기 때문에 **WAN** 활용의 효율성이 향상됩니다.

디렉토리 복제는 원본 디렉토리 내용의 모든 변경 내용을 순서대로 복제해야 하지만 **MTree** 복제와 함께 스냅샷을 사용하면 일부 중간 변경 내용을 건너뛸 수 있습니다. 이러한 변경 내용을 건너뛰면 네트워크를 통해 전송되는 데이터의 양이 줄어들어 복제 지연이 줄어듭니다.

MTree 복제를 사용하면 DD 시스템 하나가 동시에 한 복제 컨텍스트에서는 소스이고 다른 복제 컨텍스트에서는 대상일 수 있습니다. 또한 데이터를 복제하는 동안에도 DD 시스템이 백업 및 아카이브 애플리케이션에서 데이터를 수신할 수 있습니다.

MTree 복제는 관리되는 파일 복제(DD Boost에서 사용하는 유형)와 동일한 유연한 네트워크 구축 토폴로지와 사이트 간 데이터 중복 제거 효과를 갖고 있습니다.

MTree 복제를 사용할 때 추가로 고려할 몇 가지 사항은 다음과 같습니다.

- 복제가 초기화되면 대상 읽기 전용 MTree가 자동으로 생성됩니다.
- 데이터를 여러 MTree로 논리적으로 분할하여 복제 성능을 향상시킬 수 있습니다.
- 스냅샷은 소스 컨텍스트에 생성되어야 합니다.
- 스냅샷을 복제 대상에 생성할 수는 없습니다.
- 스냅샷은 1년이라는 고정된 보존 기간으로 복제되지만 이 기간은 대상에서 조정 가능하며 반드시 대상에서 조정해야 합니다.
- 복제 컨텍스트는 소스와 대상 모두에서 구성되어야 합니다.
- DD VTL 테이프 카트리지(또는 풀)는 DD VTL 테이프 카트리지가 포함된 MTree 또는 디렉토리를 복제하는 것을 의미합니다. 미디어 풀은 기본적으로 MTree 복제를 통해 복제됩니다. 미디어 풀을 이전 버전과의 호환성 모드에서 생성한 다음 디렉토리 기반 복제를 통해 복제할 수도 있습니다. 명령줄에서 pool:// 구문을 사용해 복제 컨텍스트를 생성할 수는 없습니다. DD System Manager에서 풀 기반 복제를 지정할 경우 미디어 풀 유형에 따라 디렉토리 또는 MTree 복제가 생성됩니다.
- MTree 아래의 디렉토리를 복제할 수 없습니다.
- 대상 DD 시스템에는 최소한 소스 MTree의 예상 최대 크기, 즉 압축 후 크기 이상의 가용 스토리지 용량이 있어야 합니다.
- 복제가 초기화된 후에는 대상 MTree의 소유권과 사용 권한이 항상 소스 MTree와 동일하게 유지됩니다. 컨텍스트가 구성된 경우 대상 MTree가 읽기 전용 상태로 유지되고 소스 MTree에서만 데이터를 수신할 수 있습니다.
- 전역 압축 방식의 차이로 인해 언제든 소스와 대상 MTree의 크기가 달라질 수 있습니다.
- DD Extended Retention을 사용하는 시스템에서 DD Extended Retention을 사용하지 않는 시스템으로 MTree 복제가 지원됩니다. 단, 두 시스템 모두 DD OS 5.5 이상을 실행하고 있어야 합니다.
- MTree 복제에서는 기본적으로 DD Retention Lock Compliance가 지원됩니다. 소스에 DD Retention Lock 라이선스가 있는 경우 대상에도 DD Retention Lock 라이선스가 있어야 합니다. 그렇지 않을 경우 복제가 실패합니다. (이 상황을 방지하려면 DD Retention Lock을 비활성화해야 합니다.) 복제 컨텍스트에 DD Retention Lock이 활성화된 경우 Retention Lock이 활성화된 데이터가 항상 복제된 대상 컨텍스트에 포함됩니다.

MTree 복제 세부 정보

MTree 복제에는 다음 단계가 포함됩니다.

1. 원본 복제 컨텍스트에서 스냅샷이 생성됩니다.
2. 이 스냅샷은 마지막 이전 스냅샷과 비교됩니다.
3. 두 스냅샷 간의 차이가 대상 복제 컨텍스트로 전송됩니다.
4. 대상에서 MTree가 업데이트되지만 대상 시스템에서 모든 변경 내용을 수신할 때까지 사용자에게 파일이 공개되지 않습니다.

이러한 단계는 스냅샷이 원본 MTree에서 생성될 때마다 반복됩니다. 다음 상황은 원본 시스템의 스냅샷 생성을 트리거합니다.

- 시스템 생성 주기적 스냅샷 - 복제 지연이 15분보다 길고 현재 복제 중인 스냅샷이 없습니다.
- 사용자 생성 스냅샷 - 사용자가 지정한 시간(예: 백업 작업이 완료된 이후).

다양한 스냅샷 유형의 상호 작용을 보여 주는 예제를 보려면 https://support.emc.com/kb/180832에서 KB 문서, *MTree 복제 작동 방식*을 참조하십시오.

스냅샷이 복제되면 대상에 대한 연결이 닫힙니다. 원본과 대상 간의 새 연결은 다음 스냅샷이 복제될 때 설정됩니다.

AMS(Automatic Multi-Streaming)

AMS(Automatic Multi-Streaming)는 MTree 복제 성능을 향상시킵니다. 다중 스트림을 사용하여 큰 단일 파일(32GB 이상)을 복제하여 복제 중에 네트워크 대역폭 활용도를 향상시킵니다. AMS는 개별 파일의 복제 속도를 높임으로써 복제 대기열의 파이프라인 효율성을 향상시키며 복제 처리량을 증가시키고 복제 지연을 감소시킵니다.

워크로드에 여러 최적화 옵션이 있는 경우 AMS는 자동으로 워크로드에 가장 적합한 옵션을 선택합니다. 예를 들어 워크로드가 fastcopy 속성이 있는 큰 파일인 경우 복제 작업은 fastcopy 최적화를 사용하여 복제 쌍 간에서 고유한 세그먼트를 식별하는 파일 스캔 오버헤드를 방지합니다. 워크로드가 신세틱을 사용하는 경우 복제는 AMS 상위에서 신세틱 복제를 사용하여 각 복제 스트림이 파일을 생성하도록 대상 시스템의 로컬 작업을 활용합니다.

AMS는 항상 활성화되며 비활성화할 수 없습니다.

컬렉션 복제

*컬렉션 복제*는 일대일 토폴로지로 전체 시스템 미러링을 수행하여 DD 파일 시스템의 모든 논리적 디렉토리와 파일을 포함해 기본 컬렉션의 변경 사항을 지속적으로 전송합니다.

컬렉션 복제는 다른 유형만큼 유연하지는 않지만 더 높은 처리량을 제공할 수 있으며 더 낮은 오버헤드로 더 많은 객체를 지원할 수 있어 대규모 엔터프라이즈 활용 사례에서 효과가 더 높을 수 있습니다.

컬렉션 복제에서는 소스 DD 시스템의 전체 `/data/col1` 영역을 대상 DD 시스템에 복제합니다.

참고

클라우드 계층이 활성화된 시스템에서는 컬렉션 복제가 지원되지 않습니다.

컬렉션 복제를 사용할 때 추가로 다음과 같은 몇 가지 사항을 고려하십시오.

- 세부적인 복제 제어는 불가능합니다. 모든 데이터는 소스에서 대상으로 복제되며 읽기 전용 복사본이 생성됩니다.
- 컬렉션 복제를 위해서는 대상 시스템의 스토리지 용량이 소스 시스템의 용량과 같거나 그보다 커야 합니다. 대상 용량이 소스 용량보다 적을 경우에는 소스에서 사용할 수 있는 용량이 대상의 용량으로 줄어듭니다.
- 컬렉션 복제 대상으로 사용되는 DD 시스템은 복제를 구성하기 전에 먼저 비어 있어야 합니다. 복제가 구성된 후에는 이 시스템이 소스 시스템의 데이터를 수신하는 용도로 사용됩니다.
- 컬렉션 복제를 사용할 경우 모든 사용자 계정과 암호가 소스에서 대상으로 복제됩니다. 그러나 DD OS 5.5.1.0부터는 구성의 다른 요소와 DD 시스템의 사용자 설정이 대상으로 복제되지 않으므로 복구 후에 명시적으로 재구성해야 합니다.
- 컬렉션 복제는 DD SMT(Secure Multitenancy)에서 지원됩니다. UUID가 일치하는 테넌트 및 테넌트 유닛 정의를 포함하여 레지스트리 네임스페이스에 포함된 핵심

SMT 정보가 복제 작업 중에 자동으로 전송됩니다. 하지만 다음과 같은 SMT 정보는 복제에 자동으로 포함되지 않으므로 대상 시스템에서 수동으로 구성해야 합니다.

- 각 테넌트 유닛에 대한 알림 목록
- DD Boost가 시스템에 구성되어 있는 경우 SMT 테넌트가 사용할 수 있도록 DD Boost 프로토콜에 할당된 모든 사용자
- DD Boost가 시스템에 구성되어 있는 경우 각 DD Boost 사용자와 관련된 기본 테넌트 유닛(있는 경우)

SMT를 사용한 재해 복구에 컬렉션 복제 사용(450페이지)에서는 복제 대상에서 이러한 항목을 수동으로 구성하는 방법에 대해 설명합니다.

- DD Retention Lock Compliance는 컬렉션 복제를 지원합니다.
- 클라우드 계층을 사용하는 시스템에서는 컬렉션 복제가 지원되지 않습니다.
- 컬렉션 복제를 사용하면 복제되지 않은 소스 시스템의 복제 컨텍스트에 있는 데이터를 파일 시스템 정리를 위해 처리할 수 없습니다. 소스 및 대상 시스템이 동기화되지 않아 파일 시스템 정리를 완료할 수 없는 경우 시스템은 정리 작업의 상태를 `partial`로 보고하며 정리 작업에 대해 제한적인 시스템 상태 통계만 사용할 수 있습니다. 컬렉션 복제를 비활성화하면 복제 소스 및 대상 시스템이 동기화되지 않은 상태로 유지되기 때문에 파일 시스템 정리에서 처리할 수 없는 데이터의 양이 증가합니다. KB 문서 *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*에서 자세한 정보를 제공하며, 이 문서는 온라인 지원 사이트(https://support.emc.com)에서 사용할 수 있습니다.
- 고대역폭 환경에서 처리량을 향상시키려면 **`replication modify <destination> crepl-gc-gw-optim`** 명령을 실행하여 컬렉션 복제 대역폭 최적화를 비활성화하십시오.

DD Replicator에서 DD Encryption 사용

DD Replicator와 선택 사항인 *DD Encryption* 기능을 함께 사용하면 암호화된 데이터를 컬렉션 복제, 디렉토리 복제 또는 MTree 복제 기능을 사용하여 복제할 수 있습니다.

복제 컨텍스트는 항상 *공유 암호*를 사용하여 인증됩니다. 이 공유 암호는 Diffie-Hellman 키 교환 프로토콜을 사용하여 세션 키를 설정하는 데 사용되며, 이 세션 키는 해당되는 경우 Data Domain 시스템 암호화 키를 암호화하고 해독하는 데 사용됩니다.

각 복제 유형은 암호화와 고유하게 작동하며 동일한 수준의 보안을 제공합니다.

- *컬렉션 복제*를 사용하려면 대상 데이터가 소스 데이터와 정확히 일치하는 복제본이어야 하므로 소스와 대상의 암호화 구성이 동일해야 합니다. 특히 소스와 대상 모두에서 암호화 기능이 설정되거나 해제되어야 하며, 암호화 기능이 설정된 경우에는 암호화 알고리즘과 시스템 암호도 일치해야 합니다. 매개 변수는 복제 연결 단계에서 확인됩니다.
  컬렉션 복제 중에 소스는 암호화된 형식으로 데이터를 전송하고 암호화 키도 대상에 전송합니다. 대상에 동일한 암호 및 시스템 암호화 키가 있으므로 대상에서 데이터를 복구할 수 있습니다.

  참고

  클라우드 계층이 활성화된 시스템에서는 컬렉션 복제가 지원되지 않습니다.

- *MTree 복제 또는 디렉토리 복제*의 경우에는 암호화 구성이 소스와 대상 모두에서 동일하지 않아도 됩니다. 대신 소스와 대상이 복제 연결 단계 중에 대상의 암호화 키를 안전하게 교환하며, 데이터가 대상의 암호화 키를 사용하여 소스에서 다시 암호화된 후 대상에 전송됩니다.

대상의 암호화 구성이 다른 경우에는 전송되는 데이터가 적절하게 준비됩니다. 예를 들어 암호화 기능이 대상에서 해제된 경우 소스는 데이터를 해독하여 암호화되지 않은 상태로 대상에 전송합니다.

- *다중 구간(Cascaded) 복제* 토폴로지에서는 복제본이 세 Data Domain 시스템 간에 체인으로 연결됩니다. 체인의 마지막 시스템은 컬렉션, MTree 또는 디렉토리로 구성할 수 있습니다. 마지막 시스템이 컬렉션 복제 대상인 경우, 동일한 암호화 키와 암호화된 데이터를 소스로 사용합니다. 마지막 시스템이 MTree 또는 디렉토리 복제 대상인 경우에는 자체 키를 사용하고 데이터가 소스에서 암호화됩니다. 각 링크에서 대상의 암호화 키가 암호화에 사용됩니다. 체인으로 연결된 시스템에 대한 암호화는 복제 페어의 경우처럼 작동합니다.

복제 토폴로지

DD Replicator는 일대일, 일대일 양방향, 일대다, 다대일 및 다단계(Cascaded)의 다섯 가지 복제 토폴로지를 지원합니다. 이 섹션의 표에는 (1) 세 가지 유형의 복제(MTree, 디렉토리 및 컬렉션)와 두 가지 유형의 DD 시스템[SN(Single Node) 및 DD Extended Retention]에서 이러한 토폴로지가 작동하는 방식과 (2) 다단계(Cascaded) 복제에서의 혼합 토폴로지 지원 방식이 나열되어 있습니다.

일반 정보:

- SN(Single Node) 시스템은 모든 복제 토폴로지를 지원합니다.
- 단일 노드 간 복제(SN -> SN)는 모든 복제 유형에 사용할 수 있습니다.
- DD Extended Retention 시스템은 디렉토리 복제의 소스가 될 수 없습니다.
- 컬렉션 복제는 SN(Single Node) 시스템에서 DD Extended Retention을 사용하는 시스템으로의 복제 또는 DD Extended Retention 활성화 시스템에서 SN 시스템으로의 복제로 구성될 수 없습니다.
- 컬렉션 복제는 SN 시스템에서 DD 고가용성 지원 시스템으로 또는 DD 고가용성 지원 시스템에서 SN 시스템으로 구성할 수 없습니다.
- MTtree 및 디렉토리 복제의 경우 DD 고가용성 시스템은 SN 시스템과 동일하게 취급됩니다.
- 두 시스템 중 하나 또는 둘 모두에 Cloud Tier가 활성화된 경우 컬렉션 복제를 구성할 수 없습니다.

이 표에 사용된 약어의 의미는 다음과 같습니다.

- SN = 단일 노드 DD 시스템(DD Extended Retention 없음)
- ER = DD Extended Retention 시스템

표 188 복제 유형 및 DD 시스템 유형별 지원 토폴로지

토폴로지	MTree 복제	디렉토리 복제	컬렉션 복제
일대일	{SN | ER} -> {SN | ER} ER->SN[5.5 릴리즈부터 지원됨, 5.5 이전 버전에서는 복구만 가능]	SN -> SN SN -> ER	SN -> SN ER -> ER
일대일 양방향	{SN | ER} -> {SN | ER}	SN -> SN	지원되지 않음

표 188 복제 유형 및 DD 시스템 유형별 지원 토폴로지 (계속)

토폴로지	MTree 복제	디렉토리 복제	컬렉션 복제
일대다	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	지원되지 않음
다대일	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	지원되지 않음
다단계	{SN | ER } -> {SN | ER} -> {SN | ER}	SN -> SN -> SN SN -> SN -> ER	ER -> ER -> ER SN -> SN -> SN

다단계 복제는 다단계 연결의 두 번째 단계가 연결의 첫 번째 유형과 다른 혼합 토폴로지를 지원합니다(예: A -> B는 디렉토리 복제이고 B -> C는 컬렉션 복제).

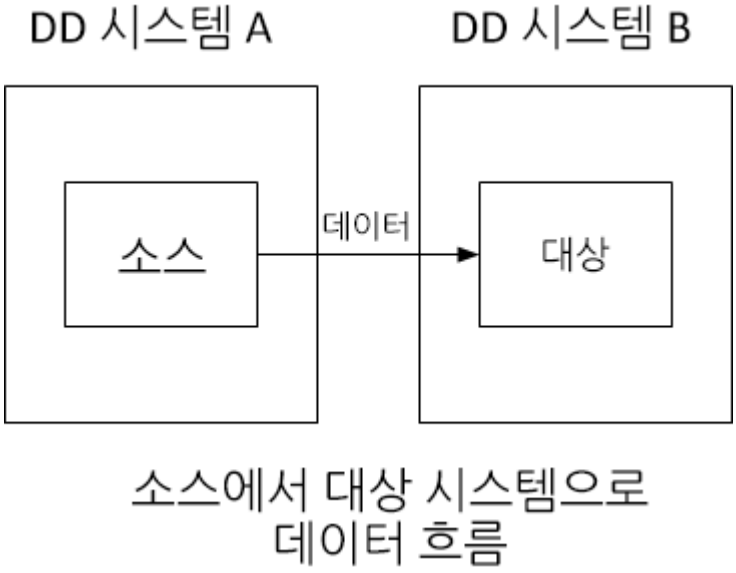
표 189 다단계 복제에서 지원되는 혼합 토폴로지

혼합 토폴로지	
SN – 디렉토리 복제 -> ER – MTree 복제 -> ER – MTree 복제	SN – 디렉토리 복제 -> ER – 컬렉션 복제 -> ER – 컬렉션 복제
SN – MTree 복제 -> SN – 컬렉션 복제 -> SN – 컬렉션 복제	SN – MTree 복제 -> ER – 컬렉션 복제 -> ER – 컬렉션 복제

일대일 복제

가장 간단한 복제 유형은 DD 소스 시스템으로부터 DD 대상 시스템으로 복제하는 것으로, *일대일* 복제 페어라고 합니다. 이 복제 토폴로지는 디렉토리, MTree 또는 컬렉션 복제 유형으로 구성할 수 있습니다.

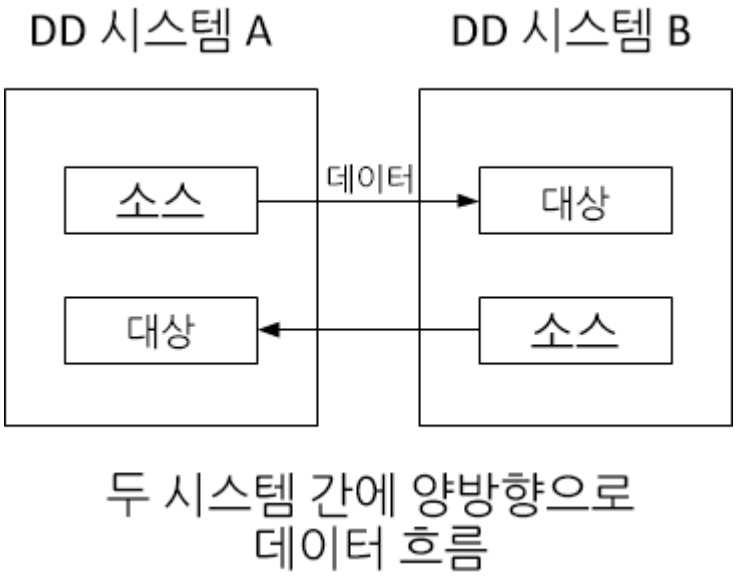
그림 18 일대일 복제 페어



양방향 복제

양방향 복제 페어에서는 DD 시스템 A에 있는 디렉토리 또는 MTree의 데이터가 DD 시스템 B에 복제되고, DD 시스템 B에 있는 MTree 또는 또 다른 디렉토리의 데이터가 DD 시스템 A로 복제됩니다.

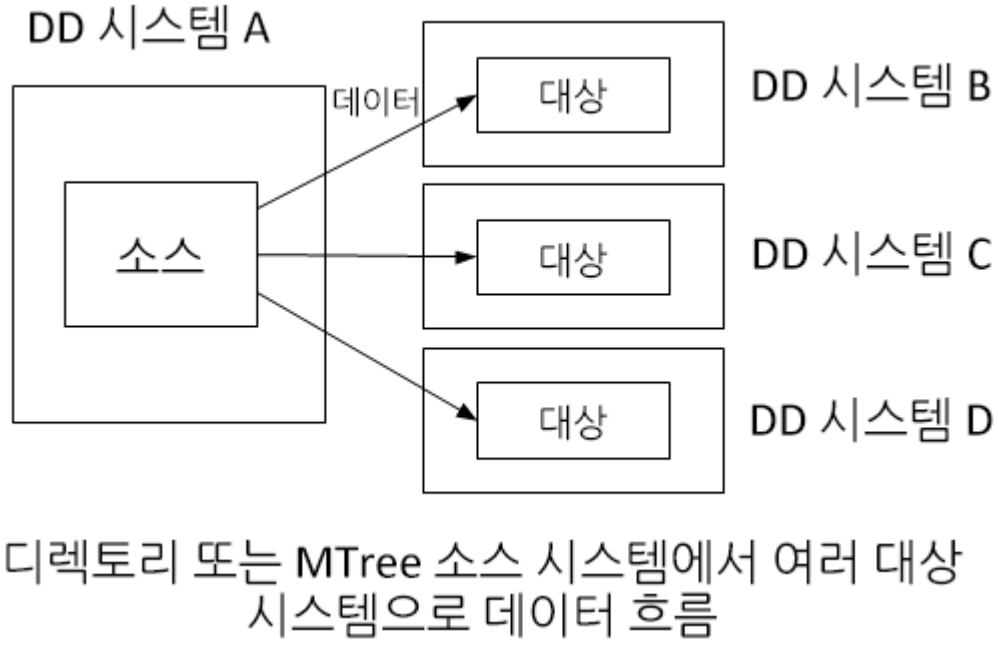
그림 19 양방향 복제



일대다 복제

일대다 복제에서는 한 DD 시스템에 있는 소스 디렉토리 또는 MTree의 데이터가 여러 대상 DD 시스템으로 이동합니다. 이 복제 유형을 사용하여 두 개 이상의 복제본을 생성함으로써 데이터 보호를 향상시키거나 여러 사이트에서 사용할 수 있도록 데이터를 배포할 수 있습니다.

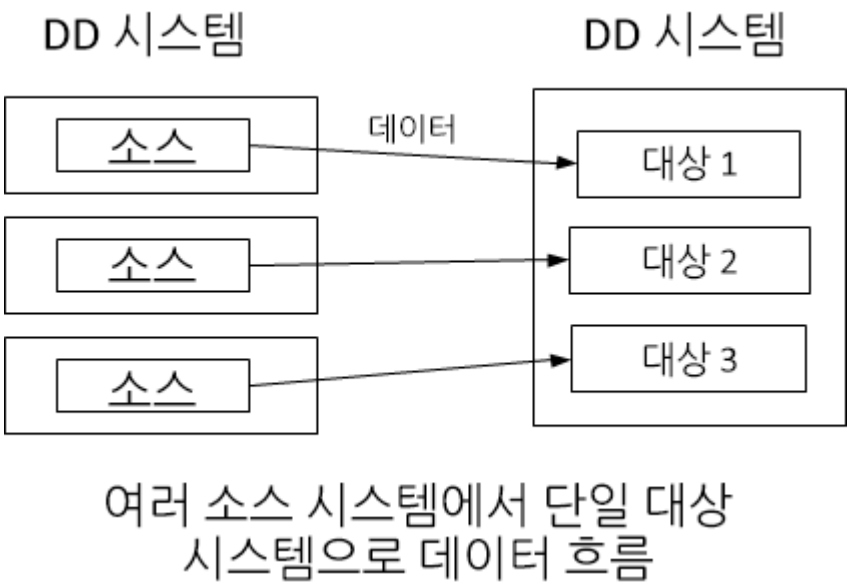
그림 20 일대다 복제



다대일 복제

다대일 복제에서는 MTree 또는 디렉토리에 상관없이 복제 데이터가 여러 소스 DD 시스템에서 단일 대상 DD 시스템으로 흐릅니다. 이 복제 유형은 본사의 IT 시스템에서 여러 지사 사무소에 데이터 복구 기능을 제공하는 데 사용할 수 있습니다.

그림 21 다대일 복제

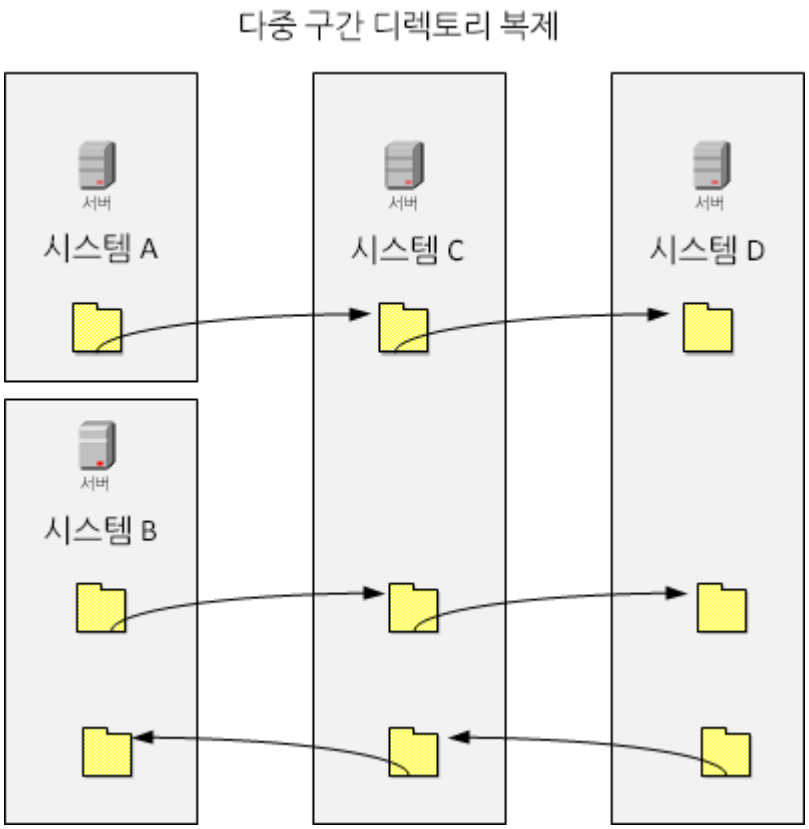


다중 구간(Cascaded) 복제

다중 구간 복제 토폴로지에서는 소스 디렉토리 또는 MTree가 세 DD 시스템 간에 체인으로 연결됩니다. 체인의 마지막 홉은 소스가 디렉토리인지 또는 MTree인지에 따라 컬렉션, MTree 또는 디렉토리 복제로 구성할 수 있습니다.

예를 들어 DD 시스템 A는 하나 이상의 MTree를 DD 시스템 B에 복제하고 DD 시스템 B는 해당 MTree를 DD 시스템 C에 복제합니다. DD 시스템 B의 Mtree는 대상(DD 시스템 A의 대상)이자 소스(DD 시스템 C의 소스)입니다.

그림 22 다중 구간 디렉토리 복제



성능이 저하되지 않은 복제 페어 컨텍스트로부터 데이터 복구를 수행할 수 있습니다. 예를 들면 다음과 같습니다.

- DD 시스템 A에 복구가 필요한 경우 DD 시스템 B에서 데이터를 복구할 수 있습니다.
- DD 시스템 B에 복구가 필요한 경우에는 DD 시스템 A에서 (교체용) DD 시스템 B로 복제 재동기화를 수행하는 것이 가장 간단한 방법입니다. 이 경우 DD 시스템 B에서 DD 시스템 C로의 복제 컨텍스트를 먼저 분리해야 합니다. DD 시스템 A에서 DD 시스템 B로 복제 컨텍스트가 재동기화를 완료한 후, DD 시스템 B에서 DD 시스템 C로 새 컨텍스트를 구성하고 재동기화해야 합니다.

복제 관리

DD System Manager(Data Domain System Manager) 또는 DD OS(Data Domain Operating System) CLI(Command Line Interface)를 사용하여 복제를 관리할 수 있습니다.

GUI(Graphical User Interface)를 사용하여 복제를 관리하려면 DD System Manager에 로그인합니다.

절차

1. DD System Manager 왼쪽의 메뉴에서 **Replication**을 선택합니다. 아직 라이센스가 추가되지 않은 경우 **Add License**를 선택합니다.
2. **Automatic** 또는 **On-Demand**를 선택합니다. On-Demand를 선택할 경우 DD Boost 라이센스가 있어야 합니다.

   CLI 절차

   CLI에서 로그인할 수도 있습니다.

   ```
   login as: sysadmin
   Data Domain OS 6.0.x.x-12345
   Using keyboard-interactive authentication.
   Password:
   ```

Replication Status

*Replication Status*는 경고(노란색 텍스트) 또는 오류(빨간색 텍스트) 상태를 나타내는 시스템 전체의 복제 컨텍스트 수 또는 조건이 정상인지 여부를 표시합니다.

Summary 보기

Summary 보기에는 DD 시스템에 대해 구성된 복제 컨텍스트가 나열되고 선택한 DD 시스템에 대해 집계된 정보, 즉 인바운드 및 아웃바운드 복제 페어에 대한 요약 정보가 표시됩니다. 중점 대상은 DD 시스템 자체와 이 시스템에 대한 입력과 출력입니다.

Summary 표는 Source 또는 Destination 이름을 입력하거나 State(Error, Warning 또는 Normal)를 선택하여 필터링할 수 있습니다.

표 190 Replication Summary 보기

항목	설명
Source	*system.path* 형식을 가진 소스 컨텍스트의 시스템 및 경로 이름입니다. 예를 들어 `system dd120-22`의 `dir1` 디렉토리에 대해 `dd120-22.chaos.local/data/col1/dir1`이 표시됩니다.
Destination	*system.path* 형식을 가진 대상 컨텍스트의 시스템 및 경로 이름입니다. 예를 들어 `system dd120-44`의 `MTree1` MTree에 대해 `dd120-44.chaos.local/data/col1/MTree1`이 표시됩니다.
Type	컨텍스트의 유형으로, MTree, 디렉토리(Dir) 또는 Pool입니다.
State	복제 페어의 가능한 상태에는 다음이 포함됩니다. • Normal – 복제본이 Initializing, Replicating, Recovering, Resyncing 또는 Migrating인 경우. • Idle – MTree 복제의 경우 복제 프로세스가 현재 활성 상태가 아니거나 대상 시스템에 액세스할 수 없는 등의 네트워크 오류가 발생하면 이 상태가 표시될 수 있습니다. • Warning – 처음 5가지 상태에 대한 비정상적인 지연이 있거나 Uninitialized 상태인 경우.

표 190 Replication Summary 보기 (계속)

항목	설명
	• Error – Disconnected와 같은 모든 가능한 오류 상태.
Synced As Of Time	소스에서 수행하는 마지막 자동 복제 동기화 작업에 대한 타임 스탬프입니다. MTree 복제의 경우 스냅샷이 대상에 노출될 때 이 값이 업데이트됩니다. 디렉토리 복제의 경우에는 소스에서 삽입한 동기화 지점이 적용될 때 이 값이 업데이트됩니다. unknown 값이 복제 초기화 중에 표시됩니다.
Pre-Comp Remaining	복제될 나머지 압축 전 데이터의 양입니다.
Completion Time (Est.)	값은 `Completed`이거나, 지난 24시간의 전송 속도를 기준으로 복제 데이터 전송을 완료하는 데 필요한 예상 시간입니다.

복제 컨텍스트의 세부 정보

Summary 보기에서 복제 컨텍스트 하나를 선택하면 Detailed Information, Performance Graph, Completion Stats 및 Completion Predictor의 컨텍스트 정보가 입력됩니다.

표 191 Detailed Information

항목	설명
State Description	복제본의 상태에 대한 메시지입니다.
원본	`system.path` 형식으로 된 소스 컨텍스트의 시스템 및 경로 이름입니다. 예를 들어 `dir1` 디렉토리가 시스템 `dd120-22`에 있는 경우 `dd120-22.chaos.local/data/col1/dir1`이 표시됩니다.
대상	`system.path` 형식으로 된 대상 컨텍스트의 시스템 및 경로 이름입니다. 예를 들어 `MTree1` MTree가 시스템 `dd120-44`에 있는 경우 `dd120-44.chaos.local/data/col1/MTree1`이 표시됩니다.
Connection Port	복제 접속에 사용되는 시스템 이름과 수신 포트입니다.

표 192 Performance Graph

항목	설명
Pre-Comp Remaining	복제해야 할 남은 압축 전 데이터입니다.
Pre-Comp Written	소스에 기록된 압축 전 데이터입니다.
Post-Comp Replicated	복제된 압축 후 데이터입니다.

표 193 Completion Stats

항목	설명
Synced As Of Time	소스에서 수행하는 마지막 자동 복제 동기화 작업에 대한 타임 스탬프입니다. MTree 복제의 경우 스냅샷이 대상에 노출될 때 이 값이 업데이트됩니다. 디렉토리 복제의 경우에는 소스에서 삽입한 동

표 193 Completion Stats (계속)

항목	설명
	기화 지점이 적용될 때 이 값이 업데이트됩니다. unknown 값이 복제 초기화 중에 표시됩니다.
Completion Time (Est.)	값은 `Completed`이거나, 지난 24시간의 전송 속도를 기준으로 복제 데이터 전송을 완료하는 데 필요한 예상 시간입니다.
Pre-Comp Remaining	복제해야 할 남은 데이터의 양입니다.
Files Remaining	(디렉토리 복제만 해당) 아직 복제되지 않은 파일의 수입니다.
상태	소스 및 대상 엔드포인트의 경우 다음과 같이 시스템에 있는 주요 구성 요소의 상태(Enabled, Disabled, Not Licensed 등)를 표시합니다. • 복제 • 파일 시스템 • DD Retention Lock • 저장된 데이터 DD 암호화 • 회선을 통한 DD 암호화 • 사용 가능한 용량 • Low Bandwidth Optimization • 압축률 • 저대역폭 최적화 비율

Completion Predictor
Completion Predictor는 백업 작업의 진행률을 추적하고 선택한 컨텍스트에 대한 복제가 완료될 시점을 예측하는 위젯입니다.

복제 페어 생성

복제 페어를 생성하기 전에 대상이 *없는지* 확인하십시오. 대상이 있는 경우 오류가 발생합니다.

절차

1. **Replication** > **Automatic** > **Summary 탭** > **Create Pair**를 선택합니다.
2. Create Pair 대화 상자에서 다음 섹션에 설명된 대로 정보를 추가해 인바운드 또는 아웃바운드 MTree, 디렉토리, 컬렉션 또는 풀 복제 페어를 생성합니다.

복제를 위한 DD 시스템 추가

복제 페어를 생성하려면 먼저 DD 시스템을 호스트 또는 대상으로 추가해야 할 수 있습니다.

참고

추가하는 시스템에서 호환되는 DD OS 버전이 실행되고 있는지 확인하십시오.

절차

1. Create Pair 대화 상자에서 Add System을 선택합니다.
2. System에 추가할 시스템의 호스트 이름 또는 IP 주소를 입력합니다.

3. User Name 및 Password에 sysadmin의 사용자 이름과 암호를 입력합니다.
4. 또는 **More Options**를 선택해 직접 연결할 수 없는 시스템의 프록시 IP 주소(또는 시스템 이름)를 입력합니다. 구성된 경우 기본 포트 3009 대신 사용자 지정 포트를 입력합니다.

   참고

   IPv6 주소는 DD OS 5.5 이상을 사용해 관리 시스템에 DD OS 5.5 이상의 시스템을 추가할 경우에만 지원됩니다.

5. **OK**를 선택합니다.

   참고

   DD System Manager에 시스템을 추가한 후 시스템에 연결할 수 없는 경우 관리하는 시스템에서 추가 중인 시스템까지 라우트가 있는지 확인합니다. 호스트 이름(FQDN(Fully Qualified Domain Name) 또는 비 FQDN)을 입력할 경우 관리 대상 시스템에서 확인 가능해야 합니다. 관리 대상 시스템에 대해 도메인 이름을 구성하거나, 시스템에 대한 DNS 항목이 있는지 확인하거나, 호스트 이름 매핑에 대한 IP 주소가 정의되었는지 확인합니다.

6. 시스템 인증서가 검증되지 않은 경우 Verify Certificate 대화 상자에 인증서에 대한 자세한 정보가 표시됩니다. 시스템 자격 증명을 확인합니다. 인증서를 신뢰할 경우 **OK**를 선택하거나 **Cancel**을 선택합니다.

컬렉션 복제 페어 생성

이 유형의 복제에 대한 일반적인 정보는 *컬렉션 복제* 섹션을 참조하십시오.

컬렉션 복제 페어를 생성하기 전에 다음 사항에 유의하십시오.

- 대상 시스템의 스토리지 용량은 소스 시스템의 스토리지 용량보다 크거나 같습니다. 대상 용량이 소스의 용량보다 작을 경우 소스에서 사용 가능한 용량은 대상의 용량으로 줄어듭니다.
- 대상은 제거된 후 다시 생성되었지만, 설정되지는 않았습니다.
- 각 대상과 소스는 한 번에 한 가지 컨텍스트에서만 존재합니다.
- 소스에서 암호를 구성하고 설정하는 동안 복제본의 파일 시스템은 해제됩니다.
- 복제본에서 암호화를 구성하고 설정하는 동안 소스의 파일 시스템은 해제됩니다.

절차

1. Create Pair 대화 상자의 **Replication Type** 메뉴에서 **Collection**을 선택합니다.
2. **Source System** 메뉴에서 소스 시스템 호스트 이름을 선택합니다.
3. **Destination System** 메뉴에서 대상 시스템 호스트 이름을 선택합니다. 목록에는 DD-Network 목록의 호스트만 포함되어 있습니다.
4. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
5. **OK**를 선택합니다. 소스에서 대상으로 복제가 시작됩니다.

결과

Data Domain에서 테스트한 결과 복제 초기화에 대해 다음과 같은 성능 지침이 설정되었습니다. 아래의 내용은 *단지* 지침일 뿐이며 운영 환경에서 나타나는 실제 성능은 다를 수 있습니다.

- 기가비트 LAN을 통한 복제의 경우: 최대 입출력과 이상적인 조건을 생성하는 데 충분한 많은 수의 셸프가 있으면 컬렉션 복제가 플랫폼에 따라 1GigE 링크(모듈로

10% 프로토콜 오버헤드)를 포화시킬 수 있으며 10gigE에서 400-900MB/sec에 이를 수 있습니다.

- WAN을 통한 복제의 경우: 성능이 WAN 링크 회선 속도, 대역폭, 지연 시간 및 패킷 손실율에 의해 제어됩니다.

MTree, 디렉토리 또는 풀 복제 페어 생성

이러한 유형의 복제에 대한 일반 정보는 *MTree 복제* 및 *디렉토리 복제* 섹션을 참조하십시오.

MTree, 디렉토리 또는 풀 복제 페어를 생성할 때는 다음을 확인하십시오.

- 복제 작업이 올바른 인터페이스를 통해 전송되고 종료되는지 확인하십시오. 복제 컨텍스트를 정의할 때 소스 및 대상의 호스트 이름은 정방향 및 역방향 조회를 통해 확인되어야 합니다. 시스템의 기본 확인 인터페이스가 아닌 대체 인터페이스를 통해 데이터를 전송하려면 복제 컨텍스트를 생성한 후 수정해야 합니다. 확인 이외의 (크로스오버) 인터페이스에서 컨텍스트가 정의되도록 하려면 호스트 파일을 설정해야 할 수 있습니다.
- MTree 복제의 컨텍스트를 반대로 "전환"할 수 있습니다. 즉, 대상과 소스를 바꿀 수 있습니다.
- MTree 전체가 복제되지 않으므로 MTree 내의 하위 디렉토리를 복제할 수 없습니다.
- DD Extended Retention을 사용하는 시스템과 기타 시스템에서 모두 DD OS 5.5 이상을 실행 중인 경우 DD Extended Retention을 사용하는 시스템에서 기타 시스템으로의 MTree 복제가 지원됩니다.
- 대상 DD 시스템에는 최소한 소스 디렉토리 또는 MTree의 예상 최대 크기, 즉 압축 후 크기 이상의 가용 스토리지 용량이 있어야 합니다.
- 복제가 초기화되면 대상 디렉토리가 자동으로 생성됩니다.
- DD 시스템 하나가 동시에 한 컨텍스트에서는 소스이고 다른 컨텍스트에서는 대상일 수 있습니다.

절차

1. Create Pair 대화 상자의 **Replication Type** 메뉴에서 **Directory**, **MTree**(기본값) 또는 **Pool**을 선택합니다.
2. **Source System** 메뉴에서 소스 시스템 호스트 이름을 선택합니다.
3. **Destination System** 메뉴에서 대상 시스템 호스트 이름을 선택합니다.
4. **Source Path** 입력란에 소스 경로를 입력합니다. 이때 경로의 첫 부분은 선택한 복제의 유형에 따라 바뀌는 상수입니다.
5. **Destination Path** 입력란에 대상 경로를 입력합니다. 이때 경로의 첫 부분은 선택한 복제의 유형에 따라 바뀌는 상수입니다.
6. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
7. **OK**를 선택합니다.

   소스에서 대상으로 복제가 시작됩니다.

   Data Domain에서의 테스트 결과가 복제 초기화에 필요한 시간 예상에 대해 다음과 같은 지침을 반환합니다.

   이는 *오직* 지침용으로만 제공되며, 특정 운영 환경에서는 정확하지 않을 수 있습니다.

   - 100ms WAN의 T3 접속을 사용할 경우 성능은 압축 전 데이터의 약 40MiB/sec이며 다음과 같은 데이터 전송 속도를 제공합니다.
     40MiB/sec = 25초/GiB = 3.456TiB/day

- 기가비트 LAN의 2진 표기법을 사용할 경우 성능은 압축 전 데이터의 경우 약 80MiB/sec이며 T3 WAN의 약 2배에 달하는 데이터 전송 속도를 제공합니다.

예제 2 CLI 절차

다음은 CLI에서 MTree 복제 페어를 생성하는 예입니다. 이 예제에서는 원본 Data Domain 시스템이 **dd640**이고 대상 Data Domain 시스템이 **dlh5**입니다. 다른 시나리오에서의 사용에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

1. 원본 Data Domain 시스템에 MTree를 생성합니다.

```
sysadmin@dd640# mtree create /data/col1/Oracle2
MTree "/data/col1/Oracle2" created successfully.
```

2. 전체 호스트 이름을 사용하여 대상 Data Domain 시스템에서 복제 컨텍스트를 생성합니다.

```
sysadmin@dlh5# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

3. 전체 호스트 이름을 사용하여 원본 Data Domain 시스템에서 복제 컨텍스트를 생성합니다.

```
sysadmin@dd640# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

4. MTree 복제 컨텍스트가 생성되었는지 확인하려면 `replication show config` 명령을 사용합니다.
   이 예제에서는 출력이 가로로 잘립니다.

```
sysadmin@dlh5# replication show config
CTX  Source                                          Destination
---  ----------------------------------------------
-----------------------------------------
1    dir://dd640.chaos.local/backup/Oracle2          dir://dlh5.chaos.local/backup/
Oracle2
2    mtree://dd640.chaos.local/data/col1/Oracle2     mtree://dlh5.chaos.local/data/col1/
Oracle2
---  ----------------------------------------------
-----------------------------------------
 * Used for recovery only.
```

5. 소스와 대상 간의 복제를 시작하려면 명령을 `replication initialize` 소스에서 사용합니다. 이 명령 옵션은 구성과 접속이 올바른지 확인하고 문제가 발생하는 경우 오류 메시지를 반환합니다.

```
sysadmin@dd640# replication initialize mtree://dlh5.chaos.local/data/col1/Oracle2
 (00:08) Waiting for initialize to start...
 (00:10) Intialize started.
 Use 'replication watch mtree://dlh5.chaos.local/data/col1/Oracle2' to monitor progress.
```

양방향 복제 구성
양방향 복제 페어를 생성하려면 호스트 A에서 호스트 B로의 디렉토리 또는 MTree 복제 페어 절차(예: mtree2 사용)를 사용합니다. 동일한 절차를 사용하여 호스트 B에서 호스트 A로의 복제 페어(예: mtree1 사용)를 생성합니다. 이 구성에서 대상 경로 이름은 동일할 수 없습니다.

일대다 복제 구성
일대다 복제 페어를 생성하려면 호스트 A에서 다음으로의 디렉토리 또는 MTree 복제 페어 절차(예: mtree1 사용)를 사용합니다. (1) 호스트 B의 mtree1, (2) 호스트 C의 mtree1 및 (3) 호스트 D의 mtree1. 소스 컨텍스트의 경로가 다른 컨텍스트의 소스 경로인 경우 해당 소스 컨텍스트로의 복제 복구를 수행할 수 없습니다. 다른 컨텍스트를 분리하고 복구 후에 재동기화해야 합니다.

다대일 복제 구성
다대일 복제 페어를 생성하려면 디렉토리 또는 MTree 복제 페어 절차를 사용합니다. 예를 들어 (1) 호스트 A의 mtree1과 호스트 C의 mtree1 간에 복제 페어를 생성하고, (2) 호스트 B의 mtree2와 호스트 C의 mtree2 간에 복제 페어를 생성합니다.

다중 구간(Cascaded) 복제 구성
다중 구간(Cascaded) 복제 페어를 생성하려면 디렉토리 또는 MTree 복제 페어 생성 절차를 따르십시오. (1) 호스트 A의 mtree1과 호스트 B의 mtree1 간 페어 생성 (2) 호스트 B의 mtree1과 호스트 C의 mtree1 간 페어 생성. 최종 대상 컨텍스트(이 예에서는 호스트 C임. 하지만 3개 이상의 홉이 지원됨)는 컬렉션 복제나 디렉토리 또는 MTree 복제본이 될 수 있습니다.

복제 페어 해제 및 설정

복제 페어를 일시적으로 해제하면 소스와 대상 간의 활성 데이터 복제가 일시 중지됩니다. 소스에서 대상으로의 데이터 전송이 중지되고 대상에서 소스에 대한 활성 접속을 더 이상 지원하지 않습니다.

절차

1. Summary 테이블에서 하나 이상의 복제 페어를 선택하고 **Disable Pair**를 선택합니다.
2. Display Pair 대화 상자에서 **Next**와 **OK**를 차례로 선택합니다.
3. 해제된 복제 페어의 작동을 재개하려면 Summary 테이블에서 하나 이상의 복제 페어를 선택하고 **Enable Pair**를 선택해 Enable Pair 대화 상자를 표시합니다.
4. **Next**와 **OK**를 차례로 선택합니다. 데이터 복제가 재개됩니다.

CLI 절차

```
# replication disable {destination | all}

# replication enable {destination | all}
```

복제 페어 삭제

디렉토리 또는 MTree 복제 페어가 삭제되면 각각 대상 디렉토리 또는 MTree가 쓰기 가능한 상태가 됩니다. 컬렉션 복제 페어가 삭제되면 대상 DD 시스템이 독립 실행형 읽기/쓰기 시스템이 되고 파일 시스템이 해제됩니다.

절차

1. Summary 표에서 하나 이상의 복제 페어를 선택하고 **Delete Pair**를 선택합니다.
2. Delete Pair 대화 상자에서 **Next**를 선택한 다음 **OK**를 선택합니다. 복제 페어가 삭제됩니다.

CLI 절차
이 명령을 실행하기 전에 항상 `filesys disable` 명령을 실행하십시오. 그 후에 `filesys enable` 명령을 실행합니다.

```
# replication break {destination | all}
```

문제를 해결하기 위해 복제를 다시 동기화해야 하는 특정 상황이 발생할 수 있습니다. 복제를 중단하고 다시 동기화하는 방법에 대한 내용은 https://support.emc.com/kb/180668에서 *디렉토리 복제 중단 및 다시 동기화* KB 문서를 참조하십시오.

호스트 접속 설정 변경

특정 포트의 트래픽을 전달하려면 이전에 로컬 호스트 파일에 정의된 호스트 이름을 사용하는 접속 호스트 매개 변수를 대체 시스템에 대한 것으로 변경하여 현재 컨텍스트를

수정하십시오. 여기서 호스트 이름은 대상에 해당합니다. 호스트 항목은 해당 호스트의 대체 대상 주소를 나타냅니다. 소스와 대상 시스템 모두에서 이 작업을 수행해야 할 수 있습니다.

