SANtricity 소프트웨어 11.8 설명서

SANtricity software

NetApp
August 22, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/e-series-santricity-118/index.html on August 22, 2025. Always check docs.netapp.com for the latest.

목차

SANtricity 소프트웨어 11.8 설명서 1
릴리스 정보 2
SANtricity OS 11.80의 새로운 기능 2
버전 11.80.1R4의 새로운 기능 2
버전 11.80.1R3의 새로운 기능 2
버전 11.80.1R2의 새로운 기능 2
버전 11.80.1R1의 새로운 기능 2
버전 11.80.1의 새로운 기능 2
버전 11.80의 새로운 기능 3
릴리스 정보 5
시작하십시오 6
SANtricity 소프트웨어 개요 6
SANtricity 시스템 관리자 6
SANtricity 유니파이드 관리자 7
지원되는 브라우저 및 운영 체제 9
브라우저 9
운영 체제 9
SANtricity 시스템 관리자 설정 10
SANtricity 시스템 관리자에 액세스합니다 10
설정 마법사 개요 11
FAQ 를 참조하십시오 12
SANtricity Unified Manager 설정 14
SANtricity Unified Manager를 설치합니다 14
SANtricity Unified Manager에 액세스합니다 14
SANtricity System Manager 11.8를 사용한 단일 어레이 관리 15
기본 인터페이스 15
SANtricity System Manager 인터페이스 개요 15
성능 데이터를 봅니다 16
스토리지 계층 구조 보기 25
인터페이스 설정을 관리합니다 26
알림을 관리합니다 29
FAQ 를 참조하십시오 33
풀 및 볼륨 그룹 37
풀 및 볼륨 그룹 개요 37
개념 38
스토리지를 구성합니다 46
스토리지 관리 58
풀 및 그룹 설정을 수정합니다 63
SSD 캐시를 관리합니다 70

예약된 용량을 관리합니다 76
FAQ 를 참조하십시오 85
볼륨 및 워크로드 97
볼륨 및 워크로드 개요 97
개념 98
스토리지를 구성합니다 113
볼륨 관리 123
설정을 관리합니다 129
복사 서비스를 사용합니다 137
FAQ 를 참조하십시오 143
호스트 및 호스트 클러스터 147
호스트 및 호스트 클러스터 개요 147
개념 148
호스트 액세스를 구성합니다 151
호스트 및 클러스터 관리 156
설정을 관리합니다 158
FAQ 를 참조하십시오 161
스냅샷 수 164
스냅샷 개요 164
개념 166
스냅샷 및 스냅샷 객체를 생성합니다 176
스냅샷 스케줄을 관리합니다 188
스냅샷 이미지를 관리합니다 190
스냅샷 정합성 보장 그룹을 관리합니다 195
스냅샷 볼륨 관리 199
FAQ 를 참조하십시오 204
미러링 207
개요 207
비동기 개념 209
동기화 개념 219
비동기식 미러 정합성 보장 그룹을 관리합니다 227
비동기 미러링 쌍을 관리합니다 233
동기화 미러링 페어를 관리합니다 237
미러링을 비활성화합니다 240
Async FAQ를 참조하십시오 241
동기화 FAQ 246
원격 스토리지 249
원격 스토리지 기능 개요 249
개념 250
원격 스토리지 관리 254
FAQ 를 참조하십시오 258

하드웨어 구성 요소 260
하드웨어 구성 요소 개요 260
관련 정보 261
개념 261
쉘프 구성요소 관리 270
컨트롤러 관리 274
복구 작업을 수행합니다 515
AutoSupport 관리 517
이벤트를 봅니다 523
업그레이드 관리 526
FAQ 를 참조하십시오 538
SANtricity Unified Manager 6을 통한 다중 어레이 관리 544
기본 인터페이스 544
SANtricity Unified Manager 인터페이스 개요 544
지원되는 브라우저 545
관리자 암호 보호를 설정합니다 545
admin 암호를 변경합니다 546
세션 시간 제한을 관리합니다 547
지원합니다 547
검색 개요 547
개념 548
스토리지를 검색합니다 549
스토리지 관리 552
설정을 가져옵니다 554
설정 가져오기 개요 554
개념 555
일괄 가져오기를 사용합니다 557
FAQ 를 참조하십시오 561
스토리지 그룹 562
그룹 개요 562
스토리지 어레이 그룹을 구성합니다 562
그룹에서 스토리지 배열을 제거합니다 563
스토리지 어레이 그룹을 삭제합니다 563
스토리지 그룹 이름을 바꿉니다 564
업그레이드 564
업그레이드 센터 개요 564
소프트웨어 및 펌웨어를 업그레이드합니다 566

SANtricity 소프트웨어 11.8 설명서

릴리스 정보

SANtricity OS 11.80의 새로운 기능

다음 표에서는 SANtricity System Manager 11.8의 새로운 기능에 대해 설명합니다.

버전 11.80.1R4의 새로운 기능

이 버전에는 사소한 변경 사항만 포함되어 있으며 새로운 기능이나 제한 사항은 없습니다. 이 릴리스의 변경 사항에 대한 자세한 내용은 README 파일을 참조하십시오.

버전 11.80.1R3의 새로운 기능

이 버전에는 사소한 변경 사항만 포함되어 있으며 새로운 기능이나 제한 사항은 없습니다. 이 릴리스의 변경 사항에 대한 자세한 내용은 README 파일을 참조하십시오.

버전 11.80.1R2의 새로운 기능

이 버전에는 사소한 변경 사항만 포함되어 있으며 새로운 기능이나 제한 사항은 없습니다. 이 릴리스의 변경 사항에 대한 자세한 내용은 README 파일을 참조하십시오.

버전 11.80.1R1의 새로운 기능

새로운 기능	설명
자체 서명된 새 관리 인증서와 CA 서명 관리 인증서의 키 크기가 늘어납니다.	SANtricity System Manager 및 Unified Manager 애플리케이션 자체 서명 인증서의 관리 인증서 키 크기 길이가 2048비트에서 3072비트로 수정되었습니다. 변경 사항은 SANtricity 응용 프로그램에서 새로 생성된 자체 서명 및 CA 서명 인증서에 적용됩니다. 키 길이는 고정되어 있으며 NVSRAM의 기본 키 크기 정의에 영향을 받지 않습니다.

버전 11.80.1의 새로운 기능

새로운 기능	설명
`-identifyDevices` 매개 변수입니다	이제 SMcli에서 새 `-identifyDevices` 매개 변수를 사용할 수 있습니다. 이 새로운 매개변수를 사용하여 스토리지 배열과 연결된 모든 SCSI 기본 블록 장치를 찾을 수 있습니다. 자세한 내용은 을 "다운로드 가능한 SMcli 명령줄 매개변수"참조하십시오.
이더넷 커널 통계	이제 System Manager의 iSCSI 통계 패키지 보기 페이지에서 새 이더넷 커널 통계 옵션을 사용할 수 있습니다. 이 새로운 옵션을 사용하면 iSCSI 장치의 플랫폼 커널 드라이버에 대한 통계를 볼 수 있습니다. 자세한 내용은 을 "iSCSI 통계 패키지를 봅니다"참조하십시오.

새로운 기능	설명
REST API 엔드포인트를 통해 IP 주소를 차단하는 기능이 추가되었습니다	이제 사용자는 설정 끝점을 통해 특정 IP 주소를 차단할 수 (`/devmgr/v2/settings`있습니다. 설정 엔드포인트를 통해 구성한 후에는 화이트리스트를 통해 지정된 IP 주소만 스토리지 디바이스와 통신할 수 있습니다. 이 새로운 기능은 IPv4 및 IPv6 주소 목록을 지원합니다.
vCenter 스토리지 플러그인	vCenter Storage 플러그인이 E-Series 11.80.1 릴리즈와의 호환성을 위해 업데이트되었습니다.
웹 서비스 프록시	E-Series 11.80.1 릴리즈와의 호환성을 위해 웹 서비스 프록시가 버전 6.1로 업데이트되었습니다.

버전 **11.80**의 새로운 기능

새로운 기능	설명
향상된 볼륨 패리티 검사	이제 REST API 또는 CLI를 통해 볼륨 패리티 검사를 백그라운드 프로세스로 시작할 수 있습니다. 결과 패리티 검사는 스캔 작업을 완료하는 데 필요한 한 백그라운드에서 실행됩니다. 스캔 작업은 컨트롤러 재부팅 및 페일오버 작업에 영향을 줍니다.
Unified Manager를 위한 SAML 지원	Unified Manager는 이제 SAML(Security Assertion Markup Language)을 지원합니다. Unified Manager에 대해 SAML이 활성화된 경우 사용자는 ID 공급자에 대해 다중 요소 인증을 사용하여 사용자 인터페이스와 상호 작용해야 합니다. SAML이 Unified Manager에서 활성화된 후에는 IDP를 통해 요청을 인증하지 않고 REST API를 사용할 수 없습니다.
자동 구성 기능	이제 초기 어레이 설정을 위해 자동 구성 기능과 함께 사용할 볼륨 블록 크기 매개 변수를 설정하는 기능이 지원됩니다. 이 기능은 CLI에서만 "blocksize" 매개 변수로 사용할 수 있습니다.
컨트롤러 펌웨어 암호화 서명	컨트롤러 펌웨어가 암호로 서명됩니다. 서명은 초기 다운로드 및 각 컨트롤러 부팅 중에 검사됩니다. 최종 사용자에게 미치는 영향이 예상되지 않습니다. 서명은 CA에서 발급한 Extended Validation 인증서를 통해 백업됩니다.
드라이브 펌웨어 암호화 서명	드라이브 펌웨어가 암호로 서명되었습니다. 서명은 초기 다운로드 중에 확인되며 CA에서 발급한 Extended Validation 인증서를 통해 백업됩니다. 이제 드라이브 펌웨어 컨텐츠가 ZIP 파일로 전달되며, 여기에는 기존의 서명되지 않은 펌웨어와 새로 서명된 펌웨어가 포함됩니다. 사용자는 대상 시스템에서 실행 중인 코드의 릴리스 버전을 기반으로 적절한 파일을 선택해야 합니다.

새로운 기능	설명

외부 키 서버 관리 - 인증서 키 크기	새 기본 인증서 키 크기는 3072비트(2048비트)입니다. 최대 4096비트의 키 크기가 지원됩니다. 기본값이 아닌 키 크기를 지원하려면 NVSRAM 비트를 변경해야 합니다.
	
	키 크기 선택 값은 다음과 같습니다.
	