절차

1. Summary 테이블에서 복제 페어를 선택하고 **Modify Settings**를 선택합니다. **Advanced** 탭을 선택해 Create Pair, Start Resync 또는 Start Recover를 수행할 때에도 이러한 설정을 변경할 수 있습니다.
2. Modify Connection Settings 대화 상자에서 다음 설정 중 하나 또는 모두를 수정합니다.

   a. **Use Low Bandwidth Optimization** - 데이터 세트의 크기가 작고 6Mb/s 이하의 네트워크 대역폭을 보유한 기업에서는 DD Replicator의 *저대역폭 최적화*를 사용하여 전송할 데이터 양을 더욱 줄일 수 있습니다. 따라서 대역폭이 제한된 원격 사이트의 경우 대역폭 사용량을 줄이거나 기존 네트워크를 통해 더 많은 데이터를 복제하고 보호할 수 있습니다. 저대역폭 최적화는 소스와 대상 DD 시스템 모두에 활성화되어야 합니다. 소스와 대상의 저대역폭 최적화 설정이 일치하지 않으면 해당 컨텍스트의 저대역폭 최적화가 비활성화됩니다. 소스 및 대상에서 저대역폭 최적화를 활성화하면 두 시스템 모두 기존 데이터를 준비하기 위해 전체 정리 사이클을 거쳐야 하므로 두 시스템 모두에서 `filesys clean start`를 실행하십시오. 정리 사이클 기간은 DD 시스템에 있는 데이터의 양에 따라 다르지만 일반적인 정리보다 시간이 더 오래 걸립니다. `filesys` 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

   중요: DD Extended Retention 소프트웨어 옵션이 어느 한 DD 시스템에 활성화되어 있는 경우에는 저대역폭 최적화가 지원되지 않습니다. 컬렉션 복제의 경우에도 지원되지 않습니다.

   b. **Enable Encryption Over Wire** – DD Replicator는 ADH-AES256-GCM-SHA384 및 DHE-RSA-AES256-GCM-SHA384 암호 그룹을 통해 보안 복제 접속을 활성화하는 표준 SSL(Secure Socket Layer) 프로토콜 버전 1.0.1을 사용해 이동 중인 데이터의 암호화를 지원합니다. 접속하는 양쪽 모두에서 이 기능이 활성화되어 있어야만 암호화가 진행됩니다.

   c. **Network Preference** – IPv4 또는 IPv6를 선택할 수 있습니다. IPv6를 사용하는 복제 서비스는 IPv4를 통해 서비스에 연결할 수 있는 경우 계속해서 IPv4 복제 클라이언트로부터 접속을 수신할 수 있습니다. IPv6를 사용하는 복제 클라이언트는 IPv4를 통해 서비스에 연결할 수 있는 경우 계속해서 IPv4 복제 서비스와 통신할 수 있습니다.

   d. **Use Non-default Connection Host** – 소스 시스템이 대상 시스템 수신 포트에 데이터를 전송합니다. 소스 시스템에서 여러 대상 시스템에 대해 복제를 구성할 수 있으며, 각 대상 시스템은 서로 다른 수신 포트를 사용할 수 있습니다. 소스의 각 컨텍스트는 대상의 해당 수신 포트에 대한 연결 포트를 구성할 수 있습니다.
3. **Next**와 **Close**를 차례로 선택합니다.

   복제 페어 설정이 업데이트되고 복제가 재개됩니다.

CLI 절차

```
#replication modify <destination> connection-host <new-host-name> [port <port>]
```

복제 시스템 관리

Manage Systems 대화 상자에서 복제에 사용할 Data Domain 시스템을 추가하거나 삭제할 수 있습니다.

절차

1. **Manage Systems**를 선택합니다.
2. Manage Systems 대화 상자에서 Data Domain 시스템을 필요에 따라 추가하고 삭제합니다.
3. **Close**를 선택합니다.

복제 페어에서 데이터 복구

소스 복제 데이터에 액세스할 수 없게 되면 복제 페어에서 해당 데이터를 *복구*할 수 있습니다. 소스가 비어 있어야 복구를 계속 진행할 수 있습니다. MTree 복제를 제외한 모든 복제 토폴로지에 대해 복구를 수행할 수 있습니다.

디렉토리 풀에서 데이터를 복구하는 방법과 디렉토리 및 컬렉션 복제 페어에서 데이터를 복구하는 방법은 다음 섹션에서 설명합니다.

디렉토리 풀 데이터 복구

디렉토리 기반 풀에서 데이터를 복구할 수 있지만 MTree 기반 풀에서는 복구할 수 없습니다.

절차

1. **More** > **Start Recover**를 선택합니다.
2. Start Recover 대화 상자의 **Replication Type** 메뉴에서 **Pool**을 선택합니다.
3. **System to recover to** 메뉴에서 소스 시스템 호스트 이름을 선택합니다.
4. **System to recover from** 메뉴에서 대상 시스템 호스트 이름을 선택합니다.
5. 데이터가 복구되는 대상에 대한 컨텍스트를 선택합니다.
6. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
7. **OK**를 선택하여 복구를 시작합니다.

컬렉션 복제 페어 데이터 복구

컬렉션 복제 페어 데이터를 성공적으로 복구하려면 소스 파일 시스템이 온전한 상태이고 대상 컨텍스트가 완전히 초기화되어야 합니다.

절차

1. **More** > **Start Recover**를 선택하여 Start Recover 대화 상자를 표시합니다.
2. **Replication Type** 메뉴에서 **Collection**을 선택합니다.
3. **System to recover to** 메뉴에서 소스 시스템 호스트 이름을 선택합니다.
4. **System to recover from** 메뉴에서 대상 시스템 호스트 이름을 선택합니다.
5. 데이터가 복구되는 대상에 대한 컨텍스트를 선택합니다. 대상에는 컬렉션이 하나만 있습니다.
6. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
7. **OK**를 선택하여 복구를 시작합니다.

디렉토리 복제 페어 데이터 복구

디렉토리 복제 페어 데이터를 성공적으로 복구하려면 원래 컨텍스트에 사용된 디렉토리와 동일하되 비어 있는 디렉토리를 생성해야 합니다.

절차

1. **More** > **Start Recover**를 선택하여 Start Recover 대화 상자를 표시합니다.
2. **Replication Type** 메뉴에서 **Directory**를 선택합니다.
3. *데이터가 복구되어야 하는 대상 시스템*의 호스트 이름을 **System to recover to** 메뉴에서 선택합니다.
4. *데이터 소스가 될 시스템*의 호스트 이름을 **System to recover from** 메뉴에서 선택합니다.
5. 컨텍스트 목록에서 복원할 컨텍스트를 선택합니다.
6. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
7. **OK**를 선택하여 복구를 시작합니다.

복제 페어 복구 중단

복제 페어 복구가 실패하거나 종료해야 할 경우 복제 복구를 중지할 수 있습니다.

절차

1. More 메뉴를 선택하고 **Abort Recover**를 선택해 현재 수행 중인 복구를 보여 주는 Abort Recover 대화 상자를 표시합니다.
2. 목록에서 중단할 하나 이상의 컨텍스트에 해당하는 확인란을 선택합니다.
3. **OK**를 선택합니다.

사후 요구 사항

가능한 한 빨리 소스에서 복구를 재시작해야 합니다.

MTree, 디렉토리 또는 풀 복제 페어 재동기화

*재동기화*는 소스와 대상 복제 페어의 데이터를 수동으로 분리한 후 복구, 즉 동기화 상태로 되돌리는 프로세스입니다. 복제 페어를 재동기화함으로써 양쪽 엔드포인트에 동일한 데이터가 존재하게 됩니다. MTree, 디렉토리 및 풀 복제에는 재동기화를 사용할 수 있지만, 컬렉션 복제에는 사용할 수 없습니다.

다음과 같은 경우에 복제 재동기화를 사용할 수도 있습니다.

- 삭제된 컨텍스트를 다시 생성할 경우
- 대상의 공간이 부족하지만 소스에는 아직 복제할 데이터가 있는 경우
- 디렉토리 복제 페어를 MTree 복제 페어로 변환할 경우

절차

1. 복제 소스와 복제 대상 시스템 모두에서 컨텍스트를 삭제합니다.
2. 복제 소스 또는 복제 대상 시스템에서 **More** > **Start Resync**를 선택하여 Start Resync 대화 상자를 표시합니다.
3. 동기화할 Replication Type을 선택합니다. **Directory**, **MTree** 또는 **Pool** 중에서 선택합니다.
4. **Source System** 메뉴에서 복제 소스 시스템 호스트 이름을 선택합니다.
5. **Destination System** 메뉴에서 복제 대상 시스템 호스트 이름을 선택합니다.

6. **Source Path** 입력란에 복제 소스 경로를 입력합니다.
7. **Destination Path** 입력란에 복제 대상 경로를 입력합니다.
8. 호스트 접속 설정을 변경하려면 **Advanced** 탭을 선택합니다.
9. **OK**를 선택합니다.

CLI 절차

```
# replication resync destination
```

복제 페어 재동기화 중단

복제 페어 재동기화가 실패하거나 종료해야 할 경우 재동기화를 중지할 수 있습니다.

절차

1. 복제 소스 또는 복제 대상 시스템에서 **More** > **Abort Resync**를 선택하면 현재 재동기화를 수행 중인 모든 컨텍스트를 나열하는 Abort Resync 대화 상자가 표시됩니다.
2. 재동기화를 중단할 하나 이상의 컨텍스트에 해당하는 확인란을 선택합니다.
3. **OK**를 선택합니다.

DD Boost 보기

DD Boost 보기에서는 DD Boost AIR(Automatic Image Replication) 또는 관리되는 파일 복제를 사용하는 DD Boost 애플리케이션을 사용하도록 DD 시스템을 구성한 NetBackup 관리자에게 구성 및 문제 해결 정보를 제공합니다.

DD Boost AIR 구성 지침은 *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

File Replication 탭에는 다음 정보가 표시됩니다.

- Currently Active File Replication:
  - 방향(Out-Going 및 In-Coming)과 각 방향의 파일 수.
  - 복제될 나머지 데이터(GiB 단위의 압축 이전 값)와 이미 복제된 데이터(GiB 단위의 압축 이전 값).
  - Total size: 복제될 데이터와 이미 복제된 데이터의 양(GiB 단위의 압축 이전 값).
- Most Recent Status: 총 파일 복제 및 완료 또는 실패 여부
  - 지난 1시간 동안
  - 지난 24시간 동안
- Remote Systems:
  - 목록에서 복제를 선택합니다.
  - 메뉴에서 해당하는 기간을 선택합니다.
  - 이러한 원격 시스템 파일에 대한 자세한 내용을 보려면 **Show Details**를 선택합니다.

Storage Unit Associations 탭에는 스토리지 유닛의 이미지 복제에 사용되는 DD Boost AIR 이벤트의 상태를 확인하는 데 사용하거나 감사 목적으로 사용할 수 있는 다음 정보가 표시됩니다.

- 시스템에 알려진 모든 스토리지 유닛 **Associations**의 목록. 소스는 왼쪽에 있고 대상은 오른쪽에 있습니다. 이 정보는 Data Domain 시스템의 AIR 구성을 보여 줍니다.

- **Event Queue**는 보류 중인 이벤트 목록입니다. 여기에는 로컬 스토리지 유닛, 이벤트 ID 및 이벤트의 상태가 표시됩니다.

페어를 형성하기 위해 DD Boost 경로의 양쪽 끝을 일치시키고 이를 하나의 페어/레코드로 제공하려고 시도합니다. 다양한 이유로 일치가 불가능하면 원격 경로가 *Unresolved*로 나열됩니다.

원격 시스템 파일

Show Details 버튼을 클릭하면 선택한 원격 파일 복제 시스템에 대한 정보가 제공됩니다. File Replications에는 선택한 원격 파일 복제 시스템에 대한 시작 및 종료 정보뿐만 아니라 크기 및 데이터 양도 표시됩니다. Performance Graph에는 선택한 원격 파일 복제 시스템에 대한 시간에 따른 성능이 표시됩니다.

표 194 File Replications

항목	설명
Start	기간의 시작 시점입니다.
End	기간의 종료 시점입니다.
File Name	특정 복제 파일의 이름입니다.
Status	가장 최근의 상태(Success, Failure)입니다.
Pre-Comp Size (MiB)	네트워크 처리량 또는 압축 후 데이터와 비교해 압축 전 아웃바운드 및 인바운드 데이터의 양(MiB)입니다.
Network Bytes (MiB)	네트워크 처리량 데이터의 양(MiB)입니다.

표 195 Performance Graph

항목	설명
Duration	복제의 기간(1d, 7d 또는 30d)입니다.
Interval	복제의 간격(Daily 또는 Weekly)입니다.
Pre-Comp Replicated	압축 전 아웃바운드 및 인바운드 데이터의 양(GiB)입니다.
Post-Comp Replicated	압축 후 데이터의 양(GiB)입니다.
Network Bytes	네트워크 처리량 데이터의 양(GiB)입니다.
Files Succeeded	성공적으로 복제된 파일의 수입니다.
Files Failed	복제되지 못한 파일의 수입니다.
Show in new window	별도의 창을 표시합니다.
Print	그래프를 인쇄합니다.

Performance 보기

Performance 보기에는 복제 중에 데이터의 변동을 보여 주는 그래프가 표시됩니다. 이 수치는 이 DD 시스템에 대한 각 복제 페어의 누적된 통계입니다.

- **Duration**(x축)은 기본적으로 30일입니다.
- **Replication Performance**(y축)는 GiB(GibiByte) 또는 MiB(MebiByte) 단위입니다(기가바이트 및 메가바이트의 2진 표기법).

- **Network In**은 시스템으로 들어오는 복제 네트워크의 총 바이트입니다(모든 컨텍스트).
- **Network Out**은 시스템에서 나가는 복제 네트워크의 총 바이트입니다(모든 컨텍스트).
- 특정 시점에 대한 데이터를 보려면 그래프의 위치로 커서를 이동합니다.
- 비활성 시간(전송 중인 데이터가 없음) 중에는 그래프의 선이 예상대로 급격히 내려가는 대신 점차적으로 내려가는 모양이 표시될 수 있습니다.

Advanced Settings 보기

Advanced Setting에서 스로틀 및 네트워크 설정을 관리할 수 있습니다.

스로틀 설정

- **Throttle Override** – 구성된 경우 스로틀 속도가 표시되거나 모든 복제 트래픽이 중지되었음을 의미하는 0이 표시됩니다.
- **Permanent Schedule** – 스로틀 조절이 예약된 시간 및 요일이 표시됩니다.

네트워크 설정

- **Bandwidth** – 대역폭이 구성된 경우 구성된 데이터 스트림이 표시되거나 구성되지 않은 경우 Unlimited(기본값)가 표시됩니다. 복제 대상에 대한 평균 데이터 스트림은 최소한 초당 98,304비트(12KiB)입니다.
- **Delay** – 구성된 경우 구성된 네트워크 지연 설정이 표시되거나 구성되지 않은 경우 None(기본값)이 표시됩니다.
- **Listen Port** – 구성된 경우 구성된 수신 포트 값이 표시되거나 구성되지 않은 경우 2051(기본값)이 표시됩니다.

스로틀 설정 추가

네트워크에서 복제에 사용되는 대역폭 양을 수정하기 위해 복제 트래픽에 대한 *복제 스로틀*을 설정할 수 있습니다.

복제 스로틀 설정의 유형은 다음 세 가지입니다.

- **Scheduled throttle** – 미리 정해진 시간 또는 기간에 스로틀 속도가 설정됩니다.
- **Current throttle** – 다음에 예약된 변경 또는 시스템 재부팅 전까지 스로틀 속도가 설정됩니다.
- **Override throttle** – 위에 있는 두 유형의 스로틀이 재정의됩니다. 이 스로틀은 **Clear Throttle Override**를 선택하거나 `replication throttle reset override` 명령을 실행할 때까지 계속되며 재부팅 시에도 유지됩니다.

또한 다음과 같이 기본 스로틀을 설정하거나 특정 대상에 대한 스로틀을 설정할 수도 있습니다.

- **Default throttle** – 기본 스로틀이 구성된 경우 대상 스로틀(다음 항목 참조)로 지정된 대상을 제외한 모든 복제 컨텍스트가 기본 스로틀로 제한됩니다.
- **Destination throttle** – 이 스로틀은 몇몇 대상만 스로틀이 조절되어야 하거나 대상에 기본 스로틀과 다른 스로틀 설정이 필요한 경우에만 사용됩니다. 기본 스로틀이 이미 있으면 지정된 대상의 경우 이 스로틀이 우선 적용됩니다. 예를 들어 기본 복제 스로틀을 *10kbps*로 설정하고 대상 스로틀을 사용하여 단일 컬렉션 복제 컨텍스트를 *Unlimited*로 설정할 수 있습니다.

참고

현재 CLI(Command-Line Interface)를 사용해서만 대상 스로틀을 설정하고 수정할 수 있습니다. 이 기능은 DD System Manager에서 사용할 수 없습니다. 이 기능에 대한 설명은 *Data Domain Operating System 명령 참조 가이드*에서 `replication throttle` 명령을 참조하십시오. DD System Manager가 하나 이상의 대상 스로틀이 설정된 것을 감지하는 경우 경고가 표시되며 계속하려면 CLI를 사용해야 합니다.

복제 스로틀에 대한 추가 참고:

- 스로틀은 소스에서만 설정됩니다. 대상에 적용되는 유일한 스로틀은 모든 복제 트래픽을 비활성화하는 **0 Bps (Disabled)** 옵션입니다.
- 복제 스로틀의 최소값은 초당 98,304비트입니다.

절차

1. **Replication** > **Advanced Settings** > **Add Throttle Setting**을 선택하여 Add Throttle Setting 대화 상자를 표시합니다.
2. **Every Day**를 선택하거나 개별 요일 옆의 확인란을 선택하여 스로틀 조절이 활성화될 요일을 설정합니다.
3. **Start Time** 드롭다운 선택기에서 스로틀 조절을 시작할 시간(시:분 및 AM/PM)을 설정합니다.
4. **Throttle Rate**에 대해 다음 중 하나를 수행합니다.
   - 제한을 설정하지 않으려면 **Unlimited**를 선택합니다.
   - 입력란에 숫자(예: 20000)를 입력하고 메뉴에서 속도(bps, Kbps, Bps 또는 KBps)를 선택합니다.
   - **0 Bps (Disabled)** 옵션을 선택하여 모든 복제 트래픽을 비활성화합니다.
5. **OK**를 선택하여 스케줄을 설정합니다. 새 스케줄이 **Permanent Schedule** 아래에 표시됩니다.

결과

다음에 예정된 변경 또는 새로운 스로틀 설정으로 인한 변경이 있기 전까지 지정된 속도로 복제가 실행됩니다.

스로틀 설정 삭제

단일 스로틀 설정을 삭제하거나 전체 스로틀 설정을 한 번에 삭제할 수 있습니다.

절차

1. **Replication** > **Advanced Settings** > **Delete Throttle Setting**을 선택하여 Delete Throttle Setting 대화 상자를 표시합니다.
2. 삭제할 스로틀 설정에 해당하는 확인란을 선택하거나 머리글 확인란을 선택해 모든 설정을 삭제합니다. 이 목록에는 "disabled" 상태의 설정이 포함될 수 있습니다.
3. **OK**를 선택해 설정을 제거합니다.
4. Delete Throttle Setting Status 대화 상자에서 **Close**를 선택합니다.

일시적으로 스로틀 설정 재정의

스로틀 재정의는 일시적으로 스로틀 설정을 변경합니다. 현재 설정이 창의 맨 위에 나열됩니다.

절차

1. **Replication** > **Advanced Settings** > **Set Throttle Override**를 선택하여 Throttle Override 대화 상자를 표시합니다.
2. 새 스로틀 재정의를 설정하거나 이전 재정의를 지웁니다.
   a. 새 스로틀 재정의를 설정하려면 다음 중 하나를 수행합니다.
      - 시스템에서 설정한 스로틀 속도(스로틀 조절을 수행하지 않음)로 되돌리려면 **Unlimited**를 선택합니다.
      - 입력란에서 스로틀 작동 비트(예: 20000) 및 속도(bps, Kbps, Bps 또는 KBps)를 설정합니다.
      - 스로틀 속도를 0으로 설정하여 모든 복제 네트워크 트래픽을 효과적으로 중지하려면 **0 Bps (Disabled)**를 선택합니다.
      - 일시적으로 변경 내용을 적용하려면 **Clear at next scheduled throttle event**를 선택합니다.

   b. 이전에 설정된 재정의를 지우려면 **Clear Throttle Override**를 선택합니다.
3. **OK**를 선택합니다.

네트워크 설정 변경

복제는 대역폭과 네트워크 지연 설정을 함께 사용해 복제 사용량에 알맞은 TCP(Transmission Control Protocol) 버퍼 크기를 계산합니다. 이 네트워크 설정은 DD 시스템 전역에 적용되며 시스템 한 대당 한 번만 설정해야 합니다.

다음을 참조하십시오.

- `ping` 명령을 사용해 각 서버에 대한 실제 대역폭 및 실제 네트워크 지연 값을 결정할 수 있습니다.
- Restorer의 기본 네트워크 매개 변수는 지연 시간 라운드 트립 시간(`ping` 명령에 의해 측정됨)이 보통 1밀리초 미만인 로컬 100Mbps 또는 1,000Mbps 이더넷 네트워크처럼 지연 시간이 낮은 구성의 복제에서 효과가 높습니다. 기본값은 지연 시간이 최고 50~100밀리초에 이를 수 있는 대역폭이 낮거나 보통인 WAN을 통한 복제에서도 효과가 높습니다. 그러나 대역폭과 지연 시간이 높은 네트워크의 경우 네트워크 매개 변수를 어느 정도 튜닝해야 합니다.
  튜닝을 위한 주요 수치는 네트워크의 대역폭과 라운드 트립 지연 시간을 곱한 대역폭 지연 수치입니다. 이 수치는 반대쪽에서 확인을 반환하기 전에 네트워크에서 얼마나 많은 데이터를 전송할 수 있는지 측정한 값입니다. 복제 네트워크의 대역폭 지연 수치가 100,000보다 클 경우 두 Restorer에서 네트워크 매개 변수를 설정하면 복제 성능이 향상됩니다.

절차

1. **Replication** > **Advanced Settings** > **Change Network Settings**를 선택하면 Network Settings 대화 상자가 표시됩니다.
2. Network Settings 영역에서 **Custom Values**를 선택합니다.
3. 입력란에 **Delay** 및 **Bandwidth** 값을 입력합니다. 네트워크 지연 설정은 밀리초, 대역폭은 초당 바이트 단위입니다.
4. Listen Port 영역의 입력란에 새 값을 입력합니다. 복제 소스에서 데이터 스트림을 수신하기 위한 복제 대상의 기본 IP 수신 포트는 2051입니다. 이는 DD 시스템의 전역 설정입니다.
5. **OK**를 선택합니다. Network Settings 테이블에 새 설정이 나타납니다.

복제 모니터링

DD System Manager에서는 다양한 방법으로 복제 상태를 추적할 수 있습니다. 여기에는 복제 페어 상태 확인, 백업 작업 추적 성능 확인 및 복제 프로세스 추적이 포함됩니다.

백업 작업의 예상 완료 시간 보기

Completion Predictor를 사용해 백업 복제 작업이 완료되는 예상 시간을 볼 수 있습니다.

절차

1. **Replication** > **Summary**를 선택합니다.
2. Detailed Information을 표시할 복제 컨텍스트를 선택합니다.
3. Completion Predictor 영역에서 복제 완료 시간에 대한 **Source Time** 드롭다운 목록에서 옵션을 선택하고 **Track**을 선택합니다.

   Completion Time 영역에 특정 백업 작업이 대상으로의 복제를 언제 마칠지에 대한 예상 시간이 표시됩니다. 복제가 완료되면 영역에 `Completed`가 표시됩니다.

복제 컨텍스트 성능 확인

시간에 따른 컨텍스트의 성능을 확인하려면 Summary 보기에서 복제 컨텍스트를 선택하고 Detailed Information 영역에서 **Performance Graph**를 선택하십시오.

복제 프로세스 상태 추적

복제 초기화, 재동기화 또는 복구 작업의 진행 상태를 표시하려면 **Replication** > **Summary** 보기를 사용해 현재 상태를 확인하십시오.

CLI 절차

```
# replication show config all
CTX  Source                                    Destination
Connection Host and Port     Enabled
---  ----------------------        ----------------------        ------------------------
-------
1       dir://host2/backup/dir2     dir://host3/backup/dir3
host3.company.com               Yes
2       dir://host3/backup/dir3     dir://host2/backup/dir2
host3.company.com               Yes
```

IP 버전을 지정하는 경우 다음 명령을 사용해 설정을 확인합니다.

```
# replication show config rctx://2

CTX:                          2
Source:                       mtree://ddbeta1.dallasrdc.com/data/col1/EDM1
Destination:                  mtree://ddbeta2.dallasrdc.com/data/col1/EDM_ipv6
Connection Host:              ddbeta2-ipv6.dallasrdc.com
Connection Port:              (default)
Ipversion:                    ipv6
Low-bw-optim:                 disabled
Encryption:                   disabled
Enabled:                      yes
Propagate-retention-lock:     enabled
```

복제 지연

두 데이터 복사본 사이의 시간을 복제 지연이라고 합니다.

복제 상태 명령을 사용하여 두 컨텍스트 간의 복제 지연을 측정할 수 있습니다. 복제 지연의 원인을 확인하고 그 영향을 완화하는 방법에 대한 내용은 https://support.emc.com/kb/180482에서 사용할 수 있는 KB 문서 *복제 지연 문제 해결*을 참조하십시오.

HA를 지원하는 복제

유동 IP 주소를 사용하면 HA 시스템이 HA 쌍에서 어느 노드가 액티브 노드인지에 관계없이 작동하는 복제 구성을 위해 단일 IP 주소를 지정할 수 있습니다.

HA 시스템은 어느 물리적 노드가 액티브 노드인지에 관계없이 유동 IP 주소를 사용하여 IP 네트워크를 통해 Data Domain HA 쌍에 대한 데이터 액세스를 제공합니다. net config 명령은 유동 IP 주소를 구성하는 `[type {fixed | floating}]` 옵션을 제공합니다. *Data Domain Operating System 명령 참조 가이드*에 자세한 내용이 나와 있습니다.

유동 IP 주소에 액세스하는 데 도메인 이름이 필요한 경우 HA 시스템 이름을 도메인 이름으로 지정합니다. `ha status` 명령을 실행하여 HA 시스템 이름을 찾습니다.

참고

`net show hostname type ha-system` 명령을 실행하여 HA 시스템 이름을 표시하고 필요한 경우 `net set hostname ha-system command`를 사용하여 HA 시스템 이름을 변경합니다.

모든 파일 시스템 액세스는 유동 IP 주소를 통해 이루어져야 합니다. HA 쌍에서 백업 및 복제 작업을 구성하는 경우 항상 유동 IP 주소를 Data Domain 시스템의 IP 주소로 지정하십시오. DD Boost 및 복제와 같은 Data Domain 기능은 비 HA 시스템의 시스템 IP 주소를 수락하는 것과 같은 방식으로 HA 쌍의 유동 IP 주소를 수락합니다.

HA 시스템과 비 HA 시스템 간 복제

DD OS 5.7.0.3 이하 버전을 실행하는 시스템과 HA(High-Availability) 시스템 간의 복제를 설정하려는 경우 DD System Manager GUI를 사용하려면 HA 시스템에서 해당 복제를 생성하고 관리해야 합니다.

하지만 CLI를 사용하면 HA 시스템에서 비 HA 시스템으로의 복제는 물론, 비 HA 시스템에서 HA 시스템으로의 복제도 수행할 수 있습니다.

HA 시스템과 비 HA 시스템 간의 컬렉션 복제는 지원되지 않습니다. HA 시스템과 비 HA 시스템 간에서 데이터를 복제하려면 디렉토리 또는 MTree 복제가 필요합니다.

할당량 지원 시스템을 할당량 비지원 시스템에 복제

할당량을 지원하는 DD OS 기반의 Data Domain 시스템을 할당량이 없는 DD OS 기반의 시스템에 복제합니다.

- 할당량이 없는 시스템의 데이터를 사용하여 할당량이 설정된 시스템의 MTree로 복제한 후 계속해서 할당량이 설정되도록 하는 역방향 재동기화
- 내부 데이터를 사용하여 할당량을 지원하는 시스템의 새 MTree를 생성하지만 할당량이 없는 시스템의 데이터에서 생성되었기 때문에 할당량이 설정되지 않은, 할당량이 없는 시스템의 역방향 초기화

참고

DD OS 5.2부터 할당량이 도입되었습니다.

복제 확장 컨텍스트

복제 컨텍스트를 구성할 때 복제 확장 컨텍스트 기능으로 보다 유연하게 작업할 수 있습니다.

디렉토리 및 MTree 복제 컨텍스트를 모두 포함하는 299개 이상의 복제 컨텍스트가 있는 환경에서 이 기능을 사용하면 원하는 순서로 컨텍스트를 구성할 수 있습니다. 이전에는 디렉토리 복제 컨텍스트를 먼저 구성한 다음 MTree 복제 컨텍스트를 구성해야 했습니다.

총 복제 컨텍스트 수는 540을 초과할 수 없습니다.

참고

이 기능은 DD OS 버전 6.0을 실행하는 Data Domain 시스템에만 나타납니다.

D2M(Directory-to-MTree) 복제 마이그레이션

D2M(Directory-to-MTree) 복제 최적화 기능을 사용하면 기존 디렉토리 복제 컨텍스트를 파일 시스템의 논리 파티션인 MTree를 기반으로 하는 새로운 복제 컨텍스트로 마이그레이션할 수 있습니다. 또한 이 기능을 사용하면 진행 중인 프로세스를 모니터링하고 성공적으로 완료되었는지 확인할 수 있습니다.

D2M 기능은 Data Domain Operating System 버전 6.0, 5.7 및 5.6과 호환됩니다.

이 기능을 사용하려면 소스 Data Domain 시스템은 DD OS 6.0을 실행해야 하지만 대상 시스템은 6.0, 5.7 또는 5.6을 실행할 수 있습니다. 하지만 성능 최적화 이점은 소스 및 대상 시스템이 모두 6.0을 실행하는 경우에만 나타납니다.

참고

이 작업에 GUI(Graphical User Interface)를 사용할 수 있지만 최적의 성능을 위해서는 CLI(Command Line Interface)를 사용하는 것이 좋습니다.

디렉토리 복제에서 MTree 복제로의 마이그레이션 수행

D2M(Directory-to-MTree) 마이그레이션을 수행하는 동안 시스템을 종료하거나 재부팅하지 마십시오.

절차

1. 디렉토리 복제 소스 디렉토리에 대한 모든 수집 작업을 중지합니다.
2. 소스 DD 시스템에서 MTree를 생성합니다. **`mtree create /data/col1/`*`mtree-name`***

   참고

   대상 DD 시스템에서 MTree를 생성하지 마십시오.

3. (선택 사항) MTree에서 DD Retention Lock을 활성화합니다.

참고

소스 시스템에 Retention Lock이 설정된 파일이 포함되어 있는 경우 새 MTree에서 DD Retention Lock을 유지할 수 있습니다.

MTree에서 DD Retention Lock Compliance 활성화를 참조하십시오.

4. 소스 및 대상 DD 시스템 모두에서 MTree 복제 컨텍스트를 생성합니다.
replication add source mtree://*source-system-name/source mtree*
replication add destination mtree://*destination-system-name/destination mtree*
5. D2M 마이그레이션을 시작합니다. **replication dir-to-mtree start from *rctx://1* to *rctx://2***

   위 예제에서
   `rctx://1`
   은 소스 시스템의 `backup backup/dir1` 디렉토리를 복제하는 디렉토리 복제 컨텍스트를 나타내고,
   `rctx://2`
   는 소스 시스템의 `/data/col1/mtree1` MTree를 복제하는 MTree 복제 컨텍스트를 나타냅니다.

참고

이 명령을 완료하는 데 예상보다 오래 걸릴 수 있습니다. 이 프로세스 중에 Ctrl+C를 누르지 마십시오. 이 키를 누르면 D2M 마이그레이션이 취소됩니다.

```
Phase 1 of 4 (precheck):
    Marking source directory /backup/dir1 as read-only...Done.

Phase 2 of 4 (sync):
    Syncing directory replication context...0 files flushed.
current=45 sync_target=47 head=47
current=45 sync_target=47 head=47
Done. (00:09)

Phase 3 of 4 (fastcopy):
    Starting fastcopy from /backup/dir1 to /data/col1/
mtree1...
    Waiting for fastcopy to complete...(00:00)
    Fastcopy status: fastcopy /backup/dir1 to /data/col1/
mtree1: copied 24
files, 1 directory in 0.13 seconds
    Creating snapshot 'REPL-D2M-
mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
    Initializing MTree replication context...
(00:08) Waiting for initialize to start...
(00:11) Initialize started.

Use 'replication dir-to-mtree watch rctx://2' to monitor
progress.
```

D2M(Directory-to-MTree) 마이그레이션 진행률 보기

D2M(Directory-to-MTree) 복제에서 현재 진행 중인 마이그레이션 단계를 확인할 수 있습니다.

절차

1. 진행 상태를 확인하려면 **replication dir-to-mtree watch *rctx://2***를 입력합니다.

   `rctx://2`
   는 복제 컨텍스트를 지정합니다.

   다음과 같이 출력되어야 합니다.

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
(00:00) Replication initialize started...
(00:02) initializing:
(00:14)     100% complete, pre-comp: 0 KB/s, network: 0 KB/
s
(00:14) Replication initialize completed.
Migration for ctx 2 successfully completed.
```

D2M(Directory-to-MTree) 복제 마이그레이션 상태 확인

`replication dir-to-mtree status` 명령을 사용하여 D2M(Directory-to-MTree) 마이그레이션이 완료되었는지 확인할 수 있습니다.

절차

1. 다음 명령을 실행합니다. 여기서,
   `rctx://2`
   는 소스 시스템의 MTree 복제 컨텍스트를 나타냅니다. **replication dir-to-mtree status rctx://2**

   출력은 다음과 비슷한 형태입니다.

```
Directory Replication CTX:          1
MTree Replication CTX:              2
Directory Replication Source:       dir://127.0.0.2/backup/dir1
MTree Replication Source:           mtree://127.0.0.2/data/
col1/mtree1
MTree Replication Destination:      mtree://127.0.0.3/data/
col1/mtree1
Migration Status:                   completed
```

   진행 중인 마이그레이션이 없는 경우 다음을 확인해야 합니다.

```
# replication dir-to-mtree status rctx://2
No migration status for context 2.
```

2. 마이그레이션 프로세스가 완료되면 소스 DD 시스템에서 MTree로 데이터 수집을 시작합니다.
3. (선택 사항) 소스 및 타겟 시스템에서 디렉토리 복제 컨텍스트를 분리합니다.

   `replication break` 명령에 대한 자세한 내용은 *Data Domain Operating System Version 6.0 명령 참조 가이드*를 참조하십시오.

D2M 복제 중단

필요한 경우 D2M(Directory-to-MTree) 마이그레이션을 중단할 수 있습니다.

`replication dir-to-mtree abort` 명령은 진행 중인 마이그레이션 프로세스를 중단하고 디렉토리를 읽기 전용 상태에서 읽기/쓰기 상태로 되돌립니다.

절차

1. CLI(Command-Line Interface)에서 다음 명령을 입력합니다. 이 경우 `rctx://2`는 MTree 복제 컨텍스트입니다. **`replication dir-to-mtree abort rctx://2`**

   다음과 같이 출력되어야 합니다.

   ```
   Canceling directory to MTree migration for context dir-name.
   Marking source directory dir-name as read-write...Done.
   The migration is now aborted.
   Remove the MTree replication context and MTree on both source
   and destination
   host by running 'replication break' and 'mtree delete'
   commands.
   ```

2. MTree 복제 컨텍스트를 중단: **`replication break rctx://2`**
3. 소스 시스템에서 MTree 삭제: **`mtree delete mtree-path`**

D2M 문제 해결

D2M(Directory-to-MTree) 복제 설정에 문제가 발생하는 경우 여러 가지 다양한 문제를 해결하기 위해 수행할 수 있는 작업이 있습니다.

`dir-to-mtree abort` 절차는 D2M 프로세스를 중단하는 데 도움이 됩니다. 다음과 같은 경우 이 절차를 실행해야 합니다.

- D2M 마이그레이션의 상태가 중단된 상태로 나열됩니다.
- D2M 마이그레이션 중에 Data Domain 시스템이 재부팅됩니다.
- `replication dir-to-mtree start` 명령을 실행하면 오류가 발생합니다.
- 마이그레이션을 시작하기 전에 수집이 중지되지 않았습니다.
- `replication dir-to-mtree start` 명령을 입력하기 전에 MTree 복제 컨텍스트가 초기화되었습니다.

참고

D2M 프로세스를 마치기 전에 MTree 복제 컨텍스트에서 **`replication break`**를 실행하지 마십시오.
mrepl ctx에서 **`replication break`** 명령을 실행하기 전에 항상 **`replication dir-to-mtree abort`**를 실행하십시오.

너무 일찍 **`replication break`** 명령을 실행하면 drepl 소스 디렉토리가 영구적으로 읽기 전용으로 처리됩니다.

이 경우 지원 팀에 문의하십시오.

절차

1. **`replication dir-to-mtree abort`**를 입력하여 프로세스를 중단합니다.

2. 소스 및 대상 Data Domain 시스템 모두에서 새로 생성된 MTree 복제 컨텍스트를 분리하십시오.

   다음 예제에서 MTree 복제 컨텍스트는 `rctx://2` 입니다.

   ```
   replication break rctx://2
   ```

3. 소스 및 대상 시스템 모두에서 해당 MTree를 삭제합니다.

   ```
   mtree delete mtree-path
   ```

   참고

   삭제 표시가 된 MTree는 `filesys clean` 명령이 실행될 때까지 파일 시스템에 남아 있습니다.

   자세한 내용은 *Data Domain Operating System 버전 6.0 명령 참조 가이드*를 참조하십시오.

4. 소스 및 대상 시스템 모두에서 `filesys clean start` 명령을 실행합니다.

   `filesys clean` 명령에 대한 자세한 내용은 *Data Domain Operating System 버전 6.0 명령 참조 가이드*를 참조하십시오.

5. 프로세스를 다시 시작합니다.

   디렉토리 복제에서 MTree 복제로의 마이그레이션 수행을 참조하십시오.

추가적인 D2M 문제 해결

새 MTree에 대해 DD Retention Lock을 활성화하는 것을 잊었거나 D2M(Directory-to-MTree) 마이그레이션을 초기화한 후 오류가 발생한 경우 사용할 수 있는 솔루션이 있습니다.

DD Retention Lock을 활성화하지 않은 경우

새 MTree에 대해 DD Retention Lock을 활성화하는 것을 잊었으며 소스 디렉토리에 Retention Lock이 활성화된 파일 또는 디렉토리가 포함된 경우 다음 옵션을 사용할 수 있습니다.

- D2M 마이그레이션을 계속 진행합니다. 이 경우 마이그레이션 후 MTree에 DD Retention Lock 정보가 없습니다.
- D2M 복제 중단 (448페이지)에 설명된 대로 현재 D2M 프로세스를 중단하고 소스 MTree에서 DD Retention Lock을 활성화하여 프로세스를 다시 시작합니다.

초기화 후 오류 발생

`replication dir-to-mtree start` 프로세스는 오류 없이 완료되었지만 MTree 복제 초기화 도중(D2M 마이그레이션 프로세스의 단계 4) 오류가 감지되는 경우 다음 단계를 수행할 수 있습니다.

1. 네트워크 문제가 없는지 확인합니다.
2. MTree 복제 컨텍스트를 초기화합니다.

SMT를 사용한 재해 복구에 컬렉션 복제 사용

재해 복구를 위한 교체 시스템으로 SMT로 구성된 컬렉션 복제 쌍의 대상 시스템을 사용하려면 교체 시스템을 온라인 상태로 만드는 데 필요한 다른 구성 단계 이외에도 추가적인 SMT 구성 단계를 수행해야 합니다.

시작하기 전에

이 방식으로 컬렉션 복제 대상 시스템을 사용하려면 자동 지원 보고서를 구성하고 저장해야 합니다. https://support.emc.com에서 사용할 수 있는 KB 문서 *Collection replica with smt enabled*에 추가 정보가 나와 있습니다.

복제 시스템에는 다음과 같은 SMT 세부 정보가 없습니다.

- 각 테넌트 유닛에 대한 알림 목록
- DD Boost가 시스템에 구성되어 있는 경우 SMT 테넌트가 사용할 수 있도록 DD Boost 프로토콜에 할당된 모든 사용자
- DD Boost가 시스템에 구성되어 있는 경우 각 DD Boost 사용자와 관련된 기본 테넌트 유닛(있는 경우)

교체 시스템에 SMT를 구성하려면 다음 단계를 완료합니다.

절차

1. 자동 지원 보고서에서 `smt tenant-unit show detailed` 명령의 출력을 찾습니다.

```
Tenant-unit: "tu1"
Summary:
Name   Self-Service   Number of Mtrees   Types           Pre-Comp(GiB)
----   ------------   ----------------   --------        -------------
tu1    Enabled        2                  DD Boost        2.0
----   ------------   ----------------   --------        -------------

Management-User:
User     Role
------   ------------
tu1_ta   tenant-admin
tu1_tu   tenant-user
tum_ta   tenant-admin
------   ------------

Management-Group:
Group    Role
------   ------------
qatest   tenant-admin
------   ------------

DDBoost:
Name   Pre-Comp (GiB)   Status   User    Tenant-Unit
----   --------------   ------   -----   -----------
su1               2.0   RW/Q     ddbu1   tu1
----   --------------   ------   -----   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write

Getting users with default-tenant-unit tu1
DD Boost user   Default tenant-unit
-------------   -------------------
ddbu1           tu1
-------------   -------------------

Mtrees:
Name              Pre-Comp (GiB)   Status   Tenant-Unit
--------------    --------------   ------   -----------
```

```
/data/col1/m1                0.0   RW/Q     tu1
/data/col1/su1               2.0   RW/Q     tu1
--------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tu1
Mtree            Pre-Comp (MiB)   Soft-Limit (MiB)   Hard-Limit(MiB)
--------------   --------------   ----------------   ----------------
/data/col1/m1                 0              71680             81920
/data/col1/su1             2048              30720             51200
--------------   --------------   ----------------   ----------------

Alerts:
Tenant-unit: "tu1"
Notification list "tu1_grp"
Members
------------------
tom.tenant@abc.com
------------------

No such active alerts.
```

2. 교체 시스템에서 SMT를 활성화합니다(아직 활성화되지 않은 경우).
3. 교체 시스템에서 DD Boost 라이센스가 아직 활성화되지 않았으면 필요한 경우 라이센스를 부여하고 활성화합니다.
4. DD Boost가 구성된 경우 "smt tenant-unit show detailed" 출력의 `DD Boost` 섹션에 나열된 각 사용자를 DD Boost 사용자로 할당합니다.

   ```
   # ddboost user assign ddbu1
   ```

5. DD Boost가 구성된 경우 `smt tenant-unit show detailed` 출력의 `DD Boost` 섹션에 나열된 각 사용자를 출력에 표시된 기본 테넌트 유닛(있는 경우)에 할당합니다.

   ```
   # ddboost user option set ddbu1 default-tenant-unit tu1
   ```

6. `smt tenant-unit show detailed` 출력의 `Alerts` 섹션에 있는 알림 그룹과 동일한 이름을 사용하여 새 알림 그룹을 생성합니다.

   ```
   # alert notify-list create tu1_grp tenant-unit tu1
   ```

7. `smt tenant-unit show detailed` 출력의 `Alerts` 섹션에 있는 알림 그룹의 각 이메일 주소를 새 알림 그룹에 할당합니다.

   ```
   # alert notify-list add tu1_grp emails tom.tenant@abc.com
   ```

17장

DD Secure Multitenancy

이 장에서 다루는 내용은 다음과 같습니다.

Data Domain Secure Multi-tenancy 개요

Data Domain *SMT(Secure Multi-tenancy)*는 내부 IT 부서 또는 외부 공급업체가 여러 소비자 또는 워크로드(사업부, 부서 또는 테넌트)에 대한 IT 인프라스트럭처를 동시에 호스팅하는 것을 의미합니다.

SMT는 공유 인프라스트럭처에서 다수의 사용자 및 워크로드를 안전하게 분리하여 한 테넌트의 작업이 다른 테넌트에게 표시되거나 보이지 않도록 합니다.

*테넌트*는 호스팅된 환경에 계속해서 존재하는 소비자(사업부, 부서 또는 고객)입니다.

기업 내에서 테넌트는 IT 직원이 구성하고 관리하는 Data Domain 시스템에 있는 하나 이상의 사업부 또는 부서로 구성될 수 있습니다.

- BU(Business Unit) 활용 사례에서 회사의 재무 및 인사 부서가 같은 Data Domain 시스템을 공유할 수 있지만 각 부서는 다른 부서의 사용 여부를 인지하지 못합니다.
- SP(Service Provider) 활용 사례의 경우 SP는 하나 이상의 Data Domain 시스템을 구축해 여러 최종 고객을 위해 다양한 보호 스토리지 서비스를 수용할 수 있습니다.

두 활용 사례 모두 동일한 물리적 Data Domain 시스템에서 여러 고객 데이터의 분리를 강조합니다.

SMT 아키텍처 기본 사항

SMT(Secure Multitenancy)는 Mtree를 사용하여 테넌트 및 테넌트 유닛을 설정할 수 있는 간단한 접근 방식을 제공합니다. SMT는 DD Management Center 및/또는 DD OS 명령줄 인터페이스에서 설정할 수 있습니다. 이 관리 가이드에서는 SMT의 이론과 일반적인 몇 가지 명령줄 지침을 제공합니다.

SMT의 기본 아키텍처는 다음과 같습니다.

- 테넌트는 DD Management Center 및/또는 DD 시스템에 생성됩니다.
- 테넌트 유닛은 테넌트의 DD 시스템에 생성됩니다.
- 테넌트의 다양한 백업 유형에 대한 스토리지 요구 사항을 충족하기 위해 하나 이상의 Mtree가 생성됩니다.
- 새로 생성된 MTree는 테넌트 유닛에 추가됩니다.
- 각 백업을 구성된 테넌트 유닛 MTree로 전송하도록 백업 애플리케이션이 구성됩니다.

참고

DD Management Center에 대한 자세한 내용은 *DD Management Center 사용자 가이드*를 참조하십시오. DD OS 명령줄 인터페이스에 대한 자세한 정보는 *DD OS 명령 참조*를 참조하십시오.

SMT(Secure Multitenancy)에 사용되는 용어

SMT에 사용되는 용어를 이해하면 이 고유한 환경을 이해하는 데 도움이 됩니다.

MTree

*MTree*는 파일 시스템의 논리적 파티션으로 최고 수준의 관리 정밀도를 제공하므로 사용자가 전체 파일 시스템에 영향을 주지 않고 특정 MTree에서 작업을 수행할 수 있습니다. MTree는 테넌트 유닛에 할당되며 SMT를 관리하고 모니터링하기 위해 테넌트 유닛의 개별화된 설정을 포함합니다.

멀티 테넌시(Multi-Tenancy)
*멀티 테넌시*는 내부 IT 부서 또는 외부 서비스 공급업체가 여러 소비자 또는 워크로드(사업부, 부서 또는 테넌트)에 대한 IT 인프라스트럭처를 동시에 호스팅하는 것을 의미합니다. Data Domain SMT는 *Data Protection-as-a-Service*를 가능하게 합니다.

RBAC(Role-based Access Control)
*RBAC*는 권한 수준이 다른 여러 역할을 제공합니다. 이 역할은 멀티 테넌트 Data Domain 시스템에서 관리 격리를 제공하기 위해 결합됩니다. 이 역할의 정의는 다음 섹션에 나와 있습니다.

스토리지 유닛(Storage Unit)
*스토리지 유닛*은 DD Boost 프로토콜에 맞게 구성된 MTree입니다. 스토리지 유닛을 생성하고 DD Boost 사용자에게 할당하는 방식으로 데이터 격리가 이루어집니다. DD Boost 프로토콜은 Data Domain 시스템에 접속한 DD Boost 사용자에게 할당된 스토리지 유닛에 대한 액세스만 허용합니다.

테넌트(Tenant)
*테넌트*는 호스팅된 환경에 계속해서 존재하는 소비자(사업부/부서/고객)입니다.

테넌트 셀프 서비스(Tenant Self-Service)
*테넌트 셀프 서비스*는 테넌트가 Data Domain 시스템에 로그인하여 일부 기본적인 서비스(로컬 사용자, NIS 그룹 및/또는 AD 그룹 추가, 편집 또는 삭제)를 수행하는 방법을 의미합니다. 셀프 서비스를 사용하면 이 기본적인 작업을 항상 관리자를 통해 수행함으로써 발생하는 병목 현상이 줄어듭니다. 테넌트는 각자에게 할당된 테넌트 유닛에만 액세스할 수 있습니다. 테넌트 사용자와 테넌트 관리자의 권한은 당연히 다릅니다.

테넌트 유닛(Tenant Unit)
*테넌트 유닛*은 테넌트 사이에서 관리 격리 단위 역할을 하는 Data Domain 시스템의 파티션입니다. 테넌트에 할당되는 테넌트 유닛은 동일하거나 서로 다른 Data Domain 시스템에 있을 수 있으며 보안이 유지되고 서로 논리적으로 격리되므로 공유 인프라스트럭처에서 동시에 여러 테넌트를 실행할 경우 제어 경로의 보안과 격리가 보장됩니다. 테넌트 유닛에는 멀티 테넌시 설정에 필요한 모든 구성 요소를 보유한 하나 이상의 *MTree*가 포함될 수 있습니다. 사용자, 관리 그룹, 알림 그룹 및 기타 구성 요소가 테넌트 유닛에 속합니다.

제어 경로 및 네트워크 격리

*제어 경로 격리*는 테넌트 유닛에 대한 *tenant-admin* 및 *tenant-user* 역할을 사용자에게 지정하는 방식으로 이루어집니다. 데이터 및 관리자 액세스를 위한 *네트워크 격리*는 고정된 *데이터 액세스 IP 주소* 및 *관리 IP 주소* 세트를 테넌트 유닛에 연결하는 방식으로 이루어집니다.

tenant-admin 및 *tenant-user* 역할의 범위와 기능은 특정 테넌트 유닛과 이 테넌트 유닛에 수행할 수 있는 특정 작업 세트로 제한됩니다. 논리적으로 안전하고 격리된 데이터 경로를 보장하기 위해 시스템 관리자는 SMT 환경에 있는 각 프로토콜에 대해 하나 이상의 테넌트 유닛 MTree를 구성해야 합니다. 지원되는 프로토콜에는 DD Boost, NFS, CIFS, DD VTL이 있습니다. 액세스는 각 프로토콜의 기본 액세스 제어 메커니즘에 의해 엄격하게 제한됩니다.

테넌트 셀프 서비스 세션(ssh 사용)을 DD 시스템의 고정된 *관리 IP 주소* 세트로 제한할 수 있습니다. 또한 관리 액세스 세션(ssh/http/https 사용)도 DD 시스템의 고정된 관리 IP 주소 세트로 제한할 수 있습니다. 그러나 테넌트 유닛에는 기본적으로 관리 IP 주소가 연결되지 않으므로 *tenant-admin* 및 *tenant-user* 역할을 사용하여 제한하는 방법이 유일한 표준입니다. 테넌트 유닛에 대한 관리 IP 주소를 추가하고 유지하려면 `smt tenant-unit management-ip`를 사용해야 합니다.

마찬가지로, 테넌트 유닛 내/외부로의 데이터 액세스 및 데이터 흐름을 고정된 로컬 또는 원격 *데이터 액세스 IP 주소* 세트로 제한할 수도 있습니다. 할당된 데이터 액세스 IP

주소를 사용하면 SMT 관련 보안 검사를 추가하여 DD Boost 및 NFS 프로토콜의 보안을 강화할 수 있습니다. 예를 들어, DD Boost RPC를 통해 반환되는 스토리지 유닛의 목록을 할당된 로컬 데이터 액세스 IP 주소를 사용하는 테넌트 유닛에 속하는 스토리지 유닛으로 제한할 수 있습니다. NFS의 경우 구성된 로컬 데이터 액세스 IP 주소를 기준으로 내보내기의 액세스 및 가시성을 필터링할 수 있습니다. 예를 들어, 테넌트 유닛의 로컬 데이터 액세스 IP 주소에서 `showmount -e` 명령을 사용하면 해당 테넌트 유닛에 속한 NFS 내보내기만 표시됩니다.

테넌트 유닛에 대한 데이터 액세스 IP 주소를 추가하고 유지 관리하려면 *sysadmin*이 `smt tenant-unit data-ip` 명령을 사용해야 합니다.

참고

SMT에서 SMT 이외의 IP 주소를 사용하여 MTree를 마운트하려고 하면 작업이 실패합니다.

여러 테넌트 유닛이 동일한 테넌트에 속하는 경우 기본 게이트웨이를 공유할 수 있습니다. 하지만 여러 테넌트 유닛이 서로 다른 테넌트에 속하는 경우 동일한 기본 게이트웨이를 사용할 수 없습니다.

동일한 테넌트에 속하는 여러 테넌트 유닛은 기본 게이트웨이를 공유할 수 있습니다. 서로 다른 테넌트에 속하는 테넌트 유닛은 동일한 기본 게이트웨이를 사용할 수 없습니다.

SMT의 RBAC 이해

SMT(Secure Multi-Tenancy)에서 작업을 수행할 수 있는 사용 권한은 사용자에게 할당된 역할에 따라 다릅니다. DD Management Center에서는 RBAC(Role-Based Access Control)를 사용하여 이러한 사용 권한을 제어합니다.

모든 DD Management Center 사용자는 다음을 수행할 수 있습니다.

- 모든 테넌트 보기
- 모든 테넌트에 속하는 테넌트 유닛 생성, 읽기, 업데이트 또는 삭제(사용자가 테넌트 유닛을 호스팅하는 Data Domain 시스템의 관리자인 경우)
- 테넌트에 대한 테넌트 유닛의 할당 및 할당 취소(사용자가 테넌트 유닛을 호스팅하는 Data Domain 시스템의 관리자인 경우)
- 모든 테넌트에 속하는 테넌트 유닛 보기(사용자에게 테넌트 유닛을 호스팅하는 Data Domain 시스템에 대해 할당된 역할이 있는 경우)

더 많은 고급 작업을 수행하려면 다음과 같은 사용자 역할이 필요합니다.

admin 역할

admin 역할의 사용자는 Data Domain 시스템에서 모든 관리 작업을 수행할 수 있습니다. *admin* 역할은 또한 Data Domain 시스템에서 SMT 설정, SMT 사용자 역할 할당, 테넌트 셀프 서비스 모드 활성화, 테넌트 생성 등을 포함하는 모든 SMT 관리 작업을 수행할 수 있습니다. SMT 컨텍스트에서 *admin*을 일반적으로 *landlord*라고 합니다. DD OS에서 이 역할은 *sysadmin*이라고도 합니다.

테넌트 편집 또는 삭제를 위한 사용 권한을 가지려면 해당 테넌트의 테넌트 유닛과 연결된 모든 Data Domain 시스템에서 DD Management Center *admin* 역할과 DD OS *sysadmin* 역할이 있어야 합니다. 테넌트에 테넌트 유닛이 없는 경우 DD Management Center *admin* 역할만 있으면 테넌트를 편집하거나 삭제할 수 있습니다.

제한된 관리자 역할

limited-admin 역할의 사용자는 *admin*으로서 Data Domain 시스템에서 모든 관리 작업을 수행할 수 있습니다. 그러나 *limited-admin* 역할의 사용자는 MTree를 삭제하거나 제거할 수 없습니다. DD OS에도 동일한 *limited-admin* 역할이 있습니다.

tenant-admin 역할

tenant-admin 역할이 할당된 사용자는 특정 테넌트 유닛에서 *tenant self-service* 모드를 사용할 수 있는 경우에만 특정 작업을 수행할 수 있습니다. 테넌트에 대한 백업 애플리케이션 예약 및 실행, 할당된 테넌트 유닛 내에서 리소스와 통계 모니터링 등을 책임집니다. *tenant-admin*은 감사 로그를 볼 수 있지만 RBAC가 *tenant-admin*에게 속한 테넌트 유닛의 감사 로그만 액세스할 수 있도록 제한합니다. 또한 tenant self-service 모드가 활성화된 경우 *tenant-admin* 역할은 관리 분리를 보장합니다. SMT 컨텍스트에서 일반적으로 *tenant-admin* 역할을 *backup admin*이라고 합니다.

tenant-user 역할

tenant-user 역할의 사용자는 사용자에게 할당된 테넌트 유닛에서 테넌트 셀프 서비스가 활성화된 경우에만 SMT 구성 요소의 성능 및 사용량을 모니터링할 수 있습니다. 하지만 이 역할의 사용자는 자신에게 할당된 테넌트 유닛의 감사 로그를 볼 수 없습니다. 또한 *tenant-user* 역할은 `show` 및 `list` 명령을 실행할 수 있습니다.

none 역할

none 역할의 사용자는 자신의 암호를 변경하고 DD Boost를 사용하여 데이터에 액세스하는 것 외에는 Data Domain 시스템에서 어떤 작업도 수행할 수 없습니다. 그러나 SMT가 활성화된 후에 *admin* 역할은 Data Domain 시스템에서 *none* 역할의 사용자를 선택해 *tenant-admin* 또는 *tenant-user*의 SMT별 역할을 할당할 수 있습니다. 그러면 해당 사용자가 SMT 관리 객체에서 작업을 수행할 수 있습니다.

관리 그룹

BSP(Backup Service Provider)는 단일 외부 AD(Active Directory) 또는 NIS(Network Information Service)에서 정의된 *관리 그룹*을 사용해 테넌트 유닛에서 사용자 역할을 간편하게 관리할 수 있습니다. 각 BSP 테넌트는 별도의 외부 회사가 될 수 있으며 AD 또는 NIS 같은 name-service를 사용할 수 있습니다.

AD 및 NIS 서버는 *admin*이 SMT Management Group을 사용해 SMT 로컬 사용자와 동일한 방식으로 설정하고 관리합니다. *admin*은 AD 또는 NIS 관리자에게 그룹을 생성하고 채울 것을 요청할 수 있습니다. 그러면 *admin*이 전체 그룹에 SMT 역할을 할당합니다. 그룹 내에 있는 사용자 중 Data Domain 시스템에 로그인하는 사용자는 그룹에 할당된 역할로 로그인됩니다.

사용자가 테넌트의 회사에서 퇴사하거나 합류할 경우 AD 또는 NIS 관리자가 해당 사용자를 제거하거나 추가할 수 있습니다. 그룹에 속한 사용자가 추가되거나 제거될 경우 Data Domain 시스템에서 RBAC 구성을 수정할 필요가 없습니다.

테넌트 유닛 프로비저닝

구성 마법사를 실행하면 SMT(Secure Multitenancy)의 초기 프로비저닝 절차가 시작됩니다. 절차 중에 마법사가 테넌트 구성 요구 사항에 따라 새 테넌트 유닛을 생성하고 프로비저닝합니다. 메시지가 나타나면 관리자가 정보를 입력합니다. 절차를 완료한 후에 관리자는 Tenant Self-Service 모드를 설정하는 것을 시작으로 다음 작업을 순차적으로 진행합니다. 초기 설정 이후에 필요에 따라 수동 절차 및 구성 수정을 수행할 수도 있습니다.

절차

1. SMT를 시작합니다.

   ```
   # smt enable SMT enabled.
   ```

2. SMT가 설정되었는지 확인합니다.

   ```
   # smt status SMT is enabled.
   ```

3. SMT 구성 마법사를 시작합니다.

   ```
   # smt tenant-unit setup No tenant-units.
   ```

4. 구성 마법사의 메시지를 따릅니다.

```
SMT TENANT-UNIT Configuration

  Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes

  Do you want to create new tenant-unit (yes/no)? : yes

Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit

Pending Tenant-unit Settings
Create Tenant-unit   SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes

port  enabled  state  DHCP        IP address             netmask     type additional
                                                      /prefix length        setting
----- ------- ------- ---- -------------------------- -------------- ---- ----------
ethMa   yes   running  no  192.168.10.57              255.255.255.0   n/a
                           fe80::260:16ff:fe49:f4b0** /64
eth3a   yes   running ipv4 192.168.10.236*            255.255.255.0*  n/a
                           fe80::260:48ff:fe1c:60fc** /64
eth3b   yes   running  no  192.168.50.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1c:60fd** /64
eth4b   yes   running  no  192.168.60.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1f:5183** /64
----- ------- ------- ---- -------------------------- -------------- ---- ----------
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip    192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:
```

```
SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
-------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
  Enter MTree name
  :  SMT_57_tenant_unit
Invalid mtree path name.
  Enter MTree name
  :
SMT_57_tenant_unit


Invalid mtree path name.
  Enter MTree name
  : /data/col1/SMT_57_tenant_unit

MTree Soft-Quota
  Enter the quota soft-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

MTree Hard-Quota
  Enter the quota hard-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

Pending MTree Settings
Create MTree        /data/col1/SMT_57_tenant_unit
MTree Soft Limit    none
MTree Hard Limit    none

  Do you want to save these settings (Save|Cancel|Retry): save
  MTree "/data/col1/SMT_57_tenant_unit" created successfully.
  MTree "/data/col1/SMT_57_tenant_unit" assigned to tenant-unit  "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
-------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
```

```
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create another mtree for this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT SELF-SERVICE Configuration

  Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
  Self-service of this tenant-unit is disabled

  Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes

  Do you want to configure a management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes

Management-Group Name
  Enter the group name to be assigned to this tenant-unit
  : SMT_57_tenant_unit_group

What role do you want to assign to this group  (tenant-user|tenant-admin) [tenant-user]:
tenant-admin

Management-Group Type
  What type do you want to assign to this group (nis|active-directory)?
  : nis

Pending Self-Service Settings
Enable Self-Service       SMT_57_tenant_unit
Assign Management-group   SMT_57_tenant_unit_group
Management-group role     tenant-admin
Management-group type     nis

  Do you want to save these settings (Save|Cancel|Retry): save
  Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
  Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
  "SMT_57_tenant_unit" as "tenant-admin".

SMT Tenant-unit Self-Service Configurations saved.

SMT TENANT-UNIT SELF-SERVICE Configuration

  Do you want to configure another management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure another management group for this tenant-unit? (yes|no)
[no]:

SMT TENANT-UNIT ALERT Configuration

  Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
  No notification lists.

Alert Configuration

Alert Group Name
  Specify alert notify-list group name to be created
  : SMT_57_tenant_unit_notify

Alert email addresses
  Enter email address to receive alert for this tenant-unit
  : dd_proserv@emc.com

  Do you want to add more emails (yes/no)?
  : no

Pending Alert Settings
```

```
Create Notify-list group   SMT_57_tenant_unit_notify
Add emails                 dd_proserv@emc.com

  Do you want to save these settings (Save|Cancel|Retry): save
  Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
  Added emails to notification list "SMT_57_tenant_unit_notify".

SMT Tenant-unit Alert Configurations saved.

Configuration complete.
```

Tenant Self-Service 모드 활성화

관리 작업의 의무와 위임을 관리적인 측면에서 분리해 제어 경로 격리에 필요한 Tenant Self-Service를 구축하기 위해, 시스템 관리자는 테넌트 유닛에서 이 모드를 활성화한 후 tenant-admin 또는 tenant-user의 역할로 유닛을 관리하도록 사용자를 할당할 수 있습니다. 이러한 역할을 통해서 관리자가 아닌 사용자는 자신이 할당된 테넌트 유닛에서 특정 작업을 수행할 수 있습니다. Tenant Self-Service 모드는 관리 분리 외에도 내부 IT 및 서비스 공급업체 직원들의 관리 부담을 덜어 줍니다.

절차

1. 하나 또는 모든 테넌트 유닛에서 Tenant Self-Service 모드의 상태를 봅니다.

   ```
   # smt tenant-unit option show { tenant-unit | all }
   ```

2. 선택한 테넌트 유닛에서 Tenant Self-Service 모드를 활성화합니다.

   ```
   # smt tenant-unit option set tenant-unit self-service { enabled
   | disabled }
   ```

프로토콜에 의한 데이터 액세스

프로토콜별 액세스 제어를 사용하는 보안 데이터 경로에서는 테넌트 유닛에 대한 보안 및 격리가 가능합니다. SMT(Secure Multitenancy) 환경의 데이터 액세스 프로토콜 관리 명령도 테넌트 유닛 매개 변수를 통해 통합 보고를 사용할 수 있도록 향상되었습니다.

DD 시스템은 DD Boost, NFS, CIFS 및 DD VTL을 포함해 여러 데이터 액세스 프로토콜을 동시에 지원합니다. DD 시스템은 이더넷에서 NFS 또는 CIFS 액세스 권한을 제공하는 파일 서버, DD VTL 디바이스 또는 DD Boost 디바이스와 같은 애플리케이션별 인터페이스로 사용할 수 있습니다.

지원되는 각 프로토콜의 기본 액세스 제어 메커니즘은 각 테넌트의 데이터 경로가 분리되고 격리된 상태로 유지되도록 해 줍니다. 이러한 메커니즘에는 CIFS를 위한 ACL(Access Control List), NFS에 대한 내보내기 및 DD Boost 자격 증명과 Multi-User Boost 자격 증명 인식 액세스 제어가 포함됩니다.

SMT의 Multi-User DD Boost 및 스토리지 유닛

SMT(Secure Multi-Tenancy)에서 Multi-User DD Boost를 사용하는 경우 사용자 사용 권한은 스토리지 소유권에 의해 설정됩니다.

*Multi-User DD Boost*는 DD Boost 액세스 제어에 대해 여러 DD Boost 사용자 자격 증명을 사용함으로써 사용자가 각자의 사용자 이름 및 암호를 갖는 것을 의미합니다.

*스토리지 유닛*은 DD Boost 프로토콜에 맞게 구성된 MTree입니다. 사용자는 하나 이상의 스토리지 유닛과 연결하거나 이를 "소유"할 수 있습니다. 한 명의 사용자가 소유한 스토리지 유닛을 다른 사용자가 소유할 수 없습니다. 따라서 스토리지 유닛을 소유한 사용자만 백업/복구 같은 유형의 데이터 액세스를 위해 스토리지 유닛에 액세스할 수 있습니다. DD Boost 사용자 이름의 개수는 MTree의 최대 개수를 초과할 수 없습니다.

(현재 각 DD 모델의 최대 MTree 수는 이 문서의 “MTree” 장을 참조하십시오.) SMT에 연결된 스토리지 유닛에는 *none* 역할이 할당되어야 합니다.

각 백업 애플리케이션은 해당 DD Boost 사용자 이름 및 암호를 사용해 인증해야 합니다. 인증 후에 DD Boost는 스토리지 유닛의 소유권을 확인하기 위해 인증된 자격 증명을 확인합니다. 백업 애플리케이션에는 백업 애플리케이션에서 제공하는 사용자 자격 증명이 스토리지 유닛과 연결된 사용자 이름과 일치하는 경우에만 스토리지 유닛에 대한 액세스 권한이 부여됩니다. 사용자 자격 증명과 사용자 이름이 일치하지 않으면 권한 오류와 함께 작업이 실패합니다.

CIFS에 대한 액세스 구성

CIFS(Common Internet File System)는 원격 파일 액세스를 위한 파일 공유 프로토콜입니다. SMT(Secure Multitenancy) 구성에서 백업 및 복구를 위해서는 연결된 테넌트 유닛의 MTree에 상주하는 CIFS 공유에 대한 클라이언트 액세스가 필요합니다. 데이터 격리는 CIFS 공유 및 CIFS ACL을 사용해 이루어집니다.

절차

1. CIFS에 대한 MTree를 생성하고 테넌트 유닛에 MTree를 할당합니다.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. MTree에 대한 용량의 유동 및 고정 할당량을 설정합니다.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. MTree에서 *pathname*의 CIFS 공유를 생성합니다.

   ```
   # cifs share create share path pathname clients clients
   ```

NFS 액세스 구성

NFS는 원격 파일 액세스를 위한 UNIX 기반 파일 공유 프로토콜입니다. SMT(Secure Multitenancy) 환경에서 백업 및 복구를 위해서는 연결된 테넌트 유닛의 MTree에 상주하는 NFS 내보내기에 대한 클라이언트 액세스가 필요합니다. 데이터 격리는 NFS 내보내기 및 네트워크 격리를 사용해 이루어집니다. NFS는 MTree가 네트워크 격리된 테넌트 유닛과 연결되어 있는지 확인합니다. 연결되어 있으면 NFS가 테넌트 유닛과 연결된 접속 속성을 확인합니다. 접속 속성에는 대상 IP 주소와 인터페이스 또는 클라이언트 호스트 이름이 포함됩니다.

절차

1. NFS에 대한 MTree를 생성하고 테넌트 유닛에 MTree를 할당합니다.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. MTree에 대한 용량의 유동 및 고정 할당량을 설정합니다.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. MTree에 하나 이상의 클라이언트를 추가해 NFS 내보내기를 생성합니다.

   ```
   # nfs add path client-list
   ```

DD VTL에 대한 액세스 구성

DD VTL 테넌트 데이터 격리는 호스트 시스템과 DD VTL 사이에 가상 액세스 경로를 생성하는 DD VTL 액세스 그룹을 사용해 이루어집니다. 호스트 시스템 및 DD VTL 사이에 물리적 Fibre Channel 접속이 이미 존재해야 합니다.

DD VTL에 테이프를 넣으면 호스트 시스템의 백업 애플리케이션이 이 테이프에 기록하고 테이프를 읽을 수 있습니다. DD VTL 테이프는 MTree에 해당하는 DD VTL 풀에서 생

성됩니다. DD VTL 풀이 MTree이기 때문에 풀은 테넌트 유닛에 할당될 수 있습니다. 이와 같은 연결을 통해 SMT 모니터링 및 보고가 가능합니다.

예를 들어 tenant-admin이 DD VTL 풀을 포함하는 테넌트 유닛에 할당된 경우 해당 tenant-admin이 MTree 명령을 실행해 읽기 전용 정보를 표시할 수 있습니다. 명령은 테넌트 유닛에 할당된 DD VTL 풀에서만 실행할 수 있습니다.

이러한 명령에는 다음이 포함됩니다.

- `mtree list` - 테넌트 유닛의 MTree 목록 보기
- `mtree show compression` - MTree 압축 통계 보기
- `mtree show performance` - 성능 통계 보기

대부분의 `list` 및 `show` 명령에서 나온 출력에는 서비스 공급업체가 공간 사용량을 측정하고 차지백 요금을 계산하는 데 사용할 수 있는 통계가 포함됩니다.

DD VTL 작업은 영향을 받지 않으며 계속해서 정상적으로 작동합니다.

DD VTL NDMP TapeServer 사용

DD VTL 테넌트 데이터 격리는 NDMP를 통해서도 이루어집니다. DD OS가 NDMP(Network Data Management Protocol) 가능 시스템에서 3방향 NDMP 백업을 통해 DD 시스템에 백업 데이터를 보낼 수 있도록 허용하는 NDMP Tape Server를 구축합니다.

백업 데이터는 특수 DD VTL 그룹 *TapeServer*에 할당된 DD VTL에 의해 (풀에 있는) 가상 테이프에 기록됩니다.

풀에 있는 테이프에 백업 데이터가 기록되므로 MTree와 관련된 DD VTL 항목에 나와 있는 정보는 Data Domain NDMP TapeServer에도 적용됩니다.

데이터 관리 작업

SMT(Secure Multitenancy) 관리 작업에는 테넌트 유닛 및 기타 객체(예: 스토리지 유닛 및 MTree)의 모니터링이 포함됩니다. 일부 SMT 객체의 경우 추가 구성 또는 수정이 필요할 수도 있습니다.

성능 통계 수집

각 MTree에서 성능 또는 "사용량" 통계 및 기타 실시간 정보를 측정할 수 있습니다. DD Boost 스토리지 유닛에 대한 기간별 사용률이 제공됩니다. 명령 출력을 사용하면 테넌트 관리자가 테넌트 유닛에 연결된 MTree 또는 모든 MTree 및 연결된 테넌트 유닛에 대한 사용량 통계 및 압축 비율을 수집할 수 있습니다. 출력은 분에서 개월 단위에 이르는 간격으로 사용량을 표시하도록 필터링할 수 있습니다. 결과는 통계를 차지백 메트릭으로 사용하는 관리자에게 전달됩니다. 스토리지 유닛에 대한 사용량 통계 및 압축 비율을 수집하기 위해 비슷한 방법이 사용됩니다.

절차

1. MTree 실시간 성능 통계를 수집합니다.

   ```
   # mtree show stats
   ```

2. 테넌트 유닛과 연결된 MTree에 대한 성능 통계를 수집합니다.

   ```
   # mtree show performance
   ```

3. 테넌트 유닛과 연결된 MTree에 대한 압축 통계를 수집합니다.

   ```
   # mtree show compression
   ```

할당량 수정

QoS 조건을 만족하기 위해 시스템 관리자는 DD OS "옵션"을 사용해 테넌트 구성에서 요구하는 설정을 조정합니다. 예를 들어 관리자는 DD Boost 스토리지 유닛에서 "가변 할당량(soft quota)" 및 "고정 할당량(hard quota)" 제한을 설정할 수 있습니다. 스트림의 "가변 할당량(soft quota)" 및 "고정 할당량(hard quota)" 제한은 테넌트 유닛에 할당된 DD Boost 스토리지 유닛에만 할당할 수 있습니다. 관리자가 할당량을 설정한 후에 tenant-admin 역할은 하나 또는 모든 테넌트 유닛을 모니터링하여 할당량을 초과하고 다른 객체로부터 시스템 리소스를 뺏는 객체가 없는지 확인할 수 있습니다.

할당량은 구성 마법사에서 메시지가 나타날 때 처음 설정되지만 나중에 조정하거나 수정할 수 있습니다. 아래의 예는 DD Boost에 대한 할당량을 수정하는 방법을 보여 줍니다. 용량 및 스트림의 할당량과 제한을 해결하기 위해 `quota capacity` 및 `quota streams`를 사용할 수도 있습니다.

절차

1. DD Boost 스토리지 유닛 "su33"에서 가변 할당량(soft quota) 및 고정 할당량(hard quota) 제한을 수정하려면 다음을 입력합니다.

   ```
   ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
   ```

2. DD Boost 스토리지 유닛 "su33"에서 스트림 유동적 및 고정적 제한을 수정하려면 다음을 입력합니다.

   ```
   ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
   ```

3. DD Boost 스토리지 유닛 "su33"의 물리적 크기를 보고하려면 다음을 입력합니다.

   ```
   ddboost storage-unit modify su33 report-physical-size 8 GiB
   ```

SMT 및 복제

재해 발생 시 user 역할은 사용자가 데이터 복구 작업에 어떤 도움을 줄 수 있는지 결정합니다. SMT 구성에서는 여러 복제 유형을 사용할 수 있습니다. 복제를 수행하는 방법에 대한 자세한 내용은 *DD Replicator* 장을 참조하십시오.

user 역할과 관련하여 고려해야 할 몇 가지 사항은 다음과 같습니다.

- 관리자가 복제본에서 MTree를 복구할 수 있습니다.
- 테넌트 관리자가 DD Boost 관리 파일 복제를 사용해 한 시스템에서 다른 시스템으로 MTree를 복제할 수 있습니다.
- 테넌트 관리자가 역시 DD Boost 관리 파일 복제를 사용해 복제본에서 MTree를 복구할 수 있습니다.

컬렉션 복제
컬렉션 복제는 핵심 테넌트 유닛 구성 정보를 복제합니다.

공용 인터넷을 통한 안전한 복제
공용 인터넷 연결을 통해 복제할 때 MITM(man-in-the-middle) 공격을 방지하기 위해 인증에 복제 소스 및 대상에서 SSL 인증서 관련 정보의 유효성을 검사하는 과정이 포함됩니다.

DD Boost 관리 파일 복제를 사용한 MTree 복제(NFS/CIFS)
MTree 복제는 DD Boost 관리 파일 복제를 사용해 테넌트 유닛에 할당된 MTree에서 지원됩니다. MTree 복제 중에 한 시스템의 테넌트 유닛에 할당된 MTree를 다른 시스템

의 테넌트 유닛에 할당된 MTree로 복제할 수 있습니다. 두 개의 DD 시스템에 있는 서로 다른 두 테넌트 간에는 MTree 복제가 허용되지 않습니다. 보안 모드를 *strict*로 설정한 경우 MTree 복제는 MTree 가 동일한 테넌트에 속하는 경우에만 허용됩니다.

이전 버전과의 호환성을 위해 테넌트 유닛에 할당된 MTree에서 할당 취소된 MTree로 MTree 복제가 지원되기는 하지만 수동으로 구성해야 합니다. 수동 구성은 테넌트 유닛에 대해 대상 MTree의 올바른 설정을 보장합니다. 반대로 할당 취소된 MTree에서 테넌트 유닛에 할당된 MTree로의 MTree 복제 또한 지원됩니다.

SMT 인식 MTree 복제를 설정할 때 *보안 모드*는 테넌트에 수행되는 검사 정도를 정의합니다. *default* 모드는 소스와 대상이 서로 다른 테넌트에 속하지 않는지를 검사합니다. *strict* 모드는 소스와 대상이 동일한 테넌트에 속하는지 확인합니다. 그러므로 strict 모드를 사용할 때는 복제 중인 MTree와 연결된 소스 머신의 테넌트와 동일한 UUID를 사용하여 대상 시스템에 테넌트를 생성해야 합니다.

DD Boost 관리 파일 복제(DD Boost AIR 포함)

DD Boost 관리 파일 복제는 테넌트 유닛에 스토리지 유닛이 하나 또는 둘 다 할당된 경우 모두 스토리지 유닛 사이에서 지원됩니다.

DD Boost 관리 파일 복제 중에 스토리지 유닛은 전체가 복제되지 않습니다. 대신 스토리지 유닛 내의 특정 파일이 복제를 위해 백업 애플리케이션에 의해 선택됩니다. 스토리지 유닛에서 선택되고 한 시스템의 테넌트 유닛에 할당된 파일을 다른 시스템의 테넌트 유닛에 할당된 스토리지 유닛으로 복제할 수 있습니다.

이전 버전과의 호환성을 위해 테넌트 유닛에 할당된 스토리지 유닛에서 선택된 파일을 할당 취소된 스토리지 유닛으로 복제할 수 있습니다. 반대로 할당 취소된 스토리지 유닛에서 선택된 파일을 테넌트 유닛에 할당된 스토리지 유닛으로 복제할 수 있습니다.

DD Boost 관리 파일 복제는 DD Boost AIR 구축에서도 사용할 수 있습니다.

QoS를 위한 복제 제어

MTree의 복제 처리량에 대한 상한(`repl-in`)을 지정할 수 있습니다. 각 테넌트에 대한 MTree가 테넌트 유닛에 할당되기 때문에 이러한 제한을 적용하여 각 테넌트의 복제 리소스 사용량을 제한할 수 있습니다. 이 기능과 SMT의 관계 때문에 MTree 복제에 이 처리량 제한이 적용됩니다.

SMT 테넌트 알림

DD 시스템은 소프트웨어 또는 하드웨어에서 잠재적인 문제가 발견되었을 때 *이벤트*를 생성합니다. 이벤트가 생성되면 알림 목록에서 지정된 이메일을 통해 구성원과 Data Domain의 관리자에게 *알림*이 즉시 전송됩니다.

SMT 알림은 테넌트 유닛마다 다르며 DD 시스템 알림과 차이가 있습니다. Tenant Self-Service 모드가 설정된 경우 테넌트 관리자는 예기치 않은 시스템 종료처럼 자신과 연결되어 있는 다양한 시스템 객체에 대한 알림 및 중요 이벤트를 받도록 선택할 수 있습니다. 테넌트 관리자는 자신이 연결된 알림 목록만 보거나 수정할 수 있습니다.

아래 예에서는 샘플 알림을 보여 줍니다. 알림 맨 아래에 있는 두 개의 이벤트 메시지는 멀티 테넌트 환경("Tenant"라는 단어로 표시됨)에만 나타납니다. DD OS 및 SMT 알림의 전체 목록은 *Data Domain MIB Quick Reference Guide* 또는 SNMP MIB를 참조하십시오.

```
EVT-ENVIRONMENT-00021 - Description: The system has been shutdown by
abnormal method; for example, not by one of the following: 1) Via
IPMI chassis control command 2) Via power button 3) Via OS shutdown.
Action: This alert is expected after loss of AC (main power) event.
If this shutdown is not expected and persists, contact your
contracted support provider or visit us online at https://
my.datadomain.com. Tenant description: The system has experienced an
unexpected power loss and has restarted. Tenant action: This alert is
generated when the system restarts after a power loss. If this alert
repeats, contact your System Administrator.
```

스냅샷 관리

*스냅샷*은 특정 시점에 캡처된 MTree의 읽기 전용 복제본입니다. 스냅샷은 시스템 오작동 시 복원 지점 등 여러 가지 용도로 사용될 수 있습니다. `snapshot`을 사용하기 위해 필요한 역할은 admin 또는 tenant-admin입니다.

MTree 또는 테넌트 유닛에 대한 스냅샷 정보를 보려면 다음을 입력합니다.

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

MTree 또는 테넌트 유닛에 대한 스냅샷 스케줄을 보려면 다음을 입력합니다.

```
# snapshot schedule show [name | mtrees mtree-listmtree-list | tenant-unit tenant-unit]
```

파일 시스템 빠른 복제 수행

빠른 복제는 소스 디렉토리의 파일 및 디렉토리 트리를 DD 시스템의 타겟 디렉토리로 복제하는 작업입니다. SMT(Secure Multitenancy)에서 빠른 복제는 특수한 상황에서 수행됩니다.

다음은 Tenant Self-Service 모드를 설정한 상태에서 파일 시스템 빠른 복제를 수행할 때 고려해야 할 사항입니다.

- tenant-admin은 한 테넌트 유닛에서 다른 테넌트 유닛으로 파일의 빠른 복제를 수행할 수 있습니다. 이때 tenant-admin은 두 테넌트 유닛 모두의 tenant-admin이어야 하고 두 테넌트 유닛은 동일한 테넌트에 속해야 합니다.
- tenant-admin은 같은 테넌트 유닛 내에서 파일의 빠른 복제를 수행할 수 있습니다.
- tenant-admin은 소스 및 대상에 있는 테넌트 유닛 내에서 파일의 빠른 복제를 수행할 수 있습니다.

파일 시스템 빠른 복제를 수행하려면