	• 기본값 = 0
	• 길이 2048 = 1
	• 길이 3072 = 2
	• 길이 4096 = 3
	
	SMcli를 통해 키 크기를 4096으로 변경하려면:
	
	`set controller[b] globalnvsrambyte[0xc0]=3;`
	`set controller[a] globalnvsrambyte[0xc0]=3;`
	
	키 크기 조회:
	
	`show allcontrollers globalnvsrambyte[0xc0];`

Disk Pool 기능 향상	11.80 이상을 실행하는 컨트롤러로 생성된 디스크 풀은 _ 버전 0_pool과 달리 _ 버전 1_pool입니다. 버전 1_ 디스크 풀이 있으면 다운그레이드 작업이 제한됩니다. 디스크 풀의 버전은 스토리지 배열 프로파일에서 확인할 수 있습니다.
최소 브라우저 요구 사항이 충족되지 않으면 System Manager 및 Unified Manager가 실행되지 않습니다	System Manager 또는 Unified Manager를 실행하기 전에 브라우저의 최소 버전이 필요합니다. 다음은 지원되는 최소 버전입니다. • Firefox 최소 버전 80 • Chrome 최소 버전 89 • 모서리 최소 버전 90 • Safari 최소 버전 14
FIPS 140-3개 NVMe SSD 드라이브 지원	이제 NetApp 인증 FIPS 140-3의 NVMe SSD 드라이브가 지원됩니다. 스토리지 어레이 프로필 및 System Manager에서 올바르게 식별됩니다.
EF300 및 EF600에서 SSD 읽기 캐시 지원	이제 SAS 확장 시 HDD를 사용하는 EF300 및 EF600 컨트롤러에서 SSD 읽기 캐시가 지원됩니다.
EF300 및 EF600에서 iSCSI 및 파이버 채널 비동기 원격 미러링 지원	이제 ARVM(비동기식 원격 미러링)이 NVMe 및 SAS 기반 볼륨을 사용하는 EF300 및 EF600 컨트롤러에서 지원됩니다.

새로운 기능	설명
기본 트레이에 드라이브 없이 EF300 및 EF600 지원	이제 기본 트레이에 NVMe 드라이브가 없는 EF300 및 EF600 컨트롤러 구성이 지원됩니다.
모든 플랫폼에 대해 USB 포트가 비활성화되었습니다	이제 모든 플랫폼에서 USB 포트가 비활성화되었습니다.

릴리스 정보

릴리스 정보는 이 사이트 외부에서 사용할 수 있습니다. NetApp Support 사이트 자격 증명을 사용하여 로그인하라는 메시지가 표시됩니다.

- "11.80 릴리스 정보"
- "11.70 릴리스 정보"
- "11.60 릴리스 정보"
- "11.50 릴리스 정보"

시작하십시오

SANtricity 소프트웨어 개요

E-Series 시스템에는 스토리지 프로비저닝 및 기타 작업을 위한 SANtricity 소프트웨어가 포함되어 있습니다.

이 사이트에서는 다음 SANtricity 관리 인터페이스를 사용하는 방법을 설명합니다.

- System Manager — 네트워크에서 개별 스토리지 어레이를 관리하는 데 사용되는 웹 기반 인터페이스입니다.
- Unified Manager — 네트워크의 모든 스토리지 어레이를 보고 관리하는 데 사용되는 웹 기반 인터페이스입니다.

EF600 및 EF300 스토리지 어레이는 동기식 미러링 또는 씬 볼륨을 지원하지 않습니다.

SANtricity 시스템 관리자

System Manager는 각 컨트롤러에 내장된 웹 기반 관리 소프트웨어입니다. 사용자 인터페이스에 액세스하려면 브라우저에서 컨트롤러의 IP 주소를 가리킵니다. 설치 마법사를 사용하면 시스템 구성을 시작할 수 있습니다.

System Manager는 다음과 같은 다양한 관리 기능을 제공합니다.

* 성능 *
I/O 지연 시간, IOPS, CPU 활용률, 처리량을 비롯하여 최대 30일 성능 데이터를 봅니다.
* 스토리지 *
풀 또는 볼륨 그룹을 사용하여 스토리지를 프로비저닝하고 애플리케이션 워크로드를 생성합니다.
* 데이터 보호 *
스냅샷, 볼륨 복사본 및 원격 미러링을 사용하여 백업 및 재해 복구를 수행합니다.

* 하드웨어 *
구성 요소 상태를 확인하고 이러한 구성 요소와 관련된 일부 기능(예: 핫 스페어 드라이브 할당)을 수행합니다.
* 알림 *
스토리지 시스템에서 발생하는 중요한 이벤트에 대해 관리자에게 알립니다. 알림은 이메일, SNMP 트랩 및 syslog를 통해 보낼 수 있습니다.
* 액세스 관리 *
사용자가 할당된 자격 증명을 사용하여 시스템에 로그인해야 하는 사용자 인증을 구성합니다.
* 시스템 설정 *
SSD 캐시 및 자동 로드 밸런싱과 같은 다른 시스템 성능 기능을 구성합니다.
* 지원 *
진단 데이터를 보고, 업그레이드를 관리하고, AutoSupport를 구성하여 스토리지 어레이의 상태를 모니터링하고, 자동 디스패치를 기술 지원 부서에 보냅니다.

SANtricity 유니파이드 관리자

Unified Manager는 전체 도메인을 관리하는 데 사용되는 웹 기반 소프트웨어입니다. 중앙 뷰에서 E2800, EF280, EF300, E5700, EF570, 기타 최신 E-Series 및 EF-Series 어레이의 상태를 확인할 수 있습니다. EF600을 지원합니다. 선택한 스토리지 배열에 대해 배치 작업을 수행할 수도 있습니다.

Unified Manager는 웹 서비스 프록시와 함께 관리 서버에 설치됩니다. Unified Manager에 액세스하려면 브라우저를 열고 웹 서비스 프록시가 설치된 서버를 가리키는 URL을 입력합니다.

Unified Manager는 다음과 같은 다양한 관리 기능을 제공합니다.

* 스토리지 어레이 검색 *

조직의 네트워크에서 관리할 스토리지 어레이를 찾아 추가합니다. 그런 다음 단일 페이지에서 모든 스토리지 어레이의 상태를 볼 수 있습니다.

* 시작 *

System Manager의 인스턴스를 열어 특정 스토리지 어레이에 대한 개별 관리 작업을 수행합니다.

* 설정 가져오기 *

경고, AutoSupport 및 디렉토리 서비스에 대한 설정을 포함하여 하나의 스토리지 어레이에서 여러 어레이로 일괄 가져오기를 수행합니다.

* 미러링 *

두 스토리지 시스템 간에 비동기식 또는 동기식 미러링 쌍을 구성합니다.

* 그룹 관리 *

스토리지 배열을 그룹으로 구성하여 보다 쉽게 관리할 수 있습니다.

* 업그레이드 센터 *

여러 스토리지 어레이에서 SANtricity OS 소프트웨어를 업그레이드합니다.

인증서
CSR(인증서 서명 요청)을 생성하고 인증서를 가져오고 여러 스토리지 어레이에 대한 기존 인증서를 관리합니다.
* 액세스 관리 *
할당된 자격 증명을 사용하여 Unified Manager에 로그인해야 하는 사용자 인증을 구성합니다.

지원되는 브라우저 및 운영 체제

SANtricity 소프트웨어는 다양한 유형의 브라우저와 운영 체제를 지원합니다.

브라우저

다음 브라우저 및 버전이 지원됩니다.

브라우저	최소 버전
Google Chrome	89
Mozilla Firefox	80
사파리	14
Microsoft Edge를 참조하십시오	90

Unified Manager의 경우 웹 서비스 프록시를 설치하고 브라우저에서 사용할 수 있어야 합니다. 자세한 내용은 을 참조하십시오 "SANtricity 웹 서비스 프록시 개요"

운영 체제

지원되는 운영 체제 및 버전은 다음과 같습니다.

운영 체제	최소 버전/아키텍처
Red Hat Enterprise Linux(RHEL)	8.x(SP8), 9.x(SP2)/64비트
SUSE Linux Enterprise Server(SLES)	12.x(SP4, SP5), 15.x(SP4, SP5)/64비트

운영 체제	최소 버전/아키텍처
Oracle Linux(OL)	8.x(U8), 9.x(U2)/64비트
Windows Server를 선택합니다	2019, 2022/64비트
우분투	20.04, 22.04/64비트

SANtricity 시스템 관리자 설정

SANtricity 시스템 관리자에 액세스합니다

SANtricity System Manager 사용자 인터페이스에 액세스하려면 브라우저에서 컨트롤러의 IP 주소를 지정하면 됩니다. 설치 마법사를 사용하면 시스템 구성을 시작할 수 있습니다.

시작하기 전에

- Express 구성 가이드 중 하나에 설명된 대로 하드웨어를 설치 및 구성합니다.
  - "Linux Express 구성"
  - "VMware Express 구성"
  - "Windows Express 구성"
- 다음 요구 사항을 충족하는 관리 스테이션을 구성합니다.
  - 1Gbps 이상의 네트워크에 연결되었습니다.
  - 스토리지 관리 포트와 동일한 서브넷에 연결됩니다.
  - 데이터 관리에 사용되는 호스트(I/O 연결)가 아닌 별도의 스테이션으로 사용됩니다.
  - 스토리지 관리 스테이션에서 컨트롤러에 대한 이더넷 연결을 통해 스토리지 시스템에 명령을 전송하는 대역외 관리를 설정합니다.
  - 지원되는 브라우저를 사용하여 설정합니다. 을 "지원되는 브라우저 및 운영 체제"참조하십시오.

단계

1. 브라우저에서 다음 URL을 입력합니다. `https://<IPAddress>`

   `IPAddress` 스토리지 배열 컨트롤러 중 하나의 주소입니다.

   구성되지 않은 어레이에서 System Manager를 처음 열면 Set Administrator Password 프롬프트가 나타납니다.

2. 관리자 암호 설정 및 암호 확인 필드에 관리자 역할에 대한 System Manager 암호를 입력한 다음 * 암호 설정 * 을 클릭합니다.

   처음 로그인할 때 설정 마법사가 시작됩니다.

3. 설정 마법사를 사용하여 다음 작업을 수행합니다.
   - * 하드웨어(컨트롤러 및 드라이브) 확인 * — 스토리지 배열의 컨트롤러 및 드라이브 수를 확인합니다. 어레이에 이름을 할당합니다.

- * 호스트 및 운영 체제 확인 * — 스토리지 배열이 액세스할 수 있는 호스트 및 운영 체제 유형을 확인합니다.
- * 풀 수락 * — 빠른 설치 방법에 대해 권장되는 풀 구성을 수락합니다. 풀은 드라이브의 논리적 그룹입니다.
- * 경고 구성 * — 스토리지 배열에 문제가 발생하면 System Manager가 자동 알림을 수신할 수 있도록 합니다.
- * AutoSupport 활성화 * — 스토리지 어레이의 상태를 자동으로 모니터링하고 기술 지원 부서에 디스패치를 보냅니다.

설치 마법사에 대한 자세한 내용은 를 "설치 마법사 개요"참조하십시오.

설정 마법사 개요

설치 마법사를 사용하여 하드웨어, 호스트, 애플리케이션, 워크로드 등 스토리지 시스템을 구성합니다. 풀, 알림 및 AutoSupport

최초 설정

System Manager를 처음 열면 설정 마법사가 시작됩니다. 설치 마법사는 스토리지 배열 이름 지정, 호스트 구성, 애플리케이션 선택 및 스토리지 풀 생성 등의 기본 구성 작업을 수행하라는 메시지를 표시합니다.

초기 설정을 계속하기 전에 업그레이드 센터(메뉴: 지원 [업그레이드 센터])로 이동하여 SANtricity OS 소프트웨어가 최신 버전인지 확인하십시오. 필요한 경우 최신 버전으로 업그레이드하고 브라우저를 새로 고쳐 설치를 계속합니다. 자세한 내용은 을 "업그레이드 센터 개요"참조하십시오.

마법사를 취소하면 수동으로 다시 시작할 수 없습니다. System Manager를 열거나 브라우저를 새로 고치면 마법사가 자동으로 다시 시작되고, 다음 중 _ 개 이상의 조건이 충족됩니다.

- 풀 및 볼륨 그룹이 감지되지 않습니다.
- 감지된 워크로드가 없습니다.
- 알림이 구성되지 않았습니다.

용어

설치 마법사는 다음 용어를 사용합니다.

기간	설명
공유합니다	애플리케이션은 Microsoft SQL Server 또는 Microsoft Exchange와 같은 소프트웨어 프로그램입니다.
경고	알림은 스토리지 시스템에서 발생하는 중요한 이벤트를 관리자에게 알립니다. 알림은 이메일, SNMP 트랩 또는 syslog를 통해 보낼 수 있습니다.
AutoSupport	AutoSupport 기능은 스토리지 배열의 상태를 모니터링하고 자동 디스패치를 기술 지원 부서에 보냅니다.
하드웨어	스토리지 시스템 하드웨어에는 스토리지 어레이, 컨트롤러 및 드라이브가 포함됩니다.

기간	설명
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.
오브젝트	개체는 논리적 또는 물리적 스토리지 구성 요소입니다. 논리적 객체에는 볼륨 그룹, 풀 및 볼륨이 포함됩니다. 물리적 객체에는 스토리지 어레이, 어레이 컨트롤러, 호스트 및 드라이브가 포함됩니다.
수영장	풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)
볼륨	볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다. 볼륨은 풀 또는 볼륨 그룹에서 사용할 수 있는 용량에서 생성됩니다. 볼륨에 정의된 용량이 있습니다. 볼륨이 두 개 이상의 드라이브로 구성될 수 있지만 볼륨은 호스트에 하나의 논리적 구성 요소로 나타납니다.
볼륨 그룹	볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.
워크로드	워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.

FAQ 를 참조하십시오

내 하드웨어 구성 요소가 모두 표시되지 않으면 어떻게 합니까?

하드웨어 확인 대화 상자에 모든 하드웨어 구성 요소가 표시되지 않으면 드라이브 쉘프가 올바로 연결되지 않았거나 스토리지 어레이에 호환되지 않는 쉘프가 설치되어 있는 것일 수 있습니다.

모든 드라이브 쉘프가 올바로 연결되었는지 확인합니다. 어떤 드라이브 쉘프가 호환되는지 확실하지 않은 경우 기술 지원 팀에 문의하십시오.

모든 호스트가 표시되지 않으면 어떻게 합니까?

연결된 호스트가 표시되지 않으면 자동 감지에 실패했거나, 호스트가 잘못 연결되었거나, 현재 접속된 호스트가 없는 것입니다.

설치를 완료한 후 나중에 호스트를 구성할 수 있습니다. 다음과 같이 호스트를 수동으로 생성할 수 있습니다.

- 스토리지 [호스트] 메뉴로 이동하여 호스트를 수동으로 생성하고 적절한 호스트 포트 식별자를 연결할 수 있습니다. 수동으로 생성된 호스트는 * 초기 설정 * 마법사에도 표시됩니다.
- 호스트와 호스트는 호스트 포트 유형(예: iSCSI 또는 NVMe over RoCE)에 맞게 구성해야 하며 자동 탐지 기능이 작동되기 전에 설정된 스토리지에 대한 세션도 구성해야 합니다.

애플리케이션을 식별하면 스토리지 어레이를 관리하는 데 어떤 도움이 됩니까**?**

애플리케이션이 있는 경우 SANtricity System Manager에서는 애플리케이션 유형에 따라 스토리지를 최적화하는 볼륨 구성을 자동으로 권장합니다.

애플리케이션별로 볼륨을 최적화하면 데이터 스토리지 운영 효율성을 높일 수 있습니다. 볼륨 구성에는 I/O 유형, 세그먼트 크기, 컨트롤러 소유권, 읽기 및 쓰기 캐시 같은 특성이 포함됩니다. 또한 애플리케이션 및 워크로드별로 성능 데이터를 보고 지연 시간, IOPS, MiB/s와 관련 워크로드를 평가할 수 있습니다.

워크로드란**?**

네트워크의 일부 애플리케이션(예: SQL Server 또는 Exchange)에서 해당 애플리케이션에 맞게 스토리지를 최적화하는 워크로드를 정의할 수 있습니다.

워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.

볼륨을 생성하는 동안 시스템에서 워크로드 사용에 대한 질문에 답하라는 메시지를 표시합니다. 예를 들어 Microsoft Exchange용 볼륨을 만드는 경우 필요한 메일박스 수, 평균 메일박스 용량 요구 사항, 원하는 데이터베이스 복제본 수를 묻는 메시지가 표시됩니다. 시스템에서는 이 정보를 사용하여 최적의 볼륨 구성을 생성합니다. 이 구성은 필요에 따라 편집할 수 있습니다.

AutoSupport에 대한 전달 방법을 구성하려면 어떻게 합니까**?**

AutoSupport 제공 방법에 대한 구성 작업에 액세스하려면 지원 [지원 센터] 메뉴로 이동한 다음 * AutoSupport * 탭을 클릭합니다.

HTTPS, HTTP 및 SMTP 프로토콜이 지원됩니다.

권장 풀 구성을 수락해야 하는지 어떻게 알 수 있습니까**?**

권장 풀 구성을 수락할지 여부는 몇 가지 요소에 따라 달라집니다.

다음 질문에 대답하여 요구 사항에 가장 적합한 스토리지 유형을 결정합니다.

- 용량이 더 작은 풀을 여러 개 선호하십니까?
- 풀보다 RAID 볼륨 그룹을 선호합니까?
- 권장 구성이 아닌 드라이브를 수동으로 프로비저닝하고 싶으십니까?

이러한 질문 중 하나라도 "예"로 답한 경우 권장 풀 구성을 거부하십시오.

SANtricity 시스템 관리자가 호스트를 감지하지 못했습니다**.** 어떻게 해야 합니까**?**

연결된 호스트가 표시되지 않으면 자동 감지에 실패했거나, 호스트가 잘못 연결되었거나, 현재 접속된 호스트가 없는 것입니다.

설치를 완료한 후 나중에 호스트를 구성할 수 있습니다. 다음과 같이 호스트를 수동으로 생성할 수 있습니다.

- 스토리지 [호스트] 메뉴로 이동하여 호스트를 수동으로 생성하고 적절한 호스트 포트 식별자를 연결할 수 있습니다. 수동으로 생성된 호스트는 * 초기 설정 * 마법사에도 표시됩니다.
- 호스트와 호스트는 호스트 포트 유형(예: iSCSI 또는 NVMe over RoCE)에 맞게 구성해야 하며 자동 탐지 기능이 작동되기 전에 설정된 스토리지에 대한 세션도 구성해야 합니다.

SANtricity Unified Manager 설정

SANtricity Unified Manager를 설치합니다

SANtricity Unified Manager는 NetApp E-Series 스토리지 시스템을 관리할 수 있도록 호스트 시스템에 별도로 설치된 RESTful API 서버인 웹 서비스 프록시와 함께 제공됩니다.

웹 서비스 프록시 및 Unified Manager를 설치하려면 E-Series 및 SANtricity 문서 센터에서 다음 지침을 참조하십시오.

1. "설치 및 업그레이드 요구 사항 검토"
2. "웹 서비스 프록시 파일을 다운로드하여 설치합니다"

SANtricity Unified Manager에 액세스합니다

웹 서비스 프록시를 설치한 후 SANtricity Unified Manager에 액세스하여 웹 기반 인터페이스에서 여러 스토리지 시스템을 관리할 수 있습니다.

지원되는 브라우저는 를 참조하십시오"지원되는 브라우저 및 운영 체제".

단계

1. 브라우저를 열고 다음 URL을 입력합니다.

   `http[s]://<server>:<port>/um`

   이 URL에서 는 `<server>` 웹 서비스 프록시가 설치된 서버의 IP 주소 또는 FQDN을 나타내며 `<port>` 수신 포트 번호를 나타냅니다(HTTP의 경우 8080, HTTPS의 경우 8443 기본값).

   Unified Manager 로그인 페이지가 열립니다.

2. 처음 로그인할 경우 사용자 이름에 을 입력한 `admin` 다음 admin 사용자의 암호를 설정하고 확인합니다.

   암호는 최대 30자까지 입력할 수 있습니다.

사용자 및 암호에 대한 자세한 내용은 를 "액세스 관리 작동 방식"참조하십시오.

SANtricity System Manager 11.8를 사용한 단일 어레이 관리

기본 인터페이스

SANtricity System Manager 인터페이스 개요

SANtricity System Manager는 스토리지 어레이를 단일 뷰에서 관리할 수 있는 웹 기반 인터페이스입니다.

홈 페이지

홈 페이지는 스토리지 시스템의 일일 관리를 위한 대시보드 보기를 제공합니다. System Manager에 로그인하면 홈 페이지가 첫 번째 화면으로 표시됩니다.

대시보드 뷰는 스토리지 어레이의 상태 및 상태에 대한 주요 정보가 포함된 4개의 요약 영역으로 구성됩니다. 요약 영역에서 더 많은 정보를 찾을 수 있습니다.

영역	설명
알림	알림 영역에는 스토리지 배열 및 해당 구성 요소의 상태를 나타내는 문제 알림이 표시됩니다. 또한 이 포틀릿은 스토리지 환경의 다른 영역에 영향을 주기 전에 문제를 해결하는 데 도움이 되는 자동화된 경고를 표시합니다.
성능	Performance(성능) 영역에서 시간에 따른 리소스 사용량을 비교하고 대조할 수 있습니다. 응답 시간(IOPS), 전송 속도(MiB/s) 및 사용 중인 처리 용량(CPU)에 대한 스토리지 시스템의 성능 메트릭을 볼 수 있습니다.
용량	용량 영역에는 스토리지 배열에서 할당된 용량, 사용 가능한 스토리지 용량 및 할당되지 않은 스토리지 용량에 대한 차트 보기가 표시됩니다.
스토리지 계층 구조입니다	스토리지 계층 영역은 스토리지 배열에 의해 관리되는 다양한 하드웨어 구성 요소 및 스토리지 개체에 대한 체계적인 보기를 제공합니다. 드롭다운 화살표를 클릭하여 해당 하드웨어 구성 요소 또는 스토리지 개체에 대한 특정 작업을 수행합니다.

인터페이스 설정

기본 인터페이스에서 디스플레이 기본 설정 및 기타 설정을 변경할 수 있습니다.