```
# filesys fastcopy source <src> destination <dest>
```

18장

DD Cloud Tier

이 장에서 다루는 내용은 다음과 같습니다.

DD Cloud Tier 개요

DD Cloud Tier는 DD OS 6.0 이상의 기본 기능이며, 데이터를 활성 계층에서 장기간 보존을 위해 퍼블릭, 프라이빗 또는 하이브리드 클라우드의 대용량 저가 오브젝트 스토리지로 이동하는 기능입니다. DD Cloud Tier는 자주 액세스하지 않지만 규정 준수, 규제 준수 및 거버넌스 때문에 보관해야 하는 데이터를 장기간 저장하는 데 가장 적합합니다. DD Cloud Tier에 적합한 데이터는 일반적인 복구 기간이 경과한 데이터입니다.

DD Cloud Tier는 단일 Data Domain 네임스페이스를 사용하여 관리됩니다. 별도의 클라우드 게이트웨이나 가상 어플라이언스가 필요하지 않습니다. 데이터 이동은 기본 Data Domain 정책 관리 프레임워크로 지원됩니다. 개념적으로 클라우드 스토리지는 Data Domain 시스템에 연결된 추가적인 스토리지 계층(DD Cloud Tier)으로 간주되며 필요에 따라 데이터가 계층 간에서 이동됩니다. 클라우드에 저장된 데이터와 연결된 파일 시스템 메타데이터는 로컬 스토리지에 유지 관리되며 클라우드에도 미러링됩니다. 로컬 스토리지에 상주하는 메타데이터는 중복 제거, 정리, 빠른 복사 및 복제와 같은 작업을 용이하게 만듭니다. 이 로컬 스토리지는 관리가 용이하도록 클라우드 유닛이라는 독립형 버킷으로 나뉩니다.

지원 플랫폼

Cloud Tier는 다른 스토리지 계층을 수용하기 위해 필요한 메모리, CPU 및 스토리지 접속 구성이 있는 물리적 플랫폼에서 지원됩니다.

DD Cloud Tier는 다음 시스템에서 지원됩니다.

표 196 DD Cloud Tier가 지원되는 구성

모델	메모리	클라우드 용량	필요한 개수의 SAS 입출력 모듈	메타데이터 스토리지에 지원되는 디스크 셸프 유형	필요한 ES30 셸프 또는 DS60 디스크 팩 수	메타데이터 스토리지에 필요한 용량
DD990	256GB	1140TB	4	ES30	4	60 x 3TB HDD = 180TB
DD3300 4TB	16GB	8TB	해당 없음	해당 없음	해당 없음	1 x 1TB 가상 디스크 = 1TB
DD3300 8TB	48GB	16TB	해당 없음	해당 없음	해당 없음	2 x 1TB 가상 디스크 = 2TB
DDD3300 16TB	48GB	32TB	해당 없음	해당 없음	해당 없음	2 x 1TB 가상 디스크 = 2TB
DD3300 32TB	64GB	64TB	해당 없음	해당 없음	해당 없음	4 x 1TB 가상 디스크 = 4TB
DD4200	128GB	378TB	3	DS60 또는 ES30	2	30 x 3TB HDD = 90TB
DD4500	192GB	570TB	3	DS60 또는 ES30	2	30 x 4TB HDD = 120TB
DD6800	192GB	576TB	2	DS60 또는 ES30	2	30 x 4TB HDD = 120TB
DD7200	256GB	856TB	4	DS60 또는 ES30	4	60 x 4TB HDD = 240TB

표 196 DD Cloud Tier가 지원되는 구성 (계속)

모델	메모리	클라우드 용량	필요한 개수의 SAS 입출력 모듈	메타데이터 스토리지에 지원되는 디스크 셸프 유형	필요한 ES30 셸프 또는 DS60 디스크 팩 수	메타데이터 스토리지에 필요한 용량
DD9300	384GB	1400TB	2	DS60 또는 ES30	4	60 x 4TB HDD = 240TB
DD9500	512GB	1728TB	4	DS60 또는 ES30	5	75 x 4TB HDD = 300TB
DD9800	768GB	2016TB	4	DS60 또는 ES30	5	75 x 4TB HDD = 300TB
DD VE 16TB	32GB	32TB	해당 없음	해당 없음	해당 없음	1 x 500GB 가상 디스크 = 500GB[a]
DD VE 64TB	60GB	128TB	해당 없음	해당 없음	해당 없음	1 x 500GB 가상 디스크 = 500GB[a]
DD VE 96TB	80GB	192TB	해당 없음	해당 없음	해당 없음	1 x 500GB 가상 디스크 = 500GB[a]

a. 최소 메타데이터 크기는 고정적 제한입니다. 메타데이터 스토리지는 처음에 1TB부터 시작하여 1TB 증분으로 확장하는 것이 좋습니다. DD VE에서 DD Cloud Tier를 사용하는 것에 대한 자세한 내용은 *Data Domain Virtual Edition 설치 및 관리 가이드*를 참조하십시오.

참고

DD Cloud Tier는 Data Domain HA(High Availability) 환경에서 지원됩니다. 두 노드 모두 DD OS 6.0 이상을 실행하고 있어야 하며 HA가 활성화되어 있어야 합니다.

참고

DD Cloud Tier는 나열되지 않은 시스템에서 지원되지 않으며 Extended Retention 기능이 활성화되거나 Collection Replication으로 구성된 시스템에서 지원되지 않습니다.

참고

Cloud Tier 기능은 특히 낮은 대역폭 구성(1Gbps)에서 공유 WAN 링크의 모든 사용 가능한 대역폭을 소비할 수 있으며 WAN 링크를 공유하는 다른 애플리케이션에 영향을 미칠 수 있습니다. WAN 기반의 공유 애플리케이션이 있는 경우 정체를 방지하고 일관된 시간별 성능을 유지하려면 QoS 또는 기타 네트워크 제한 기능을 사용하는 것이 좋습니다.
대역폭이 제한되는 경우 데이터의 이동 속도가 느려지고 많은 양의 데이터를 클라우드로 이동할 수 없습니다. Cloud Tier로 이동하는 데이터에 대해 전용 링크를 사용하는 것이 좋습니다.

참고

온보드 관리 네트워크 인터페이스 컨트롤러(ethMx 인터페이스)를 통해 트래픽을 보내지 마십시오.

DD Cloud Tier 성능

Data Domain 시스템은 내부 최적화를 사용하여 DD Cloud Tier 성능을 극대화합니다.

클라우드 시딩
클라우드로의 현재 마이그레이션 엔진은 파일을 기반으로 하며, 효율적인 중복 제거 최적화 엔진이 고유 세그먼트만 식별하여 클라우드로 마이그레이션하는 데 사용됩니다. 이 파일 기반 마이그레이션 엔진은 더 높은 세대 데이터를 클라우드 계층으로 마이그레이션할 때 효율성이 뛰어납니다. 이러한 경우는 중복을 제거할 데이터가 이미 있는 상태이기 때문입니다. 그러나 클라우드 계층이 비어 있거나 거의 비어 있는 경우에는 중복을 제거할 데이터가 없습니다. 중복 제거에 투자되는 컴퓨팅 주기의 오버 헤드가 있습니다. 시드 기반 마이그레이션을 사용하는 경우 중복 제거 필터링이 활성 계층 자체에서 유지되며, 고유한 데이터만 클라우드 계층으로 대량으로 마이그레이션됩니다. 클라우드 시딩에서 엔진은 중복 제거 처리를 하지 않고 로컬 스토리지에서 클라우드 스토리지로 콘텐츠를 마이그레이션합니다. 클라우드 시드가 활성화되면 시드로 확인된 모든 파일의 마이그레이션이 완료될 때까지, 클라우드 스토리지로 마이그레이션되도록 표시된 파일이 활성 계층 파일 시스템 정리의 일부로 정리되지 않습니다(예: 공간이 사용 가능하게 해제되지 않음). 많은 양의 데이터를 클라우드 스토리지로 마이그레이션해야 하는 환경에서는 이 기능을 고려하여 활성 계층을 사이징해야 합니다. DD Cloud Tier 스토리지의 용량이 5% 미만이고 show space 명령에 표시된 것처럼 구성 후 데이터 사용량이 30TiB(또는 이상)이면 Data Domain 시스템은 데이터를 클라우드 스토리지로 마이그레이션할 때 자동으로 클라우드 시딩을 사용합니다.

DD Cloud Tier 용량의 5%가 소비되면 클라우드 시딩이 자동으로 비활성화되고 클라우드 스토리지로 마이그레이션하기 전에 중복 제거를 위해 데이터를 처리합니다.

다음은 시드 마이그레이션을 사용할 때 추가적으로 고려할 사항입니다.

- 다음과 같은 경우에만 시드 모드에서 마이그레이션이 지원됩니다.
  - 활성 계층 구성 후 사용된 크기는 filesys show space 출력에 보고된 것처럼 30TiB 이상입니다.
  - 활성 계층이 70% 미만으로 채워져 있으며 이때 filesys show space 출력에 보고된 것처럼 마이그레이션이 시작됩니다.

    참고

    시드 모드에서 진행 중인 마이그레이션 주기 동안의 활성 계층 사용량이 90%를 초과하면 마이그레이션이 중단되고 일반 Filecopy 모드로 마이그레이션이 다시 시작됩니다.
- 시드 모드의 마이그레이션은 활성 계층의 전체 정리 기간 동안 활성 계층을 정리하면 자동으로 일시 중단됩니다. 정리가 완료되면 시드가 자동으로 다시 시작되고 클라우드로의 마이그레이션이 다시 시작됩니다.
- 시드 모드의 마이그레이션은 마이그레이션하는 클라우드 유닛에서 클라우드 UNAVAIL 이벤트가 수신될 경우(cloud-unit이 “disconnected”로 보고됨) 자동으로 일시 중단되었다가 클라우드 유닛이 사용 가능해지고 활성 상태임을 보고해야만 다시 시작됩니다.
- 시드 모드에서 진행 중인 마이그레이션 작업의 대상에 해당하는 클라우드 유닛에서는 정리를 시작할 수 없습니다.

참고

두 클라우드 유닛 시스템에서 시드되지 않는 두 번째 클라우드 유닛에 대해 강제로 정리를 시작하려면 data-movement suspend CLI를 사용하여 시드 모드의 마이그레이션을 일시 중단하고 두 번째 클라우드 유닛에서 execute cloud clean start CLI를 실행합니다.

- 시드 모드에서 마이그레이션이 진행 중인 클라우드 유닛에서는 기본 정책에 따라 예약된 경우에도 클라우드의 확률적 파일 검증이 생략되고 수행되지 않습니다.
- 클라우드 계층 또는 활성 계층에서 정리가 이미 진행 중이며 예약된 데이터 이동이 시드 모드에서 시작될 경우 정리 작업 기간 동안 데이터 이동이 자동으로 일시 중단됩니다.
- 시드 모드의 마이그레이션에서는 파일이 마이그레이션에 적합한 경우에도 복제 대상에 해당하는 MTree의 파일 마이그레이션을 건너뜁니다. 복제 대상 MTree(RO/RD)에 해당하는 이러한 MTree의 파일은 모든 적격 MTree에서의 시드 모드 마이그레이션이 완료되면 filecopy 엔진을 사용하여 마이그레이션됩니다.
- 물리적 용량 보고 기능이 활성화되고 예약된 경우, 시드 모드 마이그레이션은 시드 기반 마이그레이션 기간 동안 용량 보고 기능을 일시 중단합니다.
- 시드 모드의 마이그레이션은 80Gb 이상의 RAM이 있는 모든 클라우드 지원 Data Domain 시스템 및 구성에서만 지원됩니다. 시드 기반 마이그레이션은 DD VE에 대해 기본적으로 비활성화됩니다.

큰 객체 크기

DD Cloud Tier는 1MB 또는 4MB의 객체 크기(클라우드 스토리지 공급업체에 따라 다름)를 사용하여 메타데이터 오버헤드를 줄이고 클라우드 스토리지로 마이그레이션하는 객체 수를 줄입니다.

Cloud Tier 구성

Cloud Tier를 구성하려면 라이센스 및 엔클로저를 추가하고 시스템 암호를 설정한 후 클라우드로의 데이터 이동을 지원하는 파일 시스템을 생성합니다.

- Cloud Tier에는 클라우드 용량 라이센스가 필요합니다.
- Cloud Tier 라이센스를 등록하려면 해당 *Data Domain Operating System Release Notes*에서 제품 기능, 소프트웨어 업데이트, 소프트웨어 호환성 가이드에 대한 최신 정보와 Data Domain 제품, 라이센스 등록 및 서비스에 대한 정보를 참조하십시오.
- 시스템 암호를 설정하려면 **Administration** > **Access** > **Administrator Access** 탭을 사용합니다.
  시스템 암호가 설정되지 않은 경우 Passphrase 영역에 **Set Passphrase** 버튼이 나타납니다. 시스템 암호가 구성된 경우 **Change Passphrase** 버튼이 나타나며 사용자는 암호 변경만 수행할 수 있습니다.
- 스토리지를 구성하려면 **Hardware** > **Storage** 탭을 사용합니다.
- 파일 시스템을 생성하려면 File System Create 마법사를 사용합니다.

DD Cloud Tier를 위한 스토리지 구성

DD 시스템의 Cloud Tier 스토리지는 클라우드 유닛에 필요합니다. 이 스토리지는 클라우드에 데이터가 상주하는 파일의 메타데이터를 유지합니다.

절차

1. **Hardware** > **Storage**를 선택합니다.

2. Overview 탭에서 **Cloud Tier**를 확장합니다.
3. **Configure**를 클릭합니다.

   Configure Cloud Tier 대화 상자가 표시됩니다.
4. Addable Storage 섹션에서 추가할 셸프의 확인란을 선택합니다.

   ⚠ 주의

   DD3300 시스템의 DD Cloud Tier 메타데이터 스토리지에는 1TB 스토리지 디바이스를 사용해야 합니다.
5. **Add to Tier** 버튼을 클릭합니다.
6. **Save**를 클릭하여 스토리지를 추가합니다.
7. **Data Management** > **File System**을 선택하고 Cloud Tier 기능을 활성화합니다.
8. 화면 맨 아래에 있는 **Disable** 을 클릭하여 파일 시스템을 비활성화합니다.
9. **OK**를 클릭합니다.
10. 파일 시스템이 비활성화된 후 **Enable Cloud Tier**를 선택합니다.

    클라우드 계층을 활성화하려면 라이센스가 부여된 용량에 대한 스토리지 요구 사항이 충족되어야 합니다. 파일 시스템의 클라우드 계층을 구성합니다. **Next**를 클릭합니다.
    클라우드 파일 시스템에는 클라우드 메타데이터의 로컬 복사본을 위한 로컬 저장소가 필요합니다.
11. **Enable file system**을 선택합니다.

    클라우드 계층이 지정된 스토리지로 활성화됩니다.
12. **OK**를 클릭합니다.

    파일 시스템이 생성된 후 개별적으로 클라우드 유닛을 생성해야 합니다.

Cleanable Space Estimation

Cleanable Space Estimation 툴은 `data-movement`가 적격 파일을 클라우드로 이동하고 GC가 파일 시스템을 정리하는 경우 활성 계층에서 사용 가능 상태로 해제할 수 있는 공간 크기를 평가합니다.

이 툴은 클라우드/아카이브 라이선스 존재 여부와 관계없이 작동할 수 있습니다.

클라우드/활성 라이선스가 없는 경우 활성 계층의 총 정리 가능 공간을 평가하는 데 사용해야 하는 사용 기간 임계값을 제공합니다. MTree에 설정된 정책과 사용 기간 임계값이 있는 경우 사용자가 제공한 사용 기간 임계값이 우선적으로 적용됩니다.

다음과 같은 세 가지 워크플로가 진행됩니다.

- 클라우드 마이그레이션 정책이 설정된 시스템: 파일은 각 MTree에 설정된 정책에 따라 "적격"으로 식별되고 정리 가능 공간이 계산됩니다.
- 클라우드 마이그레이션 정책이 설정되어 있으나 사용자가 제공한 사용 기간 임계값이 있는 시스템: 파일은 사용자가 제공한 사용 기간 임계값에 따라 식별되고 시스템 정책은 재정의됩니다.
- 클라우드를 사용하지 않는 시스템: 사용자는 총 정리 가능 공간을 결정하는 데 사용되는 사용 기간 임계값을 제공해야 합니다.

몇 가지 추가적으로 고려할 사항은 다음과 같습니다.

- 데이터 이동을 데이터 이동 자격 검사와 함께 실행할 수 없고 그 반대의 경우도 마찬가지입니다.

- 자격 검사가 실행 중인 경우 활성 계층에 대한 정리를 시작할 수 없으며 그 반대의 경우도 마찬가지입니다.
- 자격 검사가 실행 중인 경우 클라우드 계층에 대한 정리를 시작할 수 없으며 그 반대의 경우도 마찬가지입니다.
- UNAVAIL 이벤트가 수신되어도 자격 검사 작업에 영향을 주지 않습니다.
- 파일 시스템이 중지되거나 충돌하는 경우, 자격 검사가 중지되고, 파일 시스템이 다시 가동되어도 자동으로 다시 시작되지 않습니다.

참고

Data Domain System Manager GUI의 자격 검사 시작에 대한 프로비저닝은 없습니다.

클라우드 유닛 구성

클라우드 계층은 최대 두 개의 클라우드 유닛으로 구성되며 각 클라우드 유닛은 클라우드 공급업체에 매핑되므로 한 Data Domain 시스템에서 여러 클라우드 공급업체를 사용할 수 있습니다. Data Domain 시스템은 클라우드에 연결되어야 하고 지원되는 클라우드 공급업체에 계정이 있어야 합니다.

클라우드 유닛은 다음 단계를 통해 구성됩니다.

- 방화벽 및 프록시 설정을 포함한 네트워크 구성
- CA 인증서 가져오기
- 클라우드 유닛 추가

방화벽 및 프록시 설정

네트워크 방화벽 포트

- 양방향 트래픽을 위해 엔드포인트 IP와 공급업체 인증 IP 모두 포트 443(HTTPS) 및/또는 포트 80(HTTP)이 클라우드 공급업체 네트워크에 대해 열려 있어야 합니다.
  예를 들어 Amazon S3의 경우 s3-ap-southeast-1.amazonaws.com 및 s3.amazonaws.com 모두 포트 80 및/또는 포트 443의 차단을 해제하고 양방향 IP 트래픽을 허용하도록 설정해야 합니다.

  참고

  몇몇 퍼블릭 클라우드 공급업체는 엔드포인트 및 인증 주소로 IP 범위를 사용합니다. 이 경우 잠재적인 IP 변경 사항을 수용할 수 있도록 공급업체에서 사용하는 IP 범위를 차단하지 않아야 합니다.
- 원격 클라우드 공급업체 대상 IP 및 액세스 인증 IP 주소 범위는 방화벽을 통과하도록 허용되어야 합니다.
- ECS 프라이빗 클라우드의 경우 로컬 ECS 인증 및 웹 스토리지(S3) 액세스 IP 범위와 포트 9020(HTTP) 및 9021(HTTPS)이 로컬 방화벽을 통과하도록 허용해야 합니다.

  참고

  ECS 프라이빗 클라우드 로드 밸런싱 장치 IP 액세스 및 포트 규칙도 구성해야 합니다.

프록시 설정

특정 크기보다 큰 데이터를 거부하도록 설정된 기존 프록시 설정이 있는 경우 해당 설정을 최대 4.5MB의 객체 크기를 허용하도록 변경해야 합니다.

고객 트래픽이 프록시를 통해 라우팅되는 경우 자체 서명/CA 서명 프록시 인증서를 가져와야 합니다. 자세한 내용은 "CA 인증서 가져오기"를 참조하십시오.

OpenSSL 암호 그룹

- 암호 - ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384
- TLS 버전: 1.2

참고

모든 클라우드 공급업체와의 기본 통신은 강력한 암호로 초기화됩니다.

지원되는 프로토콜

- HTTP
- HTTPS

참고

모든 퍼블릭 클라우드 공급업체와의 통신은 기본적으로 보안 HTTP인 HTTPS를 통해 이루어지지만 기본 설정을 무시하고 HTTP를 사용할 수도 있습니다.

CA 인증서 가져오기

ECS(Elastic Cloud Storage), Virtustream Storage Cloud, Alibaba Cloud, AWS(Amazon Web Services) S3 및 Azure 클라우드를 위한 클라우드 유닛을 추가하려면 먼저 CA 인증서를 가져와야 합니다.

시작하기 전에

AWS, Virtustream 및 Azure 퍼블릭 클라우드 공급업체의 경우 https://www.digicert.com/digicert-root-certificates.htm에서 루트 CA 인증서를 다운로드할 수 있습니다.

- AWS 클라우드 공급업체의 경우 Baltimore CyberTrust Root 인증서를 다운로드합니다.
- Virtustream 클라우드 공급업체의 경우 DigiCert High Assurance EV Root CA 인증서를 다운로드합니다.
- ECS의 경우 루트 인증 기관이 고객마다 다릅니다.
  ECS에 클라우드 스토리지를 구축하려면 로드 밸런싱 장치가 필요합니다. HTTPS 엔드포인트가 구성의 엔드포인트로 사용되는 경우 루트 CA 인증서를 가져와야 합니다. 자세한 내용은 로드 밸런싱 장치 공급업체에 문의하십시오.
- Azure 클라우드 공급업체의 경우 Baltimore CyberTrust Root 인증서를 다운로드합니다.
- S3 Flexible 공급업체인 경우 루트 CA 인증서를 가져옵니다. 자세한 내용은 S3 Flexible 공급업체에 문의하십시오.

다운로드한 인증서는 .crt 확장자를 가지며, 이 인증서를 PEM 인코딩된 인증서로 변환해야 할 수 있습니다. 이 경우 OpenSSL을 사용하여 파일을 .crt 형식으로 .pem 형식으로 변환합니다(예: `openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`).

Alibaba 정보:

1. https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates에서 GlobalSign Root R1 인증서를 다운로드합니다.

2. 다운로드한 인증서를 PEM 인코딩 형식으로 변환합니다. 이 변환을 위한 OpenSSL 명령은 다음과 같습니다. `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. 인증서를 Data Domain 시스템으로 가져옵니다.

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. 툴 모음에서 **Manage Certificates**를 클릭합니다.

   Manage Certificates for Cloud 대화 상자가 표시됩니다.
3. **Add**를 클릭합니다.
4. 다음 중 한 옵션을 선택합니다.
   - **I want to upload the certificate as a .pem file.**
     인증서 파일을 찾아 선택합니다.
   - **I want to copy and paste the certificate text.**
     - .pem 파일의 내용을 복사 버퍼에 복사합니다.
     - 대화 상자에 버퍼를 붙여 넣습니다.
5. **Add**를 클릭합니다.

ECS(Elastic Cloud Storage)를 위한 클라우드 유닛 추가

Data Domain 시스템 또는 DD VE 인스턴스를 사용할 경우 Data Domain 클라우드 유닛을 구성하는 ECS 시스템과의 완벽한 시간 동기화가 필요합니다. ECS 시스템과 Data Domain 시스템 또는 DD VE 인스턴스에서 NTP를 구성하여 이 문제를 해결합니다.

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**에 대해 드롭다운 목록에서 **EMC Elastic Cloud Storage (ECS)**를 선택합니다.
5. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
6. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.
7. 공급업체 **엔드포인트**를 **`http://<ip/hostname>:<port>`** 형식으로 입력합니다. 보안 엔드포인트를 사용하는 경우 **`https`**를 사용합니다.

   참고

   ECS에 클라우드 스토리지를 구축하려면 로드 밸런싱 장치가 필요합니다.

   기본적으로 ECS는 HTTP의 경우 포트 9020에서, HTTPS의 경우 9021에서 S3 프로토콜을 실행합니다. 로드 밸런싱 장치가 사용되면 이러한 포트가 HTTP의 경우 80, HTTPS의 경우 443으로 재매핑되는 경우가 있습니다. 적절한 포트는 네트워크 관리자에게 문의하십시오.

8. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

   프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

   참고

   클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

9. **Add**를 클릭합니다.

   이제 File System 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

Virtustream을 위한 클라우드 유닛 추가

Virtustream은 다양한 스토리지 클래스를 제공합니다. http://compatibilityguide.emc.com:8080/CompGuideApp/에서 사용할 수 있는 *Cloud Providers Compatibility Matrix*에는 지원되는 스토리지 클래스에 대한 최신 정보가 나와 있습니다.

스토리지 클래스 및 지역에 따라 다음과 같은 엔드포인트가 Virtustream 클라우드 공급업체에 사용됩니다. 클라우드 유닛을 구성하기 전에 DNS에서 이러한 호스트 이름을 확인할 수 있는지 확인하십시오.

- s-us.objectstorage.io
- s-eu.objectstorage.io
- s-eu-west-1.objectstorage.io
- s-eu-west-2.objectstorage.io
- s-us-central-1.objectstorage.io

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**에 대해 드롭다운 목록에서 **Virtustream Storage Cloud**를 선택합니다.
5. 드롭다운 목록에서 스토리지 클래스를 선택합니다.
6. 드롭다운 목록에서 계정 유형과 일치하는 적절한 지역을 선택합니다.
7. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
8. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.
9. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

   프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

참고

클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

10. **Save**를 클릭합니다.

    이제 파일 시스템 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

Alibaba를 위한 클라우드 유닛 추가

리전은 객체 수준이 아닌 버킷 수준에서 구성됩니다. 따라서 버킷에 포함된 모든 객체는 동일한 리전에 저장됩니다. 리전은 버킷을 생성할 때 지정되며 일단 생성된 후에는 변경할 수 없습니다.

표 197 Alibaba 리전

Regions	위치	리전 이름
중국 본토 리전	중국 동부 1(항저우)	oss-cn-hangzhou
	중국 동부 2(상하이)	oss-cn-shanghai
	중국 북부 1(칭다오)	oss-cn-qingdao
	중국 북부 2(베이징)	oss-cn-beijing
	중국 북부 3(장자커우)	oss-cn-zhangjiakou
	중국 북부 5(후후호트)	oss-cn-huhehaote
	중국 남부 1(선전)	oss-cn-shenzhen
국제 리전	홍콩	oss-cn-hongkong
	미국 서부 1(실리콘 밸리)	oss-us-west-1
	미국 동부 1(버지니아)	oss-us-east-1
	아시아 태평양 SE 1(싱가포르)	oss-ap-southeast-1
	아시아 태평양 SE 2(시드니)	oss-ap-southeast-2
	아시아 태평양 SE 3(쿠알라룸푸르)	oss-ap-southeast-3
	아시아 태평양 SE 5(자카르타)	oss-ap-southeast-5
	아시아 태평양 NE 1(도쿄)	oss-ap-northeast-1
	아시아 태평양 SOU 1(뭄바이)	oss-ap-south-1
	EU 중부 1(프랑크푸르트)	oss-eu-central-1
	중동 1(두바이)	oss-me-east-1

Alibaba Cloud 사용자 자격 증명에는 버킷을 생성 및 삭제하고, 생성한 버킷 내의 파일을 추가, 수정 및 삭제할 수 있는 사용 권한이 있어야 합니다. AliyunOSSFullAccess는 권장 사항이지만 다음은 최소 요구 사항입니다.

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**의 경우 드롭다운 목록에서 **Alibaba Cloud**를 선택합니다.
5. **Storage class** 드롭다운 목록에서 **Standard** 또는 **IA**를 선택합니다.
6. **Storage region** 드롭다운 목록에서 리전을 선택합니다.
7. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
8. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.
9. 방화벽에서 포트 443(HTTPS)이 차단되어 있지 않은지 확인합니다. Alibaba 클라우드 공급업체와의 통신은 포트 443에서 발생합니다.
10. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

    프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

    참고

    클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

    ---

11. **Add**를 클릭합니다.

    이제 파일 시스템 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

Amazon Web Services S3을 위한 클라우드 유닛 추가

AWS는 다양한 스토리지 클래스를 제공합니다. http://compatibilityguide.emc.com:8080/CompGuideApp/에서 사용할 수 있는 *Cloud Providers Compatibility Matrix*에는 지원되는 스토리지 클래스에 대한 최신 정보가 나와 있습니다.

보안 강화를 위해 Cloud Tier 기능은 모든 AWS 요청에 대해 Signature Version 4를 사용합니다. Signature Version 4 서명은 기본적으로 활성화됩니다.

스토리지 클래스 및 지역에 따라 다음과 같은 엔드포인트가 AWS 클라우드 공급업체에 사용됩니다. 클라우드 유닛을 구성하기 전에 DNS에서 이러한 호스트 이름을 확인할 수 있는지 확인하십시오.

- s3.amazonaws.com
- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

참고

중국 지역은 지원되지 않습니다.

참고

AWS 사용자 자격 증명에는 버킷을 생성 및 삭제하고, 생성한 버킷 내의 파일을 추가, 수정 및 삭제할 수 있는 사용 권한이 있어야 합니다. S3FullAccess는 권장 사항이지만 다음은 최소 요구 사항입니다.

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**의 경우 드롭다운 목록에서 **Amazon Web Services S3**을 선택합니다.
5. 드롭다운 목록에서 스토리지 클래스를 선택합니다.
6. 드롭다운 목록에서 적절한 **스토리지 지역**을 선택합니다.
7. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
8. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.

9. 방화벽에서 포트 443(HTTPS)이 차단되어 있지 않은지 확인합니다. AWS 클라우드 공급업체와의 통신은 포트 443에서 발생합니다.
10. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

    프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

    참고

    클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

11. **Add**를 클릭합니다.

    이제 파일 시스템 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

Azure를 위한 클라우드 유닛 추가

Microsoft Azure는 다양한 스토리지 계정 유형을 제공합니다. http://compatibilityguide.emc.com:8080/CompGuideApp/에서 사용할 수 있는 *Cloud Providers Compatibility Matrix*에는 지원되는 스토리지 클래스에 대한 최신 정보가 나와 있습니다.

스토리지 클래스 및 지역에 따라 다음과 같은 엔드포인트가 Azure 클라우드 공급업체에 사용됩니다. 클라우드 유닛을 구성하기 전에 DNS에서 이러한 호스트 이름을 확인할 수 있는지 확인하십시오.

- *계정 이름*.blob.core.windows.net

계정 이름은 Azure 클라우드 공급업체 콘솔에서 얻습니다.

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**에 대해 드롭다운 목록에서 **Microsoft Azure Storage**를 선택합니다.
5. **Account type**에서 **Government** 또는 **Public**을 선택합니다.
6. 드롭다운 목록에서 스토리지 클래스를 선택합니다.
7. 공급업체 **계정 이름**을 입력합니다.
8. 암호 텍스트로 공급업체 **기본 키**를 입력합니다.
9. 암호 텍스트로 공급업체 **보조 키**를 입력합니다.
10. 방화벽에서 포트 443(HTTPS)이 차단되어 있지 않은지 확인합니다. Azure 클라우드 공급업체와의 통신은 포트 443에서 발생합니다.
11. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

    프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

참고

클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

12. **Add**를 클릭합니다.

    이제 파일 시스템 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

Google Cloud 공급업체를 위한 클라우드 유닛 추가

다음 표에서는 데이터를 저장하는 데 사용할 수 있는 클라우드 스토리지 위치를 나열합니다.

표 198 다중 리전 위치

다중 리전 이름	다중 리전 설명
아시아	아시아의 데이터 센터
US	미국의 데이터 센터
EU	유럽 연합의 데이터 센터

표 199 리전 위치

리전 위치	위치	리전 이름
북미	northamerica-northeast1	몬트리올
	us-central1	아이오와
	us-east1	사우스캐롤라이나
	us-east4	버지니아 북부
	us-west1	오리건
	us-west2	로스엔젤레스
남미	southamerica-east1	상파울로
유럽	europe-north1	핀란드
	europe-west1	벨기에
	europe-west2	런던
	europe-west3	프랑크푸르트
	europe-west4	네덜란드
아시아	asia-east1	대만
	asia-northeast1	도쿄
	asia-south1	뭄바이
	asia-southeast1	싱가포르
오스트레일리아	australia-southeast1	시드니

Google Cloud 공급업체 사용자 자격 증명에는 버킷을 생성 및 삭제하고, 생성한 버킷 내의 파일을 추가, 수정 및 삭제할 수 있는 사용 권한이 있어야 합니다. 최소 요구 사항은 다음과 같습니다.

- ListBucket
- PutBucket
- GetBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

참고

DD Cloud 계층은 Nearline만 지원하며 설치 중에 자동으로 선택됩니다.

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**에 대해 드롭다운 목록에서 **Virtustream Storage Cloud**를 선택합니다.
5. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
6. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.
7. **Storage class**는 기본적으로 **Nearline**으로 설정됩니다.

   다중 리전 위치를 선택하는 경우(아시아, 유럽 연합 또는 미국) 스토리지 클래스와 위치 제약 조건이 Nearline 다중 리전입니다. 다른 모든 리전 위치에서는 스토리지 클래스가 Nearline 리전으로 설정됩니다.
8. **Region**을 선택합니다.
9. 방화벽에서 포트 443(HTTPS)이 차단되어 있지 않은지 확인합니다. Google Cloud 공급업체와의 통신은 포트 443에서 발생합니다.
10. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

    프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

    참고

    클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.
11. **Add**를 클릭합니다.

이제 파일 시스템 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

S3 Flexible 공급업체 클라우드 유닛 추가

Cloud Tier 기능은 추가 검증된 S3 클라우드 공급업체를 S3 Flexible 공급업체 구성 옵션으로 지원합니다.

S3 Flexible 공급업체 옵션은 표준(Standard) 스토리지 클래스와 더불어, 액세스 빈도가 낮지만 필요할 때 빠르게 액세스해야 하는 데이터를 위한 표준-IA(Standard-Infrequent-Access) 스토리지 클래스를 지원합니다. 엔드포인트는 클라우드 공급업체, 스토리지 클래스 및 영역에 따라 다릅니다. 클라우드 유닛을 구성하기 전에 DNS에서 이러한 호스트 이름을 확인할 수 있는지 확인하십시오.

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. **Add**를 클릭합니다.

   Add Cloud Unit 대화 상자가 표시됩니다.
3. 이 클라우드 유닛의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

   Add Cloud Unit 대화 상자의 나머지 필드는 클라우드 공급업체 계정과 관련이 있습니다.
4. **Cloud provider**에 대해 드롭다운 목록에서 **Flexible Cloud Tier Provider Framework for S3**을 선택합니다.
5. 암호 텍스트로 공급업체 **액세스 키**를 입력합니다.
6. 암호 텍스트로 공급업체 **암호 키**를 입력합니다.
7. 적절한 **Storage region**을 지정합니다.
8. 공급업체 **엔드포인트**를 `http://<ip/hostname>:<port>` 형식으로 입력합니다. 보안 엔드포인트를 사용하는 경우 `https`를 사용합니다.
9. **Storage class**에 대해 드롭다운 목록에서 적절한 스토리지 클래스를 선택합니다.
10. 방화벽에서 포트 443(HTTPS)이 차단되어 있지 않은지 확인합니다. S3 클라우드 공급업체와의 통신은 포트 443에서 발생합니다.
11. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.

    프록시 호스트 이름, 포트, 사용자 이름 및 암호를 입력합니다.

    참고

    클라우드 유닛을 추가하기 전에 클라우드 공급업체 확인 툴을 실행하는 선택적인 단계가 제공됩니다. 이 툴은 사전 검사 테스트를 수행하여 실제 클라우드 유닛을 추가하기 전에 모든 요구 사항을 충족하는지 확인합니다.

    ---

12. **Add**를 클릭합니다.

    이제 File System 기본 창에 새 클라우드 유닛에 대한 요약 정보와 클라우드 유닛을 활성화하거나 비활성화할 수 있는 컨트롤이 표시됩니다.

클라우드 유닛 또는 클라우드 프로파일 수정

클라우드 유닛 자격 증명, S3 Flexible 공급업체 이름 또는 클라우드 프로파일의 세부 정보를 수정합니다.

클라우드 유닛 자격 증명 수정

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. 자격 증명을 수정하려는 클라우드 유닛의 연필 아이콘을 클릭합니다.

   Modify Cloud Unit 대화 상자가 표시됩니다.
3. **Account name**에 새 계정 이름을 입력합니다.
4. **Access key**에 새 공급업체 액세스 키를 암호 텍스트로 입력합니다.

   참고

   ECS 환경에서는 액세스 키 수정이 지원되지 않습니다.
5. **Secret key**에 새 공급업체 암호 키를 암호 텍스트로 입력합니다.
6. **Primary key**에 새 공급업체 기본 키를 암호 텍스트로 입력합니다.

   참고

   기본 키 수정은 Azure 환경에서만 지원됩니다.
7. 이 공급업체에서 방화벽을 우회하기 위해 HTTP 프록시 서버가 필요한 경우 **HTTP Proxy Server**의 **Configure**를 클릭합니다.
8. **OK**를 클릭합니다.

S3 Flexible 공급업체 이름 수정

절차

1. **Data Management** > **File System** > **Cloud Units**를 선택합니다.
2. 이름을 수정하려는 S3 Flexible 클라우드 유닛의 연필 아이콘을 클릭합니다.

   Modify Cloud Unit 대화 상자가 표시됩니다.
3. **S3 Provider Name**에 새 공급업체 이름을 입력합니다.
4. **OK**를 클릭합니다.

CLI를 사용하여 클라우드 프로파일 수정

절차

1. `cloud profile modify` 명령을 실행하여 클라우드 프로파일의 세부 정보를 수정합니다. 클라우드 프로파일의 개별 세부 정보를 수정하라는 메시지가 표시됩니다.

   Virtustream, AWS S3 또는 Azure 프로파일의 경우 이 명령을 실행하여 기존 클라우드 프로파일에 스토리지 클래스를 추가합니다.

   수정할 수 있는 프로파일 세부 정보는 클라우드 공급업체에 따라 다릅니다.

- Alibaba Cloud는 액세스 키 및 암호 키의 수정을 지원합니다.
- AWS S3은 액세스 키 및 암호 키의 수정을 지원합니다.
- Azure는 액세스 키, 암호 키 및 기본 키의 수정을 지원합니다.
- ECS는 암호 키 수정을 지원합니다.
- Virtustream은 액세스 키 및 암호 키의 수정을 지원합니다.
- S3 Flexible은 액세스 키, 암호 키 및 공급업체 이름의 수정을 지원합니다.

클라우드 유닛 삭제

이 작업으로 인해 삭제하도록 선택한 클라우드 유닛의 모든 데이터가 손실됩니다. 클라우드 유닛을 삭제하기 전에 모든 파일을 삭제해야 합니다.

시작하기 전에

- 클라우드로의 데이터 이동이 실행 중인지 확인하십시오(CLI 명령: data-movement status). 실행 중인 경우 "data-movement stop" CLI 명령을 사용하여 데이터 이동을 중지해야 합니다.
- 이 클라우드 유닛에 대해 클라우드 정리를 실행하고 있는지 확인하십시오(CLI 명령: cloud clean status). 실행 중인 경우 "cloud clean" CLI 명령을 사용하여 클라우드 정리를 중지해야 합니다.
- 데이터 이동 정책이 클라우드 유닛에 대해 구성되어 있는지 확인하십시오(CLI 명령: data-movement policy show). 구성된 경우 "data-movement policy reset" CLI 명령을 사용하여 데이터 이동 정책을 제거해야 합니다.

절차

1. 다음 CLI 명령을 사용하여 클라우드 유닛에 있는 파일을 식별합니다.

   ```
   # filesys report generate file-location
   ```

2. 삭제할 클라우드 유닛에 있는 파일을 삭제합니다.
3. 다음 CLI 명령을 사용하여 클라우드 정리를 실행합니다.

   ```
   # cloud clean start unit-name
   ```

   정리가 완료될 때까지 기다립니다. 정리하는 데 걸리는 시간은 클라우드 유닛에 있는 데이터 양에 따라 달라질 수 있습니다.
4. 파일 시스템을 비활성화합니다.
5. 다음 CLI 명령을 사용하여 클라우드 유닛을 삭제합니다.

   ```
   # cloud unit del unit-name
   ```

   내부적으로 클라우드 유닛이 DELETE_PENDING으로 표시됩니다.
6. 다음 CLI 명령을 사용하여 클라우드 유닛이 DELETE_PENDING 상태인지 확인합니다.

   ```
   # cloud unit list
   ```

7. 파일 시스템을 활성화합니다.

   파일 시스템은 클라우드의 버킷에서 이 클라우드 유닛에 대해 남은 모든 객체를 삭제하는 절차를 백그라운드로 시작한 후 버킷을 삭제합니다. 이 프로세스가 완료되는 시간은 이들 버킷에 남은 객체 수에 따라 오래 걸릴 수 있습니다. 버킷 정리가 완료될 때까지 이 클라우드 유닛이 Data Domain 시스템의 슬롯을 계속 사

용하므로 두 슬롯이 모두 점유되어 새 클라우드 유닛을 생성하지 못할 수 있습니다.

8. 다음 CLI 명령을 사용하여 상태를 주기적으로 확인합니다.

```
# cloud unit list
```

백그라운드 정리 작업이 실행되는 동안 상태는 DELETE_PENDING으로 유지됩니다.

9. 클라우드 공급업체 S3 포털에서 모든 해당 버킷이 삭제되었고 관련 공간이 확보되었는지 확인합니다.
10. 필요한 경우 영향받는 Mtree에 대한 데이터 이동 정책을 재구성하고 데이터 이동을 다시 시작합니다.

결과

이 절차를 완료하는 데 문제가 있는 경우 지원 담당자에게 문의하십시오.

데이터 이동

데이터는 개별 데이터 이동 정책에 지정된 대로 활성 계층에서 클라우드 계층으로 이동됩니다. 정책은 MTree별로 설정됩니다. 데이터 이동은 수동으로 시작하거나 스케줄을 사용하여 자동으로 시작할 수 있습니다.

MTree에 데이터 이동 정책 추가

파일은 마지막으로 수정된 날짜를 기준으로 활성 계층에서 클라우드 계층으로 이동됩니다. 데이터 무결성을 위해 전체 파일이 이 시기에 이동됩니다. *데이터 이동 정책*은 파일 사용 기간 임계값, 사용 기간 범위 및 대상을 설정합니다.

참고

/backup MTree에 대해서는 데이터 이동 정책을 구성할 수 없습니다.

절차

1. **Data Management** > **MTree**를 선택합니다.
2. 상부 패널에서 데이터 이동 정책을 추가할 MTree를 선택합니다.
3. **Summary** 탭을 클릭합니다.
4. **Data Movement Policy**에서 **Add**를 클릭합니다.
5. **File Age in Days**에서 파일 사용 기간 임계값(**Older than**)을 설정하고, 선택적으로 사용 기간 범위(**Younger than**)를 설정합니다.

   참고

   Older than의 최소 일 수는 14입니다. 비통합 백업 애플리케이션의 경우 클라우드 계층으로 이동된 파일은 직접 액세스할 수 없으며 이러한 파일을 액세스하려면 먼저 활성 계층으로 파일을 리콜해야 합니다. 따라서, 사용 기간 임계값을 적절하게 선택하여 클라우드 계층으로 이동된 파일에 액세스할 필요성을 최소화하거나 차단해야 합니다.

6. **Destination**에 대상 클라우드 유닛을 지정합니다.
7. **Add**를 클릭합니다.

수동으로 데이터 이동

데이터 이동을 수동으로 시작하고 중지할 수 있습니다. 유효한 데이터 이동 정책이 있는 모든 MTree에서 파일이 이동됩니다.

절차

1. **Data Management** > **File System**을 선택합니다.
2. 페이지 맨 아래에서 **Show Status of File System Services**를 클릭합니다.

   다음과 같은 상태 항목이 표시됩니다.

   - 파일 시스템
   - 물리적 용량 측정
   - 데이터 이동
   - Active Tier Cleaning

3. **Data Movement**에서 **Start**를 클릭합니다.

자동으로 데이터 이동

스케줄과 스로틀을 사용하여 데이터를 자동으로 이동할 수 있습니다. 스케줄은 매일, 매주 또는 매월이 될 수 있습니다.

절차

1. **Data Management** > **File System** > **Settings**를 선택합니다.
2. **Data Movement** 탭을 클릭합니다.
3. 스로틀 및 스케줄을 설정합니다.

참고

스로틀은 내부 Data Domain 프로세스에 대한 리소스를 조정하기 위한 것으로, 네트워크 대역폭에는 영향을 미치지 않습니다.

참고

클라우드 계층 데이터 이동이 실행될 때 클라우드 유닛에 액세스할 수 없는 경우 해당 클라우드 유닛은 실행을 건너뜁니다. 클라우드 유닛을 사용할 수 있게 되면 다음번 실행에서 해당 클라우드 유닛의 데이터 이동이 실행됩니다. 데이터 이동 스케쥴은 두 실행 사이의 기간을 결정합니다. 클라우드 유닛을 사용할 수 있으며 다음번 스케줄이 실행될 때까지 기다릴 수 없는 경우 수동으로 데이터 이동을 시작할 수 있습니다.

Cloud Tier에서 파일 리콜

비통합 백업 애플리케이션의 경우 데이터를 복구하려면 먼저 활성 계층으로 데이터를 리콜해야 합니다. 클라우드 기반 백업을 복구하려면 먼저 백업 관리자가 리콜을 트리거하거나 백업 애플리케이션이 리콜을 수행해야 합니다. 파일이 리콜되면 파일의 사용 기간이 재설정되어 0부터 다시 시작되며 파일은 사용 기간 정책 설정의 대상이 될 수 있습니다. 파일은 동일한 MTree에서만 리콜할 수 있습니다. 통합 애플리케이션은 파일을 직접 복원할 수 있습니다.

참고

MTree 복제 컨텍스트에서는 파일이 대상 MTree에서 읽기 전용입니다.

참고

파일이 스냅샷에만 상주하는 경우 직접 리콜할 수 없습니다. 스냅샷에서 파일을 리콜하려면 fastcopy를 사용하여 파일을 스냅샷에서 다시 활성 MTree로 복제한 후 클라우드에서 파일을 리콜해야 합니다. 클라우드에서 활성 MTree로만 파일을 리콜할 수 있습니다.

절차

1. **Data Managment** > **File System** > **Summary**를 선택합니다.
2. 다음 중 하나를 수행합니다.
   - Space Usage 패널의 Cloud Tier 섹션에서 **Recall**을 클릭합니다.
   - 화면 맨 아래의 File System 상태 패널을 확장하고 **Recall**을 클릭합니다.

     참고

     Recall 링크는 클라우드 유닛이 생성되고 클라우드 유닛에 데이터가 있는 경우에만 사용할 수 있습니다.
3. Recall File from Cloud 대화 상자에서 리콜할 파일의 정확한 파일 이름(와일드카드 사용 안 함)과 전체 경로를 입력합니다. 예를 들면 `/data/col1/mt11/file1.txt`와 같습니다. **Recall**을 클릭합니다.
4. 리콜의 상태를 확인하려면 다음 중 하나를 수행합니다.
   - Space Usage 패널의 Cloud Tier 섹션에서 **Details**를 클릭합니다.
   - 화면 맨 아래의 File System 상태 패널을 확장하고 **Details**를 클릭합니다.

   파일 경로, 클라우드 공급업체, 리콜 진행률 및 전송된 데이터의 양을 보여 주는 Cloud File Recall Details 대화 상자가 표시됩니다. 리콜하는 동안 복구할 수 없는 오류가 있는 경우 오류 메시지가 표시됩니다. 오류 메시지 위에 커서를 올리면 툴 설명이 더 많은 세부 정보 및 가능한 조치 작업과 함께 표시됩니다.

결과

파일이 활성 계층으로 리콜된 후 데이터를 복구할 수 있습니다.

참고

비통합 애플리케이션의 경우, 클라우드 계층에서 활성 계층으로 파일을 리콜한 후 파일이 데이터 이동의 대상이 되려면 최소 14일이 경과해야 합니다. 14일 후 파일에 대해 정상적인 데이터 이동 프로세스가 발생합니다. 이제 mtime이 아닌 ptime이 검사되므로 이 파일은 클라우드로 다시 이동되려면 시간 임계값 또는 사용 기간 범위만큼 기다려야 합니다. 이 제한 사항은 통합 애플리케이션에는 적용되지 않습니다.

참고

비통합 애플리케이션은 Data Domain 시스템에 경과 시간에 따른 데이터 이동 정책을 구성하고 클라우드 계층으로 마이그레이션할 파일을 지정합니다. 그리고 이 정책은 MTree에 있는 모든 파일에 일관되게 적용됩니다. 통합 애플리케이션은 애플리케이션으로 관리되는 데이터 이동 정책을 사용하므로 사용자가 클라우드 계층으로 마이그레이션할 특정 파일을 지정할 수 있습니다.

CLI를 사용하여 Cloud Tier에서 파일 리콜

비통합 백업 애플리케이션의 경우 데이터를 복구하려면 먼저 활성 계층으로 데이터를 리콜해야 합니다. 클라우드 기반 백업을 복구하려면 먼저 백업 관리자가 리콜을 트리거하거나 백업 애플리케이션이 리콜을 수행해야 합니다. 파일이 리콜되면 파일의 사용 기간이 재설정되어 0부터 다시 시작되며 파일은 사용 기간 정책 설정의 대상이 될 수 있습니다. 파일은 소스 MTree에서만 리콜할 수 있습니다. 통합 애플리케이션은 파일을 직접 리콜할 수 있습니다.

참고

파일이 스냅샷에만 상주하는 경우 직접 리콜할 수 없습니다. 스냅샷에서 파일을 리콜하려면 fastcopy를 사용하여 파일을 스냅샷에서 다시 활성 MTree로 복제한 후 클라우드에서 파일을 리콜해야 합니다. 클라우드에서 활성 MTree로만 파일을 리콜할 수 있습니다.

절차

1. 파일 위치를 확인하려면 다음 명령을 사용합니다.
   `filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]`

   경로 이름은 파일이거나 디렉토리일 수 있습니다. 디렉토리인 경우 디렉토리 내의 모든 파일이 나열됩니다.

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Cloud Unit 1
   ```

2. 다음 명령을 사용하여 파일을 리콜합니다.
   `data-movement recall path <path-name>`

   이 명령은 비동기식으로 리콜을 시작합니다.

   ```
   data-movement recall path /data/col1/mt11/file1.txt
   Recall started for "/data/col1/mt11/file1.txt".
   ```

3. 다음 명령을 사용하여 리콜 상태를 모니터링합니다.
   `data-movement status [path {pathname | all | [queued] [running] [completed] [failed]} | to-tier cloud | all]`

   ```
   data-movement status path /data/col1/mt11/file1.txt
   Data-movement recall:
   ---------------------
   Data-movement for "/data/col1/mt11/file1.txt": phase 2 of 3
   (Verifying)
   80% complete; time: phase  XX:XX:XX total  XX:XX:XX
   Copied (post-comp): XX XX, (pre-comp) XX XX
   ```

   상태에 지정된 경로에서 리콜이 실행되고 있지 않다고 표시되면 리콜이 완료되었거나 실패했을 수 있습니다.

4. 다음 명령을 사용하여 파일 위치를 확인합니다.
   `filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]`

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Active
   ```

결과

파일이 활성 계층으로 리콜된 후 데이터를 복구할 수 있습니다.

참고

비통합 애플리케이션의 경우, 클라우드 계층에서 활성 계층으로 파일을 리콜한 후 파일이 데이터 이동의 대상이 되려면 최소 14일이 경과해야 합니다. 14일 후 파일에 대해 정상적인 데이터 이동 프로세스가 발생합니다. 이 제한 사항은 통합 애플리케이션에는 적용되지 않습니다.

참고

비통합 애플리케이션은 Data Domain 시스템에 경과 시간에 따른 데이터 이동 정책을 구성하고 클라우드 계층으로 마이그레이션할 파일을 지정합니다. 그리고 이 정책은 MTree에 있는 모든 파일에 일관되게 적용됩니다. 통합 애플리케이션은 애플리케이션으로 관리되는 데이터 이동 정책을 사용하므로 사용자가 클라우드 계층으로 마이그레이션할 특정 파일을 지정할 수 있습니다.

Cloud Tier에서 직접 복구

직접 복구를 사용하면 비통합 애플리케이션이 활성 계층을 거치지 않고 Cloud Tier에서 직접 파일을 읽을 수 있습니다.

직접 복구를 사용하도록 선택하는 경우 고려해야 할 주요 사항은 다음과 같습니다.

- 직접 복구는 통합 애플리케이션을 필요로 하지 않으며 비통합 애플리케이션에 영향을 미치지 않습니다.
- Cloud Tier에서 읽기 위해 먼저 활성 계층으로 복사할 필요가 없습니다.
- 히스토그램과 통계를 사용하여 Cloud Tier에서 직접 읽기를 추적할 수 있습니다.
- 직접 복구는 ECS 클라우드 공급업체에 대해서만 지원됩니다.
- 애플리케이션에 Cloud Tier 지연 시간이 발생합니다.
- Cloud Tier에서 직접 읽기 시에는 대역폭이 최적화되지 않습니다.
- 직접 복구는 소수의 작업을 지원합니다.

직접 복구는 Cloud Tier를 인지할 필요가 없고 클라우드 파일을 자주 복구할 필요가 없는 비통합 애플리케이션에 유용합니다.

CLI(Command Line Interface)를 사용하여 DD Cloud Tier 구성

Data Domain 명령줄 인터페이스를 사용하여 DD Cloud Tier를 구성할 수 있습니다.

절차

1. 활성 계층과 클라우드 계층 모두에 대해 스토리지를 구성합니다. 사전 요구 사항으로, 활성 계층과 클라우드 계층 모두에 대해 적절한 용량 라이선스를 설치해야 합니다.

   a. CLOUDTIER-CAPACITY 및 CAPACITY-ACTIVE 기능에 대한 라이선스가 설치되어 있는지 확인합니다. ELMS 라이선스를 확인하려면 다음을 수행합니다.

   ```
   # elicense show
   ```

   라이선스가 설치되어 있지 않다면 `elicense update` 명령을 사용하여 라이선스를 설치합니다. 명령을 입력하고 이 프롬프트 다음에 라이선스 파일의 내용을 붙여 넣으십시오. 붙여 넣은 다음 캐리지 리턴이 있는지 확인하고 **Control-D**를 눌러 저장합니다. 라이선스를 교체할지 묻는 메시지가 나타납니다. **yes**로 답하면 라이선스가 적용되고 표시됩니다.

```
# elicense update
Enter the content of license file and then press Control-D,
or press Control-C to cancel.
```

b. 사용 가능한 스토리지를 표시합니다.

```
# storage show all# disk show state
```

c. 활성 계층에 스토리지를 추가합니다.

```
# storage add enclosures <enclosure no> tier active
```

d. 클라우드 계층에 스토리지를 추가합니다.

```
# storage add enclosures <enclosure no> tier cloud
```

2. 인증서를 설치합니다.

   클라우드 프로파일을 생성하려면 먼저 연결된 인증서를 설치해야 합니다. 자세한 내용은 인증서 가져오기(574페이지) 섹션을 참조하십시오.

   AWS, Virtustream 및 Azure 퍼블릭 클라우드 공급업체의 경우 https://www.digicert.com/digicert-root-certificates.htm에서 루트 CA 인증서를 다운로드할 수 있습니다.

   - AWS 또는 Azure 클라우드 공급업체의 경우 Baltimore CyberTrust Root 인증서를 다운로드합니다.
   - Alibaba의 경우 https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates에서 GlobalSign 루트 R1 인증서를 다운로드합니다.
   - Virtustream 클라우드 공급업체의 경우 DigiCert High Assurance EV Root CA 인증서를 다운로드합니다.
   - ECS의 경우 루트 인증 기관이 고객마다 다릅니다. 자세한 내용은 로드 밸런싱 장치 공급업체에 문의하십시오.

   다운로드한 인증서 파일은 확장자가 .crt입니다. 파일이 설치된 Linux 또는 Unix 시스템에서 openssl을 사용하여 파일을 .crt 형식에서 .pem 형식으로 변환합니다.

```
$openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
-out DigiCertHighAssuranceEVRootCA.pem
```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press
Control-C to cancel.
```

3. 클라우드로 데이터를 이동할 수 있도록 Data Domain 시스템을 구성하려면 먼저 "클라우드" 기능을 활성화하고 시스템 암호가 아직 설정되지 않은 경우 이를 설정해야 합니다.

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. 클라우드 공급업체 자격 증명을 사용하여 클라우드 프로파일을 구성합니다. 프롬프트와 변수는 공급업체마다 다릅니다.

   ```
   # cloud profile add <profilename>
   ```

   참고

   보안상의 이유로 이 명령은 사용자가 입력하는 액세스/비밀 키를 표시하지 않습니다.

   공급업체를 선택합니다.

   ```
   Enter provider name (alibabacloud|aws|azure|ecs|google|
   s3_flexible|virtustream)
   ```

   - Alibaba Cloud를 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 리전이 필요합니다.
   - AWS S3을 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 리전이 필요합니다.
   - Azure에는 계정 이름, 계정이 Azure Government 계정인지 여부, 기본 키, 보조 키 및 스토리지 클래스가 필요합니다.
   - ECS를 사용하려면 액세스 키, 암호 키 및 엔드포인트를 입력해야 합니다.
   - Google Cloud Platform에는 액세스 키, 암호 키 및 리전이 필요합니다. (스토리지 클래스는 Nearline입니다.)
   - S3 Flexible 공급업체에는 공급업체 이름, 액세스 키, 암호 키, 영역, 엔드포인트 및 스토리지 클래스가 필요합니다.
   - Virtustream을 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 지역이 필요합니다.

   각 프로파일을 추가할 때마다 프록시를 설정할지 묻는 메시지가 나타납니다. 프록시를 설정하려면 *프록시 호스트 이름*, *프록시 포트*, *프록시 사용자 이름* 및 *프록시 암호* 값이 필요합니다.

5. 클라우드 프로파일 구성을 확인합니다.

   ```
   # cloud profile show
   ```

6. 아직 생성되지 않은 경우 활성 계층 파일 시스템을 생성합니다.

   ```
   # filesys create
   ```

7. 파일 시스템을 활성화합니다.

   ```
   # filesys enable
   ```

8. 클라우드 유닛을 구성합니다.

   ```
   # cloud unit add unitname profile profilename
   ```

   `cloud unit list` 명령을 사용하여 클라우드 유닛을 나열합니다.

9. 필요에 따라 클라우드 유닛에 대한 암호화를 구성합니다.

   a. ENCRYPTION 라이선스가 설치되어 있는지 확인합니다.

      ```
      # elicense show
      ```

   b. 클라우드 유닛에 대한 암호화를 활성화합니다.

      ```
      # filesys encryption enable cloud-unit unitname
      ```

c. 암호화 상태를 확인합니다.

```
# filesys encryption status
```

10. 하나 이상의 MTree를 생성합니다.

```
# mtree create /data/col1/mt11
```

11. DD Cloud Tier 구성을 확인합니다.

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. 이 MTree에 대한 파일 마이그레이션 정책을 구성합니다. 이 명령에 여러 MTree를 지정할 수 있습니다. 정책은 사용 기간 임계값 또는 범위에 기반할 수 있습니다.

a. 사용 기간 임계값을 구성하려면(지정된 사용 기간보다 오래된 파일을 클라우드로 마이그레이션하려면) 다음을 수행합니다.

```
# data-movement policy set age-threshold age_in_days to-tier
cloud cloud-unit unitname mtrees mtreename
```

b. 사용 기간 범위를 구성하려면(지정된 사용 기간 범위에 속하는 파일만 마이그레이션하려면) 다음을 수행합니다.

```
# data-movement policy set age-range min-age age_in_days max-
age age_in_days to-tier cloud cloud-unit unitname mtrees
mtreename
```

13. 파일 시스템을 내보내고 클라이언트에서 파일 시스템을 마운트하고 활성 계층에 데이터를 수집합니다. 데이터 마이그레이션 대상이 될 수 있도록 수집된 파일의 수정 날짜를 변경합니다. (날짜를 데이터 이동 정책을 구성할 때 지정한 사용 기간 임계값보다 오래된 날짜로 설정합니다.)
14. 사용 기간이 지난 파일의 마이그레이션을 시작합니다. 이전과 마찬가지로, 이 명령에 여러 MTree를 지정할 수 있습니다.

    ```
    # data-movement start mtrees mtreename
    ```

    데이터 이동의 상태를 확인합니다.

    ```
    # data-movement status
    ```

    데이터 이동의 진행 상황을 확인할 수도 있습니다.

    ```
    # data-movement watch
    ```

15. 파일 마이그레이션이 처리되었으며 이제 모든 파일이 클라우드 계층에 있는지 확인합니다.

    ```
    # filesys report generate file-location path all
    ```

16. 파일을 클라우드 계층으로 마이그레이션한 후에는 파일에서 직접 읽을 수 없습니다(시도 시 오류가 발생 함). 먼저 파일을 활성 계층으로 리콜해야 합니다. 파일을 활성 계층으로 리콜하려면 다음을 수행합니다.

    ```
    # data-movement recall path pathname
    ```

DD 클라우드 유닛을 위한 암호화 구성

암호화를 활성화할 수 있는 세 가지 레벨은 Data Domain 시스템, 활성 계층 및 클라우드 유닛입니다. 활성 계층의 암호화는 Data Domain 시스템에서 암호화가 활성화된 경우에만 적용됩니다. 클라우드 유닛에는 암호화를 활성화할 수 있는 별도의 컨트롤이 있습니다.

절차

1. **Data Management** > **File System** > **DD Encryption**을 선택합니다.

   참고

   시스템에 암호화 라이센스가 없으면 Add Licenses 페이지가 표시됩니다.

2. DD Encryption 패널에서 다음 중 하나를 수행합니다.
   - **클라우드 유닛 *x***에 대해 암호화를 활성화하려면 **Enable**을 클릭합니다.
   - **클라우드 유닛 *x***에 대해 암호화를 비활성화하려면 **Disable**을 클릭합니다.

   참고

   암호화를 활성화하려면 보안 책임자의 자격 증명을 입력하라는 메시지가 나타납니다.

3. 보안 책임자의 **Username** 및 **Password**를 입력합니다. 필요에 따라 **Restart file system now**를 선택합니다.
4. **Enable** 또는 **Disable**을 적절하게 클릭합니다.
5. File System Lock 패널에서 파일 시스템을 잠그거나 잠금을 해제합니다.

6. Key Management 패널에서 **Configure**를 클릭합니다.
7. Change Key Manager 대화 상자에서 보안 책임자 자격 증명 및 키 관리자를 구성합니다.

참고

클라우드 암호화는 Data Domain Embedded Key Manager에서만 사용할 수 있습니다. 외부 Key Manager는 지원되지 않습니다.

8. **OK**를 클릭합니다.
9. DD Encryption Keys 패널을 사용하여 암호화 키를 구성합니다.

시스템 손실에 대비하여 필요한 정보

Data Domain 시스템에 Cloud Tier를 구성한 후 다음과 같은 시스템 관련 정보를 기록하고 Data Domain 시스템이 아닌 안전한 위치에 저장해야 합니다. Data Domain 시스템이 손실되는 경우에 Cloud Tier 데이터를 복구하려면 이 정보가 필요합니다.

참고

복구 프로세스는 긴급 상황에만 적합하며 이를 완료하려면 Data Domain 엔지니어링 담당자가 상당한 시간과 노력을 들여야 합니다.

- 원래 Data Domain 시스템의 일련 번호
- 원래 Data Domain 시스템의 시스템 암호
- 원래 Data Domain 시스템의 DD OS 버전 번호
- Cloud Tier 프로파일 및 구성 정보

클라우드 계층에서 DD Replicator 사용

클라우드 계층이 활성화된 Data Domain 시스템에서는 컬렉션 복제가 지원되지 않습니다.

디렉토리 복제는 / backup MTree에서만 작동하며 이 MTree는 클라우드 계층에 할당할 수 없습니다. 따라서 디렉토리 복제는 클라우드 계층의 영향을 받지 않습니다.

관리되는 파일 복제 및 MTree 복제는 클라우드 계층이 활성화된 Data Domain 시스템에서 지원됩니다. 두 시스템 중 하나 또는 둘 모두에서 클라우드 계층을 활성화할 수 있습니다. 소스 시스템에 클라우드 계층이 활성화되어 있으면 파일이 이미 클라우드 계층으로 마이그레이션된 경우 클라우드에서 데이터를 읽어야 할 수 있습니다. 클라우드 계층이 활성화된 경우에도 복제된 파일은 항상 대상 시스템의 활성 계층에 먼저 배치됩니다. 파일은 클라우드 계층에서 소스 MTree의 활성 계층으로 리콜할 수 있습니다. 대상 MTree에 있는 파일의 리콜은 허용되지 않습니다.

참고

소스 시스템이 DD OS 5.6 또는 5.7을 실행 중이고 MTree 복제를 사용하여 클라우드 계층이 활성화된 시스템에 복제하는 경우 소스 시스템을 클라우드 계층이 활성화된 시스템으로 복제할 수 있는 릴리즈로 업그레이드해야 합니다. *DD OS 릴리즈 노트*에서 시스템 요구 사항을 참조하십시오.

참고

클라우드 계층의 파일은 가상 신세틱 작업의 기본 파일로 사용할 수 없습니다. 파일이 새 백업의 가상 신세틱에 사용될 경우에도 활성 계층에 남아 있도록 하려면 영구적으로 계속되는 증분 백업이나 신세틱 전체 백업이 필요합니다.

Cloud Tier와 함께 DD VTL(Virtual Tape Library) 사용

Cloud Tier 및 DD VTL을 사용하도록 구성된 시스템에서 클라우드 스토리지는 VTL 볼팅(vaulting)으로 사용할 수 있습니다. DD VTL 테이프를 클라우드에서 사용하려면 먼저 클라우드 스토리지를 라이센스 등록 및 구성한 후 VTL의 볼팅 위치로 선택합니다.

Cloud Tier와 함께 VTL을 사용하는 방법에 대한 자세한 내용은 클라우드에 DD VTL 테이프 저장(362페이지)에 나와 있습니다.

DD Cloud Tier에 대한 용량 사용량 차트 표시

Cloud Tier 사용량 통계를 표시하기 사용할 수 있는 차트는 Space Usage, Consumption 및 Daily Written의 세 가지입니다.

절차

1. **Data Management** > **File System** > **Charts**를 선택합니다.
2. **Chart**로 다음 중 하나를 선택합니다.
   - Space Usage
   - Consumption
   - Daily Written
3. **Scope**로 **Cloud Tier**를 선택합니다.
   - Space Usage 탭에 시간별 공간 사용량이 MiB 단위로 표시됩니다. 기간(1주, 1개월, 3개월, 1년 또는 All)을 선택할 수 있습니다. 데이터는 색으로 구분되어 압축 전 사용량(파란색), 압축 후 사용량(빨간색) 및 압축 비율(녹색)로 표시됩니다.
   - Consumption 탭에는 압축 후 스토리지의 사용량과 시간별 압축 비율이 표시되므로, 사용량 추세를 분석 할 수 있습니다. 기간(1주, 1개월, 3개월, 1년 또는 All)을 선택할 수 있습니다. 데이터는 색으로 구분되어 용량(파란색), 압축 후 사용량(빨간색), 압축 비율(녹색), 정리(주황색) 및 데이터 이동(보라색)으로 표시됩니다.
   - Daily Written 탭에는 하루에 기록한 데이터 양이 표시됩니다. 기간(1주, 1개월, 3개월, 1년 또는 All)을 선택할 수 있습니다. 데이터는 색으로 구분되어 압축 전 기록된 용량(파란색), 압축 후 사용량(빨간색) 및 총 압축 비율(녹색)로 표시됩니다.

DD Cloud Tier 로그

DD Cloud Tier의 구성이나 운영에서 종류와 관계없이 오류가 발생할 경우 시스템에서 자동으로 장애 시간과 연관된 타임스탬프가 포함된 폴더를 생성합니다.

로그에 액세스하려면 `/ddvar/log/debug` 디렉토리를 마운트합니다.

참고

`log list view` 명령 출력에는 DD Cloud Tier 오류에 대해 생성된 상세 로그 파일이 모두 나열되지 않습니다.

CLI(Command Line Interface)를 사용하여 DD Cloud Tier 제거

Data Domain 명령줄 인터페이스를 사용하여 DD Cloud Tier 구성을 제거할 수 있습니다.

시작하기 전에

시스템에서 DD Cloud Tier 구성을 제거하기 전에 클라우드 유닛의 모든 파일을 삭제하십시오. `filesys report generate file-location path all output-file file_loc` 명령을 실행하여 클라우드 유닛의 모든 파일을 식별하고 MTree의 NFS 마운트 지점에서 삭제합니다.

참고

위 명령은 `/ddr/var/` 디렉토리에 `file_loc` 보고서를 생성합니다.

절차

1. 파일 시스템을 비활성화합니다.

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Please wait.............
The filesystem is now disabled.
```

2. 시스템에서 클라우드 유닛을 나열합니다.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
------------   ------------   ------
```

3. 클라우드 유닛을 개별적으로 삭제합니다.

```
# cloud unit del cloud_unit-1

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-1".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
```

```
 in the cloud unit "cloud_unit-2".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.
```

4. 삭제 작업이 진행 중인지 확인합니다.

```
# cloud unit list
Name           Profile         Status
------------   ------------    ------
cloud_unit-1   cloudProfile    Delete-Pending
cloud_unit-2   cloudProfile2   Delete-Pending
------------   ------------    ------
```

5. 파일 시스템을 다시 시작합니다.

```
# filesys enable
Please wait.....................................
The filesystem is now enabled.
```

6. `cloud unit list` 명령을 실행하여 어느 클라우드 유닛도 나타나지 않는지 확인합니다.

   어느 한 클라우드 유닛이나 두 클라우드 유닛 모두 여전히 `Delete-Pending` 상태로 표시되는 경우 지원 팀에 문의하십시오.