설정	설명
기본 설정을 표시합니다	인터페이스의 오른쪽 위에 있는 기본 설정 드롭다운에서 용량 값 및 기간을 변경합니다.
세션 시간 초과	지정된 시간 후에 사용자의 비활성 세션의 연결이 끊길 수 있도록 시간 제한을 구성합니다.

설정	설명
도움말	인터페이스의 오른쪽 위 모서리에 있는 드롭다운 메뉴에서 도움말 설명서 및 기타 리소스에 액세스합니다.

사용자 로그인 및 암호

시스템에 로그인한 현재 사용자가 인터페이스의 오른쪽 상단에 표시됩니다.

사용자 및 암호에 대한 자세한 내용은 다음을 참조하십시오.

- "관리자 암호 보호를 설정합니다"
- "암호를 변경합니다"

성능 데이터를 봅니다

성능 개요

성능 페이지를 사용하면 스토리지 배열의 성능을 쉽게 모니터링할 수 있습니다.

성능 데이터로부터 배울 수 있는 것은 무엇입니까**?**

성능 그래프와 표는 성능 데이터를 거의 실시간으로 보여 주며, 이를 통해 스토리지 어레이에 문제가 있는지 여부를 확인할 수 있습니다. 성능 데이터를 저장하여 스토리지 배열의 기간별 뷰를 구성하고 문제가 시작된 시기 또는 문제가 발생한 원인을 파악할 수도 있습니다.

자세한 내용:

- "성능 그래프 및 지침"
- "성능 조건"

성능 데이터는 어떻게 볼 수 있습니까**?**

성능 데이터는 홈 페이지 및 스토리지 페이지에서 사용할 수 있습니다.

자세한 내용:

- "그래픽 성능 데이터를 봅니다"
- "표 형식의 성능 데이터를 보고 저장합니다"
- "성능 데이터를 해석합니다"

성능 그래프 및 지침

성능 페이지에서는 여러 주요 영역에서 스토리지 어레이의 성능을 평가할 수 있는 데이터 그래프와 표를 제공합니다.

성능 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- 성능 데이터를 거의 실시간으로 확인하여 스토리지 어레이에 문제가 있는지 여부를 확인할 수 있습니다.
- 성능 데이터를 내보내 스토리지 배열의 기간별 뷰를 구성하고 문제가 시작된 시기 또는 문제가 발생한 원인을 파악합니다.
- 보려는 객체, 성능 메트릭 및 기간을 선택합니다.
- 메트릭을 비교합니다.

성능 데이터는 다음 세 가지 형식으로 볼 수 있습니다.

- * 실시간 그래픽 * — 거의 실시간으로 그래프에 성능 데이터를 표시합니다.
- * 거의 실시간 표 형식 * — 거의 실시간으로 테이블의 성능 데이터를 나열합니다.
- * 내보낸 CSV 파일 * — 추가 보기 및 분석을 위해 표 형식 성능 데이터를 쉼표로 구분된 값 파일로 저장할 수 있습니다.

성능 데이터 형식의 특성

* 성능 모니터링 유형 *	* 샘플링 간격 *	* 표시된 시간의 길이 *	* 표시되는 최대 개체 수 *	* 데이터 저장 기능 *
실시간 그래픽, 라이브 실시간 그래픽, 기록	10초(라이브) 5분(기록) 표시된 데이터 지점은 선택한 기간에 따라 다릅니다	기본 기간은 1시간입니다. 선택 사항: • 5분 • 1시간 • 8시간 • 1일 • 7일 • 30일	5	아니요
거의 실시간 테이블 형식(테이블 보기)	10초 - 1시간	가장 현재 값입니다	무제한	예
CSV(쉼표로 구분된 값) 파일	선택한 기간에 따라 다릅니다	선택한 기간에 따라 다릅니다	무제한	예

성능 데이터 보기 지침

- 성능 데이터 수집은 항상 켜져 있습니다. 이 기능을 해제하는 옵션은 없습니다.
- 샘플링 간격이 경과할 때마다 스토리지 배열이 쿼리되고 데이터가 업데이트됩니다.
- 그래픽 데이터의 경우 5분 동안의 시간 프레임에서 평균 5분 동안의 10초 업데이트를 지원합니다. 다른 모든 시간 프레임은 5분마다 업데이트되며, 선택한 시간 프레임 전체의 평균이 됩니다.
- 그래픽 뷰의 성능 데이터는 실시간으로 업데이트됩니다. 테이블 보기의 성능 데이터는 거의 실시간으로 업데이트됩니다.

- 데이터가 수집되는 동안 모니터링되는 개체가 변경되면 개체에 선택한 기간을 확장하는 전체 데이터 요소 집합이 없을 수 있습니다. 예를 들어, 볼륨 세트는 볼륨이 생성, 삭제, 할당 또는 할당되지 않을 때 변경하거나 드라이브를 추가, 제거 또는 장애가 발생할 수 있습니다.

성능 용어

스토리지 어레이에 적용되는 성능 조건에 대해 알아보십시오.

기간	설명
공유합니다	애플리케이션은 SQL 또는 Exchange와 같은 소프트웨어 프로그램입니다.
CPU	CPU는 "중앙 처리 장치"의 약어입니다. CPU는 사용 중인 스토리지 시스템의 처리 용량 비율을 나타냅니다.
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.
IOPS	IOPS는 초당 입출력 작업의 약어입니다.
지연 시간	지연 시간은 읽기 또는 쓰기 명령에 대한 요청과 호스트 또는 스토리지 시스템의 응답 사이의 시간 간격입니다.
LUN입니다	LUN(Logical Unit Number)은 호스트가 볼륨을 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다.
MIB	MIB는 mibibyte(mega binary byte)의 약어입니다. 1MiB는 220 또는 1,048,576바이트입니다. 기본 10 값을 나타내는 MB와 비교합니다. 1MB는 1,024바이트입니다.
오브젝트	개체는 논리적 또는 물리적 스토리지 구성 요소입니다. 논리적 객체에는 볼륨 그룹, 풀 및 볼륨이 포함됩니다. 물리적 객체에는 스토리지 어레이, 어레이 컨트롤러, 호스트 및 드라이브가 포함됩니다.
수영장	풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)
읽기	읽기 작업은 "읽기 작업"에 대한 짧은 것으로, 호스트가 스토리지 시스템에서 데이터를 요청할 때 발생합니다.

기간	설명
볼륨	볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다. 볼륨은 풀 또는 볼륨 그룹에서 사용할 수 있는 용량에서 생성됩니다. 볼륨에 정의된 용량이 있습니다. 볼륨이 두 개 이상의 드라이브로 구성될 수 있지만 볼륨은 호스트에 하나의 논리적 구성 요소로 나타납니다.
볼륨 이름입니다	볼륨 이름은 볼륨 생성 시 볼륨에 할당된 문자열, 기본 이름을 그대로 사용하거나 볼륨에 저장된 데이터의 유형을 나타내는 보다 설명이 포함된 이름을 제공할 수 있습니다.
볼륨 그룹	볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.
워크로드	워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.
쓰기	"쓰기 작업"에 대한 쓰기 작업이 짧아 호스트에서 스토리지에 데이터를 전송할 때 쓰기가 짧습니다.

그래픽 성능 데이터를 봅니다

논리적 오브젝트, 물리적 오브젝트, 애플리케이션 및 워크로드의 그래픽 성능 데이터를 볼 수 있습니다.

이 작업에 대해

성능 그래프에는 기록 데이터와 현재 캡처 중인 라이브 데이터가 표시됩니다. 실시간 업데이트 라고 표시된 그래프의 세로선은 기록 데이터를 라이브 데이터와 구분합니다.

- 홈 페이지 보기 *

홈 페이지에는 스토리지 레벨 성능을 보여 주는 그래프가 포함되어 있습니다. 이 보기에서 제한된 메트릭을 선택하거나 * 성능 세부 정보 보기 * 를 클릭하여 사용 가능한 모든 메트릭을 선택할 수 있습니다.

- 상세 보기 *

상세 성능 보기에서 사용할 수 있는 그래프는 다음 세 가지 탭 아래에 있습니다.

- * Logical View * — 볼륨 그룹 및 풀별로 그룹화된 논리 오브젝트의 성능 데이터를 표시합니다. 논리적 객체에는 볼륨 그룹, 풀 및 볼륨이 포함됩니다.
- * Physical View * — 컨트롤러, 호스트 채널, 드라이브 채널 및 드라이브에 대한 성능 데이터를 표시합니다.

- * 애플리케이션 및 워크로드 보기 * — 정의한 애플리케이션 유형 및 워크로드별로 그룹화된 논리적 오브젝트(볼륨) 목록을 표시합니다.

단계

1. Home * 을 선택합니다.
2. 스토리지 레벨 뷰를 선택하려면 IOPS, MiB/s 또는 CPU 버튼을 클릭합니다.
3. 자세한 내용을 보려면 * 성능 세부 정보 보기 * 를 클릭하십시오.
4. Logical View * 탭, * Physical View * 탭 또는 * Applications & 워크로드 View * 탭을 선택합니다.

   개체 유형에 따라 각 탭에 다른 그래프가 표시됩니다.

보기 탭	각 오브젝트 유형에 대한 성능 데이터가 표시됩니다
논리적 뷰	• * 스토리지 어레이 *: IOPS, MiB/s • * 풀 *: 지연 시간, IOPS, MiB/s • * 볼륨 그룹 *: 지연 시간, IOPS, MiB/s • * 볼륨 *: 지연 시간, IOPS, MiB/s
물리적 보기	• * 컨트롤러 *: IOPS, MiB/s, CPU, 여유 공간 • * 호스트 채널 *: 지연 시간, IOPS, MiB/s, 여유 공간 • * 드라이브 채널 *: 지연 시간, IOPS, MiB/s • * 드라이브 *: 지연 시간, IOPS, MiB/s
애플리케이션 및 워크로드 뷰	• * 스토리지 어레이 *: IOPS, MiB/s • * 애플리케이션 *: 지연 시간, IOPS, MiB/s • * 워크로드 *: 지연 시간, IOPS, MiB/s • * 볼륨 *: 지연 시간, IOPS, MiB/s

5. 필요한 개체 및 정보를 보려면 옵션을 사용합니다.

옵션

개체 보기 옵션	설명
문서함을 확장하여 개체 목록을 봅니다.	*Navigation* 드로어 에는 풀, 볼륨 그룹 및 드라이브와 같은 스토리지 객체가 포함됩니다. 문서함을 클릭하여 문서함의 개체 목록을 표시합니다.
보려는 객체를 선택합니다.	각 개체의 왼쪽에 있는 확인란을 선택하여 보려는 성능 데이터를 선택합니다.
필터를 사용하여 개체 이름 또는 부분 이름을 찾습니다.	필터 상자에 드로어에 있는 개체만 나열할 개체의 이름이나 부분 이름을 입력합니다.
개체를 선택한 후 * 그래프 새로 고침 * 을 클릭합니다.	문서함에서 개체를 선택한 후 * 그래프 새로 고침 * 을 선택하여 선택한 항목에 대한 그래픽 데이터를 봅니다.
그래프를 숨기거나 표시합니다	그래프를 숨기거나 표시하려면 그래프 제목을 선택합니다.

6. 필요에 따라 성능 데이터를 볼 수 있는 추가 옵션을 사용합니다.

추가 옵션

옵션을 선택합니다	설명
시간 프레임	보려는 시간(5분, 1시간, 8시간, 1일, 7일, 또는 30일). 기본값은 1시간입니다. 30일 기간 동안 성능 데이터를 로드하는 데 몇 분이 걸릴 수 있습니다. 데이터가 로드되는 동안 웹 페이지에서 멀리 이동하거나 웹 페이지를 새로 고치거나 브라우저를 닫지 마십시오.
데이터 포인트 세부 정보	그래프 위로 커서를 이동하면 특정 데이터 지점에 대한 메트릭이 표시됩니다.
스크롤 막대	그래프 아래의 스크롤 막대를 사용하여 이전 또는 이후 기간을 봅니다.
확대/축소 막대	그래프 아래에서 확대/축소 막대 핸들을 끌어 시간 범위를 축소합니다. 확대/축소 막대가 넓을수록 그래프의 상세 정보가 덜 세분됩니다. 그래프를 재설정하려면 시간 프레임 옵션 중 하나를 선택합니다.
끌어서 놓기	그래프에서 특정 시점에서 다른 지점으로 커서를 드래그하여 기간을 확대합니다. 그래프를 재설정하려면 시간 프레임 옵션 중 하나를 선택합니다.

표 형식의 성능 데이터를 보고 저장합니다

성능 그래프 데이터를 표 형식으로 보고 저장할 수 있습니다. 이렇게 하면 표시하려는 데이터를 필터링할 수 있습니다.

단계

1. 성능 데이터 그래프에서 * 테이블 보기 시작 * 을 클릭합니다.

   선택한 객체에 대한 모든 성능 데이터가 나열된 테이블이 나타납니다.

2. 필요에 따라 개체 선택 풀다운과 필터를 사용합니다.
3. 열 표시/숨기기 * 단추를 클릭하여 표에 포함할 열을 선택합니다.

   각 확인란을 클릭하여 항목을 선택하거나 선택 취소할 수 있습니다.

4. 화면 하단의 * Export * 를 선택하여 표 형식 보기를 CSV(쉼표로 구분된 값) 파일로 저장합니다.

   내보낼 행의 수와 내보내기 파일 형식(쉼표로 구분된 값 또는 CSV 형식)을 나타내는 테이블 내보내기 대화 상자가 나타납니다.

5. 다운로드를 계속하려면 * 내보내기 * 를 클릭하거나 * 취소 * 를 클릭합니다.

   브라우저 설정에 따라 파일이 저장되거나 파일의 이름과 위치를 선택하라는 메시지가 표시됩니다.

기본 파일 이름 형식은 파일을 내보낸 날짜와 시간이 포함된 입니다 `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`.

성능 데이터를 해석합니다

성능 데이터를 통해 스토리지 어레이의 성능을 튜닝할 수 있습니다.

성능 데이터를 해석할 때는 여러 요소가 스토리지 어레이의 성능에 영향을 미친다는 점을 염두에 두십시오. 다음 표에서는 고려해야 할 주요 영역에 대해 설명합니다.

성능 데이터	성능 튜닝에 미치는 영향
지연 시간(밀리초 또는 ms)	특정 객체의 입출력 작업을 모니터링합니다. 병목 현상이 있는 개체를 식별할 수 있습니다. • 볼륨 그룹이 여러 볼륨 간에 공유되는 경우, 개별 볼륨은 드라이브의 순차적 성능을 개선하고 지연 시간을 단축하기 위해 자체 볼륨 그룹이 필요할 수 있습니다. • 풀을 사용할 경우 지연 시간이 더 길어지며, 드라이브 간에 워크로드가 불균일하여 지연 시간의 가치가 더 적고 일반적으로 더 높습니다. • 드라이브 유형과 속도가 지연 시간에 영향을 미칩니다. 랜덤 I/O를 사용하면 회전식 드라이브를 더욱 빠르게 디스크의 서로 다른 위치로 이동하는 데 드는 시간이 줄어듭니다. • 드라이브 수가 너무 적으면 명령 대기 시간이 많아지고 드라이브에서 명령을 처리하는 데 더 오랜 시간이 소요되어 시스템의 일반적인 지연 시간이 길어집니다. • I/O가 클수록 데이터 전송에 따른 추가 시간 때문에 지연 시간이 길어집니다. • 지연 시간이 길수록 I/O 패턴이 자연에서 랜덤으로 나타날 수 있습니다. 랜덤 I/O가 있는 드라이브는 순차적 스트림을 사용하는 드라이브보다 지연 시간이 더 짧습니다. • 공통 볼륨 그룹의 드라이브 또는 볼륨 간 지연 시간 차이가 있으면 드라이브 속도가 느릴 수 있습니다.

성능 데이터	성능 튜닝에 미치는 영향
IOPS	IOPS 또는 IO/초(Input/Output Operation per Second)에 영향을 주는 요인은 다음과 같습니다. • 액세스 패턴(랜덤 또는 순차) • I/O 크기 • RAID 레벨 • 캐시 블록 크기 • 읽기 캐싱 설정 여부 • 쓰기 캐싱 설정 여부 • 동적 캐시 읽기 프리페치 • 세그먼트 크기 • 볼륨 그룹 또는 스토리지 배열의 드라이브 수입니다 캐시 적중률이 높을수록 입출력 속도가 높아집니다. 쓰기 캐시가 설정된 경우 해제된 경우에 비해 쓰기 입출력 속도가 더 높습니다. 개별 볼륨에 대해 쓰기 캐시를 사용할지 여부를 결정할 때 현재 IOPS와 최대 IOPS를 확인합니다. 랜덤 I/O 패턴보다 순차적 I/O 패턴의 속도가 더 높습니다. I/O 패턴과 상관없이 쓰기 캐시를 설정하여 I/O 속도를 최대화하고 애플리케이션 응답 시간을 단축합니다. 볼륨의 IOPS 통계에서 세그먼트 크기를 변경하여 성능이 향상된 것을 확인할 수 있습니다. 최적의 세그먼트 크기를 결정하거나 파일 시스템 크기 또는 데이터베이스 블록 크기를 사용하십시오.
MIB/s	전송 또는 처리 속도는 애플리케이션 입출력 크기 및 입출력 속도에 따라 결정됩니다. 일반적으로 애플리케이션 입출력 요청이 작을수록 전송 속도는 낮아지지만 입출력 속도가 빨라지고 응답 시간이 단축됩니다. 애플리케이션 I/O 요청이 클수록 처리 속도가 더 높아질 수 있습니다. 일반적인 애플리케이션 I/O 패턴을 이해하면 특정 스토리지 어레이에 대한 최대 I/O 전송 속도를 결정하는 데 도움이 됩니다.
CPU	이 값은 사용 중인 처리 용량의 백분율입니다. 동일한 유형의 객체에 대한 CPU 사용량의 차이를 확인할 수 있습니다. 예를 들어, 한 컨트롤러의 CPU 사용량이 무겁거나 시간이 지남에 따라 증가하는 반면 다른 컨트롤러의 CPU 사용량은 더 가볍고 안정적입니다. 이 경우 하나 이상의 볼륨에서 컨트롤러 소유권을 더 낮은 CPU 비율의 컨트롤러로 변경할 수 있습니다. 스토리지 배열의 CPU를 모니터링할 수 있습니다. 애플리케이션 성능이 저하되면서 CPU가 시간이 지나면서 계속 증가하는 경우 스토리지 어레이를 추가해야 할 수 있습니다. 기업에 스토리지 어레이를 추가하면 허용되는 성능 수준에서 애플리케이션 요구를 계속해서 충족할 수 있습니다.

성능 데이터	성능 튜닝에 미치는 영향
여유 공간	여유 공간은 컨트롤러, 컨트롤러 호스트 채널 및 컨트롤러 드라이브 채널의 나머지 성능 기능을 나타냅니다. 이 값은 백분율로 표현되며 이러한 개체가 제공할 수 있는 최대 성능과 현재 성능 수준 사이의 간격을 나타냅니다. • 컨트롤러의 경우 여유 공간은 최대 IOPS의 비율입니다. • 채널의 여유 공간은 최대 처리량 또는 MiB/s의 비율입니다 이 계산에는 읽기 처리량, 쓰기 처리량, 양방향 처리량이 포함됩니다.

스토리지 계층 구조 보기

기본 인터페이스의 스토리지 계층 구조는 스토리지 배열에 의해 관리되는 다양한 하드웨어 구성 요소 및 스토리지 개체에 대한 조직화된 보기를 제공합니다.

스토리지 계층을 보려면 홈 페이지로 이동하여 스토리지 배열 구성 요소 또는 스토리지 개체의 드롭다운 화살표를 클릭합니다. 스토리지 배열은 물리적 구성 요소와 논리적 구성 요소의 모음으로 구성됩니다.

물리적 구성 요소

스토리지 배열의 물리적 구성 요소는 이 표에 설명되어 있습니다.

구성 요소	설명
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
쉘프	쉘프는 캐비닛 또는 랙에 설치된 엔클로저입니다. 여기에는 스토리지 어레이의 하드웨어 구성 요소가 포함됩니다. 쉘프는 컨트롤러 쉘프와 드라이브 쉘프의 두 가지 유형이 있습니다. 컨트롤러 쉘프는 컨트롤러와 드라이브를 포함합니다. 드라이브 쉘프는 입/출력 모듈(IOM) 및 드라이브를 포함합니다. 스토리지 어레이에 미디어 유형 또는 인터페이스 유형이 서로 다른 경우 각 드라이브 유형에 대한 드라이브 쉘프가 표시됩니다.
드라이브	드라이브는 물리적 데이터 저장 매체를 제공하는 전자기 기계 장치 또는 솔리드 스테이트 메모리 장치입니다.
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.
호스트 버스 어댑터(HBA)	HBA(호스트 버스 어댑터)는 호스트에 상주하며 하나 이상의 호스트 포트를 포함하는 보드입니다.
호스트 포트	호스트 포트는 컨트롤러에 대한 물리적 연결을 제공하고 I/O 작업에 사용되는 호스트 버스 어댑터(HBA)의 포트입니다.

구성 요소	설명
관리 클라이언트	관리 클라이언트는 System Manager 액세스를 위해 브라우저가 설치된 컴퓨터입니다.

논리적 구성 요소

스토리지 배열의 드라이브는 데이터의 물리적 스토리지 용량을 제공합니다. System Manager를 사용하여 물리적 용량을 풀, 볼륨 그룹, 볼륨 등과 같은 논리적 구성 요소로 구성합니다. 이러한 구성 요소는 스토리지 어레이에서 데이터를 구성, 저장, 유지 관리 및 보존하는 데 사용하는 도구입니다. 스토리지 배열의 논리적 구성 요소는 이 표에 설명되어 있습니다.