7. DD Cloud Tier에 할당된 디스크 엔클로저를 식별합니다.

```
# storage show tier cloud

Cloud tier details:
Disk   Disks               Count   Disk     Additional
Group                              Size     Information
------ ------------------- ------  -------- ------------
dgX    2.1-2.15, 3.1-3.15  30      3.6 TiB
------ ------------------- ------  -------- ------------
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

8. DD Cloud Tier에서 디스크 엔클로저를 제거합니다.

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done

Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfuly removed: 3 done
```

19장

DD Extended Retention

이 장에는 다음과 같은 내용이 포함됩니다.

DD Extended Retention 개요

Data Domain Extended Retention(DD Extended Retention)은 내부 계층화 방식을 사용하여 백업 데이터를 DD 시스템에 경제적으로 장기간 보존할 수 있는 방법을 제공합니다. DD Extended Retention을 사용하면 DD 시스템을 활용하여 백업을 디스크에 장기간 보존하고 테이프에 대한 의존도를 최소화할 수 있습니다.

참고

DD Extended Retention의 이전 명칭은 *Data Domain Archiver*입니다.

2계층형 파일 시스템

DD Extended Retention을 사용하는 DD 시스템의 내부 2계층형 파일 시스템은 *활성 계층* 및 *보존 계층*으로 구성됩니다. 그러나 파일 시스템은 하나의 개체로 표시됩니다. 수신 데이터는 먼저 파일 시스템의 활성 계층에 배치됩니다. 완전한 파일 형태의 데이터는 나중에 개별 *데이터 이동 정책*에 의해 지정된 파일 시스템의 보존 계층으로 이동됩니다. 예를 들어 활성 계층은 90일 동안 주간 전체 및 일일 증분 백업을 유지할 수 있지만 보존 계층은 7년 동안 월간 전체 백업을 유지할 수 있습니다.

보존 계층은 하나 이상의 보존 유닛으로 구성됩니다. 각 보존 유닛은 하나 이상의 셸프에서 스토리지를 가져올 수 있습니다.

참고

DD OS 5.5.1부터는 보존 계층당 하나의 보존 유닛만 허용됩니다. 그러나 DD OS 5.5.1 이전에 설정된 시스템의 경우 계속해서 2개 이상의 보존 유닛이 있을 수 있지만 여기에 더 많은 보존 유닛을 추가할 수는 없습니다.

무중단 작업

DD Extended Retention을 사용하는 DD 시스템은 이더넷에서 NFS 및 CIFS 파일 서비스 프로토콜, 개방형 시스템 및 IBMi를 위한 DD VTL을 통해서나 DD Boost 같은 애플리케이션별 인터페이스를 사용하는 디스크 기반 타겟으로 동시 데이터 액세스 방법을 사용해 기존 백업 애플리케이션을 지원합니다(Avamar®, NetWorker®, GreenPlum, Symantec OpenStorage 및 Oracle RMAN과 함께 사용).

DD Extended Retention은 활성 계층에서 보존 계층으로 다른 작업에 영향을 주지 않으면서 자동으로 데이터를 이동하여 DD 아키텍처를 확장합니다. 2개 계층에 있는 모든 데이터에 액세스할 수 있지만 보존 계층에 있는 데이터에 처음 액세스할 때 약간 지연될 수 있습니다. 시스템의 네임스페이스는 전역이며 데이터 이동의 영향을 받지 않습니다. 2계층형 파일 시스템 활용을 위한 파일 시스템의 파티셔닝은 필요하지 않습니다.

데이터 이동 정책

사용자가 지정할 수 있는 *데이터 이동 정책*은 파일이 활성에서 보존 계층으로 이동하는 정책입니다. 파일을 마지막으로 수정한 시간을 기반으로 합니다. 정책을 MTree당 기반으로 설정할 수 있기 때문에 다른 데이터 하위 집합마다 다른 정책을 설정할 수 있습니다. 업데이트할 수 있는 파일의 경우 변경되지 않는 파일과 다른 정책이 필요합니다.

보존 유닛 내에서 중복 제거

장애 격리를 목적으로 중복 제거가 DD Extended Retention을 사용하는 DD 시스템의 보존 유닛 내에서 전적으로 발생합니다. 활성 및 보존 계층 또는 다른 보존 유닛 간의 교차 중복 제거는 없습니다(해당되는 경우).

각 계층에서 가져온 스토리지

계층화의 개념은 DD Extended Retention을 사용하는 DD 시스템의 스토리지 레벨로 확장됩니다. 파일 시스템의 활성 계층은 스토리지의 활성 계층에서 스토리지를 가져옵니다. 파일 시스템의 보존 계층은 스토리지의 보존 계층에서 스토리지를 가져옵니다.

참고

활성 및 보존 계층의 경우 모두 DD OS 5.2 이상 릴리즈가 ES20 및 ES30 셸프를 지원하며, DD OS 5.7 이상은 특정 모델에서 DS60 셸프를 지원합니다. 여러 Data Domain 셸프 유형을 같은 셸프 세트에서 혼합할 수 없으며, *ES30 확장 셸프 하드웨어 가이드* 또는 *DS60 확장 셸프 하드웨어 가이드*에 지정된 구성 규칙에 따라 셸프 세트의 균형을 맞춰야 합니다. DD Extended Retention을 사용하면 동일한 컨트롤러에 훨씬 더 많은 스토리지를 연결할 수 있습니다. 예를 들어 DD Extended Retention 사용 시 DD990에서 최대 56개의 ES30 셸프를 연결할 수 있습니다. 활성 계층에는 적어도 하나의 셸프로 구성된 스토리지가 포함되어야 합니다. Data Domain 컨트롤러 모델의 최소 및 최대 셸프 구성은 ES30 및 DS60의 확장 셸프 하드웨어 가이드를 참조하십시오.

데이터 보호

DD Extended Retention을 사용하는 DD 시스템에서 데이터는 내장된 장애 격리 기능, 재해 복구 기능 및 DIA(Data Invulnerability Architecture)를 통해 보호됩니다. 파일이 활성에서 보존 계층으로 이동되면 DIA가 파일을 검사합니다. 데이터가 보존 계층으로 복제된 후, 컨테이너와 파일 시스템 구조는 읽고 확인됩니다. 파일이 보존 계층에 올바로 기록되었음이 확인되면 파일의 위치가 업데이트되고 활성 계층의 공간이 재확보됩니다.

보존 유닛이 채워지면 네임스페이스 정보와 시스템 파일이 이곳으로 복제되므로 시스템의 다른 부분이 유실되더라도 보존 유닛의 데이터를 복구할 수 있습니다.

참고

완전 삭제 및 일부 복제 형태는 DD Extended Retention을 사용하는 DD 시스템에서 지원되지 않습니다.

공간 재확보

보존 계층으로 이동한 데이터를 통해 확보된 공간을 재확보하기 위해 우선 순위가 낮은 작업으로 백그라운드에서 실행되는 *공간 재확보*(DD OS 5.3부터) 기능을 사용할 수 있습니다. 데이터 이동 및 정리 같은 우선 순위가 높은 작업이 있을 경우에는 자체적으로 일시 중단됩니다.

저장된 데이터 암호화

DD OS 5.5.1부터 암호화 라이센스가 있는 경우 DD Extended Retention을 사용하는 DD 시스템에서 *저장된 데이터 암호화* 기능을 사용할 수 있습니다. 암호화는 기본적으로 활성화되어 있지 않습니다.

DD OS 5.5.1 이전에 이미 DD Extended Retention을 사용하지 않는 시스템을 위한 확장된 암호화 기능이 제공됩니다.

암호화 기능을 설정하고 사용하는 방법에 대한 전체 지침은 이 가이드의 *저장된 데이터 암호화 관리* 장을 참조하십시오.

DD Extended Retention에서 지원되는 프로토콜

DD Extended Retention을 사용하는 DD 시스템은 NFS, CIFS 및 DD Boost 프로토콜을 지원합니다. DD VTL에 대한 지원은 DD OS 5.2에서, NDMP에 대한 지원은 DD OS 5.3에서 추가되었습니다.

참고

DD Boost로 지원되는 애플리케이션의 목록은 온라인 지원 사이트의 *DD Boost Compatibility List*를 참조하십시오.

DD Extended Retention을 사용하는 경우 데이터가 먼저 활성 계층에 도달합니다. 파일은 데이터 이동 정책에 지정된 대로 모두 보존 계층의 보존 유닛으로 이동됩니다. 모든 파일은 동일한 네임스페이스에 나타납니다. 데이터를 파티션 분할할 필요가 없으며, 원하는 대로 파일 시스템을 계속 확장할 수 있습니다.

모든 데이터를 사용자가 볼 수 있으며, 모든 파일 시스템 메타데이터가 활성 계층에 있습니다.

활성 계층에서 보존 계층으로 데이터를 이동할 경우 용량이 늘어나는 반면, 액세스할 유닛에 현재 액세스할 수 없으면 액세스 시간이 약간 느려집니다.

HA(High Availability)와 Extended Retention

HA(High Availability)를 지원하는 Data Domain 시스템에서는 DD Extended Retention이 지원되지 않습니다. DD OS에서는 현재 HA와 함께 Extended Retention이 지원되지 않습니다.

DD Extended Retention 기반 DD Replicator 사용

DD Extended Retention을 사용하는 DD 시스템에서는 일부 형태의 복제가 지원됩니다.

지원되는 복제 유형은 보호할 데이터에 따라 다릅니다.

- 시스템에 있는 데이터를 *소스*로 보호하기 위해 DD Extended Retention을 사용하는 DD 시스템은 컬렉션 복제, MTree 복제 및 DD Boost 관리 파일 복제를 지원합니다.
- 다른 시스템에서 데이터를 *대상*으로 보호하기 위해 DD Extended Retention을 사용하는 DD 시스템은 디렉토리 복제는 물론 컬렉션 복제, MTree 복제 및 DD Boost 관리 파일 복제를 지원합니다.

참고

DD Extended Retention은 델타(저대역폭 최적화) 복제를 지원하지 않습니다. DD 시스템에서 DD Extended Retention을 설정하기 전에 모든 컨텍스트에서 델타 복제를 해제해야 합니다.

DD Extended Retention 기반 컬렉션 복제

컬렉션 복제는 DD Extended Retention이 설정된 두 DD 시스템의 해당 활성 계층과 보존 유닛 사이에서 발생합니다. 소스에서 활성 계층 또는 보존 유닛에 장애가 발생하면 원격 사이트의 해당 유닛에서 새 유닛으로 데이터를 복제하고 새 유닛을 사이트로 운송해 교체 유닛으로 사용할 수 있습니다.

컬렉션 복제를 설정하기 위한 사전 요구 사항에는 다음이 포함됩니다.

- 소스 시스템과 대상 시스템 모두 DD Extended Retention가 설정된 DD 시스템으로 구성해야 합니다.
- 보존 유닛이 추가되고 복제가 구성될 때까지 대상에서 파일 시스템을 사용하도록 설정해서는 안 됩니다.

DD Extended Retention 기반 디렉토리 복제

디렉토리 복제의 경우 DD Extended Retention을 사용하는 DD 시스템이 복제 타겟으로 사용되고, 지원되는 DD 시스템에서 일대일 및 다대일 토폴로지를 지원합니다. 그러나 DD Extended Retention을 사용하는 DD 시스템은 양방향 디렉토리 복제를 지원하지 않으며 디렉토리 복제의 소스가 될 수 없습니다.

참고

디렉토리 복제를 사용해 DD Extended Retention을 사용하는 DD 시스템으로 데이터를 복제하려면 소스에서 DD OS 5.0 이상 버전이 실행 중이어야 합니다. 따라서 DD OS 5.0 이전 버전을 실행 중인 시스템의 경우 먼저 DD OS 5.0 이상 버전을 실행 중인 중간 시스템으로 데이터를 가져와야 합니다. 예를 들어 DD OS 4.9 버전의 Extended Retention을 사용하는 시스템에서 DD OS 5.2 버전의 Extended Retention을 사용하지 않는 시스템으로 복제할 수 있습니다. 그런 다음 DD OS 5.2 시스템에서 DD OS 4.9 시스템으로 복제할 수 있습니다.

DD Extended Retention 기반 MTree 복제

DD Extended Retention을 사용하는 두 DD 시스템 사이에서 MTree 복제를 설정할 수 있습니다. 복제된 데이터는 먼저 대상 시스템의 활성 계층에 배치됩니다. 그러면 대상 시스템의 데이터 이동 정책에 의해 이 복제된 데이터가 보존 계층으로 이동되는 시점이 결정됩니다.

MTree 복제 제한 사항과 정책은 DD OS 릴리즈에 따라 다음과 같이 차이가 있습니다.

- DD OS 5.1부터는 데이터가 MTree 복제를 통해 DD Extended Retention을 사용하지 않는 시스템에서 DD Extended Retention을 사용하는 시스템으로 복제됩니다.
- DD OS 5.2부터는 DD Extended Retention을 사용하는 시스템의 활성 계층으로 데이터를 복제해 활성 계층 내에서 데이터를 보호할 수 있습니다.
- DD OS 5.5부터는 두 시스템 모두 DD OS 5.5 이상을 실행하는 경우 DD Extended Retention을 사용하는 시스템에서 DD Extended Retention을 사용하지 않는 시스템으로 MTree 복제가 지원됩니다.
- DD OS 5.3 및 5.4의 경우 DD Extended Retention을 사용할 계획이라면 소스 시스템에서 /backup MTree에 대한 복제를 설정하지 마십시오. DD OS 5.5 이상에는 이러한 제한 사항이 없습니다.

DD Extended Retention 기반 관리 파일 복제 사용

DD Extended Retention을 사용하는 DD 시스템의 경우 DD Boost 관리 파일 복제를 위해 지원되는 토폴로지가 일대일, 다대일, 양방향, 일대다 및 다중 구간(Cascaded)입니다.

참고

DD Boost 2.3 이상의 경우 백업 애플리케이션 내에서 여러 사본을 생성하고 관리하는 방법을 지정할 수 있습니다.

DD Extended Retention의 하드웨어 및 라이센스 등록

DD Extended Retention을 사용하는 DD 시스템에는 특정 하드웨어 구성이 필요합니다. 이 기능에는 별도의 셸프 용량 라이센스와 같은 특정 라이센스의 등록도 필요합니다.

DD Extended Retention에 대해 지원되는 하드웨어

DD Extended Retention이 활성화되어 있는 DD 시스템의 하드웨어 요구 사항에는 메모리 요구 사항, 셸프, NIC/FC 카드 등이 포함됩니다. DD Extended Retention의 필수 하드웨어 구성에 대한 자세한 내용은 해당 DD 시스템에 대한 설치 및 설정 가이드와 확장 셸프에 대한 확장 셸프 하드웨어 가이드를 참조하십시오.

다음 DD 시스템은 DD Extended Retention을 지원합니다.

DD860

- 72GB RAM
- 1 - NVRAM 입출력 모듈(1GB)
- 3 - 쿼드 포트 SAS 입출력 모듈
- 2 - 마더보드의 1GbE 포트
- 0~2 - 외부 접속 구성을 위한 1/10GbE NIC 입출력 카드
- 0~2 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 입출력 카드
- 0~2 - 결합된 NIC 및 FC 카드
- 1~24 - 142TB의 시스템 최대 가용 용량을 초과하지 않는 ES20 또는 ES30 셸프(1TB 또는 2TB 디스크)

DD Extended Retention을 DD860에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 142TB입니다. 보존 계층의 최대 가용 용량은 142TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 284TB입니다.

DD990

- 256GB RAM
- 1 - NVRAM 입출력 모듈(2GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 2 - 마더보드의 1GbE 포트
- 0~4 - 외부 접속 구성을 위한 1GbE NIC 입출력 카드
- 0~3 - 외부 접속 구성을 위한 10GbE NIC 카드
- 0~3 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~3 - 특정 입출력 모듈 하나에서 3개를 초과하지 않는 결합된 NIC 및 FC 카드
- 1~56 - 570TB의 시스템 최대 가용 용량을 초과하지 않는 ES20 또는 ES30 셸프(1, 2 또는 3TB 디스크)

DD Extended Retention을 DD990에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 570TB입니다. 보존 계층의 최대 가용 용량은 570TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 1140TB입니다.

DD4200

- 128GB RAM
- 1 - NVRAM 입출력 모듈(4GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 1GbE 포트
- 0~6 - 외부 접속 구성을 위한 1/10GbE NIC 카드
- 0~6 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~6 - 특정 입출력 모듈 하나에서 4개를 초과하지 않는 결합된 NIC 및 FC 카드
- 1~16 - 192TB의 시스템 최대 가용 용량을 초과하지 않는 ES30 SAS 셸프(2 또는 3TB 디스크). 시스템 컨트롤러 업그레이드에는 ES30 SATA 셸프(1, 2 또는 3TB 디스크)가 지원됩니다.

DD Extended Retention을 DD4200에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 192TB입니다. 보존 계층의 최대 가용 용량은 192TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 384TB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 16개의 셸프까지 지원됩니다.

DD4500

- 192GB RAM
- 1 - NVRAM 입출력 모듈(4GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 1GbE 포트
- 0~6 - 외부 접속 구성을 위한 1/10GbE NIC 입출력 카드
- 0~6 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~5 - 특정 입출력 모듈 하나에서 4개를 초과하지 않는 결합된 NIC 및 FC 카드
- 1~20 - 285TB의 시스템 최대 가용 용량을 초과하지 않는 ES30 SAS 셸프(2 또는 3TB 디스크). 시스템 컨트롤러 업그레이드에는 ES30 SATA 셸프(1TB, 2TB 또는 3TB)가 지원됩니다.

DD Extended Retention을 DD4500에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 285TB입니다. 보존 계층의 최대 가용 용량은 285TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 570TB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 24개 셸프까지 지원됩니다.

DD6800

- 192GB RAM
- 1 - NVRAM 입출력 모듈(8GB)
- 3 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 1GbE 포트
- 0~4 - 외부 접속 구성을 위한 1/10GbE NIC 카드
- 0~4 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~4 - 결합된 NIC 및 FC 카드
- 셸프 조합은 해당 DD 시스템의 설치 및 설정 가이드와 확장 셸프의 확장 셸프 하드웨어 가이드에 설명되어 있습니다.

DD Extended Retention을 DD6800에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 288TB입니다. 보존 계층의 최대 가용 용량은 288TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 0.6PB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 28개의 셸프까지 지원됩니다.

DD7200

- 256GB RAM
- 1 - NVRAM 입출력 모듈(4GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 1GbE 포트
- 0~6 - 외부 접속 구성을 위한 1/10GbE NIC 카드
- 0~6 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~5 - 특정 입출력 모듈 하나에서 4개를 초과하지 않는 결합된 NIC 및 FC 카드
- 1~20 - 432TB의 시스템 최대 가용 용량을 초과하지 않는 ES30 SAS 셸프(2 또는 3TB 디스크). 시스템 컨트롤러 업그레이드에는 ES30 SATA 셸프(1TB, 2TB 또는 3TB)가 지원됩니다.

DD Extended Retention을 DD7200에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 432TB입니다. 보존 계층의 최대 가용 용량은 432TB가 될 수 있습니다. 활성 및

보존 계층의 총 가용 스토리지 용량은 864TB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 32개 셸프까지 지원됩니다.

DD9300

- 384GB RAM
- 1 - NVRAM 입출력 모듈(8GB)
- 3 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 1GbE 포트
- 0~4 - 외부 접속 구성을 위한 1/10GbE NIC 카드
- 0~4 - 외부 접속 구성을 위한 듀얼 포트 FC HBA 카드
- 0~4 - 결합된 NIC 및 FC 카드
- 셸프 조합은 해당 DD 시스템의 설치 및 설정 가이드와 확장 셸프의 확장 셸프 하드웨어 가이드에 설명되어 있습니다.

DD Extended Retention을 DD9300에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 720TB입니다. 보존 계층의 최대 가용 용량은 720TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 1.4PB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 28개의 셸프까지 지원됩니다.

DD9500

- 512GB RAM
- 1 - NVRAM 입출력 모듈(8GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 4중 1GbE 포트
- 0~4 - 외부 접속 구성을 위한 10GbE NIC 카드
- 0~4 - 외부 접속 구성을 위한 듀얼 포트 16Gbe FC HBA 카드
- 셸프 조합은 해당 DD 시스템의 설치 및 설정 가이드와 확장 셸프의 확장 셸프 하드웨어 가이드에 설명되어 있습니다.

DD Extended Retention을 DD9500에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 864TB입니다. 보존 계층의 최대 가용 용량은 864TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 1.7PB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 56개 셸프까지 지원됩니다.

DD9800

- 768GB RAM
- 1 - NVRAM 입출력 모듈(8GB)
- 4 - 쿼드 포트 SAS 입출력 모듈
- 1 - 마더보드의 4중 1GbE 포트
- 0~4 - 외부 접속 구성을 위한 10GbE NIC 카드
- 0~4 - 외부 접속 구성을 위한 듀얼 포트 16Gbe FC HBA 카드
- 셸프 조합은 해당 DD 시스템의 설치 및 설정 가이드와 확장 셸프의 확장 셸프 하드웨어 가이드에 설명되어 있습니다.

DD Extended Retention을 DD9800에서 활성화하면 활성 계층의 최대 가용 스토리지 용량이 1008TB입니다. 보존 계층의 최대 가용 용량은 1008TB가 될 수 있습니다. 활성 및 보존 계층의 총 가용 스토리지 용량은 2.0PB입니다. 외부 접속 구성은 DD Extended Retention 구성에 대해 최대 56개 셸프까지 지원됩니다.

DD Extended Retention에 대한 라이센스 등록

DD Extended Retention은 지원되는 DD 시스템에 설치되는 라이센스가 등록된 소프트웨어 옵션입니다.

활성 계층 및 보존 계층 모두에 설치되는 셸프의 경우 스토리지 셸프마다 별도의 셸프 용량 라이센스가 필요합니다. 셸프 용량 라이센스는 활성 또는 보존 계층 셸프에 따라 다릅니다.

확장 스토리지 라이센스는 Data Domain 모델에 따라 활성 계층 스토리지를 엔트리 용량 이상으로 확장하는 데 필요합니다. 적절한 라이센스를 먼저 적용하지 않은 상태에서는 추가 스토리지를 사용할 수 없습니다.

DD Extended Retention에 대한 셸프 용량 라이센스 추가

DD Extended Retention을 사용하는 DD 시스템의 모든 셸프에는 별도의 라이센스가 있어야 합니다.

절차

1. **Administration** > **Licenses**를 선택합니다.
2. **Add Licenses**를 클릭합니다.
3. 한 줄마다 하나 이상의 라이센스를 입력하고 각 라이센스를 입력한 후에 Enter 키를 누릅니다. 완료되면 **Add**를 클릭합니다. 오류가 발생하면 추가된 라이센스와 오류로 인해 추가되지 않은 라이센스에 대한 요약이 나열됩니다. 이를 수정하려면 오류가 발생한 라이센스 키를 선택합니다.

결과

DD 시스템에 대한 라이센스는 다음 두 그룹으로 표시됩니다.

- DD Extended Retention 및 DD Boost와 같은 옵션에 필요한 소프트웨어 옵션 라이센스
- 셸프 용량(TiB 단위), 셸프 모델(예: ES30), 셸프의 스토리지 계층(활성 또는 보존 계층) 등을 표시하는 셸프 용량 라이센스

라이센스를 삭제하려면 Licenses 목록에서 라이센스를 선택하고 **Delete Selected Licenses**를 클릭하십시오. 확인 메시지가 표시되면 경고를 읽고 **OK**를 클릭하여 계속하십시오.

DD Extended Retention을 위한 스토리지 구성

DD Extended Retention을 위한 추가 스토리지를 구성하려면 적절한 라이센스가 필요하며, DD 시스템에 설치된 메모리가 이를 지원하기에 충분해야 합니다. 라이센스나 메모리가 더 필요하면 오류 메시지가 표시됩니다.

절차

1. **Hardware** > **Storage** 탭을 선택합니다.
2. Overview 탭에서 **Configure Storage**를 선택합니다.
3. Configure Storage 탭의 Addable Storage 목록에서 추가할 스토리지를 선택합니다.
4. 메뉴에서 적절한 Tier Configuration(또는 **Active** 또는 **Retention**)을 선택합니다. 활성 계층은 표준 DD 시스템과 유사하며 비슷한 크기로 지정해야 합니다. 활성 계층에 추가할 수 있는 최대 스토리지 양은 사용하는 DD 컨트롤러에 따라 다릅니다.

5. 추가할 셸프의 확인란을 선택합니다.
6. **Add to Tier** 버튼을 클릭합니다.
7. **OK**를 클릭하여 스토리지를 추가합니다.
8. 추가된 셸프를 제거하려면 Tier Configuration 목록에서 해당 항목을 선택하고 **Remove from Tier**를 선택한 다음 **OK**를 선택합니다.

DD Extended Retention을 위한 Customer-Provided 인프라스트럭처

DD Extended Retention을 설정하려면 먼전 환경 및 설정이 특정 요구 사항을 충족해야 합니다.

- **Specifications, site requirements, rack space, and interconnect cabling**: 사용 중인 DD 시스템 모델의 *Data Domain 설치 및 설정 가이드*를 참조하십시오.
- **Racking and cabling**: 향후 확장을 고려해 시스템을 랙에 장착하는 것이 좋습니다. 모든 셸프는 단일 DD 시스템에 연결됩니다.

  참고

  - 사용 중인 셸프 모델(ES20, ES30 또는 DS60)에 대한 내용은 *Data Domain 확장 셸프 하드웨어 가이드*를 참조하십시오.

DD Extended Retention 관리

DD 시스템에서 DD Extended Retention을 설정하고 사용하려는 경우 DD System Manager 및/또는 DD CLI를 사용할 수 있습니다.

- 이전에 Enterprise Manager로 알려진 DD System Manager는 GUI(Graphical User Interface)이며 이 가이드에 설명되어 있습니다.
- DD CLI(Command Line Interface)에서 입력하는 `archive` 명령은 *Data Domain Operating System 명령 참조 가이드*에 설명되어 있습니다.

DD System Manager를 사용할 때 제공되지 않는 유일한 명령은 `archive report`입니다.

DD Extended Retention에 대해 DD 시스템 활성화

DD Extended Retention에 대해 DD 시스템을 사용하려면 먼저 올바른 라이센스가 있어야 하고 파일 시스템을 정확하게 설정해야 합니다.

절차

1. 올바른 라이센스가 적용되었는지 확인합니다. **Administration** > **Licenses** 를 클릭하고 Feature Licenses 목록에서 Extended Retention을 확인합니다.
2. **Data Management** > **File System** > **More Tasks** > **Enable DD Extended Retention**을 선택합니다.

   이 옵션은 Data Domain 시스템이 DD Extended Retention을 지원하고 파일 시스템이 DD Extended Retention에 대해 아직 구성되지 않은 경우에만 사용할 수 있습니다. DD Extended Retention을 활성화한 후에는 파일 시스템을 제거해야 비활성화할 수 있습니다.

   a. 파일 시스템이 이미 비 DD Extended Retention 시스템으로 활성화된 경우에는 이를 비활성화할지 묻는 메시지가 표시됩니다. 비활성화하려면 **Disable**을 클릭합니다.

b. DD Extended Retention에 사용할 파일 시스템을 변환할지 확인하는 프롬프트가 표시되는 경우 **OK**를 클릭합니다.

파일 시스템이 DD Extended Retention 파일 시스템으로 변환된 후 파일 시스템 페이지가 새로 고쳐지면서 두 계층 모두에 대한 정보가 포함되고 **Retention Units**라는 새 탭이 표시됩니다.

CLI 절차

CLI에서 Extended Retention 라이센스가 설치되어 있는지도 확인할 수 있습니다.

기존 라이센스 등록 방식을 사용하려면 다음과 같이 합니다.

```
# license show
## License Key                    Feature
--    --------------------        -----------
1     AAAA-BBBB-CCCC-DDDD         Replication
2     EEEE-FFFF-GGGG-HHHH         VTL
--    --------------------        -----------
```

라이센스가 없는 경우 각 유닛에 제공된 설명서(빠른 설치 카드)에서 구매한 라이센스를 확인할 수 있습니다. 라이센스 키를 입력하려면 다음 명령을 입력합니다.

```
# license add license-code
```

그런 다음 Extended Retention을 활성화합니다.

```
# archive enable
```

e-라이센스 등록 방식을 사용하려면 다음과 같이 합니다.

```
# elicense show
Feature licenses:
## Feature     Count Mode             Expiration Date
-- ----------- ----- ---------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- ---------------- ---------------
```

라이센스가 없는 경우 라이센스 파일을 새로운 기능 라이센스로 업데이트합니다.

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature            Count   Mode             Expiration Date
-- -----------------  -----  ---------------  ---------------
1  REPLICATION        1      permanent (int)  n/a
2  VTL                1      permanent (int)  n/a
3  EXTENDED RETENTION 1      permanent (int)  n/a
-- ------------------ -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above
EMC ELMS licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

그런 다음 Extended Retention을 활성화합니다.

```
# archive enable
```

DD Extended Retention에 대한 2계층형 파일 시스템 생성

DD Extended Retention에는 활성 및 보존 계층을 위한 2계층형 파일 시스템이 있습니다. 이 특수 파일 시스템을 설정하려면 먼저 DD 시스템에서 DD Extended Retention을 설정해야 합니다.

절차

1. **Data Management** > **File System**을 선택합니다.
2. 파일 시스템이 있는 경우 제거합니다.
3. **More Tasks** > **Create file system**을 선택합니다.
4. 보존을 지원하는 파일 시스템을 선택하고 **Next**를 클릭합니다.
5. File System Create 대화 상자에서 **Configure**를 클릭합니다.

   파일 시스템을 생성하려면 먼저 스토리지를 구성해야 합니다.
6. Configure Storage 대화 상자를 사용해 활성 및 보존 계층의 사용 가능한 스토리지를 추가 및 제거하고 완료되면 **OK**를 클릭합니다.

   활성 계층의 스토리지는 활성 파일 시스템 계층을 생성하는 데 사용되고 보존 계층의 스토리지는 보존 유닛을 생성하는 데 사용됩니다.

   참고

   DD OS 5.5.1부터는 보존 계층당 하나의 보존 유닛만 허용됩니다. 그러나 DD OS 5.5.1 이전에 설정된 시스템의 경우 계속해서 2개 이상의 보존 유닛이 있을 수 있지만 여기에 더 많은 보존 유닛을 추가할 수는 없습니다.

   ---
7. Create File System 대화 상자에서 다음을 수행합니다.

   a. 드롭다운 목록에서 보존 유닛의 크기를 선택합니다.

   b. **Enable file system after creation** 옵션을 선택합니다.

   c. **Next**를 클릭합니다.

   Summary 페이지에 새 파일 시스템의 활성 및 보존 계층 크기가 표시됩니다.
8. **Finish**를 클릭하여 파일 시스템을 생성합니다.

   각 생성 단계의 진행률이 표시되고 진행 표시줄이 전반적인 상태를 모니터링합니다.
9. 파일 시스템 실행이 완료되면 **OK**를 클릭합니다.

   CLI 절차
   추가 셸프를 추가하려면 각 엔클로저에 대해 이 명령을 사용합니다.

   ```
   # storage add tier archive enclosure 5
   ```

   아카이브 유닛을 생성하여 파일 시스템에 추가합니다. 아카이브 유닛의 엔클로저 수를 지정해야 합니다.

   ```
   # filesys archive unit add
   ```

   아카이브 유닛이 생성되어 파일 시스템에 추가되었는지 확인합니다.

   ```
   # filesys archive unit list all
   ```

   시스템에 표시된 파일 시스템을 확인합니다.

   ```
   # filesys show space
   ```

DD Extended Retention의 File System 패널

DD 시스템에서 DD Extended Retention을 설정하고 나면 **Data Management** > **File System** 패널의 모양이 DD Extended Retention을 사용하지 않는 시스템과 약간 달라집니다.

- **State** 파일 시스템이 설정 또는 해제되었음을 보여 줍니다. 바로 오른쪽에 있는 **Disable/Enable** 버튼을 사용해 상태를 변경할 수 있습니다.
- **Clean Status** 마지막 정리 작업을 마친 시간 또는 정리 작업이 현재 실행 중인 경우 현재 정리 상태를 보여 줍니다. 정리를 실행할 수 있는 경우 **Start Cleaning** 버튼이 표시됩니다. 정리가 실행 중일 때에는 **Start Cleaning** 버튼이 **Stop Cleaning** 버튼으로 바뀝니다.
- **Data Movement Status** 마지막 데이터 이동을 마친 시간을 보여 줍니다. 데이터 이동을 실행할 수 있는 경우 **Start** 버튼이 표시됩니다. 데이터 이동이 실행 중일 때에는 **Start** 버튼이 **Stop** 버튼으로 바뀝니다.
- **Space Reclamation Status** 보존 계층에서 데이터를 삭제한 후에 재확보된 공간의 용량을 보여 줍니다. 공간 재확보를 실행할 수 있는 경우 **Start** 버튼이 표시됩니다. 이미 실행 중이면 **Stop** 및 **Suspend** 버튼이 표시됩니다. 이전에 실행되었다가 일시 중단된 경우에는 **Stop** 및 **Resume** 버튼이 표시됩니다. 시작 및 종료 시간, 완료율, 재확보된 유닛, 확보된 공간 등에 대한 자세한 정보를 표시하는 **More Information** 버튼도 있습니다.
- **More Tasks** > **Destroy**를 선택하면 가상 테이프를 포함해 파일 시스템에 있는 모든 데이터를 삭제할 수 있습니다. 이는 시스템 관리자만 수행할 수 있습니다.
- **More Tasks** > **Fast Copy**를 선택하면 소스 디렉토리의 파일과 MTree의 클론을 대상 디렉토리에 생성할 수 있습니다. DD Extended Retention을 사용하는 시스템의 경우 빠른 복제를 실행해도 활성 및 보존 계층 사이에서 데이터가 이동되지 않습니다.
- **More Tasks** > **Expand Capacity**를 선택하면 활성 또는 보존 계층을 확장할 수 있습니다.

활성 또는 보존 계층 확장

파일 시스템이 설정되어 있으면 활성 또는 보존 계층을 확장할 수 있습니다.

Active 계층을 확장하려면 다음을 수행하십시오.

절차

1. **Data Management > File System > More Tasks > Expand Capacity**를 선택합니다.
2. Expand File System Capacity 대화 상자에서 **Active Tier**를 선택하고 **Next**를 클릭합니다.
3. **Configure**를 클릭합니다.
4. Configure Storage 대화 상자에서 Active Tier가 Configure 선택 항목으로 표시되는지 확인하고 **OK**를 선택합니다.
5. 구성이 완료되면 Expand File System Capacity 대화 상자로 돌아갑니다. **Finish**를 선택해 활성 계층 확장을 완료합니다.

retention 계층을 확장하려면 다음을 수행하십시오.

절차

1. **Data Management > File System > More Tasks > Expand Capacity**를 선택합니다.
2. Expand File System Capacity 대화 상자에서 **Retention Tier**를 선택하고 **Next**를 클릭합니다.
3. 보존 유닛을 사용할 수 있는 경우 **Select Retention Unit** 대화 상자가 표시됩니다. 확장하려는 보존 유닛을 선택한 후 **Next**를 선택합니다. 보존 유닛을 사용할 수 없는 경우 **Create Retention Unit** 대화 상자가 표시되며 계속하기 전에 보존 유닛을 생성해야 합니다.

   참고

   DD Extended Retention이 설정된 DD 시스템의 성능을 최적화하려면 항상 최소 두 개의 셸프 증분에서 보존 계층을 확장해야 합니다. 또한 보존 유닛을 확장하기 전에 보존 유닛이 거의 꽉 찰 때까지 기다려서는 안 됩니다.

4. 보존 유닛을 확장할 크기를 선택한 후 **Configure**를 클릭합니다.
5. 구성이 완료되면 Expand File System Capacity 대화 상자로 돌아갑니다. **Finish**를 클릭해 보존 계층 확장을 완료합니다.

보존 계층에서 공간 재확보

공간 재확보를 실행해 보존 계층에서 삭제된 데이터에서 공간을 재확보할 수 있습니다(DD OS 5.3에 도입됨). 공간 재확보는 파일 시스템 정리 중에도 발생합니다.

절차

1. **Data Management > File System**을 선택합니다. 탭 바로 위에 있는 **Space Reclamation Status**에 보존 계층에서 데이터를 삭제한 후 재확보된 공간의 용량이 나타납니다.
2. 공간 재확보를 실행할 수 있는 경우 **Start** 버튼이 표시됩니다. 이미 실행 중이면 **Stop** 및 **Suspend** 버튼이 표시됩니다. 이전에 실행되었다가 일시 중단된 경우에는 **Stop** 및 **Resume** 버튼이 표시됩니다.
3. 주기 이름, 시작 및 종료 시간, 실제 실행 시간, 완료율(진행 중인 경우), 재확보된 유닛, 타겟 유닛에서 확보된 공간 및 확보된 총 공간에 대한 자세한 내용을 보려면 **More Information**을 클릭합니다.

   참고

   `archive space-reclamation` 명령을 사용하는 경우 one-cycle 옵션을 사용하여 수동으로 중지하기 전까지 공간 재확보가 백그라운드에서 실행됩니다. `archive space-reclamation schedule set` 명령을 사용하여 공간 재확보의 시작 시간을 설정할 수도 있습니다.

CLI 절차

공간 재확보를 설정하려면 다음을 입력합니다.

```
# archive space-reclamation start
```

공간 재확보를 해제하려면 다음을 입력합니다.

```
# archive space-reclamation stop
```

공간 재확보의 상태를 표시하려면 다음을 입력합니다.

```
# archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.
```

```
Previous Cycle:
---------------
Start time                 : Feb 21 2014 14:17
End time                   : Feb 21 2014 14:49
Effective run time         : 0   days, 00:32.
Percent completed          : 00 % (was stopped by user)
Units reclaimed            : None
Space freed on target unit : None
Total space freed          : None
```

DD Extended Retention의 File System 탭

DD 시스템에서 DD Extended Retention을 설정하고 나면 **Data Management** > **File System** 탭의 모양도 DD Extended Retention을 사용하지 않는 시스템과는 약간 달라지며 다음 추가 탭 하나가 나타납니다. **Retention Units**

Summary 탭

Summary 탭에는 디스크 공간 사용량과 활성 및 보존 계층의 압축에 대한 정보가 표시됩니다.

Space Usage: 총 공간 크기, 사용된 공간의 용량 및 사용 가능한 공간의 용량과 활성 및 보존 계층의 전체 수가 표시됩니다. 활성 계층에 대해 정리할 수 있는 공간의 용량이 나타납니다.

Active Tier and Retention Tier: 현재 사용되고 지난 24시간 안에 기록된 압축 전 및 압축 후 값을 보여 줍니다. 또한 전역, 로컬 및 총 압축(감소율) 요인을 보여 줍니다.

Retention Units 탭

Retention Units 탭에는 보존 유닛이 표시됩니다. DD OS 5.5.1.4부터는 보존 계층당 하나의 보존 유닛만 허용됩니다. 그러나 DD OS 5.5.1.4 이전에 설정된 시스템의 경우 계속해서 2개 이상의 보존 유닛이 있을 수 있지만 여기에 더 많은 보존 유닛을 추가할 수는 없습니다.

유닛의 상태(New, Empty, Sealed, Target 또는 Cleaning), 그에 대한 상태(Disabled, Ready 또는 Stand-by), 시작 날짜(보존 계층으로 이동된 시기) 및 유닛 크기가 표시됩니다. 공간 재확보가 실행 중인 경우 유닛은 정리 상태가 됩니다. 유닛이 봉인된 경우, 즉 데이터를 더 이상 추가할 수 없으면 Sealed Date가 제공됩니다. 보존 유닛의 확인란을 선택하면 Detailed Information 패널에 추가 정보(Size, Used, Available 및 Cleanable)가 표시됩니다.

여기에는 **Delete**(유닛 삭제) 및 **Expand**(유닛에 스토리지 추가) 버튼이 있습니다. 유닛을 확장하려면 New 또는 Target 상태에 있어야 합니다.

Configuration 탭

Configuration 탭에서 시스템을 구성할 수 있습니다.

Options **Edit** 버튼을 선택하면 Modify Settings 대화 상자가 나타나고 여기서 Local Compression Type(옵션으로 none, lz(기본값), gz 및 gzfast가 있음) 및 Retention Tier Local Comp(ression)(옵션으로 none, lz, gz(기본값) 및 gzfast가 있음)를 변경하고 Report Replica Writable을 사용하도록 설정할 수 있습니다.

Clean Schedule **Edit** 버튼을 선택하면 Modify Schedule 대화 상자가 나타나고 여기서 정리 스케줄과 스로틀 비율을 변경할 수 있습니다.

Data Movement Policy **Edit** 버튼을 선택하면 Data Movement Policy 대화 상자가 나타나고 여기서 몇 가지 매개 변수를 설정할 수 있습니다. File Age Threshold는 사용자 지정 기본값을 설정하지 않은 모든 MTree에 적용되는 시스템 전체의 기본값입니다. 최소값은 14일입니다. Data Movement Schedule에서는 데이터 이동을 얼마나 자주 수행할지 설정할 수 있습니다. 권장되는 스케줄은 2주에 한 번입니다. File System Cleaning에

서는 데이터 이동 후에 시스템 정리를 하지 않도록 선택할 수 있습니다. 이 옵션은 선택한 상태로 두는 것이 좋습니다.

File Age Threshold per MTree 링크

File Age Threshold per MTree 링크를 선택하면 파일 시스템에서 MTree 각각에 대해 사용자 지정된 파일 사용 기간 임계값을 설정할 수 있는 MTree 영역으로 이동합니다(**Data Management** > **MTree**를 선택하는 방법으로도 액세스할 수 있음).

MTree를 선택한 후 Data Movement Policy 옆에 있는 **Edit**를 선택하십시오. Modify Age Threshold 대화 상자에 File Age Threshold에 대한 새 값을 입력하고 **OK**를 선택하십시오. DD OS 5.5.1부터는 최소값이14일입니다.

Encryption 탭

Encryption 탭에서는 Encryption of Data at Rest를 설정하거나 해제할 수 있습니다. 이는 보존 유닛이 하나인 시스템에서만 지원됩니다. 5.5.1부터 DD Extended Retention은 단일 보존 유닛만 지원하므로 5.5.1 이상에서 설정된 시스템의 경우 이 제한 사항을 준수하는 데 아무런 문제가 없습니다. 그러나 5.5.1 이전에 설정된 시스템은 보존 유닛이 두 개 이상일 수 있지만, 한 개를 제외한 모든 보존 유닛이 제거되거나 데이터가 하나의 보존 유닛으로 이동 또는 마이그레이션될 때까지는 저장된 데이터 암호화를 사용할 수 없습니다.

Space Usage 탭

Space Usage 탭에서는 차트 유형 3개 즉, (전체) File System, Active(계층), Archive(계층) 중에서 하나를 선택해, 시간에 따른 공간 사용량을 MiB 단위로 볼 수 있습니다. 오른쪽 상단에서 기간 값(7, 30, 60 또는 120일)을 선택할 수도 있습니다. 데이터는 색으로 구분되어 기록된 압축 전(파란색), 사용된 압축 후(빨간색) 및 압축 비율(검은색)로 표시됩니다.

Consumption 탭

Consumption 탭에서는 차트 유형 3개 즉, (전체) File System, Active(계층), Archive(계층) 중에서 하나를 선택해, 사용된 압축 후 스토리지 용량과 시간에 따른 압축 비율을 볼 수 있습니다. 이를 통해 사용 추세를 확인할 수 있습니다. 오른쪽 상단에서 기간 값(7, 30, 60 또는 120일)을 선택할 수도 있습니다. Capacity 확인란을 사용하면 총 시스템 용량과 비교해 압축 후 스토리지를 표시할지 여부를 선택할 수 있습니다.

Daily Written 탭

Daily Written 탭에서는 기간(7, 30, 60 또는 120일)을 선택해 하루에 기록한 데이터 양을 볼 수 있습니다. 데이터는 색으로 구분되어 그래프와 표 형식에 기록된 압축 전(파란색), 사용된 압축 후(빨간색) 및 압축 비율(검은색)로 표시됩니다.

보존 유닛 확장

최적의 성능을 보장하기 위해서는 확장하기 전에 보존 유닛이 거의 꽉 찰 때까지 기다리지 마십시오. 또한 1개 셸프 증분에서 확장하지 마십시오. 파일 시스템을 생성한 후에는 스토리지를 활성 계층에서 보존 계층으로 이동할 수 없습니다. 사용되지 않은 엔클로저만 보존 계층에 추가할 수 있습니다.

절차

1. **Data Management** > **File System** > **Retention Units**를 선택합니다.
2. 보존 유닛을 선택합니다.

   참고로 정리가 실행 중인 경우 보존 유닛을 확장할 수 없습니다.
3. **Expand**를 클릭합니다.

   시스템에 현재 보존 계층 크기, 예상된 확장 크기 및 확장된 총 용량이 표시됩니다. 추가 스토리지를 사용할 수 있는 경우 Configure 링크를 클릭할 수 있습니다.
4. **Next**를 클릭합니다.

이 작업 후에는 파일 시스템을 원래 크기로 되돌릴 수 없다는 내용의 경고가 표시됩니다.

5. **Expand**를 클릭하여 파일 시스템을 확장합니다.

보존 유닛 삭제

보존 유닛의 모든 파일이 더 이상 필요하지 않은 경우 이러한 파일을 모두 삭제하면 유닛을 재사용할 수 있게 됩니다. 파일 위치 보고서를 생성하여 보존 유닛이 정말로 비어 있는지 확인하고 보존 유닛을 삭제한 후 새 보존 유닛으로 추가할 수 있습니다.

절차

1. 파일 시스템이 실행 중인 경우 **Data Management** > **File System**을 선택하고 **Disable**을 클릭하여 해제합니다.
2. **Data Management** > **File System** > **Retention Units**를 선택합니다.
3. 보존 유닛을 선택합니다.
4. **Delete**를 클릭합니다.

보존 계층 로컬 압축 수정

보존 계층으로의 후속 데이터 이동을 위해 로컬 압축 알고리즘을 수정할 수 있습니다.

절차

1. **Data Management** > **File System** > **Configuration**을 선택합니다.
2. **Options** 오른쪽의 **Edit**를 클릭합니다.
3. Retention Tier Local Comp 메뉴에서 압축 옵션 중 하나를 선택하고 **OK**를 클릭합니다.

   기본값은 데이터 스토리지에 가장 적은 공간을 사용하는 zip 방식의 압축인 gz로, lz에 비해 공간을 평균 10% - 20% 적게 사용하지만 일부 데이터 세트의 경우 압축률이 훨씬 더 높습니다.

데이터 이동 정책 이해

파일은 마지막으로 수정된 날짜를 기준으로 활성 계층에서 보존 계층으로 이동됩니다. 데이터 무결성을 위해 전체 파일이 이 시기에 이동됩니다. *데이터 이동 정책*은 *파일 사용 기간 임계값* 및 *데이터 이동 스케줄*을 설정합니다. 파일 사용 기간 임계값에서 설정된 기간 동안 데이터가 변경되지 않으면 해당 데이터는 데이터 이동 스케줄에서 설정한 날짜에 활성 계층에서 보존 계층으로 이동됩니다.

참고

DD OS 5.5.1부터 파일 사용 기간 임계값은 최소 14일이어야 합니다.

정의된 MTree마다 다른 파일 사용 기간 임계값을 지정할 수 있습니다. MTree는 관리 용도의 논리적 데이터 세트에 해당하는 네임스페이스 내 하위 트리입니다. 예를 들어 별도의 MTree에 재무 데이터, e-메일 및 엔지니어링 데이터를 배치할 수 있습니다.

DD OS 5.3에 도입된 *공간 재확보* 기능을 활용하려면 격주 간격으로(14일마다) 데이터 이동 및 파일 시스템 정리를 예약하는 것이 좋습니다. 기본적으로 정리는 항상 데이터 이동이 완료된 후에 실행됩니다. 이 기본값은 변경하지 않는 것이 좋습니다.

다음과 같은 일반적인 사이징 오류가 발생하지 않도록 하십시오.

- 지나치게 적극적인 데이터 이동 정책을 설정하여 데이터가 너무 빨리 이동합니다.
- 너무 소극적인 데이터 이동 정책을 설정하여 활성 계층이 채워진 후에는 시스템에 데이터를 기록할 수 없습니다.

- 활성 계층의 크기를 작게 지정한 후 이를 벌충하기 위해 지나치게 적극적인 데이터 이동 정책을 설정합니다.

스냅샷과 파일 시스템 정리와 관련하여 다음과 같은 주의 사항을 염두에 두십시오.

- 스냅샷에 있는 파일은 보존 계층으로 이동한 후에도 정리되지 않습니다. 스냅샷이 삭제된 후에야 공간을 재확보할 수 있습니다.
- 스냅샷에 대한 파일 사용 기간 임계값을 최소 14일로 설정하는 것이 좋습니다.

데이터 이동 정책을 설정하는 방법의 두 가지 예는 다음과 같습니다.

- 변경 정도가 다른 데이터를 두 개의 서로 다른 MTree로 분리하고, 데이터가 안정화되면 바로 데이터를 이동하도록 파일 사용 기간 임계값을 설정합니다. 매일 증분 백업을 위한 MTree A와 주 단위 전체 백업을 위한 MTree B를 생성하십시오. MTree A의 데이터가 이동하지 *않도록* 해당 파일 사용 기간 임계값을 설정하되 MTree B의 파일 사용 기간 임계값을 14일(최소 임계값)로 설정하십시오.
- 서로 다른 MTree로 분리할 수 없는 데이터의 경우 다음과 같이 할 수 있습니다. 매일 증분 백업의 보존 기간이 8주라고 가정하면 주 단위 전체 백업의 보존 기간은 3년이 됩니다. 이 경우 파일 사용 기간 임계값을 9주로 설정하는 것이 가장 좋습니다. 더 낮게 설정하면 곧 삭제되는 매일 증분 백업 데이터를 이동하게 됩니다.

데이터 이동 정책 수정

각 MTree별로 다른 데이터 이동 정책을 설정할 수 있습니다.