구성 요소	설명
수영장	풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)
볼륨 그룹	볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.
볼륨	볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다.
LUN(Logical Unit Number)	LUN(Logical Unit Number)은 호스트가 볼륨을 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다.

인터페이스 설정을 관리합니다

암호 보호를 관리합니다

무단 액세스로부터 스토리지 배열을 보호하려면 암호를 사용하여 스토리지 배열을 구성해야 합니다.

암호를 설정하고 변경합니다

System Manager를 처음 시작하면 관리자 암호를 설정하라는 메시지가 표시됩니다. admin 암호를 가진 사용자는 개체 또는 설정을 추가, 변경 또는 제거하는 등의 스토리지 배열 구성을 변경할 수 있습니다. 초기 시작 중에 관리자 암호를 설정하려면 를 참조하십시오"System Manager에 액세스합니다".

보안을 위해 스토리지 배열이 "잠금" 상태가 되기 5회만 암호를 입력할 수 있습니다. 이 상태에서는 스토리지 배열이 후속 암호 시도를 거부합니다. 암호를 다시 입력하기 전에 스토리지 배열이 "정상" 상태로 재설정되도록 10분 정도 기다려야 합니다.

스토리지 배열에는 관리자 암호 외에 하나 이상의 역할이 매핑된 사전 정의된 사용자 프로파일이 포함됩니다. 자세한

내용은 을 "매핑된 역할에 대한 권한"참조하십시오. 사용자 프로파일과 매핑은 변경할 수 없습니다. 암호만 수정할 수 있습니다. 관리자 암호나 다른 사용자 암호를 변경하려면 를 참조하십시오"암호를 변경합니다".

세션 시간 초과 후 암호를 다시 입력합니다

단일 관리 세션 중에 암호를 입력하라는 메시지가 한 번만 표시됩니다. 그러나 30분 동안 사용하지 않으면 세션 시간이 초과되며, 이 경우 암호를 다시 입력해야 합니다. 세션이 진행되는 동안 다른 관리 클라이언트에서 동일한 스토리지 배열을 관리하는 다른 사용자가 암호를 변경하는 경우 다음에 구성 작업 또는 보기 작업을 시도할 때 암호를 입력하라는 메시지가 표시됩니다.

세션 시간 초과를 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다. 을 "세션 시간 제한을 관리합니다 "참조하십시오.

드라이브 또는 암호 보호를 제거합니다

암호로 보호된 드라이브를 제거하거나 암호 보호를 사용하지 않으려면 다음 사항에 유의하십시오.

- * 암호 보호 기능이 있는 드라이브를 제거하면 * — 암호는 스토리지 배열의 각 드라이브의 예약된 영역에 저장됩니다. 스토리지 배열에서 모든 드라이브를 제거하면 해당 암호가 더 이상 작동하지 않습니다. 이 상태를 해결하려면 스토리지 배열에 원래 드라이브 중 하나를 다시 설치하십시오.
- * 암호 보호 * — 명령을 더 이상 암호로 보호하지 않으려면 현재 관리자 암호를 입력하고 새 암호 텍스트 상자를 비워 둡니다.

> 스토리지 어레이에서 구성 명령을 실행하면 데이터 손실을 비롯한 심각한 손상이 발생할 수 있습니다. 따라서 스토리지 배열에 대한 관리자 암호를 항상 설정해야 합니다. 15자 이상의 영숫자로 이루어진 긴 관리자 암호를 사용하여 보안을 강화합니다.

용량 값의 기본 단위를 설정합니다

SANtricity System Manager에서는 용량 값을 기비바이트(GiB) 또는 테비바이트(TiB)로 표시할 수 있습니다.

기본 설정은 브라우저의 로컬 저장소에 저장되므로 모든 사용자가 고유한 설정을 가질 수 있습니다.

단계

1. 메뉴 선택: 기본 설정 [기본 설정 설정 설정].
2. 기비바이트 * 또는 * 테비바이트 * 의 라디오 단추를 클릭하고 작업을 수행할지 확인합니다.

   약어 및 값은 다음 표를 참조하십시오.

약어	값
GiB	$1,024^3$바이트
TiB	$1,024^4$바이트

성능 그래프의 기본 기간을 설정합니다

성능 그래프에 표시되는 기본 기간을 변경할 수 있습니다.

이 작업에 대해

홈 페이지 및 성능 페이지에 표시되는 성능 그래프는 처음에 1시간의 시간 프레임을 표시합니다. 기본 설정은 브라우저의 로컬 저장소에 저장되므로 모든 사용자가 고유한 설정을 가질 수 있습니다.

단계

1. 메뉴 선택: 기본 설정 [기본 설정 설정 설정].
2. 드롭다운 목록에서 * 5분 *, * 1시간 *, * 8시간 *, * 1일 * 또는 * 7일 * 중 하나를 선택합니다. 작업을 수행할지 확인합니다.

로그인 배너를 구성합니다

SANtricity System Manager에서 세션을 설정하기 전에 사용자에게 표시되는 로그인 배너를 생성할 수 있습니다. 배너에는 권고 통지 및 동의 메시지가 포함될 수 있습니다.

이 작업에 대해

배너를 만들면 대화 상자의 로그인 화면 앞에 나타납니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 일반 섹션에서 * 로그인 배너 구성 * 을 선택합니다.

   로그인 배너 구성 대화 상자가 열립니다.

3. 로그인 배너에 표시할 텍스트를 입력합니다.

   HTML이나 다른 태그 태그를 서식 지정에 사용하지 마십시오.

4. 저장 * 을 클릭합니다.

결과

다음에 System Manager에 로그인할 때 대화 상자에서 텍스트가 열립니다. 로그인 화면으로 계속 진행하려면 * OK * 를 클릭해야 합니다.

세션 시간 제한을 관리합니다

SANtricity System Manager에서 시간 초과를 구성하여 지정된 시간 이후에 비활성 세션의 연결을 끊을 수 있습니다.

이 작업에 대해

기본적으로 System Manager의 세션 제한 시간은 30분입니다. 이 시간을 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다.

스토리지에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하여 액세스 관리를 구성하는 경우 사용자의 SSO 세션이 최대 제한에 도달하면 세션 시간 초과가 발생할 수 있습니다. 이 문제는 System Manager 세션 시간이 초과되기 전에 발생할 수 있습니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 일반 섹션에서 * 세션 제한 시간 활성화/비활성화 * 를 선택합니다.

   Enable/Disable Session Timeout(세션 시간 제한 활성화/비활성화) 대화 상자가 열립니다.

3. 스피너 컨트롤을 사용하여 시간을 분 단위로 늘리거나 줄입니다.

   System Manager에 대해 설정할 수 있는 최소 시간 초과는 15분입니다.

   세션 시간 초과를 비활성화하려면 * Set the length of time… * 확인란을 선택 취소합니다.

4. 저장 * 을 클릭합니다.

알림을 관리합니다

문제 알림 개요

SANtricity System Manager에서는 아이콘과 여러 가지 다른 방법을 사용하여 스토리지 어레이에 문제가 있음을 알립니다.

아이콘

System Manager에서는 이러한 아이콘을 사용하여 스토리지 배열 및 해당 구성 요소의 상태를 표시합니다.

아이콘을 클릭합니다	설명
	최적
	최적이 아니거나 실패했습니다
	주의 또는 고치기 필요
	주의

System Manager는 이러한 아이콘을 다양한 위치에 표시합니다.

- 홈 페이지의 알림 영역에 실패한 아이콘과 메시지가 표시됩니다.
- 탐색 영역의 홈 페이지 아이콘에 실패한 아이콘이 표시됩니다.
- 구성 요소 페이지에서 드라이브 및 컨트롤러의 그래픽에 장애 발생 아이콘이 표시됩니다.

또한 System Manager에서는 다른 방법으로 문제를 통지합니다.

- System Manager는 SNMP 알림 또는 e-메일 오류 메시지를 보냅니다.
- 하드웨어의 서비스 작업 필요 LED가 켜집니다.

문제에 대한 알림을 받으면 Recovery Guru를 사용하여 문제를 해결하십시오. 필요한 경우 복구 단계와 함께 하드웨어 설명서를 사용하여 장애가 발생한 구성 요소를 교체합니다.

진행 중인 작업을 보고 수행합니다

장기 실행 작업을 보고 작업을 실행하려면 작업 진행 중 페이지를 사용합니다.

이 작업에 대해

작업 진행 중 페이지에 나열된 각 작업에 대해 완료 비율과 작업을 완료하는 데 남은 예상 시간이 표시됩니다. 경우에 따라 작업을 중지하거나 우선 순위가 높거나 낮은 위치에 놓을 수 있습니다. 목록에서 완료된 볼륨 복사 작업을 지울 수도 있습니다.

단계

1. 홈 페이지에서 * Show operations in progress * 를 선택합니다.

   작업 진행 중 페이지가 나타납니다.

2. 필요한 경우 작업 열의 링크를 사용하여 작업의 우선 순위를 중지하거나 변경합니다.

   특히 작업을 중지할 때 대화 상자에 제공된 모든 주의 텍스트를 읽습니다.

   볼륨 복사 작업을 중지하거나 우선 순위를 변경할 수 있습니다.

3. 볼륨 복사 작업이 완료되면 * Clear * 를 선택하여 목록에서 제거할 수 있습니다.

   작업이 완료되면 홈 페이지 상단에 정보 메시지와 노란색 렌치 아이콘이 나타납니다. 이 메시지에는 작업 진행 중 페이지에서 작업을 지울 수 있는 링크가 포함되어 있습니다.

진행 중인 작업 페이지에 표시되는 작업은 다음과 같습니다.