절차

1. **Data Management** > **File System** > **Configuration**을 선택합니다.
2. **Data Movement Policy** 오른쪽의 **Edit**를 클릭합니다.
3. Data Movement Policy 대화 상자에서 시스템 전체 기본 파일 사용 기간 임계값을 일수로 지정합니다. DD OS 5.5.1부터는 이 값이 14일 이상이어야 합니다. 이 값은 새로 생성된 MTree 및 **File Age Threshold per MTree** 링크(7단계 참조)를 사용해 MTree당 사용 기간 임계값이 할당되지 않은 MTree에 적용됩니다. 데이터 이동이 시작되면 지정한 임계값 일수 동안 수정되지 않은 모든 파일이 활성 계층에서 보존 계층으로 이동합니다.
4. 데이터 이동이 발생해야 하는 데이터 이동 스케줄을 지정합니다(예: 매일, 매주, 격주(14일마다), 매달 또는 매월 말일). 특정 날짜와 시간을 시간 및 분 단위로 선택할 수도 있습니다. 공간 재확보 기능(DD OS 5.3에 도입됨)을 활용하려면 격주(14일마다) 기준으로 데이터 이동 및 파일 시스템 정리를 예약하는 것이 좋습니다.
5. Data Movement Throttle, 즉 데이터 이동에 사용할 수 있는 리소스의 백분율을 지정합니다. 값이 100%인 경우 데이터 이동이 조절되지 않습니다.
6. 기본적으로 파일 시스템 정리는 항상 데이터 이동이 완료된 후에 실행됩니다. **Start file system clean after Data Movement**는 선택한 상태로 두는 것이 좋습니다.
7. OK를 선택합니다.
8. Configuration 탭으로 돌아가 오른쪽 아래에 있는 **File Age Threshold per MTree** 링크를 사용해 개별 MTree의 사용 기간 임계값을 지정할 수 있습니다.

   CLI 절차

   사용 기간 임계값을 설정하려면 다음을 입력합니다.

   ```
   # archive data-movement policy set age-threshold {days|none}
   mtrees mtree-list
   ```

   필요한 경우 *기본* 사용 기간 임계값을 설정하려면 다음을 입력합니다.

   ```
   # archive data-movement policy set default-age-threshold days
   ```

사용 기간 임계값 설정을 확인하려면 다음을 입력합니다.

```
# archive data-movement policy show [mtree mtree-list]
```

마이그레이션 스케줄을 지정하려면 다음을 입력합니다.

```
# archive data-movement schedule set days days time time [no-
clean]
```

허용 가능한 스케줄 값은 다음과 같습니다.

- days sun time 00:00
- days mon,tue time 00:00
- days 2 time 10:00
- days 2,15 time 10:00
- days last time 10:00 - 월의 마지막 날

마이그레이션 스케줄을 확인하려면 다음을 입력합니다.

```
# archive data-movement schedule show
```

파일 정리 스케줄을 해제하려면 다음을 입력합니다.

참고

정리 스케줄을 해제하는 이유는 정리 스케줄과 데이터 이동 스케줄이 겹치는 것을 방지하기 위해서입니다. 데이터 이동이 완료되면 정리가 자동으로 시작됩니다. 데이터 이동을 해제하면 파일 시스템 정리를 다시 설정해야 합니다.

```
# filesys clean set schedule never
```

필요 시 데이터 이동 시작 또는 중지

정기적인 데이터 이동 정책이 있는 경우에도 *필요 시*에 데이터 이동을 시작하거나 중지할 수 있습니다.

절차

1. **Data Management** > **File System**을 선택합니다.
2. **Data Movement Status** 오른쪽에서 **Start**를 클릭합니다.
3. Start Data Movement 대화 상자에 데이터 이동 정책에 정의된 대로 활성에서 보존 계층으로 데이터를 이동한 후 파일 시스템 정리가 수행될 것이라는 경고가 나타납니다. **Start**를 선택해 데이터 이동을 시작합니다.

   파일 시스템 정리가 이미 진행 중이라면 정리 작업이 완료된 후에 데이터 이동이 일어납니다. 그러나 이 필요 시 데이터 이동이 완료된 후에 또 다른 정리 작업 역시 자동으로 시작됩니다.
4. **Start** 버튼이 **Stop** 버튼으로 교체됩니다.
5. 언제든지 데이터 이동을 중지하려면 **Stop**을 클릭하고 Stop Data Movement 대화 상자에서 **OK**를 클릭해 확인합니다.

데이터 이동 압축 사용

데이터는 모든 파일 마이그레이션 이후에 타겟 파티션에서 압축됩니다(DD OS 5.2부터). 이 기능을 *데이터 이동 압축*이라고 하며 기본적으로 사용하도록 설정되어 있습니다.

이 기능을 설정하면 보존 계층의 전체 압축 효과가 개선되지만 마이그레이션 시간이 약간 늘어납니다.

이 기능을 설정할 수 있는지 확인하려면 **Data Management** > **File System** > **Configuration**을 선택하십시오.

Packing data during Retention Tier data movement의 현재 값은 Enabled 또는 Disabled일 수 있습니다. 이 설정을 변경하려면 시스템 엔지니어와 상의하십시오.

DD Extended Retention 기반 업그레이드 및 복구

다음 섹션에서는 DD Extended Retention을 사용하는 DD 시스템에 대해 소프트웨어 및 하드웨어 업그레이드를 수행하는 방법과 데이터를 복구하는 방법을 설명합니다.

DD Extended Retention을 사용하는 DD OS 5.7로 업그레이드

DD Extended Retention을 사용하는 DD 시스템의 업그레이드 정책은 표준 DD 시스템의 업그레이드 정책과 동일합니다.

최대 2개의 주요 이전 릴리즈에서 업그레이드하는 프로세스가 지원됩니다. DD OS의 업그레이드 방법에 관한 지침은 타겟 DD OS 버전에 대한 *릴리즈 노트*의 업그레이드 지침 섹션을 참조하십시오.

DD Extended Retention을 사용하는 DD 시스템을 DD OS 5.7로 업그레이드할 때, 공간 재확보 기능을 이용하려면 기존 데이터 이동 스케줄을 격주(14일)로 업데이트해야 합니다.

DD Extended Retention을 사용하는 DD 시스템은 데이터 이동이 완료된 후에 자동으로 정리를 실행하므로, DD System Manager 또는 CLI(Command Line Interface)를 사용하여 정리를 따로 예약하지 않습니다.

활성 계층을 사용할 수 있는 경우 이 프로세스에서는 활성 계층과 보존 유닛을 업그레이드하고 이전 업그레이드가 완료된 것으로 확인되지 않은 상태로 시스템을 설정합니다. 이 상태는 파일 시스템이 설정되고 보존 계층이 업그레이드되었는지 확인한 후 파일 시스템을 통해 지워집니다. 후속 업그레이드는 이 상태가 지워진 후에야 허용됩니다.

활성 계층을 사용할 수 없는 경우 업그레이드 프로세스는 시스템 섀시를 업그레이드하고 파일 시스템을 생성하거나 허용할 준비가 된 상태로 설정합니다.

업그레이드 프로세스가 완료된 후 보존 유닛을 사용할 수 있게 되면 유닛을 시스템에 플러그인할 때 또는 다음에 시스템을 시작할 때 유닛이 자동으로 업그레이드됩니다.

DD Extended Retention 기반 하드웨어 업그레이드

DD Extended Retention을 사용하는 DD 시스템을 버전이 더 높거나 성능이 더 뛰어난 DD Extended Retention을 사용하는 DD 시스템으로 업그레이드할 수 있습니다. 예를 들어 DD Extended Retention을 사용하는 DD860을 DD Extended Retention을 사용하는 DD990으로 교체할 수 있습니다.

참고

계약된 서비스 공급업체에 문의하고 해당 *System Controller Upgrade Guide*의 지침을 참조하십시오.

이러한 유형의 업그레이드는 DD Extended Retention에 다음과 같은 영향을 줍니다.

- 새 시스템에 활성 및 보존 계층보다 최신 버전의 DD OS가 있는 경우 활성 및 보존 계층이 새 시스템의 버전으로 업그레이드됩니다. 그렇지 않으면 새 시스템이 활성 및 보존 계층의 버전으로 업그레이드됩니다.
- 새 시스템에 연결된 활성 및 보존 계층을 새 시스템에서 소유하게 됩니다.

- 활성 계층이 있는 경우 활성 계층의 레지스트리가 새 시스템에 설치됩니다. 그렇지 않으면 가장 최근에 레지스트리가 업데이트된 보존 계층의 레지스트리가 새 시스템에 설치됩니다.

DD Extended Retention을 사용하는 시스템 복구

DD Extended Retention을 사용하는 DD 시스템에서 활성 계층과 일부 보존 유닛이 손실되고 사용 가능한 복제본이 없는 경우 지원 센터 담당자가 봉인된 나머지 보존 유닛을 새 DD 시스템으로 재구성할 수 있습니다.

DD Extended Retention을 사용하는 DD 시스템은 보존 유닛이 하나 이상 손실되더라도 읽기 및 쓰기 요청을 처리할 수 있는 상태를 유지하도록 설계되었습니다. 파일 시스템이 재시작되거나 보존 유닛에 저장된 데이터에 액세스하기 전에는 파일 시스템이 보존 유닛 손실을 감지하지 못할 수 있습니다. 후자의 경우 파일 시스템 재시작이 트리거될 수 있습니다. 파일 시스템이 보존 유닛 손실을 감지한 후에는 해당 유닛에 저장된 데이터 요청에 대한 응답으로 오류가 반환됩니다.

복제본에서 손실된 데이터를 복구할 수 없는 경우 지원 팀 담당자가 손실된 보존 유닛과 그 안에 모두 남아 있거나 일부 남아 있는 파일을 삭제하여 시스템을 정리할 수 있습니다.

복제 복구 사용

DD Extended Retention을 사용하는 DD 시스템의 복제 복구 절차는 복제 유형에 따라 다릅니다.

- 컬렉션 복제 – 새 소스를 DD Extended Retention을 사용하는 Data Domain 시스템으로 구성해야 합니다. 이때 보존 유닛의 개수는 대상과 동일하거나 더 많아야 합니다. 보존 유닛이 추가되어 복제 복구가 시작될 때까지 새 소스에서 파일 시스템을 활성화하면 안 됩니다.

  참고

  컬렉션 복제본에서 보존 유닛 하나를 복구하는 경우와 같이 시스템의 일부만 복구해야 할 경우 지원 팀에 문의하십시오.

- MTree 복제 – *DD Replicator 작업* 장의 *MTree 복제* 섹션을 참조하십시오.
- DD Boost 관리 파일 복제 – *OpenStorage용 Data Domain Boost 관리 가이드*를 참조하십시오.

시스템 장애로부터 복구

DD Extended Retention을 사용하는 DD 시스템에는 다양한 시스템 부분의 장애를 해결하기 위한 툴이 설치되어 있습니다.

절차

1. 시스템 컨트롤러와 스토리지 간의 접속을 복원합니다. 시스템 컨트롤러가 손실된 경우 새 시스템 컨트롤러로 교체합니다.
2. 데이터가 손실되었지만 사용 가능한 복제본이 있는 경우 복제본에서 데이터 복구를 시도합니다. 복제본을 사용할 수 없는 경우에는 지원 팀을 통해 DD Extended Retention의 장애 격리 기능을 활용하여 데이터 손실을 제한하십시오.

아카이브 계층에서 DD Cloud Tier로 데이터 마이그레이션

이 절차에서는 MTree 복제를 사용하여 확장 보존이 있는 Data Domain 시스템의 아카이브 계층에서 DD Cloud Tier가 있는 단일 노드 Data Domain 또는 DD VE 인스턴스로 데이터를 마이그레이션합니다.

시작하기 전에

- 복제 및 DD Cloud Tier에 대한 라이선스가 필요합니다.
- DD Cloud Tier를 지원하려면 대상 시스템에서 Data Domain Operating System 버전 6.0 이상을 실행하고 있어야 합니다.
- 데이터가 최소 14일 동안 대상 시스템의 DD Cloud Tier 스토리지로 이동되지 않으므로 대상 시스템에는 원본 시스템의 활성 계층과 아카이브 계층 둘 다의 데이터를 보유할 수 있는 충분한 활성 계층 용량이 있어야 합니다.
- Data Domain은 모든 용량 계획에 최소 14일 동안의 복제된 데이터를 위한 충분한 활성 계층 용량을 포함할 것을 권장합니다.
- 원본 시스템의 모든 백업 작업과 기타 쓰기 작업은 대상 시스템으로 리디렉션되어야 합니다.
- 대상 시스템은 원본 시스템에서 충족하는 동일한 규정 준수 요구 사항을 모두 충족해야 합니다.
- 고객은 대상 및 원본 Data Domain 시스템에 대한 모든 해당 계정 및 자격 증명을 제공해야 합니다.

추가 고려 사항:

- DD Cloud Tier 스토리지로의 즉각적인 데이터 마이그레이션이 필요한 경우 Dell EMC 지원에 문의하십시오.
- 고객 백업 애플리케이션이 이러한 데이터 마이그레이션을 추적하지 않을 수 있습니다.
- 이 절차에는 MFR(Managed File Replication)은 포함되지 않습니다.
- 라이선싱 - Data Domain 시스템에서 다음을 사용할 수 있습니다.
  - 레거시 라이선싱 - `license show` 명령 사용
  - ELMS 라이선싱 - `elicense show` 명령 사용

레거시 라이선싱을 사용하는 Data Domain 시스템은 라이선스를 점진적으로 추가할 수 있습니다. 모든 최신 기능이 레거시 라이선싱에서 지원되는 것은 아닙니다.

DD OS 6.0 이상이 함께 설치되고 ELMS 라이선싱이 필요한 기능으로 변환되거나 업그레이드된 Data Domain 시스템은 라이선스를 적용 및 표시할 때 `elicense` 명령을 사용하며, 새 라이선스 키 파일이 적용되면 새 키 세트가 모든 이전 키를 완전히 대체합니다.

⚠ 주의

ELMS 라이선스를 업데이트할 때 기존 용량 또는 기능을 제거하지 않아야 합니다.

이 절차에서는 다음 용도에 대해 설명합니다.

- 고객은 아카이브 계층 스토리지의 데이터를 대상 시스템의 DD Cloud Tier 스토리지로 이동하려고 합니다.
- 고객은 원본 시스템의 활성 및 아카이브 계층 스토리지의 데이터를 대상 시스템의 활성 계층 스토리지로 이동하려고 합니다.

- 고객은 여러 원본 시스템의 아카이브 계층 스토리지의 데이터를 대상 시스템의 활성 또는 DD Cloud Tier 스토리지로 이동하려고 합니다.
- 고객은 마이그레이션 작업이 완료된 후 원본 시스템 또는 해당 디스크 엔클로저의 용도를 변경하려고 합니다.

용량 계획

시작하기 전에

대상 시스템에는 원본 시스템의 활성 및 아카이브 계층을 함께 저장할 수 있는 충분한 활성 계층 용량이 있어야 합니다.

또한 원본 시스템의 활성 계층에는 아카이브 계층으로의 데이터 이동이 중지될 때부터 원본 시스템에서 대상 시스템으로의 마이그레이션이 완료될 때까지 예약 백업의 모든 데이터를 보존할 수 있는 충분한 공간이 있어야 합니다.

이 절차는 두 DD9800 시스템과 하나의 10GbE LAN 연결을 사용하여 개발 및 테스트되었습니다.

절차

1. 고객이 제공한 sysadmin 계정 로그인 자격 증명을 사용하여 원본 Data Domain 시스템에 로그인하고 지난 7일 동안 원본 시스템의 활성 계층에 수집된 데이터의 양을 식별합니다.

   참고

   이 정보를 어플라이언스에서 생성된 마지막 자동 지원에서 추출할 수도 있습니다. 이 정보에 대해 자동 지원을 사용하는 경우 최신 정보인지 확인합니다.

```
# filesys show compression
From: 2018-08-29 17:00 To: 2018-09-05 17:00

Active Tier:
                 Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                    (GiB)       (GiB)        Factor       Factor          Factor
                                                                   (Reduction %)
-------------    --------   ---------   -----------   ----------   -------------
Written:
  Last 7 days    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
  Last 24 hrs    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
-------------    --------   ---------   -----------   ----------   -------------

Archive Tier:
                 Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                    (GiB)       (GiB)        Factor       Factor          Factor
…
…
Currently Used:*
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor


…
…
       Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
```

   이 예제에서 주별 수집은 주당 약 37TB로, 하루 5.28TB에 해당합니다.

2. 원본 시스템에서 `filesys show space` 명령을 실행하여 활성 계층의 여유 공간 크기를 결정합니다.

```
# filesys show space
Active Tier:
```

```
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB*
----------------   --------   --------   ---------   ----   --------------
/data: pre-comp           -    69480.4           -      -                -
/data: post-comp    30352.2       35.5     30316.7     0%              0.0
/ddvar                 47.2        9.2        35.6    21%                -
/ddvar/core           984.3        2.0       932.3     0%                -
----------------   --------   --------   ---------   ----   --------------

Cloud Tier
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -        0.0           -      -               -
/data: post-comp        0.0        0.0         0.0     0%             0.0
----------------   --------   --------   ---------   ----   -------------

Total:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -    69480.4           -      -               -
/data: post-comp    30352.2       35.5     30316.7     0%             0.0
/ddvar                 47.2        9.2        35.6    21%               -
/ddvar/core           984.3        2.0       932.3     0%               -
----------------   --------   --------   ---------   ----   -------------
 * Estimated based on last cleaning of 2018/09/04 06:03:57.
```

3. 이전 달에 소비된 공간의 양과 대상 시스템으로의 마이그레이션이 완료될 때까지 필요한 추가 공간을 예측합니다.
4. 원본 시스템의 활성 계층에 있는 사용 가능한 공간이 필요한 크기보다 작으면 마이그레이션을 계속하기 전에 활성 계층에 스토리지를 더 추가합니다.

   ⚠ 주의

   이렇게 하려면 이 절차를 중지하고 스토리지를 추가한 후 다시 시작해야 합니다.

5. 원본 시스템의 활성 계층에서 충분한 용량을 사용할 수 있게 되면 나머지 마이그레이션 단계를 계속 진행합니다.

아카이브 계층으로의 데이터 이동 중지

절차

1. 원본 시스템에 설정된 아카이브 일정을 봅니다.

   ```
   # archive data-movement schedule show
   Archive data movement is scheduled to run on day(s) "tue" at
   "06:00" hrs
   ```

2. 데이터 이동을 절대 중지하지 않도록 아카이브 일정을 설정합니다.

   ```
   # archive data-movement schedule set never
   The archive data-movement schedule will be deleted.
           Are you sure? (yes|no|?) [no]: yes
   Ok, proceeding.
   The archive data-movement is not scheduled.
   ```

3. 데이터 이동 일정이 never로 설정되어 있는지 확인합니다.

   ```
   # archive data-movement schedule show
   There is no archive data movement schedule.
   ```

4. 원본 시스템에 아카이브 계층 공간 회수 일정이 구성되어 있는지 여부를 확인합니다.

   ```
   # archive space-reclamation schedule show
   Archive space-reclamation is scheduled to run on day(s) "mon"
   at "10:10" hrs
   ```

5. 데이터 이동을 절대 중지하지 않도록 공간 회수 일정을 설정합니다.

```
# archive space-reclamation schedule set never
The archive space-reclamation schedule will be reset to "never".
        Are you sure? (yes|no|?) [no]: yes
 ok, proceeding.
 The archive space-reclamation schedule is reset to "never".
```

6. 공간 회수 일정이 never로 설정되어 있는지 확인합니다.

```
# archive space-reclamation schedule show
Archive space-reclamation does not have any schedule.
```

7. 원본 시스템에서 진행 중인 데이터 이동이 없는지 확인합니다.

```
# archive data-movement status
Data-movement was started on Jun 12 2018 06:00 and completed on
Jun 12 2018 06:01
```

8. 원본 시스템에서 공간 회수가 진행되고 있지 않은지 확인합니다.

```
# archive space-reclamation status
Space-reclamation has never been started.
```

9. 데이터 이동 또는 공간 회수 작업이 진행 중인 경우 계속하기 전에 완료되도록 허용합니다.

파일 위치 확인

필요에 따라 원본 시스템 MTree를 확인하여 각 MTree의 파일이 활성 계층 또는 아카이브 계층에 있는지를 검토합니다. 이 작업은 정보를 제공하기 위한 것으로, 원본 시스템에서 대상 시스템으로의 데이터 전송을 완료하기 위해 반드시 필요한 것은 아닙니다.

절차

1. 데이터 이동 정책이 구성된 원본 시스템의 MTree를 확인합니다. 이 정보는 대상 시스템으로의 복제를 구성할 때 필요하므로 기록해 둡니다.

```
# archive data-movement policy show
The default age-threshold value is "none".
Mtree-name                    Age-threshold
----------------------------  --------------
/data/col1/backup             none (default)
/data/col1/large_files_100gb  1
----------------------------  --------------
```

2. 특정 MTree의 파일 위치를 봅니다.

```
# archive report generate file-location path /data/col1/large_files_100gb
-------------------------------                 ---------------------------
File Name                                       Location(Tier/Archive Unit)
-------------------------------                 ---------------------------
/data/col1/large_files_100gb/File_50g.0002.0000  Active
/data/col1/large_files_100gb/File_50g.0001.0000  Active
/data/col1/large_files_100gb/File_50g.0003.0000  archive-unit-2
/data/col1/large_files_100gb/File_50g.0006.0000  archive-unit-2
```

3. 필요에 따라 `archive report generate file-location path all` 명령을 실행하여 시스템에 있는 모든 파일의 목록을 봅니다.

참고

원본 시스템에 저장된 파일의 수에 따라, 이 명령을 완료하는 데 시간이 오래 걸립니다.

Data Domain 복제 라이선스 적용

절차

1. 레거시 라이선스를 사용하여 원본 시스템의 라이선스를 확인합니다.

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
--   -------------------   ------------------
```

2. 복제 라이선스를 추가합니다.

```
# license add <license-key>
```

3. 복제 라이선스가 원본 시스템에 추가되었는지 확인합니다.

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
3    EZXW-SZZF-BGCS-VRZX   REPLICATION
--   -------------------   ------------------
```

4. ELMS 라이선스를 사용하여 대상 시스템의 라이선스를 확인합니다.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ----------------------------   -----   ---------------   ---------------
1    DDBOOST                            1   permanent         n/a
--   ----------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

5. 라이선스 포털에서 얻은 라이선스 키를 업데이트하여 복제 라이선스를 추가합니다. 텍스트 편집기에서 라이선스 파일을 열고 복사한 후 업데이트 프롬프트에 붙여넣고 **Ctrl+D**를 누릅니다.

```
# elicense update
Enter the content of license file and then press Control-D, or
press Control-C to cancel.
```

6. 복제 라이선스가 원본 시스템에 추가되었는지 확인합니다.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
```

```
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                      Count   Mode              Expiration Date
--   --------------------------   -----   ---------------   ---------------
1    REPLICATION                      1   permanent         n/a
2    DDBOOST                          1   permanent         n/a
--   --------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

원본 시스템에서 대상 시스템으로의 복제 시작

Data Domain 시스템에 포함될 수 있는 MTree 및 복제 컨텍스트의 최대 최적 개수를 기록해 둡니다. 원본 시스템의 MTree 수가 한 번에 허용되는 최대 복제 컨텍스트 수를 초과하는 경우 데이터를 대상 시스템으로 전송하기 위해 여러 개의 직렬 복제 컨텍스트가 필요할 수 있습니다. 예를 들어, DD860은 90개의 MTree 복제 컨텍스트를 지원 하며 DD990은 최대 270개의 MTree 복제 컨텍스트를 지원합니다.

절차

1. 원본 시스템의 호스트 이름을 확인합니다.

   ```
   # hostname
   The Hostname is: Source.ER.FQDN
   ```

2. 대상 시스템의 호스트 이름을 확인합니다.

   ```
   # hostname
   The Hostname is: Target.DD.FQDN
   ```

3. 원본 시스템에서 대상 시스템에 대한 MTree 복제 컨텍스트를 설정합니다.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

4. 대상 시스템에서 원본 시스템에 대한 MTree 복제 컨텍스트를 설정합니다.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

5. 원본 시스템에서 복제 작업을 시작합니다. 대상 시스템에서는 이 명령을 실행할 필요가 없습니다.

   참고

   복제 컨텍스트 초기화에 필요한 시간은 처음으로 복제되는 원본 MTree에 있는 데이터의 양에 따라 달라집니다.

   ```
   # replication initialize mtree://Target.ER.FQDN/data/col1/
   large_files_100gb
   (00:08) Waiting for initialize to start...
   (00:10) Initialize started.
   Use 'replication watch mtree://Target.DDR.FQDN/data/col1/one'
   to monitor progress.
   ```

6. 원본 시스템에서 복제 구성에 오류가 없는지 확인합니다.

참고

복제 컨텍스트 초기화에 필요한 시간은 처음으로 복제되는 원본 MTree에 있는 데이터의 양에 따라 달라집니다.

```
#  replication status mtree://target.ER.FQDN/data/col1/
large_files_100gb
CTX:                                    1
Mode:                                   source
Destination:                            mtree://Target.DD.FQDN/
data/col1/one
Enabled:                                yes
Low bandwidth optimization:             disabled
Replication encryption:                 enabled
Replication propagate-retention-lock:   enabled
Local filesystem status:                enabled
Connection:                             connected since Tue Jun
12 17:46:14
State:                                  initializing 3/3 0%
Error:                                  no error
Sync'ed-as-of time:                     -
Current throttle:                       unlimited
```

7. 원본 시스템에서 복제가 진행 중인지 확인합니다.

```
#  replication watch mtree://Source.ER.FQDN/data/col1/large_files_100gb
Use Control-C to stop monitoring.

(00:00) Replication initialize started...
(00:02) initializing:
(00:18)       0% complete, pre-comp: 213183 KB/s, network: 120855 KB/s
(00:22)       0% complete, pre-comp: 246130 KB/s, network: 120719 KB/s
```

복제 진행률 모니터링

절차

1. 원본 시스템의 모든 MTree 복제 컨텍스트에 대한 구성 세부 정보를 봅니다.

```
# replication show config
```

2. 진행 중인 모든 복제 작업에 대한 전체 진행률을 봅니다.

```
# replication show detailed-stats
```

3. 특정 복제 작업의 진행률을 봅니다.

```
# replication show detailed-stats mtree://Target.ER.FQDN/data/col1/large_files_100gb
```

4. 모든 복제 컨텍스트의 성능을 봅니다.

```
# replication show performance all
06/12 17:58:14
       rctx://1               rctx://2               rctx://3
 Pre-comp    Network     Pre-comp    Network     Pre-comp    Network
  (KB/s)     (KB/s)       (KB/s)     (KB/s)       (KB/s)     (KB/s)
 ---------  ---------    ---------  ---------    ---------  ---------
     29459      37607        36374      38071     13089559      39043
    113832      45061        38138      37327     13012122      38812
     29298      42153        33231      36388     12869385      38387
```

복제 초기화가 완료되었는지 또는 동기화 상태인지 확인

절차

1. 원본 시스템에서 복제 통계를 봅니다.

```
# replication show detailed-stats
```

복제 작업이 완료되면 출력의 `Post-comp Bytes Remaining` 열에 0 값이 표시됩니다. `Sync'ed-as-of` 열의 값은 원본 및 대상 시스템이 동기화된 가장 최근 시간을 표시합니다.

2. 복제가 아직 진행 중이면 작업이 완료될 때까지 기다립니다.
3. 원본 및 대상 시스템 둘 다의 MTree 크기가 일치하는지 확인합니다. 두 시스템에서 다음 명령을 실행합니다.

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
/data/col1/large_files_100gb          2500.0   RW
----------------------------  --------------   ------
```

복제 컨텍스트 중단

시작하기 전에

원본 시스템의 MTree가 더 이상 데이터를 수집하지 않는지 확인합니다.

절차

1. 원본 시스템에서 복제 컨텍스트를 중단합니다.

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

2. 대상 시스템에서 복제 컨텍스트를 중단합니다.

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

3. 원본 시스템에서 복제 컨텍스트가 중단되었는지 확인합니다.

```
# replication show config
```

4. 대상 시스템에서 복제 컨텍스트가 중단되었는지 확인합니다.

```
# replication show config
```

5. 대상 시스템의 MTree가 읽기/쓰기로 설정되어 있는지 확인합니다.

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
/data/col1/large_files_100gb  2500.0           RW
----------------------------  --------------   ------
```

원본 시스템 용도 변경

시작하기 전에

⚠ 주의

원본 시스템 용도를 변경하기 전에 다음 항목을 완료해야 합니다. 모든 요구 사항이 완료될 때까지 이 작업을 진행하지 마십시오.

- **원본 시스템의 모든 데이터를 대상 시스템으로 복제합니다.**
- **이제 모든 백업 작업이 대상 시스템을 가리켜야 합니다.**
- **이전 백업의 모든 읽기 및 복원이 대상 시스템에서 수행됩니다.**
- **모든 규정 준수 요구 사항이 대상 시스템에서 충족됩니다.**

절차

1. 원본 시스템에서 파일 시스템을 제거하고 제로화합니다.

```
# filesys destroy and-zero
```

참고

아카이브 계층은 비활성화할 수 없습니다. 이 계층을 제거하는 유일한 방법은 파일 시스템을 제거하는 것입니다.

2. 아카이브 계층에 연결된 디스크 엔클로저를 식별합니다.

```
# storage show tier archive
Archive tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg2       4.1-4.15   15      1.8 TiB
dg3       3.1-3.15   15      1.8 TiB
```

3. 시스템에서 아카이브 계층 스토리지 엔클로저를 제거합니다.

```
# storage remove enclosures 3
Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfully removed: 3  done

# storage remove enclosures 4
Removing enclosure 4...Enclosure 4 successfully removed.

Updating system information...done

Successfully removed: 4  done
```

4. 시스템에서 아카이브 계층 엔클로저가 제거되었는지 확인

```
# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg1       2.1-2.14   14      1.8 TiB
(spare)   2.15       1       1.8 TiB
-------   --------   -----   --------   -----------
Current active tier size: 21.8 TiB
Active tier maximum capacity: 43.7 TiB
Storage addable disks:
Disk        Disks      Count   Disk       Enclosure   Shelf
Capacity   Additional
Type                           Size       Model       License
Needed   Information
---------   --------   -----   --------   ---------
--------------   ---------
(unknown)   3.1-3.15   15      1.8 TiB    ES30        21.8 TiB
(unknown)   4.1-4.15   15      1.8 TiB    ES30        21.8 TiB
---------   --------   -----   --------   ---------
--------------   ---------
```

5. 랙에서 아카이브 계층 엔클로저를 제거합니다.

대상 시스템에서 DD Cloud Tier 구성

DD Cloud Tier는 DD OS 6.0 이상이 필요하며 특정 Data Domain 시스템 모델에서만 지원됩니다. 지원 플랫폼(468페이지)에서는 DD Cloud Tier를 지원하는 모델 목록을 제공

합니다. DD Cloud Tier 및 아카이브 계층 스토리지는 동일한 Data Domain 시스템에서 동시에 구성할 수 없습니다.

절차

1. 활성 계층과 클라우드 계층 모두에 대해 스토리지를 구성합니다. 사전 요구 사항으로, 활성 계층과 클라우드 계층 모두에 대해 적절한 용량 라이선스를 설치해야 합니다.

   a. CLOUDTIER-CAPACITY 및 CAPACITY-ACTIVE 기능에 대한 라이선스가 설치되어 있는지 확인합니다. ELMS 라이선스를 확인하려면 다음을 수행합니다.

   ```
   # elicense show
   ```

   라이선스가 설치되어 있지 않다면 `elicense update` 명령을 사용하여 라이선스를 설치합니다. 명령을 입력하고 이 프롬프트 다음에 라이선스 파일의 내용을 붙여 넣으십시오. 붙여 넣은 다음 캐리지 리턴이 있는지 확인하고 **Control-D**를 눌러 저장합니다. 라이선스를 교체할지 묻는 메시지가 나타납니다. yes로 답하면 라이선스가 적용되고 표시됩니다.

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

   b. 사용 가능한 스토리지를 표시합니다.

   ```
   # storage show all# disk show state
   ```

   c. 활성 계층에 스토리지를 추가합니다.

   ```
   # storage add enclosures <enclosure no> tier active
   ```

   d. 클라우드 계층에 스토리지를 추가합니다.

   ```
   # storage add enclosures <enclosure no> tier cloud
   ```

2. 인증서를 설치합니다.

   클라우드 프로파일을 생성하려면 먼저 연결된 인증서를 설치해야 합니다. 자세한 내용은 인증서 가져오기(574페이지) 섹션을 참조하십시오.

   AWS, Virtustream 및 Azure 퍼블릭 클라우드 공급업체의 경우 https://www.digicert.com/digicert-root-certificates.htm에서 루트 CA 인증서를 다운로드할 수 있습니다.

   - AWS 또는 Azure 클라우드 공급업체의 경우 Baltimore CyberTrust Root 인증서를 다운로드합니다.
   - Alibaba의 경우 https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates에서 GlobalSign 루트 R1 인증서를 다운로드합니다.
   - Virtustream 클라우드 공급업체의 경우 DigiCert High Assurance EV Root CA 인증서를 다운로드합니다.
   - ECS의 경우 루트 인증 기관이 고객마다 다릅니다. 자세한 내용은 로드 밸런싱 장치 공급업체에 문의하십시오.

   다운로드한 인증서 파일은 확장자가 .crt입니다. 파일이 설치된 Linux 또는 Unix 시스템에서 openssl을 사용하여 파일을 .crt 형식에서 .pem 형식으로 변환합니다.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press
Control-C to cancel.
```

3. 클라우드로 데이터를 이동할 수 있도록 Data Domain 시스템을 구성하려면 먼저 "클라우드" 기능을 활성화하고 시스템 암호가 아직 설정되지 않은 경우 이를 설정해야 합니다.

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. 클라우드 공급업체 자격 증명을 사용하여 클라우드 프로파일을 구성합니다. 프롬프트와 변수는 공급업체마다 다릅니다.

```
# cloud profile add <profilename>
```

참고

보안상의 이유로 이 명령은 사용자가 입력하는 액세스/비밀 키를 표시하지 않습니다.

공급업체를 선택합니다.

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud를 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 리전이 필요합니다.
- AWS S3을 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 리전이 필요합니다.
- Azure에는 계정 이름, 계정이 Azure Government 계정인지 여부, 기본 키, 보조 키 및 스토리지 클래스가 필요합니다.
- ECS를 사용하려면 액세스 키, 암호 키 및 엔드포인트를 입력해야 합니다.
- Google Cloud Platform에는 액세스 키, 암호 키 및 리전이 필요합니다. (스토리지 클래스는 Nearline입니다.)
- S3 Flexible 공급업체에는 공급업체 이름, 액세스 키, 암호 키, 영역, 엔드포인트 및 스토리지 클래스가 필요합니다.
- Virtustream을 사용하려면 액세스 키, 암호 키, 스토리지 클래스 및 지역이 필요합니다.

각 프로파일을 추가할 때마다 프록시를 설정할지 묻는 메시지가 나타납니다. 프록시를 설정하려면 *프록시 호스트 이름*, *프록시 포트*, *프록시 사용자 이름* 및 *프록시 암호* 값이 필요합니다.

5. 클라우드 프로파일 구성을 확인합니다.

```
# cloud profile show
```

6. 아직 생성되지 않은 경우 활성 계층 파일 시스템을 생성합니다.

```
# filesys create
```

7. 파일 시스템을 활성화합니다.

```
# filesys enable
```

8. 클라우드 유닛을 구성합니다.

```
# cloud unit add unitname profile profilename
```

`cloud unit list` 명령을 사용하여 클라우드 유닛을 나열합니다.

9. 필요에 따라 클라우드 유닛에 대한 암호화를 구성합니다.
   a. ENCRYPTION 라이선스가 설치되어 있는지 확인합니다.

```
# elicense show
```

   b. 클라우드 유닛에 대한 암호화를 활성화합니다.

```
# filesys encryption enable cloud-unit unitname
```

   c. 암호화 상태를 확인합니다.

```
# filesys encryption status
```

10. 하나 이상의 MTree를 생성합니다.

```
# mtree create /data/col1/mt11
```

11. DD Cloud Tier 구성을 확인합니다.

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
```

```
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. 이 MTree에 대한 파일 마이그레이션 정책을 구성합니다. 이 명령에 여러 MTree를 지정할 수 있습니다. 정책은 사용 기간 임계값 또는 범위에 기반할 수 있습니다.

    a. 사용 기간 임계값을 구성하려면(지정된 사용 기간보다 오래된 파일을 클라우드로 마이그레이션하려면) 다음을 수행합니다.

    ```
    # data-movement policy set age-threshold age_in_days to-tier cloud cloud-unit unitname mtrees mtreename
    ```

    b. 사용 기간 범위를 구성하려면(지정된 사용 기간 범위에 속하는 파일만 마이그레이션하려면) 다음을 수행합니다.

    ```
    # data-movement policy set age-range min-age age_in_days max-age age_in_days to-tier cloud cloud-unit unitname mtrees mtreename
    ```

13. 파일 시스템을 내보내고 클라이언트에서 파일 시스템을 마운트하고 활성 계층에 데이터를 수집합니다. 데이터 마이그레이션 대상이 될 수 있도록 수집된 파일의 수정 날짜를 변경합니다. (날짜를 데이터 이동 정책을 구성할 때 지정한 사용 기간 임계값보다 오래된 날짜로 설정합니다.)
14. 사용 기간이 지난 파일의 마이그레이션을 시작합니다. 이전과 마찬가지로, 이 명령에 여러 MTree를 지정할 수 있습니다.

    ```
    # data-movement start mtrees mtreename
    ```

    데이터 이동의 상태를 확인합니다.

    ```
    # data-movement status
    ```

    데이터 이동의 진행 상황을 확인할 수도 있습니다.

    ```
    # data-movement watch
    ```

15. 파일 마이그레이션이 처리되었으며 이제 모든 파일이 클라우드 계층에 있는지 확인합니다.

    ```
    # filesys report generate file-location path all
    ```

16. 파일을 클라우드 계층으로 마이그레이션한 후에는 파일에서 직접 읽을 수 없습니다(시도 시 오류가 발생 함). 먼저 파일을 활성 계층으로 리콜해야 합니다. 파일을 활성 계층으로 리콜하려면 다음을 수행합니다.

    ```
    # data-movement recall path pathname
    ```

20장

DD Retention Lock

이 장에는 다음과 같은 내용이 포함됩니다.

DD Retention Lock 개요

DD Retention Lock으로 활성화된 MTree에서 데이터가 잠겨 있을 때, DD Retention Lock은 데이터 무결성 유지에 도움이 됩니다. 즉, 잠긴 데이터는 사용자가 최대 70년까지 정의한 보존 기간 동안 덮어쓰기, 수정 또는 삭제가 불가능합니다.

다음과 같이 두 가지 DD Retention Lock 버전이 있습니다.

- *Data Domain Retention Lock Governance Edition*은 DD OS 5.2 이전 Data Domain Retention Lock의 기능을 유지하고 있습니다. Data Domain Retention Lock Governance를 사용하면 특정 기간 동안 유지할 데이터에 대한 보존 정책을 정의하여 시스템 관리자가 구현한 내부 IT 거버넌스 정책을 준수할 수 있습니다.
- *Data Domain Retention Lock Compliance Edition*을 사용하면 SEC 17a-4(f)의 표준과 같은 규정 표준의 가장 엄격한 데이터 영속성 요구 사항을 충족시킬 수 있습니다. 규정 표준의 전체 목록에는 다음이 포함됩니다.
  - CFTC 규칙 1.31b
  - FDA 21 CFR Part 11
  - SOX(Sarbanes-Oxley Act)
  - IRS 98025 및 97-22
  - ISO 표준 15489-1
  - MoREQ2010

  인증 정보는 다음 웹 사이트에서 *Compliance Assessments - Summary and Conclusions – EMC Data Domain Retention Lock Compliance Edition*을 참조하십시오.

  https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

  (로그인이 필요합니다.)

  이런 표준을 준수해야 보존 기간이 만료되기 전에 Data Domain Retention Lock Compliance Edition 소프트웨어를 사용하여 Data Domain 시스템에서 잠긴 파일을 변경하거나 제거하지 못하게 할 수 있습니다. Data Domain Retention Lock Compliance Edition에서는 정책 구현을 위한 보안 책임자가 필요합니다. 감사 로그 파일에는 관리자나 보안 책임자가 액세스할 수 있습니다.

각 버전마다 별개의 추가 라이센스가 필요하고, 단일 Data Domain 시스템에서 둘 중 하나 또는 둘 다 사용할 수 있습니다.

Retention Lock 프로토콜은 DD Retention Lock Governance와 Compliance Edition에서 모두 똑같습니다. 사용상의 차이점은 DD Retention Lock Compliance Edition에 대한 시스템 동작에서 비롯되는데, 이 시스템에서는 규정 준수 요구 사항을 충족시키기 위해 엄격한 제한을 두기 때문입니다. 개요를 보려면 다음 웹 사이트에서 *EMC Data Domain Retention Lock Software – A Detailed Review*(백서)를 참조하십시오.

https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf

(로그인이 필요합니다.)

DD Retention Lock Governance Edition에는 보안 책임자가 필요하지 않고 Data Domain 시스템에서 아카이브 데이터 보존 시 더욱 높은 수준의 유연성이 제공됩니다.

아카이브 규정 준수 스토리지 요구 사항을 충족시키기 위해, SEC 규칙에 따라 원본과 같은 보존 요구 사항으로 Retention Lock이 설정된 데이터의 복제본을 따로 저장해야 합니다. DD Replicator를 사용하여 Retention Lock이 설정된 파일을 또 다른 Data Domain 시스템으로 복제할 수 있습니다. Retention Lock이 설정된 파일이 복제되는 경

우 소스 파일과 같은 보호 수준으로 대상 시스템에서 Retention Lock 상태로 보존됩니다.

DD Retention Lock Governance Edition은 On-Premise, 클라우드 기반 및 DD3300 DD VE 인스턴스에서 지원됩니다. DD Retention Lock Compliance Edition은 On-Premise, 클라우드 기반 또는 DD3300 DD VE 인스턴스에서 지원되지 않습니다.

다음에 나오는 항목에서는 DD Retention Lock에 대한 추가 정보를 제공합니다.

DD Retention Lock 프로토콜

Data Domain 시스템에서는 Retention Lock이 설정된 파일이 되도록 명시적으로 커밋된 파일만 Retention Lock됩니다. 파일은 DD Retention Lock Governance 또는 Compliance가 해당 파일을 포함한 MTree에서 설정되어 있는 동안 실행된 클라이언트 측 파일 명령을 통해 Retention Lock이 설정된 파일이 되도록 커밋됩니다.

참고

Linux, Unix 및 Windows 클라이언트 환경이 지원됩니다.

DD Retention Lock Governance 또는 Compliance가 해당 파일을 포함한 MTree에서 설정되어 있지만 보존되도록 커밋되지 않은 공유 또는 내보내기에 기록된 파일은 언제든 수정하거나 삭제할 수 있습니다.

Retention Lock을 사용하면 클라이언트 측 *atime* update 명령으로 지정된 보존 기간 중에는 CIFS 공유 또는 NFS 내보내기에서 직접 보존 대상 파일을 수정하거나 삭제하지 못하게 됩니다. 적절히 구성된 경우 몇몇 아카이브 애플리케이션과 백업 애플리케이션에서 이 명령을 실행할 수 있습니다. 이 명령을 실행하지 않는 애플리케이션이나 유틸리티는 DD Retention Lock을 사용하여 파일을 잠글 수 없습니다.

Retention Lock이 설정된 파일은 Retention Lock이 이후에 해제되거나 Retention Lock 라이센스가 더 이상 유효하지 않더라도 수정 및 조기 삭제로부터 항상 보호됩니다.

Retention Lock이 설정된 MTree 내에 있는 비어 있지 않은 폴더나 디렉토리를 삭제하거나 그 이름을 바꿀 수 없습니다. 하지만 빈 폴더나 디렉토리는 이름을 바꾸거나 삭제하고 새 폴더나 디렉토리를 생성할 수 있습니다.

파일의 *atime*을 업데이트하여 Retention Lock이 설정된 파일의 보존 기간을 연장할 수는 있지만 단축할 수는 없습니다.

DD Retention Lock Governance와 Compliance 모두, 일단 파일의 보존 기간이 만료되고 나면 클라이언트 측 명령, 스크립트 또는 애플리케이션을 사용하여 파일을 삭제할 수 있습니다. 하지만 파일의 보존 기간이 만료된 후에도 파일을 수정할 수 없습니다. Data Domain 시스템에서는 파일의 보존 기간 만료 시 해당 파일이 자동으로 삭제되지 않습니다.

DD Retention Lock 흐름

DD Retention Lock을 사용한 작업의 일반적인 흐름은 다음과 같습니다.

1. DD System Manager 또는 시스템 콘솔에서 실행한 DD OS 명령을 사용하여 DD Retention Lock Governance 또는 Compliance Retention Lock을 위한 MTree를 설정합니다.
2. 적절하게 구성된 아카이빙 또는 백업 애플리케이션에서 수동으로 실행되거나 스크립트를 통해 실행되는 클라이언트 측 명령을 사용하여 Data Domain 시스템에서 Retention Lock이 설정되도록 파일을 커밋합니다.

참고

Windows 클라이언트는 DD OS 호환성을 위한 유틸리티 프로그램을 다운로드해야 할 수도 있습니다.

3. 선택적으로, 클라이언트 측 명령을 사용하여 파일 보존 시간을 연장합니다.
4. 선택적으로, 클라이언트 측 명령을 사용하여 보존 기간이 만료된 파일을 삭제합니다.

지원되는 데이터 액세스 프로토콜

DD Retention Lock은 산업 표준 NAS 기반 WORM(Write Once Read Many) 프로토콜과 호환되고, 통합은 Symantec Enterprise Vault, SourceOne, Cloud Tiering Appliance, 또는 DiskXtender 등의 아카이브 애플리케이션으로 정규화됩니다. CommVault와 같은 백업 애플리케이션을 사용하는 고객은 Data Domain Retention Lock을 사용하기 위한 사용자 지정 스크립트를 개발할 수도 있습니다.

DD Retention Lock의 프로토콜 지원은 다음과 같습니다.

- NFS는 DD Retention Lock Governance 및 Compliance에서 모두 지원됩니다.
- CIFS는 DD Retention Lock Governance 및 Compliance에서 모두 지원됩니다.
- DD VTL은 DD Retention Lock Governance에서는 지원되지만 DD Retention Lock Compliance에서는 지원되지 않습니다.
  가상 테이프(여기서는 *테이프*라 지칭함)가 파일 시스템에서는 파일로 표시됩니다.
  - 파일 시스템상의 디렉토리로 매핑하는 테이프 컬렉션인 스토리지 풀을 생성할 때, (이전 버전과의 호환성을 위해) 이전 스타일의 디렉토리 풀을 생성하기로 특별히 선택하지 않은 경우에는 MTree를 생성하는 것입니다. DD OS 5.3 이전에 생성된 스토리지 풀을 MTree로 변환할 수도 있습니다. 이런 MTree는 Retention Lock이 설정되고 복제될 수 있습니다.
  - *Data Domain Operating System 명령 참조 가이드*에 설명되어 있는 `vtl tape modify` 명령을 사용하여 하나 이상의 테이프를 Retention Lock이 가능합니다. `mtree retention-lock revert`***path*** 명령을 사용하면 `vtl tape modify` 명령으로 잠긴 테이프의 Retention Lock 상태를 되돌릴 수 있습니다. 테이프 잠금을 푼 후에는 테이프를 업데이트할 수 있습니다. DD VTL 서비스가 비활성화된 후 다시 활성화될 때까지는 DD System Manager 또는 CLI를 통해 잠금이 풀린 상태를 볼 수 없습니다. 그러나 잠금이 풀린 테이프에는 업데이트가 적용됩니다. 이 기능은 DD Retention Lock Governance Edition 전용입니다.
  - `time-display retention` 인수와 `vtl tape show` 명령을 사용하여 테이프의 보존 시간을 표시할 수 있습니다.
  - DD System Manager를 사용하여 개별 테이프의 Retention Lock이 가능합니다.
- DD Boost는 DD Retention Lock Governance 및 Compliance에서 모두 지원됩니다.
  백업 파일 또는 백업 이미지의 Retention Lock에 클라이언트 측 스크립트가 사용되고 DD Boost를 통해 시스템에서 백업 애플리케이션(예: Veritas NetBackup)도 사용되는 경우, 백업 애플리케이션이 클라이언트 측 스크립트의 컨텍스트를 공유하지 않을 수 있다는 점에 유의하십시오. 따라서 백업 애플리케이션에서 클라이언트 측 스크립트를 통해 Retention Lock이 설정된 파일을 만료시키거나 삭제하려고 할 때, Data Domain 시스템에서 공간이 확보되지 않습니다.

  관리자는 보존 기간 정책을 Retention Lock 시간에 맞춰 변경하는 것이 좋습니다. 이는 Veritas NetBackup, Veritas Backup Exec, NetWorker를 비롯한 DD Boost와 통합되는 대다수 백업 애플리케이션에 적용됩니다.

DSP 모드에서 DD Boost 파일로 데이터를 수집하는 동안 RL(Retention Lock)을 설정할 수 없으며 RL을 설정한 클라이언트에서 오류가 수신됩니다. Retention Lock은 데이터 수집이 완료된 후에 설정해야 합니다.

데이터를 OST 모드에서 DD Boost 파일로 수집하거나 NFS 파일로 수집하는 동안 RL(Retention Lock)을 설정할 수 없으며 RL이 설정되는 즉시 해당 데이터를 쓰는 클라이언트에서 오류가 수신됩니다. RL을 설정하기 전에 쓴 부분 파일은 웜(worm) 파일로 설정되고 디스크에 커밋됩니다.

MTree에서 DD Retention Lock 활성화

DD Retention Lock Governance 또는 Compliance 활성화 MTree 내의 파일만 Retention Lock을 활성화할 수 있습니다.

DD Retention Lock Compliance에 대해 활성화된 MTree는 DD Retention Lock Governance MTree로 변환할 수 없으며, 그 반대의 경우도 마찬가지입니다.

다음에 나오는 절차는 DD Retention Lock Governance 또는 DD Retention Lock Compliance에 대해 MTree를 활성화하는 방법을 보여 줍니다.

MTree에서 DD Retention Lock Governance 활성화

DD Retention Lock Governance 라이센스를 시스템에 추가한 다음, 하나 이상의 MTree에서 DD Retention Lock Governance를 활성화합니다.

절차

1. DD Retention Lock Governance 라이센스가 Feature Licenses 아래에 나열되지 않을 경우 해당 라이센스를 추가합니다.
   a. **Administration** > **Licenses**를 선택합니다.
   b. Licenses 영역에서 **Add Licenses**를 클릭합니다.
   c. License Key 입력란에 라이센스 키를 입력합니다.

   참고

   라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함합니다.

   d. **Add**를 클릭합니다.
2. Retention Lock을 위한 MTree를 선택합니다.
   a. **Data Management** > **MTree**를 선택합니다.
   b. Retention Lock에 사용할 MTree를 선택합니다. 빈 MTree를 생성한 이후에 파일을 추가할 수도 있습니다.
3. 선택한 MTree에 대한 정보를 표시하려면 MTree Summary 탭을 클릭합니다.
4. Retention Lock 영역까지 아래로 스크롤하고 Retention Lock 오른쪽에서 **Edit**를 클릭합니다.
5. MTree에서 DD Retention Lock Governance를 활성화하고 필요한 경우 MTree에 대한 기본 최소 및 최대 Retention Lock 기간을 변경합니다.

   Modify Retention Lock 대화 상자에서 다음 작업을 수행합니다.

   a. **Enable**을 선택하여 MTree에서 DD Retention Lock Governance를 활성화합니다.

b. MTree에 대한 최소 및 최대 보존 기간을 변경하려면 최소 또는 최대 기간을 수정합니다.

입력란에 간격을 나타내는 숫자를 입력합니다(예: 5 또는 14).

드롭다운 목록에서 간격(분, 시간, 일, 년)을 선택합니다.

참고

최소 보존 기간을 12시간 미만으로 지정하거나 최대 보존 기간을 70년 이상으로 지정하면 오류가 발생합니다.

c. **OK**를 클릭하여 설정을 저장합니다.

Modify Retention Lock 대화 상자를 닫고 나면 Retention Lock 영역에 업데이트된 MTree 정보가 표시됩니다.

6. MTree의 Retention Lock 정보를 확인합니다.

다음의 Retention Lock 필드를 확인합니다.

- 상단:
  - Status 필드는 MTree에 대한 읽기/쓰기 액세스, MTree에서의 Retention Lock 유형, Retention Lock 활성화 또는 비활성화 여부를 나타냅니다.
- 하단:
  - Status 필드는 MTree에 대한 Retention Lock 활성화 여부를 나타냅니다.
  - Retention Period 필드는 MTree에 대한 최소 및 최대 보존 기간을 나타냅니다. MTree에 있는 파일에 대해 지정된 보존 기간은 최소 보존 기간보다 길거나 같고 최대 보존 기간보다 짧거나 같아야 합니다.
  - UUID 필드는 MTree용으로 생성되는 고유 식별 번호입니다.

참고

임의의 MTree에 대한 Retention Lock 구성 설정을 확인하려면 탐색 패널에서 MTree를 선택한 다음 Summary 탭을 클릭합니다.

사후 요구 사항

Retention Lock이 활성화된 MTree에서 파일을 Retention Lock합니다.

MTree에서 DD Retention Lock Compliance 설정

시스템에 DD Retention Lock Compliance 라이센스를 추가하고, 시스템 관리자와 한 명 이상의 보안 책임자를 설정하고, DD Retention Lock Compliance 소프트웨어를 사용하도록 시스템을 구성 및 설정한 후에 하나 이상의 MTree에서 DD Retention Lock Compliance를 설정할 수 있습니다.

절차

1. 시스템에 DD Retention Lock Compliance 라이센스가 없는 경우 추가합니다.

a. 먼저 라이센스가 이미 설치되어 있는지 확인합니다.

```
license show
```

b. RETENTION-LOCK-COMPLIANCE 기능이 표시되지 않으면 라이센스를 설치합니다.

```
license add license-key
```

참고

라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함시킵니다.

2. RBAC(Role-Base Access Control) 규칙에 따라 하나 이상의 보안 책임자 사용자 계정을 설정합니다.
   a. System Administrator 역할에 보안 책임자 계정을 추가합니다.
      ```
      user add user role security
      ```
   b. 보안 책임자 인증을 설정합니다.
      ```
      authorization policy set security-officer enabled
      ```
3. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 설정합니다.

   참고

   DD Retention Lock Compliance를 설정하면 문제 해결 중에 사용되는 시스템 기능에 대한 낮은 레벨 액세스에 여러 가지 제한 사항을 적용합니다. 한 번 설정된 이후 DD Retention Lock Compliance를 해제하는 유일한 방법은 시스템을 초기화하고 다시 로드하는 것입니다. 이렇게 할 경우 시스템에 있는 모든 데이터가 제거됩니다.

   a. DD Retention Lock Compliance를 사용하도록 시스템을 구성합니다.
      ```
      system retention-lock compliance configure
      ```
      시스템이 자동으로 재부팅됩니다.
   b. 재시작 프로세스가 완료된 후에 시스템에서 DD Retention Lock Compliance를 설정합니다.
      ```
      system retention-lock compliance enable
      ```
4. Retention Lock이 설정된 파일을 포함할 MTree에서 Compliance를 설정합니다.
   ```
   mtree retention-lock enable mode compliance mtree mtree-path
   ```

   참고

   /backup 또는 풀 MTree에서는 Compliance를 설정할 수 없습니다.

5. Compliance 설정 MTree에 대해 기본 최소 및 최대 Retention Lock 기간을 변경하려면 보안 책임자 인증을 통해 다음 명령을 입력합니다.
   ```
   mtree retention-lock set min-retention-period period mtree mtree-path
   mtree retention-lock set max-retention-period period mtree mtree-path
   ```

   참고

   보존 *period*는 [숫자] [단위] 형식으로 지정됩니다. 예: 1 min, 1 hr, 1 day, 1 mo 또는 1 year. 최소 보존 기간을 12시간 미만으로 지정하거나 최대 보존 기간을 70년 이상으로 지정하면 오류가 발생합니다.

   4~5단계를 반복해 추가 MTree를 설정합니다.

사후 요구 사항

Retention Lock 파일은 Retention Lock을 지원하는 MTree에 상주합니다.

클라이언트 측 Retention Lock File Control

이 섹션에서는 Data Domain 시스템에 저장된 파일을 잠그기 위한 DD Retention Lock 클라이언트 명령 인터페이스를 설명합니다. 클라이언트 명령은 DD Retention Lock Governance와 Compliance에서 동일합니다. Linux, Unix 및 Windows 클라이언트 환경이 지원되지만 Windows 클라이언트의 경우 명령을 사용해 파일을 잠그기 위한 유틸리티를 다운로드해야 할 수도 있습니다.

참고

애플리케이션이 이미 업계 표준 WORM을 지원하는 경우 DD Retention Lock Governance 또는 Compliance 활성화 MTree에 WORM 파일을 기록하면 Data Domain 시스템에 있는 파일이 잠깁니다. 애플리케이션의 보존 시간이 DD Retention Lock 설정과 일치해야 합니다. 이 섹션에 설명된 명령을 사용하지 않아도 됩니다. 애플리케이션이 DD Retention Lock용으로 테스트되고 인증을 받았는지 확인하려면 *Data Domain Archive Application Compatibility Guide*를 참조하십시오.

참고

NFS를 사용하지만 기존 OS를 실행하는 일부 클라이언트 머신에서는 보존 시간을 2038년 이후로 설정할 수 없습니다. NFS 프로토콜에는 2038년이라는 제한이 적용되지 않으며 2106년까지 시간을 지정할 수 있습니다. 또한 DD OS에도 2038년이라는 제한이 적용되지 않습니다.

클라이언트 측 명령은 개별 파일의 Retention Lock을 관리하는 데 사용됩니다. 이 명령은 모든 Retention Lock 설정이 가능한 Data Domain 시스템에 적용되며 Data Domain 시스템에서 DD Retention Lock의 설정 및 구성에 추가되어 실행해야 합니다.

Windows 클라이언트에 필요한 툴

Windows 기반 클라이언트에서 Retention Lock을 수행하려면 `touch.exe` 명령이 필요합니다.

이 명령을 가져오려면 Windows 버전에 따라 Linux/Unix 기반 애플리케이션을 위한 유틸리티를 다운로드하고 설치하십시오. 이러한 유틸리티는 Data Domain의 권장 사항이며 고객 환경에 맞게 사용해야 합니다.

- Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 및 Windows Server XP의 경우:
  http://sourceforge.net/projects/unxutils/files/latest
- Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise 64비트 Edition, Windows Vista SP1, Windows Vista Ultimate 및 Windows Vista Ultimate 64비트 Edition의 경우:
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754
- Windows Server 2003 SP1 및 Windows Server 2003 R2의 경우:
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983

참고

Windows용 `touch` 명령의 경우 이 장의 Linux 예제와 형식이 다를 수 있습니다.

제공된 설치 지침을 따르고 클라이언트 시스템에서 필요에 따라 검색 경로를 설정합니다.

Data Domain 시스템 파일에 대한 클라이언트 액세스

DD Retention Lock Governance 또는 Compliance용 MTree 활성화 이후에는 다음을 수행할 수 있습니다.

- MTree를 기반으로 CIFS 공유를 생성합니다. 이 CIFS 공유는 클라이언트 시스템에서 사용할 수 있습니다.
- MTree에 대한 NFS 마운트를 생성하고 클라이언트 시스템의 NFS 마운트 지점에서 해당 파일에 액세스합니다.

참고

이 섹션에 나열된 명령은 클라이언트에서만 사용해야 합니다. DD System Manager 또는 CLI를 통해서는 실행할 수 없습니다. 명령 구문은 사용 중인 유틸리티에 따라 약간 다를 수 있습니다.

다음에 나오는 항목에서는 클라이언트 측 Retention Lock File Control을 관리하는 방법을 설명합니다.

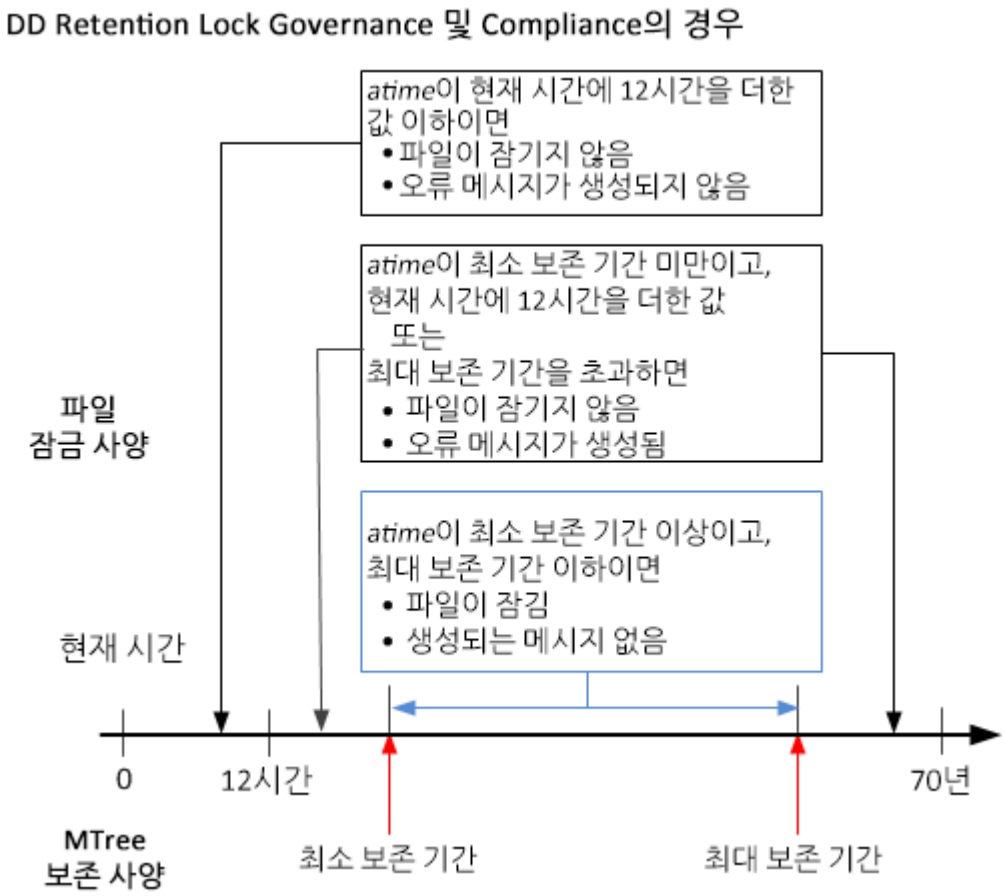
파일에서 Retention Lock 설정

파일에 Retention Lock을 수행하려면 파일의 마지막 액세스 시간(*atime*)을 원하는 파일의 보존시간(파일을 삭제할 수 있는 시간)으로 변경합니다.

이 작업은 보통 아카이브 애플리케이션을 사용하여 수행하며, 현재 Data Domain 시스템에서 자격이 입증된 모든 아카이브 애플리케이션(*Data Domain Archive Application Compatibility Guide*에 의거)은 여기에 요약된 기본 잠금 프로토콜을 따릅니다.

나중에 지정하는 *atime*은 다음 그림에서와 같이 파일의 MTree(현재 시간에서 오프셋으로) 최소 및 최대 보존 기간을 준수해야 합니다.

그림 23 파일의 Retention Lock을 위한 Valid 및 Invalid *atime*



참고

NFS를 사용하지만 기존 OS를 실행하는 일부 클라이언트 머신에서는 보존 시간을 2038년 이후로 설정할 수 없습니다. NFS 프로토콜에는 2038년이라는 제한이 적용되지 않으며 2106년까지 시간을 지정할 수 있습니다. 또한 DD OS에도 2038년이라는 제한이 적용되지 않습니다.

오류는 사용 권한 거부 오류입니다(표준 POSIX 오류인 EACCESS라고 함). 이 오류는 스크립트 또는 아카이브 애플리케이션에 반환되어 *atime*을 설정합니다.

참고

Retention Lock 설정 파일에 파일을 커밋하기 전에 Data Domain 시스템에 완전하게 기록해야 합니다.

다음 명령은 *atime*을 설정하기 위해 클라이언트에서 사용할 수 있습니다.

```
touch -a -t [atime] [filename]
```

*atime*의 형식은 다음과 같습니다.

```
[[YY]YY] MMDDhhmm[.ss]
```

예를 들어 현재 날짜와 시간이 2012년 1월 18일 오후 1시(즉, 201201181300)이고 최소 보존 기간이 12시간이라고 가정할 때, 해당 날짜와 시간에 12시간이라는 최소 보존 기간을 추가하면 값이 201201190100이 됩니다. 따라서 파일의 *atime*을 201201190100보다 큰 값으로 설정하면 파일에 Retention Lock이 설정됩니다.

다음 명령을 실행합니다.

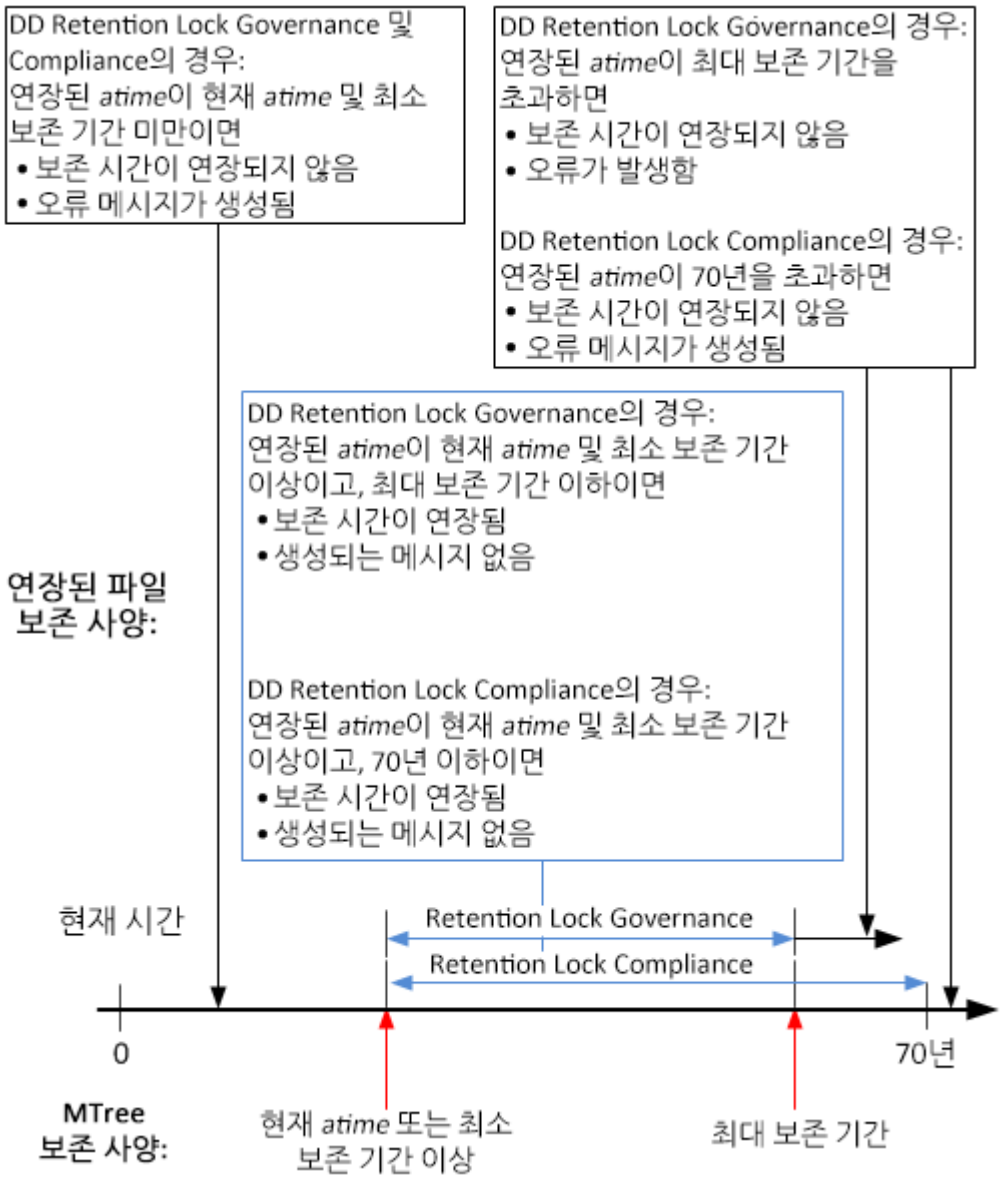
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

그러면 `SavedData.dat` 파일이 2014년 12월 31일 오후 10시 30분까지 잠깁니다.

파일에서 Retention Lock 연장

Retention Lock이 설정된 파일의 보존 시간을 연장하려면 다음 그림에서와 같이 파일의 *atime*을 파일의 현재 *atime*보다 크지만 파일의 MTree 최대 보존 기간보다 작게(현재 시간에서 오프셋으로) 설정합니다.

그림 24 파일에서 Retention Lock을 연장할 때 유효하고 유효하지 않은 *atimes*



예를 들어 다음 명령을 사용하여 *atime*을 `201412312230`에서 `202012121230`으로 변경하면,

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

2020년 12월 12일 오후 12시 30분까지 파일이 잠깁니다.

참고

NFS를 사용하지만 아주 오래된 OS를 실행하는 일부 클라이언트 머신에서는 보존 시간을 2038년 이후로 설정할 수 없습니다. NFS 프로토콜에는 2038년이라는 제한이 적용되지 않으며 2106년까지 시간을 지정할 수 있습니다. 또한 DD OS에도 2038년이라는 제한이 적용되지 않습니다.

오류는 사용 권한 거부 오류입니다(표준 POSIX 오류인 EACCESS라고 함). 이 오류는 *atime*을 설정하는 스크립트 또는 아카이브 애플리케이션에 반환됩니다.

Retention Lock 설정 파일 식별

Retention Lock 설정 파일의 *atime* 값은 파일의 보존 시간입니다. 파일에 Retention Lock이 설정되어 있는지 확인하려면 파일의 *atime*을 현재 *atime* 이전의 값으로 설정합니다. 이렇게 하면 파일이 Retention Lock 설정 파일인 경우에만 사용 권한 오류와 함께 작업이 실패합니다.

먼저 현재 *atime* 값을 나열한 후 다음 명령을 사용해 이전 *atime*으로 `touch` 명령을 실행합니다.

```
ls -l --time=atime [filename]
touch -a -t [atime] [filename]
```

다음 예는 명령 시퀀스를 보여 줍니다.

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

`SavedData.dat`의 *atime*이 202012121230(2020년 12월 12일 오후 12시 30분)이고 `touch` 명령이 그 이전의 *atime*(202012111230(2020년 12월 11일 오후 12시 30분))을 지정할 경우 `touch` 명령은 실패하는데, 이는 `SavedData.dat`에 Retention Lock이 설정되었다는 뜻입니다.

참고

`--time=atime` 옵션은 모든 Unix 버전에서 지원되지 않습니다.

디렉토리 지정 및 파일에 대한 touch 명령 사용

명령줄을 사용해 액세스 시간을 변경할 파일을 포함하는 루트 디렉토리를 생성합니다.

이 루틴에서 *root directory to start from*에는 다음 클라이언트 시스템 명령을 사용해 액세스 시간을 변경하려는 파일이 포함되어 있습니다.

```
find [root directory to start from] -exec touch -a -t
[expiration time] {} \;
```

예를 들면 다음과 같습니다.

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

파일 목록 읽기 및 touch 명령 사용

이 루틴에서 *name of file list*는 액세스 시간을 변경하려는 파일의 이름을 포함한 텍스트 파일의 이름입니다. 각 줄에는 한 파일의 이름이 포함됩니다.

다음은 클라이언트 시스템 명령 구문입니다.

```
touch -a -t [expiration time] 'cat [name of file list]'
```

예를 들면 다음과 같습니다.

```
ClientOS# touch -a -t 202012121230 'cat /backup/data1/filelist.txt'
```

파일 삭제 또는 만료

클라이언트 애플리케이션을 사용해 만료된 Retention Lock으로 파일을 삭제 또는 만료하거나 표준 file-delete 명령을 사용해 파일을 삭제합니다.

애플리케이션을 사용해 파일을 만료하면 파일에서 애플리케이션에 액세스할 수 없습니다. 만료 작업을 통해 Data Domain 시스템에서 파일이 실제로 제거되거나 제거되지 않을 수 있습니다. 제거되지 않은 경우 애플리케이션에서 별도의 삭제 작업을 제공합니다. DD Retention Lock과 별개로 파일을 삭제할 수 있는 적절한 액세스 권한이 있어야 합니다.

참고

Retention Lock 설정 파일의 보존 기간이 만료되지 않은 경우 삭제 작업을 수행하면 사용 권한 거부 오류가 발생합니다.

Privileged delete

DD Retention Lock Governance에 한해 다음의 2단계 프로세스를 사용하여 Retention Lock이 설정된 파일을 삭제할 수 있습니다.

절차

1. `mtree retention-lock revert`*path* 명령을 사용하여 Retention Lock이 설정된 파일을 되돌립니다.
2. `rm`*filename* 명령을 사용하여 클라이언트 시스템의 파일을 삭제합니다.

Retention Lock 설정 파일에서 ctime 또는 mtime 사용

*ctime*은 파일의 마지막 메타데이터 변경 시간입니다.

ctime
다음과 같은 이벤트가 발생하면 *ctime*이 현재 시간으로 설정됩니다.

- Retention Lock이 설정되지 않은 파일에 Retention Lock이 설정됩니다.
- Retention Lock 파일의 보존 시간이 연장됩니다.
- Retention Lock 설정 파일이 되돌려집니다.

참고

Retention Lock 설정 파일에 대한 사용자 액세스 사용 권한은 Linux 명령줄 툴 `chmod`를 사용하여 업데이트됩니다.

mtime
*mtime*은 파일의 마지막 수정 시간입니다. 파일의 컨텐츠가 변경될 경우에만 변경됩니다. 따라서 Retention Lock 설정 파일의 mtime은 변경할 수 없습니다.

DD Retention Lock의 시스템 동작

시스템 동작 항목은 다음 섹션에서 DD Retention Lock Governance와 DD Retention Lock Compliance에 대해 따로 설명합니다.

DD Retention Lock Governance

DD Retention Lock Governance를 사용할 경우 특정 DD OS 명령이 다르게 동작합니다. 다음 섹션에서는 각각의 차이에 대해 설명합니다.

복제

컬렉션 복제, MTree 복제 및 디렉토리 복제는 파일의 잠금 또는 잠금 해제 상태를 그대로 복제합니다.

소스에서 Governance Retention Lock이 설정된 파일은 대상에서 Governance Retention Lock이 설정되고 보호 수준도 동일합니다. 복제를 위해서는 소스 시스템에 DD Retention Lock Governance 라이센스가 설치되어 있어야 합니다. 대상 시스템에는 라이센스가 필요 없습니다.

다음의 시스템 사이에서 복제가 지원됩니다.

- 동일한 주요 DD OS 버전을 실행 중인 시스템(예: 두 시스템에서 모두 DD OS 5.5.*x.x* 실행)
- 더 높거나 낮은 쪽으로 연속된 두 주요 릴리즈 내에 있는 DD OS 버전을 실행 중인 시스템(예: 5.3.*x.x* - 5.5.*x.x* 또는 5.5.*x.x* - 5.3.*x.x*). 릴리즈 간 복제는 디렉토리 및 MTree 복제에만 지원됩니다.

참고

DD OS 5.0 이전에서는 MTree 복제가 지원되지 않습니다.

다음 사항을 참고하십시오.

- 컬렉션 복제 및 MTree 복제에서는 MTree에서 구성된 최소 및 최대 보존 기간을 대상 시스템으로 복제합니다.
- 디렉토리 복제에서는 최소 및 최대 복제 기간을 대상 시스템으로 복제하지 않습니다.

컬렉션, MTree 및 디렉토리 복제를 구성하고 사용하기 위한 절차는 DD Retention Lock Governance 라이센스가 없는 Data Domain 시스템에 대한 절차와 같습니다.

복제 재동기화

`replication resync`*destination* 명령은 MTree 또는 디렉토리 복제 컨텍스트가 대상 시스템과 소스 시스템으로 분할될 때 대상을 소스와 동기화하려고 시도합니다. 컬렉션 복제에서는 이 명령을 사용할 수 없습니다. 다음 사항에 주의하십시오.

- 컨텍스트가 분할되기 전에 파일이 클라우드 계층으로 마이그레이션되는 경우 MTree 복제 재동기화가 대상의 모든 데이터를 덮어쓰므로, 파일을 클라우드 계층으로 다시 마이그레이션해야 합니다.
- 대상 디렉토리에는 DD Retention Lock이 활성화되어 있지만 소스 디렉토리에는 DD Retention Lock이 활성화되어 있지 않은 경우에는 디렉토리 복제의 재동기화에 실패합니다.
- Mtree 복제의 경우 소스 MTree에는 Retention Lock이 활성화되어 있지 않지만 대상 MTree에는 Retention Lock이 활성화되어 있으면 재동기화에 실패합니다.
- Mtree 복제의 경우 소스 MTree와 대상 MTree 모두에 Retention Lock이 활성화되어 있지만 Retention Lock 전파 옵션이 FALSE로 설정되어 있으면 재동기화에 실패합니다.

빠른 복제

DD Retention Lock Governance 설정 MTree를 사용하여 시스템에서 `filesys fastcopy [retention-lock] source`*src*`destination`*dest* 명령을 실행할 경우 빠른 복제 작업 중에 보존 잠금 특성이 유지됩니다.

참고

대상 MTree에 보존 잠금이 설정되지 않은 경우 보존 잠금 파일 특성은 유지되지 않습니다.

Filesys destroy

DD Retention Lock Governance가 설정된 MTree가 있는 시스템에서 `filesys destroy`를 실행하면 다음과 같은 결과가 발생합니다.

- Retention Lock이 설정된 데이터를 포함해 모든 데이터가 제거됩니다.
- 모든 `filesys` 옵션이 기본값으로 돌아갑니다. 즉, Retention Lock이 해제되고 새로 생성된 파일 시스템에서 최소 및 최대 보존 기간이 기본값으로 다시 설정됩니다.

참고

시스템에 DD Retention Lock Compliance가 설정된 경우 이 명령이 허용되지 않습니다.

MTree delete

`mtree delete` *mtree-path* 명령이 현재 데이터를 포함하고 있는 DD Retention Lock Governance 설정(또는 이전에 설정됨) MTree를 삭제하려 하면 명령에서 오류가 반환됩니다.

참고

`mtree delete`의 동작은 디렉토리를 삭제하는 명령과 비슷합니다. Retention Lock 설정 MTree(또는 이전에 설정됨)는 MTree가 비어 있을 경우에만 삭제할 수 있습니다.

DD Retention Lock Compliance

특정 DD OS 명령은 DD Retention Lock Compliance를 사용할 때 다르게 동작합니다. 다음 섹션에서는 각각의 차이에 대해 설명합니다.

복제

DD Retention Lock Compliance로 활성화된 MTree는 MTree와 컬렉션 복제를 통해서만 복제할 수 있습니다. 디렉토리 복제는 지원되지 않습니다.

MTree 및 컬렉션 복제는 파일의 잠금 또는 잠금 해제 상태를 그대로 복제합니다. 소스에서 Compliance Retention Lock이 설정된 파일은 대상에서 Compliance Retention Lock이 설정되고 보호 수준도 동일합니다. MTree에서 구성된 최소 및 최대 복제 기간은 대상 시스템으로 복제됩니다.

컬렉션 복제를 수행하려면 대상 시스템으로의 복제를 시작하기 전과 그 후에 소스/복제본 페어의 수명 동안 동일한 보안 책임자 사용자가 소스 및 대상 시스템에 모두 있어야 합니다.

복제 재동기화

MTree 복제에서는 `replication resync`*destination* 명령을 사용할 수 있지만, 컬렉션 복제에서는 사용할 수 없습니다.

- 소스에는 존재하지 않는 Retention Lock이 설정된 파일이 대상 MTree에 있는 경우에는 재동기화에 실패하게 됩니다.
- 소스 및 대상 MTree가 모두 DD Retention Lock Compliance 활성화가 되어 있어야 하며, 그렇지 않으면 재동기화에 실패하게 됩니다.

복제 절차

이 섹션의 항목에서는 DD Retention Lock Compliance에 지원되는 MTree 및 복제 절차를 설명합니다.

참고

다음 항목에서 참조되는 명령에 대한 전체 설명은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

MTree 복제: 일대일 토폴로지

소스 시스템에서 대상 시스템으로 DD Retention Lock Compliance 활성화 MTree를 복제합니다.

시작하기 전에

MTree에서 DD Retention Lock을 활성화하고 클라이언트 측 Retention Lock 파일 제어를 구성한 후 복제합니다.

절차

1. 다른 지시가 있을 때까지 대상 시스템에서만 다음 단계를 수행합니다.
2. 시스템에 DD Retention Lock Compliance 라이센스가 없는 경우 추가합니다.
   a. 먼저 라이센스가 이미 설치되어 있는지 확인합니다.

      ```
      license show
      ```

   b. RETENTION-LOCK-COMPLIANCE 기능이 표시되지 않으면 라이센스를 설치합니다.

      ```
      license add license-key
      ```

      참고

      라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함시킵니다.

3. RBAC(Role-Base Access Control) 규칙에 따라 하나 이상의 보안 책임자 사용자 계정을 설정합니다.
   a. System Administrator 역할에 보안 책임자 계정을 추가합니다.

      ```
      user add userrole security
      ```

   b. 보안 책임자 인증을 설정합니다.

      ```
      authorization policy set security-officer enabled
      ```

4. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 설정합니다.

참고

DD Retention Lock Compliance를 설정하면 문제 해결 중에 사용되는 시스템 기능에 대한 낮은 레벨 액세스에 여러 가지 제한 사항을 적용합니다. 한 번 설정된 이후 DD Retention Lock Compliance를 해제하는 유일한 방법은 시스템을 초기화하고 다시 로드하는 것입니다. 이렇게 할 경우 시스템에 있는 모든 데이터가 제거됩니다.

a. DD Retention Lock Compliance를 사용하도록 시스템을 구성합니다.

```
system retention-lock compliance configure
```

시스템이 자동으로 재부팅됩니다.

b. 재시작 프로세스가 완료된 후에 시스템에서 DD Retention Lock Compliance를 설정합니다.

```
system retention-lock compliance enable
```

5. 복제 컨텍스트를 생성합니다.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

6. 소스 시스템에서만 다음 단계를 수행합니다.
7. 복제 컨텍스트를 생성합니다.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

8. 복제 컨텍스트를 초기화합니다.

```
replication initialize mtree://destination-system-name/
data/col1/mtree-name
```

9. 복제가 완료되었는지 확인합니다.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```

이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.

MTree 복제: 일대다 토폴로지

소스 시스템에서 여러 대상 시스템으로 DD Retention Lock Compliance 활성화 MTree를 복제합니다.

시작하기 전에

복제 전에 MTree에서 DD Retention Lock Compliance를 활성화하고 클라이언트 측 Retention Lock 파일 제어를 구성합니다.

절차

1. 다른 지시가 있을 때까지 대상 시스템에서만 다음 단계를 수행합니다.
2. 시스템에 DD Retention Lock Compliance 라이센스가 없는 경우 추가합니다.
   a. 먼저 라이센스가 이미 설치되어 있는지 확인합니다.

```
license show
```

   b. RETENTION-LOCK-COMPLIANCE 기능이 표시되지 않으면 라이센스를 설치합니다.

```
license add license-key
```

참고

라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함시킵니다.

3. RBAC(Role-Base Access Control) 규칙에 따라 하나 이상의 보안 책임자 사용자 계정을 설정합니다.
   a. System Administrator 역할에 보안 책임자 계정을 추가합니다.

   ```
   user add userrole security
   ```

   b. 보안 책임자 인증을 설정합니다.

   ```
   authorization policy set security-officer enabled
   ```

4. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 설정합니다.

   참고

   DD Retention Lock Compliance를 설정하면 문제 해결 중에 사용되는 시스템 기능에 대한 낮은 레벨 액세스에 여러 가지 제한 사항을 적용합니다. 한 번 설정된 이후 DD Retention Lock Compliance를 해제하는 유일한 방법은 시스템을 초기화하고 다시 로드하는 것입니다. 이렇게 할 경우 시스템에 있는 모든 데이터가 제거됩니다.

   a. DD Retention Lock Compliance를 사용하도록 시스템을 구성합니다.

   ```
   system retention-lock compliance configure
   ```

   시스템이 자동으로 재부팅됩니다.

   b. 재시작 프로세스가 완료된 후에 시스템에서 DD Retention Lock Compliance를 설정합니다.

   ```
   system retention-lock compliance enable
   ```

5. 복제 컨텍스트를 생성합니다.

   ```
   replication add source mtree://source-system-name/data/col1/mtree-namedestination mtree://destination-system-name/data/col1/mtree-name
   ```

6. 소스 시스템에서만 다음 단계를 수행합니다.
7. 각 대상 시스템에 대한 복제 컨텍스트를 생성합니다.

   ```
   replication add source mtree://source-system-name/data/col1/mtree-namedestination mtree://destination-system-name/data/col1/mtree-name
   ```

8. 각 대상 시스템 MTree에 대한 복제 컨텍스트를 초기화합니다.

   ```
   replication initialize mtree://destination-system-name/data/col1/mtree-name
   ```

9. 각 대상 시스템에 대한 복제가 완료되었는지 확인합니다.

   ```
   replication status mtree://destination-system-name/data/col1/mtree-namedetailed
   ```

   이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.

기존 MTree 복제 페어에 DD Retention Lock Compliance 보호 기능 추가

Retention Lock이 활성화되지 않은 기존 MTree 복제 페어에 DD Retention Lock Compliance 보호 기능을 추가합니다.

절차

1. 다른 지시가 있을 때까지 소스 및 대상 시스템에서 다음 단계를 수행합니다.
2. DD System Manager에 로그인합니다.

   DD System Manager 창은 탐색 패널에서 **DD Network**와 함께 나타납니다.
3. Data Domain 시스템을 선택합니다.

   탐색 패널에서 **DD Network**를 확장하여 시스템을 선택합니다.
4. DD Retention Lock Governance 라이센스가 Feature Licenses 아래에 나열되지 않을 경우 해당 라이센스를 추가합니다.

   a. **Administration** > **Licenses**를 선택합니다.

   b. Licenses 영역에서 **Add Licenses**를 클릭합니다.

   c. License Key 입력란에 라이센스 키를 입력합니다.

   참고

   라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함합니다.

   d. **Add**를 클릭합니다.
5. 복제 페어에서 현재 MTree 컨텍스트를 중단합니다.

   ```
   replication break mtree://destination-system-name/data/
   col1/mtree-name
   ```
6. 새 복제 컨텍스트를 생성합니다.

   ```
   replication add source mtree://source-system-name/data/
   col1/mtree-namedestination mtree://destination-system-
   name/data/col1/mtree-name
   ```
7. 소스 시스템에서만 다음 단계를 수행합니다.
8. Retention Lock을 위한 MTree를 선택합니다.

   Data Management > **MTree** 탭을 클릭한 다음, Retention Lock에 사용하려는 MTree에 대한 확인란을 클릭합니다. 빈 MTree를 생성한 이후에 파일을 추가할 수도 있습니다.
9. 선택한 MTree에 대한 정보를 표시하려면 MTree Summary 탭을 클릭합니다.
10. 규정 준수가 활성화된 MTree에서 파일을 잠급니다.
11. 소스 및 대상(복제본) MTree가 동일한지 확인합니다.

    ```
    replication resync mtree://destination-system-name/data/
    col1/mtree-name
    ```
12. 재동기화의 진행률을 확인합니다.

    ```
    replication watch mtree://destination-system-name/data/
    col1/mtree-name
    ```
13. 복제가 완료되었는지 확인합니다.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```
이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.

컬렉션 복제 페어를 MTree 복제 페어로 변환

DD OS 5.2의 DD Retention Lock Compliance에서는 컬렉션 복제를 사용했지만 컬렉션 복제 페어에서 규정 준수가 활성화된 MTree를 MTree 복제 페어로 변환하려는 고객을 위한 절차입니다.

절차

1. 오직 소스 시스템에서만 다음을 수행합니다.
   a. 각 DD Retention Lock Compliance 활성화 MTree의 스냅샷을 생성합니다.
      ```
      snapshot createsnapshot-name /data/col1/mtree-name
      ```
   b. 컬렉션 복제 페어를 동기화합니다.
      ```
      replication sync col://destination-system-name
      ```
   c. 복제가 완료되었는지 확인합니다.
      ```
      replication status col://destination-system-namedetailed
      ```
      이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.
   d. 각 DD Retention Lock Compliance 활성화 MTree의 스냅샷 정보를 봅니다.
      ```
      snapshot list mtree /data/col1/mtree-name
      ```
      나중에 사용하기 위한 스냅샷 이름을 기록합니다.
2. 오직 대상 시스템에서만 다음을 수행합니다.
   a. 복제가 완료되었는지 확인합니다.
      ```
      replication status mtree://destination-system-name/data/
      col1/mtree-namedetailed
      ```
      이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.
   b. 대상 시스템으로 복제된 각 MTree 스냅샷을 봅니다.
      ```
      snapshot list mtree /data/col1/mtree-name
      ```
   c. 여기서 생성된 스냅샷 이름을 소스 시스템에서 생성된 스냅샷 이름과 비교하여 모든 DD Retention Lock Compliance MTree 스냅샷이 복제되었는지 확인합니다.
      ```
      snapshot list mtree /data/col1/mtree-name
      ```
3. 소스 및 대상 시스템 양쪽에서 다음을 수행합니다.
   a. 파일 시스템을 비활성화합니다.
      ```
      filesys disable
      ```
   b. 컬렉션 복제 컨텍스트를 중단합니다.
      ```
      replication break col://destination-system-name
      ```
   c. 파일 시스템을 활성화합니다. (보안 책임자 인증이 필요할 수 있습니다.)
      ```
      filesys enable
      ```
   d. 각 DD Retention Lock Compliance 활성화 MTree에 대한 복제 컨텍스트를 추가합니다.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

참고

소스 및 대상 MTree 이름이 동일해야 합니다.

4. 오직 소스 시스템에서만 다음을 수행합니다.
   a. 소스 및 대상 MTree가 둘 다 같은지 확인합니다.

      ```
      replication resync mtree://destination-system-name
      ```

   b. 재동기화의 진행률을 확인합니다.

      ```
      replication watchdestination
      ```

   c. 복제가 완료되었는지 확인합니다.

      ```
      replication status mtree://destination-system-name/data/
      col1/mtree-namedetailed
      ```

      이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.

컬렉션 복제 수행

규정 준수가 활성화된 소스 시스템에서 규정 준수가 활성화된 대상 시스템으로 /data/col1을 복제합니다.

참고

컬렉션 복제의 경우 소스 및 대상 시스템에서 동일한 보안 책임자 계정을 사용해야 합니다.

절차

1. 다른 지시가 있을 때까지 소스 시스템에서만 다음 단계를 수행합니다.
2. DD System Manager에 로그인합니다.

   DD System Manager 창은 탐색 패널에서 **DD Network**와 함께 나타납니다.
3. Data Domain 시스템을 선택합니다.

   탐색 패널에서 **DD Network**를 확장하여 시스템을 선택합니다.
4. DD Retention Lock Governance 라이센스가 Feature Licenses 아래에 나열되지 않을 경우 해당 라이센스를 추가합니다.
   a. **Administration** > **Licenses**를 선택합니다.
   b. Licenses 영역에서 **Add Licenses**를 클릭합니다.
   c. License Key 입력란에 라이센스 키를 입력합니다.

      참고

      라이센스 키는 대/소문자를 구분하지 않습니다. 키를 입력할 때 하이픈을 포함합니다.

   d. **Add**를 클릭합니다.
5. 복제 컨텍스트를 생성합니다.

```
replication add source col://source-system-name
destination col://destination-system-name
```

6. 다른 지시가 있을 때까지 대상 시스템에서만 다음 단계를 수행합니다.
7. 파일 시스템을 제거합니다.

   ```
   filesys destroy
   ```

8. DD System Manager에 로그인합니다.

   DD System Manager 창은 탐색 패널에서 **DD Network**와 함께 나타납니다.

9. Data Domain 시스템을 선택합니다.

   탐색 패널에서 **DD Network**를 확장하여 시스템을 선택합니다.

10. 파일 시스템을 생성하되 활성화하지 않습니다.

    ```
    filesys create
    ```

11. 복제 컨텍스트를 생성합니다.

    ```
    replication add source col://source-system-name
    destination col://destination-system-name
    ```

12. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 활성화합니다.

    ```
    system retention-lock compliance configure
    ```

    시스템이 자동으로 재부팅되고 `system retention-lock compliance enable` 명령을 실행합니다.

13. 소스 시스템에서만 다음 단계를 수행합니다.
14. 복제 컨텍스트를 초기화합니다.

    ```
    replication initialize source col://source-system-
    namedestination col://destination-system-name
    ```

15. 복제가 완료되었는지 확인합니다.

    ```
    replication status col://destination-system-namedetailed
    ```

    이 명령을 실행하면 복제가 완료될 때 남은 압축 전 바이트 수가 0으로 보고됩니다.

기존 컬렉션 복제 페어에 DD Retention Lock Compliance 보호 기능 추가

소스 및 대상 시스템에서 DD Retention Lock Compliance를 활성화하지 않은 상태에서 생성된 컬렉션 복제 페어에 DD Retention Lock Compliance 보호 기능을 추가합니다.

절차

1. 다른 지시가 있을 때까지 소스 및 대상 시스템에서 다음 단계를 수행합니다.
2. 복제를 비활성화합니다.

   ```
   replication disable col://destination-system-name
   ```

3. DD System Manager에 로그인합니다.

   DD System Manager 창은 탐색 패널에서 **DD Network**와 함께 나타납니다.

4. Data Domain 시스템을 선택합니다.

   탐색 패널에서 **DD Network**를 확장하여 시스템을 선택합니다.

5. 다른 지시가 있을 때까지 소스 시스템에서 다음 단계를 수행합니다.
6. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 활성화합니다.

   ```
   system retention-lock compliance configure
   ```

시스템이 `system retention-lock compliance enable` 명령을 실행하여 자동으로 재부팅됩니다.

7. 복제 컨텍스트를 활성화합니다.

   `replication enable col://`*`destination-system-name`*

8. 다른 지시가 있을 때까지 대상 시스템에서 다음 단계를 수행합니다.
9. DD Retention Lock Compliance를 사용하도록 시스템을 구성 및 활성화합니다.

   `system retention-lock compliance configure`

   시스템이 `system retention-lock compliance enable` 명령을 실행하여 자동으로 재부팅됩니다.

10. 복제 컨텍스트를 활성화합니다.

    `replication enable col://`*`destination-system-name`*

빠른 복제

DD Retention Lock Compliance 설정 MTree를 사용해 시스템에서 `filesys fastcopy [retention-lock] source`***src***`destination`***dest*** 명령을 실행할 경우 빠른 복제 작업 중에 보존 잠금 특성이 유지됩니다.

참고

대상 MTree에 보존 잠금이 설정되지 않은 경우 보존 잠금 파일 특성은 유지되지 않습니다.

CLI 사용률

DD Retention Lock Compliance가 설정된 Data Domain 시스템에 대한 고려 사항은 다음과 같습니다.

- 규정을 위반하는 명령은 실행할 수 없습니다. 다음 명령은 차단됩니다.
  - `filesys archive unit del`*`archive-unit`*
  - `filesys destroy`
  - `mtree delete`*`mtree-path`*
  - `mtree retention-lock reset {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree retention-lock disable mtree`*`mtree-path`*
  - `mtree retention-lock revert`
  - `user reset`
- 삭제 중인 라이선스가 DD Retention Lock Compliance 라이선스일 경우 다음 명령을 사용하려면 보안 책임자 인증이 필요합니다.
  - `license del license-feature [`*`license-feature`* `...] | license-code [`*`license-code`* `...]`
- 명령에서 지정된 MTree에서 DD Retention Lock Compliance가 설정되어 있는 경우 다음 명령을 사용하려면 보안 책임자 인증이 필요합니다.
  - `mtree retention-lock set {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree rename`*`mtree-path new-mtree-path`*

- 시스템에서 DD Retention Lock Compliance가 설정되어 있는 경우 다음 명령을 사용하려면 보안 책임자 인증이 필요합니다.

  참고

  이러한 명령은 대화형 모드에서 실행해야 합니다.

  - `alerts notify-list reset`
  - `config set timezone`*`zonename`*
  - `config reset timezone`
  - `cifs set authentication active-directory realm { [`*`dc1`* `[`*`dc2`* `...]]`
  - `license reset`
  - `ntp add timeserver`*`time server list`*
  - `ntp del timeserver`*`time server list`*
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {`*`destination`* `| all}`
  - `replication disable {`*`destination`* `| all}`
  - `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]`

시스템 클록

DD Retention Lock Compliance는 시스템 클록을 악의적으로 변경하지 못하도록 내부 보안 클록을 구축합니다.

보안 클록은 시스템 클록을 면밀하게 모니터링하고 기록합니다. 1년 내 보안 클록과 시스템 클록 사이에 누적된 2주간의 시간차가 발생할 경우 파일 시스템이 비활성화되며 보안 책임자만 이를 재개할 수 있습니다.

시스템 클록 시간차 찾기

DD OS 명령 `system retention-lock compliance status`(보안 책임자 인증 필요)를 실행해 마지막으로 기록한 보안 클록 값과 누적된 시스템 클록 편차를 포함하는 시스템 및 보안 클록 정보를 얻을 수 있습니다. 이 값은 10분마다 업데이트됩니다.

시스템 클록 시간차 제거

클록 시간차는 보안 클록이 시스템 클록에 대해 새 값을 기록할 때마다 업데이트됩니다. 1년이 지나면 0으로 재설정됩니다.

언제든지 DD OS 명령 `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]`을 실행해 시스템 클록의 시간을 설정할 수 있습니다(보안 책임자 인증이 필요함). 클록 시간차가 현재 값(2주)보다 커지면 파일 시스템을 사용할 수 없게 됩니다. 이 단계를 완료해 파일 시스템을 재시작하고 보안 및 시스템 클록 사이의 시간차를 제거합니다.

절차

1. 시스템 콘솔에서 파일 시스템을 설정합니다.

   ```
   filesys enable
   ```

2. 프롬프트에서 `filesys enable` 명령을 종료할 것임을 확인하고 시스템 날짜가 올바른지 확인합니다.

3. 시스템 날짜를 표시합니다.

   ```
   system show date
   ```

4. 시스템 날짜가 올바르지 않으면 올바른 날짜를 설정하고(보안 책임자 인증이 필요함) 확인합니다.

   ```
   system set date MMDDhhmm[[CC]YY]
   system show date
   ```

5. 파일 시스템을 다시 설정합니다.

   ```
   filesys enable
   ```

6. 프롬프트에서 설정 절차를 계속합니다.
7. 보안 책임자 프롬프트가 나타납니다. 보안 책임자 인증을 완료해 파일 시스템을 시작합니다. 보안 클록이 현재 시스템 날짜로 자동 업데이트됩니다.

21장

DD Encryption

이 장에는 다음과 같은 내용이 포함됩니다.

DD 암호화 개요

데이터 암호화는 Data Domain 시스템을 도난당하거나 물리적 스토리지 미디어를 운반 중에 분실할 경우에 사용자 데이터를 보호하고, 장애가 발생한 드라이브를 교체할 때 실수로 데이터가 유출될 가능성을 없앱니다.

지원되는 프로토콜(NFS, CIFS, DD VTL, DD Boost, NDMP Tape Server)을 사용해 데이터가 Data Domain 시스템에 입력되는 경우 해당 스트림은 세그먼트로 분할되고 지문이 생성되며 중복 제거(전역 압축)됩니다. 그 후 디스크에 저장되기 전에 여러 세그먼트 압축 영역으로 그룹화되고 로컬 압축된 후 암호화됩니다.

저장된 데이터 암호화 기능을 활성화할 경우 Data Domain 시스템에 입력되는 모든 데이터가 암호화됩니다. 암호화를 더 세밀한 수준으로 활성화할 수 없습니다.

⚠ 주의

DD 암호화 기능이 활성화되기 전에 저장된 데이터는 자동으로 암호화되지 않습니다. 시스템의 모든 데이터를 보호하려면 암호화를 구성할 때 기존 데이터 암호화 옵션을 활성화해야 합니다.

추가 설명:

DD OS 5.5.1.0부터 저장된 데이터 암호화는 단일 보존 유닛이 포함된 DD Extended Retention을 사용하는 시스템을 지원합니다. 5.5.1.0부터 DD Extended Retention은 단일 보존 유닛만 지원하므로 5.5.1.0 이상에서 설정된 시스템의 경우 이 제한 사항을 준수하는 데 아무런 문제가 없습니다. 그러나 5.5.1.0 이전에 설정된 시스템은 보존 유닛이 두 개 이상일 수 있지만, 한 개를 제외한 모든 보존 유닛이 제거되거나 데이터가 하나의 보존 유닛으로 이동 또는 마이그레이션될 때까지는 저장된 데이터 암호화를 사용할 수 없습니다.

`filesys encryption apply-changes` 명령은 다음 정리 주기 동안 모든 암호화 구성 변경 사항을 파일 시스템에 있는 모든 데이터에 적용합니다. 이 명령에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

저장된 데이터 암호화는 온라인 지원 웹 사이트(http://support.emc.com)에서 사용할 수 있는 Backup Compatibility Guide에 설명된 현재 지원되는 모든 백업 애플리케이션을 지원합니다.

Data Domain Replicator에서는 암호화를 사용할 수 있으므로, 암호화된 데이터를 컬렉션, 디렉토리, MTree 또는 다양한 토폴로지를 사용하는 애플리케이션별 관리 파일 복제 기능을 사용하여 복제할 수 있습니다. 각각의 복제 형식은 암호화와 고유한 방식으로 작동하여 모두 동일한 수준의 보안을 제공합니다. 자세한 정보는 복제에 저장된 데이터 암호화 사용 섹션을 참조하십시오.

Data Domain Retention Lock을 사용해 잠긴 파일은 저장, 암호화 및 복제가 가능합니다.

자동 지원 기능에는 다음과 같이 Data Domain 시스템의 암호화 상태에 대한 정보가 포함됩니다.

- 암호화가 활성화되어 있는지 여부
- 적용된 Key Manager 및 사용 키
- 구성된 암호화 알고리즘
- 파일 시스템 상태

암호화 구성

이 절차에는 Key Manager 구성이 포함됩니다.

Data Management > **File System** > **Encryption** 탭의 Encryption Status가 Not Configured로 표시되면 **Configure**를 클릭해 Data Domain 시스템에 대한 암호화를 설정합니다.

참고

암호화를 활성화하려면 시스템 암호를 설정해야 합니다.

다음 정보를 제공합니다.

- 알고리즘
  - 드롭다운 목록에서 암호화 알고리즘을 선택하거나 기본값인 AES 256비트(CBC)를 적용합니다.
    AES 256비트 GCM(Galois/Counter Mode)이 가장 안전한 알고리즘이지만 CBC(Cipher Block Chaining) 모드에 비해 상당히 느립니다.
  - 기존/신규 데이터 모두, 신규 데이터만 등 암호화할 데이터를 결정합니다. 파일 시스템이 다시 시작된 후 첫 번째 정리 주기 동안 기존 데이터가 암호화됩니다. 기존 데이터 암호화는 표준 파일 시스템 정리 작업보다 더 오래 걸릴 수 있습니다.
- Key Manager(셋 중 하나 선택)
  - Embedded Key Manager
    RSA DPM Key Manager를 구성하지 않는 이상, 파일 시스템을 재시작하고 나면 기본적으로 Data Domain Embedded Key Manager가 적용됩니다.

    키 순환을 활성화 또는 비활성화할 수 있습니다. 설정할 경우 1~12개월 사이의 회전 간격을 입력합니다.
  - RSA DPM Key Manager
  - SafeNet KeySecure Key Manager

  참고

  Embedded Key Manager, RSA DPM Key Manager 및 SafeNet KeySecure Key Manager의 작동 방식에 대한 설명은 키 관리에 대한 섹션을 참조하십시오.

Summary에 선택한 구성 값이 표시됩니다. 올바른지 확인하십시오. 값을 변경하려면 **Back**을 클릭하여 원래 값을 입력했던 페이지로 이동 후 수정합니다.

암호화를 설정하려면 시스템을 재시작해야 합니다. 새 구성을 적용하려면 파일 시스템 재시작 옵션을 선택합니다.

참고

파일 시스템이 다시 시작되는 동안 애플리케이션이 중단될 수 있습니다.

키 관리 정보

암호화 키는 암호화 알고리즘의 출력을 결정합니다. 암호화 키는 암호로 보호됩니다. 암호는 암호화 키가 디스크의 여러 위치에 저장되기 전에 암호화 키를 암호화합니다. 암호는 사용자가 생성하며 변경 시에는 관리자와 보안 책임자 자격 증명이 모두 필요합니다.

Key Manager는 여러 암호화 키의 생성, 배포 및 수명주기 관리를 담당합니다. Data Domain 시스템은 Embedded Key Manager 또는 RSA DPM(Data Protection Manager) Key Manager 또는 SafeNet KeySecure Key Manager를 사용할 수 있으며 DD OS 6.1에 KMIP(Key Management Interoperability Protocol) 지원이 도입되었습니다.

한 번에 하나만 적용할 수 있습니다. Data Domain 시스템에 암호화를 활성화하면 기본적으로 Embedded Key Manager가 적용됩니다. RSA DPM 또는 SafeNet KeySecure Key Manager를 구성하면 Embedded Key Manager를 대신하며, 비활성화하기 전까지는 RSA DPM Key Manager가 계속 적용됩니다. 새 Key Manager를 적용하려면 파일 시스템을 재시작해야 합니다.

시스템에서는 한 번에 하나의 키만 사용하여 Data Domain 시스템으로 들어오는 데이터를 암호화하지만 Embedded Key Manager 및 DPM Key Manager 둘 다 여러 개의 키를 제공합니다. 외부 Key Manager를 구성하고 활성화한 경우, Data Domain 시스템은 RSA DPM Key Manager 서버가 제공하는 키를 사용합니다. 같은 DPM Key Manager가 여러 Data Domain 시스템을 관리하는 경우 해당 시스템이 동기화되어 있고 파일 시스템이 재시작되었다면 모든 시스템의 활성 키는 동일합니다(동일 키 클래스를 사용하는 경우). Embedded Key Manager는 키를 내부적으로 생성합니다.

두 Key Manager 모두 키를 순환 사용하며 최대 254개의 키를 지원합니다. Embedded Key Manager를 통해 사용자는 파일 시스템 재시작 후, 키 교체 전에 키가 적용되는 개월 수를 지정할 수 있습니다. 키 클래스에 따라 RSA DPM Key Manager는 주기적으로 키를 순환 사용합니다. Embedded Key Manager 키 순환은 Data Domain 시스템에서 관리되며, Key Manager 키 순환은 외부 Key Manager 서버에서 관리됩니다.

KeySecure
KMIP 규정을 준수하는 Safenet Inc/Gemalto Keysecure의 Key Manager 제품인 KeySecure 8.5 및 8.9가 지원됩니다. KMIP Key Manger를 사용하려면 Key Manager와 Data Domain 시스템/DD VE가 서로 신뢰하도록 구성해야 합니다. 사용자가 Key Manager에서 키를 사전에 생성해야 합니다. Data Domain 시스템은 보안 TLS 접속을 설정한 후에 KeySecure에서 이러한 키와 상태를 검색합니다. Data Domain 시스템에서 키를 생성하고 사용하는 방법에 대한 자세한 내용은 *Data Domain Operating System and Gemalto KeySecure Integration Guide*를 참조하십시오.

손실 또는 손상된 키 문제 해결

시스템의 현재 암호화 키를 모두 포함하는 파일을 생성합니다. 키가 손실 또는 손상된 경우 지원 제공업체가 이 파일을 사용하여 시스템에 다시 키를 가져올 수 있습니다. 주기적으로 내보내기 파일을 생성하는 것이 좋습니다.

키를 내보낼 때는 보안 책임자의 자격 증명을 묻는 메시지가 표시됩니다. 추가적인 키 파일 보호를 위해 Data Domain 시스템에 사용된 것과 다른 암호를 사용할 수 있습니다. 키 파일을 내보낸 후에는 권한이 부여된 사용자만 액세스할 수 있는 안전한 파일 서버에 키 파일을 저장하는 것이 좋습니다. 키 파일에 사용하는 암호를 기억해 두어야 합니다. 암호를 분실했거나 잊어버린 경우 Data Domain 시스템에서 키를 가져와 복원할 수 없습니다. 다음을 입력합니다.