작동	작업의 가능한 상태입니다	수행할 수 있는 작업
볼륨 복사본	완료되었습니다	지우기
볼륨 복사본	진행 중입니다	• 우선 순위를 변경합니다 • 중지
볼륨 복사본	보류 중	지우기

작동	작업의 가능한 상태입니다	수행할 수 있는 작업
볼륨 복사본	실패했습니다	• 지우기 • 다시 복사합니다
볼륨 복사본	중지되었습니다	• 지우기 • 다시 복사합니다
볼륨 생성(64TiB보다 큰 일반 풀 볼륨만 해당)	진행 중입니다	없음
볼륨 삭제(64TiB보다 큰 일반 풀 볼륨만 해당)	진행 중입니다	없음
비동기식 미러 그룹 초기 동기화	진행 중입니다	일시 중지
비동기식 미러 그룹 초기 동기화	일시 중단됨	다시 시작
동기 미러링	진행 중입니다	일시 중지
동기 미러링	일시 중단됨	다시 시작
스냅샷 이미지 롤백	진행 중입니다	취소
스냅샷 이미지 롤백	보류 중	취소
스냅샷 이미지 롤백	일시 중지되었습니다	• 취소 • 다시 시작
드라이브 대피	진행 중입니다	취소(드라이브 배출 유형에 따라 다름)
풀 또는 볼륨 그룹에 용량을 추가합니다	진행 중입니다	없음
볼륨의 RAID 레벨을 변경합니다	진행 중입니다	없음
풀의 용량을 줄입니다	진행 중입니다	없음
씬 볼륨 재확보	진행 중입니다	없음
풀 볼륨에 대한 즉시 사용 가능 형식(iaf) 작업에 남아 있는 시간을 확인합니다	진행 중입니다	없음

작동	작업의 가능한 상태입니다	수행할 수 있는 작업
볼륨 그룹의 데이터 중복성을 확인합니다	진행 중입니다	없음
볼륨 그룹 조각 모음을 수행합니다	진행 중입니다	없음
볼륨을 초기화합니다	진행 중입니다	없음
볼륨의 용량을 늘립니다	진행 중입니다	없음
볼륨의 세그먼트 크기를 변경합니다	진행 중입니다	없음
드라이브 복사	진행 중입니다	없음
데이터 재구성	진행 중입니다	없음
카피백	진행 중입니다	없음
드라이브 지우기	진행 중입니다	없음
원격 스토리지 가져오기	진행 중입니다	• 우선 순위를 변경합니다 • 중지
원격 스토리지 가져오기	중지되었습니다	• 다시 시작 • 연결을 끊습니다
원격 스토리지 가져오기	실패했습니다	• 다시 시작 • 연결을 끊습니다
원격 스토리지 가져오기	완료되었습니다	연결을 끊습니다

Recovery Guru를 사용하여 문제를 해결합니다

Recovery Guru는 스토리지 어레이 문제를 진단하고 문제를 해결하기 위한 복구 절차를 권장하는 SANtricity System Manager의 구성 요소입니다.

단계

1. Home * 을 선택합니다.
2. 창 상단의 * Recover from_n_problems * 링크를 클릭합니다.

   Recovery Guru 대화 상자가 나타납니다.

3. 요약 목록에 표시된 첫 번째 문제를 선택한 다음 복구 절차의 지침에 따라 문제를 해결하십시오. 필요한 경우 교체 지침을 사용하여 장애가 발생한 구성 요소를 교체합니다. 나열된 각 문제에 대해 이 단계를 반복합니다.

   스토리지 시스템 내의 여러 문제를 연결할 수 있습니다. 이 경우 문제가 해결된 순서는 결과에 영향을 줄 수 있습니다. 요약 목록에 나열된 순서대로 문제를 선택하고 수정합니다.

   전원 공급 장치 캐니스터에 대한 여러 오류가 그룹화되어 요약 목록에 하나의 문제로 나열됩니다. 하나의 팬 캐니스터에 대한 여러 개의 실패도 하나의 문제로 표시됩니다.

4. 복구 절차가 성공적으로 수행되었는지 확인하려면 * 재검사 * 를 클릭합니다.

   비동기 미러 그룹 또는 비동기 미러 그룹의 구성원에 대한 문제를 선택한 경우 * Clear * 를 먼저 클릭하여 컨트롤러에서 오류를 지운 다음 * Recheck * 를 클릭하여 Recovery Guru에서 이벤트를 제거합니다.

   모든 문제가 해결되면 스토리지 배열 아이콘이 결국 주의 필요 에서 최적 으로 전환됩니다. 일부 문제의 경우 재구성 등의 작업이 진행 중인 동안 수정 아이콘이 나타납니다.

5. 선택 사항**:** Recovery Guru 정보를 파일에 저장하려면 저장 아이콘을 클릭하십시오.

   파일이 브라우저의 다운로드 폴더에 이름으로 `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`저장됩니다.

6. Recovery Guru 정보를 인쇄하려면 * 인쇄 * 아이콘을 클릭하십시오.

FAQ 를 참조하십시오

지원되는 브라우저는 무엇입니까**?**

SANtricity System Manager에서는 이러한 브라우저 버전을 지원합니다.

브라우저	최소 버전
Google Chrome	89
Mozilla Firefox	80
사파리	14
Microsoft Edge를 참조하십시오	90

키보드 바로 가기는 무엇입니까**?**

키보드만 사용하여 SANtricity System Manager 주변을 탐색할 수 있습니다.

전체 탐색

조치	바로 가기 키
다음 항목으로 이동합니다.	탭을 클릭합니다

조치	바로 가기 키
이전 항목으로 이동합니다.	Shift+Tab
항목을 선택합니다.	를 입력합니다
드롭다운 목록 — 다음 또는 이전 항목으로 이동합니다.	아래쪽 화살표 키 또는 위쪽 화살표 키를 누릅니다
확인란 — 항목을 선택합니다.	스페이스바
라디오 버튼 — 항목 간 전환	아래쪽 화살표 키 또는 위쪽 화살표 키를 누릅니다
확장 가능한 텍스트 — 항목을 확장하거나 축소합니다.	를 입력합니다

테이블 탐색

조치	바로 가기 키
행을 선택합니다.	Tab 키를 눌러 행을 선택한 다음 Enter 키를 누릅니다
위 또는 아래로 스크롤합니다.	아래쪽 화살표/위쪽 화살표 또는 Page Down/Page Up
열의 정렬 순서를 변경합니다.	Tab 키를 눌러 열 머리글을 선택한 다음 Enter 키를 누릅니다

일정 탐색

조치	바로 가기 키
이전 달로 이동합니다.	페이지 위로
다음 달로 이동한다.	페이지를 아래로 내립니다
이전 연도에 이전하십시오.	컨트롤 + 페이지 위로
내년으로 넘어가.	컨트롤 + 페이지 아래로
닫힌 경우 날짜 선택을 엽니다.	Ctrl+Home을 누릅니다
현재 달로 이동합니다.	Control/Command + Home
이전 날로 이동합니다.	Control/Command+왼쪽
다음 날로 이동한다.	Control/Command + 오른쪽

조치	바로 가기 키
이전 주로 이동합니다.	Control/Command+Up
다음 주로 이동한다.	Control/Command+Down
포커스된 날짜를 선택합니다.	를 입력합니다
날짜 선택을 닫고 날짜를 지웁니다.	제어/명령+종료
선택 없이 날짜 선택을 닫습니다.	Esc를 누릅니다

개별 볼륨의 성능 통계가 총합과 어떤 관련이 있습니까**?**

풀 및 볼륨 그룹에 대한 통계는 예약된 용량 볼륨을 비롯한 모든 볼륨을 집계하여 계산합니다.

예약된 용량은 스토리지 시스템에서 씬 볼륨, 스냅샷 및 비동기 미러링을 지원하기 위해 내부적으로 사용되며 I/O 호스트에는 표시되지 않습니다. 따라서 풀, 컨트롤러 및 스토리지 어레이 통계가 볼 수 있는 볼륨의 합으로 합산되지 않을 수 있습니다.

그러나 애플리케이션 및 워크로드 통계의 경우 표시되는 볼륨만 집계됩니다.

데이터가 그래프 및 테이블에 **0**으로 표시되는 이유는 무엇입니까**?**

그래프 및 테이블의 데이터 지점에 대해 0이 표시되면 해당 시점의 오브젝트에 대한 I/O 활동이 없다는 의미입니다. 이 상황은 호스트가 해당 객체에 대한 입출력을 시작하지 않았거나 객체 자체에 문제가 있을 수 있기 때문에 발생할 수 있습니다.

객체에 대한 기록 데이터를 계속 볼 수 있습니다. 오브젝트에 대한 I/O 활동이 시작되면 그래프 및 표에 0이 아닌 데이터가 표시됩니다.

다음 표에서는 주어진 개체에 대해 데이터 요소 값이 0인 가장 일반적인 이유를 보여 줍니다.

스토리지 레벨 객체 유형입니다	이유 데이터는 **0**으로 표시됩니다
볼륨	• 볼륨에 호스트 할당이 없습니다.
볼륨 그룹	• 볼륨 그룹을 가져오는 중입니다. • 볼륨 그룹에 호스트에 할당된 볼륨이 포함되어 있지 않습니다. * _ 및 _ * 볼륨 그룹에 예약된 용량이 없습니다.
드라이브	• 드라이브에 오류가 발생했습니다. • 드라이브가 제거되었습니다. • 드라이브가 알 수 없는 상태입니다.

스토리지 레벨 객체 유형입니다	이유 데이터는 **0**으로 표시됩니다
컨트롤러	• 컨트롤러가 오프라인 상태입니다. • 컨트롤러에 장애가 발생했습니다. • 컨트롤러가 제거되었습니다. • 컨트롤러가 알 수 없는 상태입니다.
스토리지 시스템	• 스토리지 배열에 볼륨이 포함되어 있지 않습니다.

지연 시간 그래프는 무엇을 표시합니까**?**

지연 시간 그래프는 볼륨, 볼륨 그룹, 풀에 대한 지연 시간 통계(밀리초(ms))를 워크로드에 적합합니다. 이 그래프는 Logical View, Physical View 및 Applications & 워크로드 보기 탭에 나타납니다.

지연 시간은 데이터가 읽기 또는 쓰일 때 발생하는 지연을 나타냅니다. 그래프의 한 지점 위로 커서를 가져가면 해당 시점에 대한 다음 값(밀리초(ms))이 표시됩니다.

- 읽기 시간.
- 쓰기 시간.
- 평균 I/O 크기

IOPS 그래프에 표시되는 것은 무엇입니까**?**

IOPS 그래프에는 초당 입출력 작업에 대한 통계가 표시됩니다. 홈 페이지에서 이 그래프는 스토리지 배열에 대한 통계를 표시합니다. Logical View, Physical View, Applications & 워크로드 성능 타일의 보기 탭에서 이 그래프는 스토리지, 볼륨, 볼륨 그룹, 풀, 애플리케이션에 대한 통계를 표시합니다. 보장합니다.

IOPS는 초당 _INPUT/OUTPUT(I/O) 작업의 약어입니다. 그래프의 한 지점 위로 커서를 가져가면 해당 시점에 대한 다음 값을 볼 수 있습니다.

- 읽기 작업 수입니다.
- 쓰기 작업 수입니다.
- 총 읽기 및 쓰기 작업이 결합되었습니다.

MiB/s 그래프는 무엇을 표시합니까**?**

MiB/s 그래프는 전송 속도 통계를 초당 메비바이트 단위로 표시합니다. 홈 페이지에서 이 그래프는 스토리지 배열에 대한 통계를 표시합니다. Logical View, Physical View, Applications & 워크로드 성능 타일의 보기 탭에서 이 그래프는 스토리지, 볼륨, 볼륨 그룹, 풀, 애플리케이션에 대한 통계를 표시합니다. 보장합니다.

MIB/s는 초당 *mebytes* 또는 1,048,576바이트의 약어입니다. 그래프의 한 지점 위로 커서를 가져가면 해당 시점에 대한

다음 값을 볼 수 있습니다.

- 읽은 데이터의 양
- 기록된 데이터의 양
- 읽고 쓴 데이터의 총 양입니다.

CPU 그래프에 표시되는 것은 무엇입니까**?**

CPU 그래프는 각 컨트롤러(컨트롤러 A 및 컨트롤러 B)에 대한 처리 용량 통계를 표시합니다. CPU는 _ 중앙 처리 장치 _ 의 약어입니다. 홈 페이지에서 이 그래프는 스토리지 배열에 대한 통계를 표시합니다. 성능 타일의 Physical View 탭에서 이 그래프는 스토리지 배열 및 드라이브에 대한 통계를 표시합니다.