```
# filesys encryption keys export
```

Key Manager 지원

모든 Key Manager가 모든 DD OS 파일 시스템 프로토콜을 지원합니다.

복제
디렉토리 MTree 복제를 위해 Data Domain 시스템을 구성하는 경우 각 Data Domain 시스템을 개별적으로 구성합니다. 두 시스템은 동일하거나 다른 키 클래스, 그리고 동일하거나 다른 Key Manager를 사용할 수 있습니다.

컬렉션 복제 구성을 위해 Data Domain 시스템은 소스에서 구성되어야 합니다. 복제 중단 후 Key Manager에 대한 원본 복제본 Data Domain 시스템이 구성되어야 합니다. 그렇지 않은 경우 Data Domain 시스템은 계속해서 가장 최근에 알려진 키를 사용합니다.

RSA DPM Key Manager 작업

RSA DPM Key Manager를 구성하고 활성화한 경우, Data Domain 시스템은 RSA DPM Key Manager 서버가 제공하는 키를 사용합니다. 같은 DPM Key Manager가 여러 Data Domain 시스템을 관리하는 경우 해당 시스템이 동기화되어 있고 파일 시스템이 재시작되었다면 모든 시스템의 활성 키는 동일합니다(동일 키 클래스를 사용하는 경우). 키 순환은 RSA DPM Key Manager 서버에서 관리됩니다.

RSA DPM Key Manager를 구성하고 활성화한 경우, Data Domain 시스템은 RSA DPM Key Manager 서버가 제공하는 키를 사용합니다. 같은 DPM Key Manager가 여러 Data Domain 시스템을 관리하는 경우 해당 시스템이 동기화되어 있고 파일 시스템이 재시작되었다면 모든 시스템의 활성 키는 동일합니다(동일 키 클래스를 사용하는 경우). 키 순환은 RSA DPM Key Manager 서버에서 관리됩니다.

암호화 키 상태

하나의 Activated-RW 키가 항상 적용됩니다. 활성 키가 유출된 경우 RSA DPM Key Manager에서 새 키가 제공됩니다. Data Domain 시스템에서 새 키를 감지하면 관리자에게 파일 시스템을 재시작하라는 알림을 보냅니다.

만료된 키는 Data Domain 시스템의 기존 데이터에 대해 읽기 전용이 되며 새 활성 키가 수집된 모든 새 데이터에 적용됩니다. 키가 유출되면 기존 데이터는 파일 시스템 정리가 실행된 후 새 암호화 키를 사용하여 다시 암호화됩니다. 최대 키 개수에 도달하면 사용되지 않은 키를 삭제하여 새 키를 위한 공간을 만들어야 합니다.

Data Domain 시스템에 있는 암호화 키 정보를 보려면 DD System Manager를 열고 **Data Management** > **File System** > **Encryption** 탭으로 이동합니다. 키가 Encryption 탭의 **Encryption Keys** 섹션에 ID 번호별로 나열됩니다. 각 키에 대해 키의 생성 시기, 유효 기간, 유형(RSA DPM 또는 Data Domain), 상태(Data Domain이 지원하는 DPM 암호화 키 상태 참조), 압축 후 크기 등의 정보가 제공됩니다. 시스템에 Extended Retention 라이센스가 있는 경우 다음 필드도 표시됩니다.

Active Size (post comp)

이 키로 암호화된 활성 계층에 있는 물리적 공간의 크기입니다.

Retention Size (post comp)

이 키로 암호화된 보존 계층에 있는 물리적 공간의 크기입니다.

Key MUID를 클릭하면 Key Details 대화 상자에 키에 대한 Tier/Unit(예: Active, Retention-unit-2), 생성 날짜, 유효 기간, 상태(Data Domain이 지원하는 DPM 암호화 키 상태 참조), 압축 후 크기 등의 정보가 표시됩니다. Close를 클릭하여 대화 상자를 닫습니다.

표 200 Data Domain이 지원하는 DPM 암호화 키 상태

상태	정의
Pending-Activated	키가 막 생성된 상태입니다. 파일 시스템을 재시작한 후에는 키 상태가 Activated-RW가 됩니다.
Activated-RW and Activated-RO	Activated-RW 및 Activated-RO 모두 각각의 키로 암호화된 데이터를 읽습니다. Activated-RW는 최근에 활성화된 키입니다.

표 200 Data Domain이 지원하는 DPM 암호화 키 상태 (계속)

상태	정의
De-Activated	현재 시간이 유효 기간을 초과하면 키는 비활성화됩니다. 키는 읽기용으로 사용됩니다.
Compromised	키는 해독만 가능합니다. 유출된 키로 암호화된 모든 데이터를 다시 암호화하면 상태가 Destroyed Compromised로 변경됩니다. 파일 시스템 정리를 실행하면 키가 다시 암호화됩니다. 필요한 경우 Destroyed Compromised 키를 삭제할 수 있습니다.
Marked-For-Destroy	다시 암호화할 데이터에 대해 제거된 것으로 키를 표시한 상태입니다.
Destroyed	이 키로 암호화된 모든 데이터를 다시 암호화하면 DD OS에서 상태를 Marked-For-Destroy에서 Destroyed로 변경합니다. 또한 제거된 키가 유출된 경우 상태가 Compromised-Destroyed가 됩니다. 상태가 Destroyed 및 Compromised-Destroyed인 키를 삭제할 수 있습니다. 참고 키는 정리 작업이 실행되어 완료될 때까지 Data Domain 시스템에서 제거되지 않습니다.

RSA DPM Key Manager와 키를 동기화된 상태로 유지

자동 키 동기화는 매일 자정에 수행됩니다. 수동 키 동기화는 예약된 동기화를 기다릴 수 없는 경우에만 필요합니다. Data Domain 시스템에서 새 키가 동기화될 때마다 알림이 생성됩니다. 이 알림은 파일 시스템이 재시작된 후에 지워집니다.

RSA DPM Key Manager Server가 새 키를 생성한 후에 **Sync** 버튼을 클릭하면 Data Domain System Manager에서 Encryption 탭의 Encryption Key 목록에 새 키가 표시됩니다.

참고

마지막 동기화 이후에 키가 변경된 경우 파일 시스템을 재시작해야 합니다.

절차

1. DD System Manager를 사용하여 탐색 패널에서 작업할 Data Domain 시스템을 선택합니다.

   참고

   DD System Manager 기능은 항상 탐색 패널에서 선택한 시스템에서 수행하십시오.

2. **Data Management** > **File System** > **Encryption**을 클릭합니다.
3. Encryption Keys 섹션에서 **RSA DPM** 키를 선택하고 **Sync**를 클릭합니다.

키 제거(RSA DPM Key Manager)

데이터를 키로 암호화하지 않으려면 해당 키를 제거하십시오. 이 절차에서는 보안 책임자 자격 증명이 필요합니다.

참고

보안 책임자에 대한 자세한 내용은 로컬 사용자 생성 및 보안 인증 설정에 관한 섹션을 참조하십시오.

RSA DPM 키를 제거할 수 있는 상태로 변경하려면 다음을 수행하십시오.

절차

1. RSA DPM 서버에서 키를 비활성화합니다.
2. Data Domain 시스템에서 비활성화할 키의 파일 시스템을 재시작합니다.
3. DD System Manager를 사용해 **Data Management** > **File System** > **Encryption**을 선택합니다.
4. Encryption Keys 섹션의 목록에서 제거할 키를 선택합니다.
5. **Destroy...**를 클릭합니다.
   시스템에 키의 계층과 상태가 포함된 Destroy 대화 상자가 표시됩니다.
6. 보안 책임자 사용자 이름 및 암호를 입력합니다.
7. **Destroy**를 클릭하여 키를 제거할 것임을 확인합니다.

   참고

   파일 시스템 정리를 실행한 후에 키 상태가 Destroyed로 바뀝니다.

키 삭제

Destroyed 또는 Compromised-Destroyed 상태의 Key Manager 키를 삭제할 수 있습니다. 그러나 키의 개수가 최대 254개 제한에 도달했을 때에만 키를 삭제해야 합니다. 이 절차에서는 보안 책임자 자격 증명이 필요합니다.

참고

Destroyed 상태에 이르기 위해서는 키에서 Embedded Key Manager 또는 RSA DPM Key Manager에 대한 키 삭제 절차를 수행해야 하며 시스템 정리를 실행해야 합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 클릭합니다.
2. Encryption Keys 섹션에서 삭제할 키를 목록에서 선택합니다.
3. **Delete...**를 클릭합니다.
   시스템에 삭제할 키와 키의 계층 및 상태가 표시됩니다.
4. 보안 책임자 사용자 이름 및 암호를 입력합니다.
5. **Delete**를 클릭하여 키를 삭제할 것임을 확인합니다.

Embedded Key Manager 작업

Embedded Key Manager를 선택하면 Data Domain 시스템에서 자체 키가 생성됩니다.

키 순환 정책이 구성되고 나면 다음 순환 시 새 키가 자동으로 생성됩니다. 알림이 새 키의 생성을 알려 줍니다. 파일 시스템 재시작을 수행해 새 키를 활성화하고 이전 키를 비

활성화해야 합니다. Embedded Key Manager Key의 순환 상태와 연결된 **Disable** 버튼을 클릭해 키 순환 정책을 해제할 수 있습니다.

키 생성(Embedded Key Manager)

Embedded Key Manager에 대한 암호화 키를 생성합니다.

절차

1. **Data Management** > **File System** > **DD Encryption**을 선택합니다.
2. Encryption Keys 섹션에서 **Create...**를 클릭합니다.
3. 보안 책임자 사용자 이름 및 암호를 입력합니다.
4. 파일 시스템을 재시작하려면 **Restart the filesystem now**를 클릭합니다.

   새 Data Domain 키가 생성됩니다. 파일 시스템을 재시작하고 나면 이전 키가 비활성화되고 새 키가 활성화됩니다.
5. **Create**를 클릭합니다.

키 제거(Embedded Key Manager)

Embedded Key Manager에 대한 암호화 키를 제거합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 클릭합니다.
2. Encryption Keys 섹션의 목록에서 제거할 키를 선택합니다.
3. **Destroy...**를 클릭합니다.

   시스템에 키의 계층과 상태가 포함된 Destroy 대화 상자가 표시됩니다.
4. 보안 책임자 사용자 이름 및 암호를 입력합니다.
5. **Destroy**를 클릭하여 키를 제거할 것임을 확인합니다.

   참고

   파일 시스템 정리를 실행한 후에는 키 상태가 Destroyed로 바뀝니다.

KeySecure Key Manager 작업

KeySecure Key Manager는 KMIP(Key Management Interoperability Protocol)를 사용하여 외부 Key Manager를 지원하며 단일 중앙 플랫폼에서 중앙 집중식으로 암호화 키를 관리합니다.

- 키는 Key Manager에서 사전에 생성됩니다.
- 하나 이상의 클라우드 유닛에 암호화가 활성화된 시스템에서는 KMIP Key Manager를 활성화할 수 없습니다.

DD System Manager를 사용하여 KeySecure Key Manager 설정 및 관리

이 섹션에서는 DD SM(Data Domain System Manager)을 사용하여 KeySecure Key Manager를 관리하는 방법에 대해 설명합니다.

KeySecure Key Manager를 위한 키 생성

KMIP(KeySecure Key Manager)를 위한 암호화 키를 생성합니다.

절차

1. **Key Manager Encryption Keys** 테이블까지 아래로 스크롤합니다.
2. **Add**를 클릭하여 새 Key Manager 암호화 키를 생성합니다.
   a. 보안 책임자의 사용자 이름 및 암호를 입력합니다.
   b. **Restart the file system now**를 클릭합니다.
   c. **Create**를 클릭합니다.
3. **Restart the file system now**를 클릭하여 변경 사항을 적용합니다.
   새 KIMP 키가 생성됩니다. 파일 시스템을 재시작하고 나면 이전 키가 비활성화되고 새 키가 활성화됩니다.

KeySecure Key Manager에서 기존 키의 상태 수정

DD SM을 사용하여 기존 KMIP 암호화 키의 상태를 수정합니다.

시작하기 전에

키 상태 변경을 위한 조건을 검토합니다.

- 키가 이미 존재하고(활성 상태이고) 새 키가 생성되면 사용자가 파일 시스템을 재시작할 때까지 새 키가 `Pending-Activated` 상태로 변경됩니다.
- 대신할 `Pending-Activated` 키가 있는 경우에만 `Activated-RW` 상태의 키를 비활성화할 수 있습니다.
- 대신할 다른 `Pending-Activated` 키가 있는 경우에만 `Pending-Activated` 상태의 키가 비활성화됩니다.
- `Activated-RO` 키 상태의 키에는 필요한 조건이 없습니다. 언제든지 비활성화하십시오.

절차

1. **Data Management** > **File System** > **DD Encryption**을 선택합니다.
2. 아래로 스크롤하여 **Key Manager Encryption Keys** 테이블을 표시합니다.
3. **Key Manager Encryption Keys** 테이블에서 적절한 키를 선택합니다.
4. 키를 비활성화하려면 다음을 수행합니다.
   a. `Activated` 상태로 표시되는 키를 클릭합니다.
   b. 보안 책임자의 사용자 이름 및 암호를 입력합니다.
   c. **DEACTIVATE**를 클릭합니다.

그림 25 KMIP 키를 비활성화 상태로 변경

5. **Restart the filesystem now**를 클릭합니다.

결과

기존 키의 상태가 변경됩니다.

KeySecure Key Manager 구성

DD SM을 사용하여 Data Domain 시스템에서 키 순환 정책을 설정합니다.

시작하기 전에

원하는 키 순환 기간(주 또는 개월), 키 순환 시작 날짜 및 다음 키 순환 날짜를 확인합니다.

절차

1. **Data Management** > **File System** > **DD Encryption**을 선택합니다.
2. **Key Management** 섹션에서 **Configure**를 클릭합니다. **Change Key Manager** 대화 상자가 열립니다.
3. 보안 책임자 사용자 이름 및 암호를 입력합니다.
4. **Key Manager Type** 드롭다운 메뉴에서 **KeySecure Key Manager**를 선택합니다. Change Key Manager 정보가 나타납니다.
5. 키 순환 정책을 설정합니다.

   참고

   순환 정책은 주 및 월 단위로 지정됩니다. 최소 키 순환 정책 증분은 1주이며 최대 키 순환 정책 증분은 52주(또는 12개월)입니다.

   a. 키 순환 정책을 활성화합니다. **Enable Key rotation policy** 버튼을 설정하여 활성화합니다.
   b. Key rotation schedule 필드에 적절한 날짜를 입력합니다.
   c. **Weeks** 또는 **Months** 드롭다운 메뉴에서 적절한 주 또는 개월 수를 선택합니다.
   d. **OK**를 클릭합니다.
   e. 파일 시스템을 재시작하여 변경 사항을 즉시 적용하려면 **Restart the filesystem now**를 클릭합니다.

결과

키 순환 정책이 설정되거나 변경되었습니다.

Data Domain CLI를 사용하여 KeySecure Key Manager 관리

이 섹션에서는 CLI를 사용하여 KeySecure Key Manager를 관리하는 방법에 대해 설명합니다.

KeySecure Key Manager에서 새 활성 키 생성

Data Domain CLI를 사용하여 새 활성 키를 생성합니다.

시작하기 전에

적절한 사용자 자격 증명이 있는지 확인합니다. 이러한 명령을 실행하려면 보안 역할이 필요합니다.

절차

1. 보안 역할을 사용하여 Data Domain 시스템에 로그인합니다.

   사용자 이름: `<security office user>`

   암호: `<security officer password>`

2. 새 활성 키 생성:

```
# filesys encryption key-manager keys create
```

3. 다음 내용과 비슷한 결과가 표시됩니다.

```
New encryption key was successfully created.
The filesystem must be restarted to activate the new key.
```

결과

새 활성 키가 생성됩니다.

KeySecure Key Manager에서 기존 키의 상태 수정

Data Domain CLI를 사용하여 비활성화된 상태로 기존 키의 상태를 수정합니다.

시작하기 전에

적절한 사용자 자격 증명이 있는지 확인합니다. 이러한 명령을 실행하려면 보안 역할이 필요합니다.

절차

1. 보안 역할을 사용하여 Data Domain 시스템에 로그인합니다.

   사용자 이름: `<security officer user>`

   암호: `<security officer password>`

2. 기존 키의 상태를 수정합니다.

   ```
   # filesys encryption key-manager keys modify{<key-id> | muid
   <key-muid>}state deactivated
   ```

   예:

   ```
   # filesys encryption key-manager keys modify muid
   740D711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D
   41 state deactivated
   ```

3. 다음 내용과 비슷한 결과가 표시됩니다.

   ```
   Key state modified.
   ```

결과

기존 키의 상태가 수정됩니다.

KeySecure Key Manager에서 키 순환 정책 설정 또는 재설정

Data Domain CLI를 사용하여 주기적으로 키를 순환시키기 위해 Data Domain 시스템의 키 순환 정책을 설정합니다. 순환 정책은 주 및 월 단위로 지정됩니다. 최소 키 순환 정책 증분은 1주이며 최대 키 순환 정책 증분은 52주(또는 12개월)입니다.

시작하기 전에

적절한 사용자 자격 증명이 있는지 확인합니다. 이러한 명령을 실행하려면 보안 역할이 필요합니다.

절차

1. 보안 역할을 사용하여 Data Domain 시스템에 로그인합니다.

   사용자 이름: `sec`

   암호: `<security officer password>`

2. 처음으로 키 순환 정책을 설정합니다. 이 예에서는 순환 정책을 **3주**로 설정합니다.

```
# filesys encryption key-manager set key-rotation-policy
                  {every <n> {weeks | months} | none}
```

예를 들면 다음과 같습니다.

```
# filesys encryption key-manager set key-rotation-policy
every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 3 weeks.
```

3. 그런 다음 기존 키 순환 정책을 변경하려는 경우 이 명령을 실행합니다. 이 예에서는 순환 정책을 **3주**에서 ***4개월***로 설정합니다.

참고

보안 역할을 사용하여 Data Domain 시스템에 로그인합니다(여기서, 사용자 이름은 sec이고 암호는 <security officer password>).

```
# filesys encryption key-manager reset [key-rotation-policy]
```

예를 들면 다음과 같습니다.

```
filesys encryption key-manager set key-rotation-policy every
4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 4 months.
```

4. 현재 키 순환 정책을 표시하거나 정책이 올바르게 설정되었는지 확인합니다.

```
# filesys encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager:                                Enabled
```

```
Server Type:                                KeySecure
Server:                                     <IP address of
KMIP server>
Port:                                       5696
Fips-mode:                                  enabled
Status:                                     Online
Key-class:                                  <key-class>
KMIP-user:                                  <KMIP username>
Key rotation period:                        2 months
Last key rotation date:                     03:14:17 03/19
2018
Next key rotation date:                     01:01:00 05/17
2018
```

결과

키 순환 정책이 설정되거나 변경되었습니다.

정리 작업의 작동 방식

Compromised 또는 Marked-For-Destroyed 키로 암호화된 데이터가 Activated-RW 키를 사용하여 다시 키 지정될 때, 암호화는 정리 작업의 성능에 영향을 미칩니다.

정리 작업이 끝날 때는 Compromised 또는 Marked-For-Destroyed 키로 암호화된 데이터가 없을 것입니다. 또한, 정리 작업에서 기록된 모든 데이터는 Activated-RW 키로 암호화됩니다.

Key Manager 설정

사용 중인 Key Manager 유형에 대한 지침을 따르십시오.

SafeNet KeySecure Key Manager 설정에 대한 자세한 내용은 *Data Domain Operating System과 Gemalto KeySecure 통합 가이드*를 참조하십시오.

RSA DPM Key Manager 암호화 설정

RSA DPM Key Manager는 RSA DPM 서버와 Data Domain 시스템 모두에서 설정해야 합니다.

RSA DPM 서버에서 이 설정 수행

GUI를 사용해 RSA DPM 서버를 설정하는 주요 단계입니다.

참고

이 절차의 각 단계에 대한 자세한 내용은 최신 버전의 *RSA Data Protection Manager Server Administrator's Guide*를 참조하십시오.

RSA DPM Key Manager 서버에서 설정된 알고리즘과 암호 모드 설정은 Data Domain 시스템에서 무시됩니다. Data Domain 시스템에서 이러한 설정을 구성하십시오.

절차

1. X509 인증서를 사용해 Data Domain 시스템의 ID를 생성합니다. 이 인증서를 기반으로 보안 채널이 생성됩니다.
2. 다음과 같은 올바른 속성을 사용해 키 클래스를 생성합니다.
   - Key length: 256비트

- Duration: 예를 들어 6개월 또는 정책에 맞는 시간
- Auto-key generation: 키가 자동으로 생성되도록 하려면 선택

참고

여러 Data Domain 시스템에서 동일한 키 클래스를 공유할 수 있습니다. 키 클래스에 대한 자세한 내용은 RSA DPM 키 클래스에 대한 섹션을 참조하십시오.

3. Data Domain 시스템의 호스트 인증서를 ID 인증서로 사용해 ID를 생성합니다. ID와 키 클래스가 같은 ID 그룹에 있어야 합니다.
4. 인증서를 가져옵니다. 자세한 내용은 인증서 가져오기에 대한 섹션을 참조하십시오.

RSA DPM 키 클래스 정보

Data Domain 시스템은 키 클래스를 기준으로 RSA DPM Key Manager에서 키를 검색합니다. 키 클래스는 RSA DPM Key Manager에서 사용되는 보안 클래스의 특수 유형으로, 암호 키를 비슷한 특성으로 그룹화합니다.

RSA DPM Key Manager 서버에서는 현재 키를 반환하거나 매번 새 키를 생성하도록 키 클래스를 설정할 수 있습니다. Data Domain 시스템은 현재 키를 반환하도록 구성된 키 클래스만 지원합니다. 매번 새 키를 생성하도록 구성된 키 클래스는 사용하지 마십시오.

참고

키 길이가 256비트가 아니면 DPM 구성이 실패합니다.

인증서 가져오기

인증서를 취득한 후에는 인증서를 Data Domain 시스템으로 가져오십시오.

시작하기 전에

- 호스트 인증서는 PKCS12 형식을 따라야 합니다.
- CA 인증서는 PEM 형식을 따라야 합니다.
- RSA DPM Key Manager와 호환되는 CA 및 호스트 인증서를 획득해야 합니다. 이 인증서는 타사 인증 기관에 요청하거나 해당 SSL 유틸리티 툴을 사용해 생성할 수 있습니다.
- 시스템 암호가 설정되지 않은 경우 호스트 인증서를 가져올 수 없습니다. 암호는 암호화를 활성화하면 설정됩니다. 암호를 변경하려면 Data Domain 시스템 관리 장에서 시스템 암호 변경 관련 섹션을 참조하십시오.

DD OS는 Data DD Manager 및 RSA DPM Key Manager의 사용을 위해 확장 기능이 없는 인증서와 서버 및 클라이언트 확장 기능이 있는 인증서를 지원합니다. 클라이언트 확장 기능이 있는 인증서는 RSA DPM Key Manager에서만 지원하며, 서버 확장 기능이 있는 인증서는 DD System Manager에서만 지원합니다.

DD OS는 자동 등록된 인증서를 직접 업로드하거나 여러 인증서를 가져오는 RSA DPM Key Manager 서버의 자동 등록 인증서 기능을 지원하지 않습니다. 따라서 Data Domain 시스템에 대한 CA 및 호스트 인증서를 직접 가져와야 합니다.

다음 정보는 인증서 관리 중에 나타날 수 있는 몇 가지 알림에 대응하는 방법을 설명합니다.

- 가져온 인증서가 손상되었기 때문에 HTTPS를 재시작하지 못하는 경우에는 자체 서명된 인증서가 사용됩니다. 이 경우 관리 알림 UnusableHostCertificate이 실행됩니다. 알림을 지우려면 손상된 인증서를 삭제하고 새 인증서를 다시 가져오십시오.

- 예를 들어 시스템 헤드 스왑 중에 가져온 인증서가 제거되고 가져온 인증서가 복제에 실패하면 관리 알림 MissingHostCertificate이 실행됩니다. 알림을 지우려면 인증서를 다시 가져오십시오.

인증서를 취득한 후에는 인증서를 다음과 같이 Data Domain 시스템으로 가져오십시오.

절차

1. CA 및 호스트 인증서를 사용하도록 RSA DPM Key Manager Server를 구성합니다. 지침은 *RSA DPM Key Manager Server Administration Guide*를 참조하십시오.
2. `ssh` 명령 구문을 사용해 인증서 파일을 리디렉션하는 방법으로 인증서를 가져옵니다. 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

   ssh sysadmin@<*Data-Domain-system*> adminaccess certificate import {host password *password* |ca } < *path_to_the_certificate*
   예를 들어 `ssh` 명령을 사용해 개인 컴퓨터의 데스크톱에서 Data Domain 시스템 DD1으로 호스트 인증서 host.p12를 가져오려면 다음을 입력합니다.

   # ssh sysadmin@DD1 adminaccess certificate import host password abc123 < C:\host.p12

3. 다음을 입력하여 SSH를 통해 데스크톱에서 DD1으로 CA 인증서(예: ca.pem)를 가져옵니다.

   # `ssh sysadmin@DD1`**adminaccess certificate import ca < C:\ca.pem**

Data Domain 시스템에서 이 설정 수행

Data Domain System Manager에서 DPM Key Manager를 사용하여 암호화를 구성합니다.

절차

1. RSA DPM 서버에서 DPM Key Manager 설정을 완료합니다.
2. Data Domain 시스템에서 자체 호스트 이름을 사용해 IP 주소를 확인할 수 있어야 합니다. 이 매핑이 DNS 서버에 추가되지 않았다면 다음 명령줄을 사용해 `/etc/hosts` 파일에 항목을 추가합니다.

   # `net hosts add`*ipaddrhost-list*
   여기서 *ipaddr*은 Data Domain 시스템의 IP 주소이고, *host-list*는 Data Domain 시스템의 호스트 이름입니다.

   이중 스택 환경에서 작업하는 경우 시스템에 다음 오류 메시지가 표시됩니다. "RKM is not configured correctly". 그러면 `net hosts add`*ipaddrhost-list* 명령을 사용하여 Data Domain 시스템의 IPv4 주소를 /etc/hosts 파일에 추가합니다.

   참고

   IPv6 주소만 사용하는 환경에서는 DPM 서버를 사용할 수 없습니다.

   참고

   기본적으로 FIPS 모드가 설정되어 있습니다. PKCS #12 클라이언트 자격 증명이 FIPS 140-2 승인 알고리즘(예: RC2)으로 암호화되지 않은 경우 FIPS 모드를 해제해야 합니다. FIPS 모드를 해제하는 방법에 대한 자세한 내용은 *Data Domain Operating System 명령 참조 가이드*를 참조하십시오.

3. DD System Manager에 로그인하고 탐색 패널에서 작업 중인 Data Domain 시스템을 선택합니다.

   참고

   DD System Manager 기능은 항상 탐색 패널에서 선택한 시스템에서 수행하십시오.

4. **Data Management** > **File System** > **Encryption** 탭을 클릭합니다.
5. 암호화 구성에 관한 섹션의 지침을 따르고 **DPM Key Manager**를 선택합니다. 암호화가 이미 설정되어 있으면, 설정 후 Key Manager를 변경하는 방법에 관한 섹션의 지침을 따르십시오.

KMIP Key Manager 설정

KMIP 지원을 사용하는 경우 Data Domain 어플라이언스가 KMIP Key Manager에서 저장된 데이터 암호화에 사용되는 대칭형 키 객체를 검색할 수 있습니다.

절차

1. IP 주소 <IP1>을 사용하여 KeySecure 인스턴스를 설정합니다.
2. KeySecure에 SSL 서버 인증서를 생성하고 설치합니다.
3. **Device** > **Key Server**로 이동하여 KMIP를 활성화합니다.

   <IP1>이 사용되는 주소이고 포트가 <Port1>이며 2단계의 서버 인증서가 사용되는지 확인합니다.

4. Data Domain 시스템/DD VE 또는 Linux 컴퓨터에서 시스템에 대한 CSR(Certificate Signing Request)을 생성합니다.

   a. Data Domain에 로그인합니다.

   b. `adminaccess certificate cert-signing-request generate` 명령을 실행합니다.

      명령이 성공할 경우 `CertificateSigningRequest.csr` 파일이 `/ddvar/certificates/`에 생성됩니다.

   기본적으로 NFS 내보내기는 루트 사용자를 포함하여 인증서 폴더에 액세스할 수 있는 권한이 없습니다.

```
# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
drwxr-xr-x 25 root staff      4096 Apr 10 08:32 .
drwxr-xr-x 26 root root       4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff       180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff      4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff      4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff      4096 Apr  4 12:50 cdes
drwxrws---  2 root staff      4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff      4096 Jul  1  2016 core
```

5. 이 CSR을 받아 KeySecure에서 CA에 의해 발급/서명되도록 합니다.

   명령이 성공할 경우 `CertificateSigningRequest.csr` 파일이 `/ddvar/certificates/`에 생성됩니다.

6. 해당 서명된 인증서(x.509 pem 파일)를 Data Domain 시스템에 다운로드하고 CSR의 개인 키를 사용하여 pkcs#12 파일을 생성합니다.

파일 이름을 `csr`에서 `pem`으로 변경합니다.

7. KeySecure의 CA에서 루트 CA 인증서를 다운로드합니다(**Security** > **Local CAs**).
8. Data Domain 시스템/DD VE에서 `adminaccess` CLI를 사용하여 pkcs#12 클라이언트 인증서와 CA 인증서를 설치합니다. 애플리케이션 유형을 **keysecure**로 사용합니다.
9. KeySecure에서 AES-256을 알고리즘 및 키 길이로 사용해 대칭형 키를 생성합니다.
   a. Data Domain 시스템/DD VE에서 KMIP로 사용할 사용자로 소유자를 설정합니다.
   b. `Exportable` 옵션을 선택합니다.
   c. 해당 키에 대한 **Security** > **Keys** > **Attributes** 아래에서 **Application Namespace**를 **DD_DARE_KEYS**로 설정합니다. **Application Data**를 Data Domain 시스템/DD VE에서 사용할 키 클래스로 설정합니다.
10. `filesys encryption key-manager set` 명령을 사용하여 모든 매개 변수가 KeySecure Key Manager에 액세스하도록 구성합니다.
11. `filesys encryption key-manager enable` 명령을 사용하여 외부 Key Manager를 활성화합니다.
12. `filesys encryption enable` 및 `filesys restart` 명령을 사용하여 암호화를 활성화합니다.

    이 작업 시 파일 시스템이 재시작됩니다.
13. 키가 KeySecure Key Manager에서 자동으로 검색되고 로컬 키 테이블에 표시되어야 합니다.

    `filesys encryption keys show`의 로컬 키 테이블 샘플 출력:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.
```

    현재 활성 키를 사용하여 수집되는 모든 데이터가 암호화됩니다.
14. 키 상태를 동기화합니다.
    a. KeySecure 웹 인터페이스에서 앞서 설명한 새 활성 키를 생성합니다.
    b. KeySecure 웹 인터페이스에서 키를 클릭하고 **Life Cycle** 탭 아래로 이동하여 이전 키를 비활성화합니다. **Edit State**를 클릭합니다. **Cryptographic State**를 **Deactivated**로 설정합니다. **Save**를 클릭합니다.
15. Data Domain 시스템에서 `filesys encryption keys sync` 명령을 실행하여 로컬 키 테이블을 동기화합니다.

    `filesys encryption keys show`의 로컬 키 테이블 샘플 출력:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Deactivated       0
0.3   851631E574D6F02886CAEF2795896D4C401EBC57A0997EFE04A146E584E9A99A  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.
```

참고

버전 지정된 키로 키를 표시할 수 있습니다. 특정 키의 2번째 및 3번째 버전이 생성되는 경우 현재 KMIP 쿼리에서 이러한 키를 선택하지 않으므로 Data Domain 시스템 또는 DD VE에서 해당 키를 사용 중이라면 문제가 될 수 있습니다.

설정 후 Key Manager 변경

Embedded Key Manager 또는 RSA DPM Key Manager 중에서 선택합니다.

시작하기 전에

시스템의 인증서를 관리하려면 해당 시스템에서 DD System Manager를 시작해야 합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 클릭합니다.
2. Key Management 아래에서 **Configure**를 클릭합니다.
3. 보안 책임자 사용자 이름 및 암호를 입력합니다.
4. 어떤 Key Manager를 사용할지 선택합니다.
   - Embedded Key Manager: 키 회전을 사용하거나 해제할지 여부를 선택합니다. 사용하도록 설정할 경우 1~12개월 사이의 회전 간격을 입력합니다. **Restart the file system now**를 선택하고 **OK**를 클릭합니다.
   - RSA DPM Key Manager: 서버 이름, 키 클래스, 포트(기본값 443) 및 가져온 호스트 인증서가 FIPS를 준수하는지 여부를 입력합니다. 기본 모드가 설정되어 있습니다. **Restart the file system now**를 선택하고 **OK**를 클릭합니다.
5. **Manage Certificates**를 클릭해 인증서를 추가합니다.

RSA Key Manager용 인증서 관리

RSA Key Manager와 함께 호스트와 CA 인증서를 모두 사용해야 합니다.

참고

인증서는 RSA Key Manager에만 필요합니다. Embedded Key Manager에서는 인증서를 사용하지 않습니다.

RSA Key Manager용 CA 인증서 추가

CA 인증서를 업로드하거나 복사하여 붙여 넣습니다.

절차

1. 다음 중 하나를 선택합니다.
   - CA 인증서를 .pem 파일로 업로드하는 옵션을 선택하고 **Browse**를 클릭하여 파일을 찾습니다.
   - CA 인증서를 복사하여 붙여넣는 옵션을 선택하고 인증서 내용을 제공되는 필드에 붙여넣습니다.
2. **Add**를 클릭하여 인증서를 추가합니다.

RSA Key Manager용 호스트 인증서 추가

인증서를 .p12 파일로 업로드하거나 공개 키를 .pem 파일로 업로드하고 생성된 개인 키를 사용합니다.

시작하려면 다음 단계 중 첫 번째 또는 두 번째 단계를 선택합니다.

절차

1. 인증서를 .p12 파일로 업로드하는 옵션을 선택합니다.
   a. 암호를 입력합니다.
   b. **Browse**를 클릭하여 .p12 파일을 찾습니다.
2. 공개 키를 .pem 파일로 업로드하는 옵션을 선택하고 생성된 개인 키를 사용합니다.
   a. **Browse**를 클릭하여 .pem 파일을 찾습니다.
3. **Add**를 클릭합니다.

인증서 삭제

올바른 지문이 포함된 인증서를 선택합니다.

절차

1. 삭제할 인증서를 선택합니다.
2. **Delete**를 클릭합니다.
   삭제할 인증서의 지문과 함께 Delete Certificate 대화 상자가 표시됩니다.
3. **OK**를 클릭합니다.

저장된 데이터 암호화 설정 확인

DD Encryption 기능의 설정을 확인합니다.

Data Management > **File System** > **Encryption** 탭을 클릭합니다. 현재 사용되는 Key Manager가 Enabled로 표시됩니다. DD Encryption 설정에 대한 설명은 암호화 보기에 대한 섹션을 참조하십시오.

저장된 데이터 암호화 활성화 및 비활성화

DD Encryption을 구성한 후 상태가 활성화되고 Disabled 버튼이 활성화됩니다. DD Encryption이 비활성화되면 Enabled 버튼이 활성화됩니다.

저장된 데이터 암호화 활성화

DD System Manager를 사용하여 DD Encryption 기능을 활성화합니다.

절차

1. DD System Manager를 사용하여 탐색 패널에서 작업할 Data Domain 시스템을 선택합니다.
2. Encryption 보기에서 **Enable** 버튼을 클릭합니다.
3. 다음 옵션을 모두 사용할 수 있습니다.

- **Apply to existing data**를 선택하고 **OK**를 클릭합니다. 파일 시스템이 다시 시작된 후 첫 번째 정리 주기 동안 기존 데이터의 암호화가 수행됩니다.
- **Restart the file system now**를 선택하고 **OK**를 클릭합니다. 파일 시스템이 다시 시작된 후 DD Encryption이 활성화됩니다.

사후 요구 사항

참고

파일 시스템이 다시 시작되는 동안 애플리케이션이 중단될 수 있습니다.

저장된 데이터 암호화 비활성화

DD System Manager를 사용하여 DD Encryption 기능을 비활성화합니다.

절차

1. DD System Manager를 사용하여 탐색 패널에서 작업할 Data Domain 시스템을 선택합니다.
2. Encryption 보기에서 **Disable** 버튼을 클릭합니다.

   Disable Encryption 대화 상자가 표시됩니다.
3. Security Officer Credentials 영역에서 사용자 이름과 보안 책임자의 암호를 입력합니다.
4. 다음 중 하나를 선택합니다.
   - **Apply to existing data**를 선택하고 **OK**를 클릭합니다. 파일 시스템이 다시 시작된 후 첫 번째 정리 주기 동안 기존 데이터의 해독이 수행됩니다.
   - **Restart the file system now**를 선택하고 **OK**를 클릭합니다. 파일 시스템이 다시 시작된 후 DD Encryption이 비활성화됩니다.

사후 요구 사항

참고

파일 시스템이 다시 시작되는 동안 애플리케이션이 중단될 수 있습니다.

파일 시스템 잠금 및 잠금 해제

DD Encryption을 사용하는 Data Domain 시스템과 이 시스템의 외부 스토리지 디바이스를 운송하거나 교체 중인 디스크를 잠그려면 이 절차를 따릅니다. 이 절차에는 다음의 두 가지 역할 계정이 필요합니다. Security Officer 및 System Administration

절차

1. **Data Management** > **File System** > **Encryption**을 클릭합니다.

   File System Lock 영역의 Status에 파일 시스템 상태가 Locked 또는 Unlocked로 표시됩니다.
2. File System Status 영역에서 **Disabled**를 클릭하여 파일 시스템을 비활성화합니다.
3. 이 절차에 따라 파일 시스템을 잠그거나 잠금을 해제합니다.

파일 시스템 잠금

파일 시스템을 잠그려면 DD Encryption을 활성화하고 파일 시스템을 비활성화해야 합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 선택하고 **Lock File System**을 클릭합니다.
2. Lock File System 대화 상자의 텍스트 필드에 다음을 입력합니다.
   - 보안 책임자 계정(해당 Data Domain 시스템의 보안 사용자 그룹에 속한 권한이 부여된 사용자)의 사용자 이름 및 암호
   - 현재 암호와 새 암호
3. **OK**를 클릭합니다.

   이 절차는 암호화 키를 새 암호로 다시 암호화합니다. 이 프로세스는 현재 암호의 캐싱된 복제본(인메모리(in-memory) 및 온디스크)을 제거합니다.

   참고

   암호를 변경하려면 부적절한 직원이 데이터를 폐기할 가능성을 막기 위한 두 사용자의 인증이 필요합니다.

   ⚠ 주의

   암호를 세심하게 관리해야 합니다. 암호를 분실하면 다시는 파일 시스템을 잠금 해제하여 데이터를 액세스할 수 없습니다. 데이터가 영구적으로 손실됩니다.
4. 시스템을 종료합니다.

   ⚠ 주의

   섀시 전원 스위치를 사용하여 시스템 전원을 끄지 마십시오. 대신 명령 프롬프트에 다음 명령을 입력합니다.

   ```
   # system poweroff The 'system poweroff' command shuts down
   the system and turns off the power. Continue? (yes|no|?)
   [no]:
   ```
5. 시스템을 전송하거나 교체 중인 디스크를 제거합니다.
6. 시스템 전원을 켜고 파일 시스템의 잠금을 풀기 위한 절차를 따릅니다.

파일 시스템 잠금 해제

이 절차를 통해 암호화된 파일 시스템이 대상에 도착한 후 이를 사용할 준비를 합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 선택하고 **Unlock File System**을 클릭합니다.
2. 텍스트 필드에 파일 시스템을 잠그는 데 사용한 암호를 입력합니다.
3. **OK**를 클릭합니다.

4. **Close**를 클릭하여 종료합니다.

   암호가 잘못된 경우에는 파일 시스템이 시작되지 않고 시스템에서 오류를 보고합니다. 이전 단계의 지시에 따라 올바른 암호를 입력합니다.

암호화 알고리즘 변경

필요한 경우 암호화 알고리즘을 재설정하거나 새 데이터 및 기존 데이터 또는 새 데이터만 암호화하는 옵션을 선택합니다.

절차

1. **Data Management** > **File System** > **Encryption**을 선택합니다.
2. Data Domain 시스템을 암호화하는 데 사용되는 암호화 알고리즘을 변경하려면 **Change Algorithm**을 클릭합니다.

   Change Algorithm 대화 상자가 표시됩니다. 지원되는 암호화 알고리즘은 다음과 같습니다.

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. 드롭다운 목록에서 암호화 알고리즘을 선택하거나 기본값인 AES 256비트(CBC)를 적용합니다.

   AES 256비트 GCM(Galois/Counter Mode)이 가장 안전한 알고리즘이지만 CBC(Cipher Block Chaining) 모드에 비해 상당히 느립니다.

   참고

   알고리즘을 기본 AES 256비트(CBC)로 재설정하려면 Reset to default를 클릭합니다.

4. 암호화할 데이터를 결정합니다.

   - 시스템의 기존 데이터와 새 데이터를 암호화하려면 **Apply to Existing data, Restart file system now**를 선택하고 **OK**를 클릭합니다.
     파일 시스템이 다시 시작된 후 첫 번째 정리 주기 동안 기존 데이터가 암호화됩니다.

     참고

     기존 데이터의 암호화는 표준 파일 시스템 정리 작업보다 오래 걸릴 수 있습니다.

   - 새 데이터만 암호화하려면 **Restart file system now**를 선택하고 **OK**를 클릭합니다.

5. 상태가 표시됩니다. 프로세스가 완료되면 **Close**를 클릭합니다.

   참고

   파일 시스템이 다시 시작되는 동안 애플리케이션이 중단될 수 있습니다.