CPU 그래프는 스토리지의 작업에 사용되는 CPU 처리 용량의 백분율을 보여 줍니다. 외부 I/O가 발생하지 않는 경우에도 스토리지 운영 체제가 백그라운드 작업 및 모니터링을 수행할 수 있으므로 CPU 활용률이 0이 아닐 수 있습니다. 그래프의 한 지점 위로 커서를 가져가면 해당 시점에 사용되는 처리 기능의 백분율을 볼 수 있습니다.

여유 공간 그래프에 표시되는 것은 무엇입니까**?**

여유 공간 그래프는 스토리지 어레이 컨트롤러의 남은 성능 기능과 관련이 있습니다. 이 그래프는 홈 페이지와 성능 타일의 물리적 보기 탭에 표시됩니다.

여유 공간 그래프에는 스토리지 시스템에 있는 물리적 개체의 남은 성능 용량이 나와 있습니다. 그래프의 한 지점 위로 커서를 가져가면 컨트롤러 A 및 컨트롤러 B에 대해 남아 있는 IOPS 및 MiB/s 용량의 백분율이 표시됩니다

디스플레이 기본 설정에 대한 자세한 정보는 어디에서 찾을 수 있습니까**?**

사용 가능한 표시 옵션에 대한 정보를 찾으려면

- 용량 값을 표시하는 기본 단위에 대한 자세한 내용은 을 참조하십시오."용량 값의 기본 단위를 설정합니다"
- 성능 그래프를 표시하는 기본 기간에 대한 자세한 내용은 를 참조하십시오."성능 그래프의 기본 기간을 설정합니다"

풀 및 볼륨 그룹

풀 및 볼륨 그룹 개요

스토리지 어레이의 할당되지 않은 드라이브 서브셋에서 논리적 스토리지 용량을 생성할 수 있습니다. 이 논리적 용량은 환경의 요구 사항에 따라 풀 또는 볼륨 그룹의 형태를 취할 수 있습니다.

풀 및 볼륨 그룹이란 무엇입니까**?**

A_POOL_은 논리적으로 그룹화된 드라이브 집합입니다. 볼륨 그룹 _ 은(는) 공유 특성을 가진 볼륨의 컨테이너입니다. 풀 또는 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 생성할 수 있습니다.

자세한 내용:

- "풀 및 볼륨 그룹의 작동 방식"
- "용량 용어"
- "풀 또는 볼륨 그룹을 사용할지 여부를 결정합니다"

풀을 생성하려면 어떻게 해야 합니까**?**

스토리지 어레이에서 할당되지 않은 용량을 감지하면 System Manager에서 자동으로 풀을 생성하도록 허용할 수 있습니다. 또는 자동 생성으로 최적의 구성을 확인할 수 없는 경우 메뉴에서 스토리지 [풀 및 볼륨 그룹] 풀을 수동으로 생성할 수 있습니다.

자세한 내용:

- "자동 및 수동 풀 생성"
- "풀을 자동으로 생성합니다"
- "풀을 수동으로 생성합니다"
- "풀 또는 볼륨 그룹에 용량을 추가합니다"

볼륨 그룹을 어떻게 생성합니까**?**

스토리지 [풀 및 볼륨 그룹] 메뉴에서 볼륨 그룹을 생성할 수 있습니다.

자세한 내용:

- "볼륨 그룹을 생성합니다"
- "풀 또는 볼륨 그룹에 용량을 추가합니다"

관련 정보

풀 및 볼륨 그룹과 관련된 개념에 대해 자세히 알아보십시오.

- "예약 용량 작동 방식"
- "SSD Cache의 작동 방식"

개념

풀 및 볼륨 그룹의 작동 방식

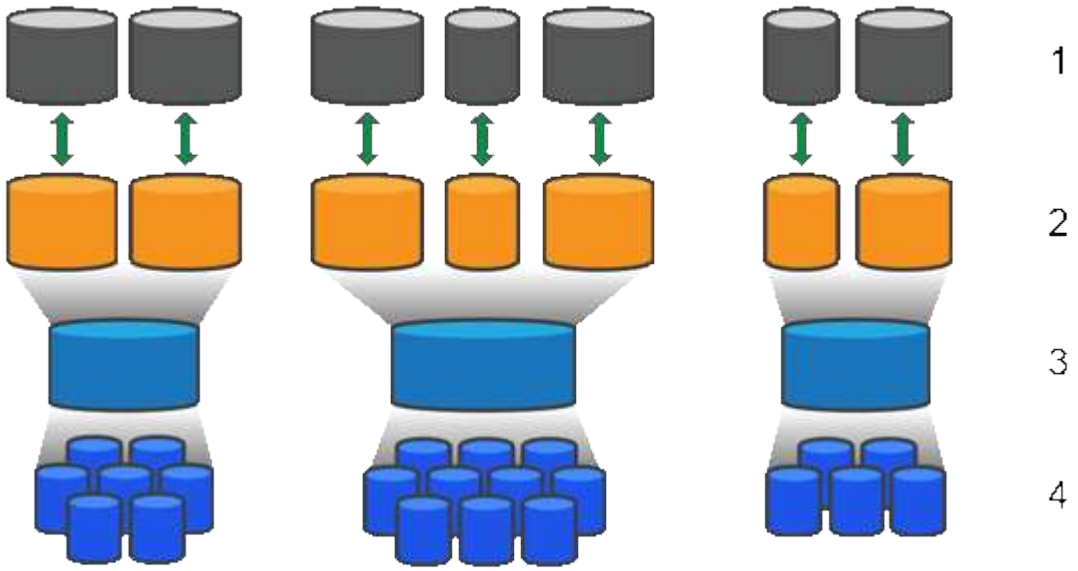
스토리지 용량을 할당하려면 스토리지 어레이에서 사용할 HDD(하드 디스크 드라이브) 또는 SSD(Solid State Disk) 드라이브가 포함될 풀 또는 볼륨 그룹을 생성합니다.

물리적 하드웨어는 논리적 구성 요소로 프로비저닝되므로 데이터를 구성하고 쉽게 검색할 수 있습니다. 지원되는 그룹 유형에는 두 가지가 있습니다.

- 풀
- RAID 볼륨 그룹

풀 및 볼륨 그룹은 스토리지 어레이에서 최상위 스토리지 단위이며, 드라이브 용량을 관리 가능한 여러 사업부로

나눕니다. 이러한 논리적 사업부 내에는 데이터가 저장되는 개별 볼륨 또는 LUN이 있습니다. 다음 그림은 이러한 개념을 보여 줍니다.



[1]호스트 LUN;[2]볼륨;[3]볼륨 그룹 또는 풀;[4]HDD 또는 SSD 드라이브

스토리지 시스템을 구축할 때 첫 번째 단계는 다음을 통해 사용 가능한 드라이브 용량을 다양한 호스트에 제공하는 것입니다.

- 용량이 충분한 풀 또는 볼륨 그룹 생성
- 성능 요구 사항을 충족하는 데 필요한 드라이브 수를 풀 또는 볼륨 그룹에 추가
- 특정 비즈니스 요구 사항을 충족하기 위해 원하는 RAID 보호 수준(볼륨 그룹을 사용하는 경우)을 선택합니다

동일한 스토리지 시스템에 풀 또는 볼륨 그룹이 있을 수 있지만 드라이브가 둘 이상의 풀 또는 볼륨 그룹에 속할 수는 없습니다. 그런 다음 호스트에게 입출력에 대해 제공되는 볼륨이 풀 또는 볼륨 그룹의 공간을 사용하여 생성됩니다.

풀

풀은 물리적 하드 디스크 드라이브를 대용량 스토리지 공간에 통합하여 RAID 보호 기능을 강화하도록 설계되었습니다. 풀은 풀에 할당된 총 드라이브 수에서 많은 가상 RAID 세트를 생성하고 모든 참여 드라이브에 데이터를 균등하게 분산시킵니다. 드라이브가 손실되거나 추가되면 System Manager는 모든 활성 드라이브에서 데이터의 균형을 동적으로 조정합니다.

풀은 또 다른 RAID 레벨로 작동하며, 기본 RAID 아키텍처를 가상화하여 재구축, 드라이브 확장, 드라이브 손실 처리 등의 작업을 수행할 때 성능과 유연성을 최적화합니다. System Manager는 8+2 구성(데이터 디스크 8개 + 패리티 디스크 2개)에서 RAID 레벨을 6으로 자동 설정합니다.

드라이브 일치

풀에서 사용할 HDD 또는 SSD 중 하나를 선택할 수 있지만 볼륨 그룹과 마찬가지로 풀의 모든 드라이브에서 동일한 기술을 사용해야 합니다. 컨트롤러는 자동으로 포함할 드라이브를 선택하므로 선택한 기술에 필요한 드라이브의 수가 충분한지 확인해야 합니다.

장애가 발생한 드라이브 관리

풀에는 최소 11개의 드라이브 용량이 있지만 드라이브 장애가 발생할 경우 여유 용량을 위해 드라이브 1개의 용량이 예약됩니다. 이 여유 용량을 "보존 용량"이라고 합니다.

풀을 생성할 때 비상 사용을 위해 특정 용량이 보존됩니다. 이 용량은 System Manager의 여러 드라이브에 대해 표현되지만 실제 구현은 드라이브 전체 풀에 분산됩니다. 기본 보존 용량은 풀의 드라이브 수를 기준으로 합니다.

풀을 생성한 후에는 보존 용량 값을 더 많이 또는 더 적은 용량으로 변경하거나 보존 용량(0개 드라이브의 값)을 사용하지 않도록 설정할 수 있습니다. 보존할 수 있는 최대 용량(드라이브 수로 표시)은 10이지만 풀의 총 드라이브 수에 따라 사용 가능한 용량이 더 적을 수 있습니다.

볼륨 그룹

볼륨 그룹은 스토리지 시스템에서 볼륨에 용량을 할당하는 방법을 정의합니다. 디스크 드라이브는 RAID 그룹으로 구성되고 볼륨은 RAID 그룹의 드라이브에 상주합니다. 따라서 볼륨 그룹 구성 설정은 그룹에 속한 드라이브와 사용되는 RAID 레벨을 식별합니다.

볼륨 그룹을 생성할 때 컨트롤러는 그룹에 포함할 드라이브를 자동으로 선택합니다. 그룹의 RAID 레벨을 수동으로 선택해야 합니다. 볼륨 그룹의 용량은 선택한 드라이브 수의 합계에 해당 용량을 곱한 값입니다.

드라이브 일치

크기와 성능을 위해서는 볼륨 그룹의 드라이브와 일치해야 합니다. 볼륨 그룹에 더 작은 드라이브와 더 큰 드라이브가 있으면 모든 드라이브가 가장 작은 용량 크기로 인식됩니다. 볼륨 그룹에 더 느리고 빠른 드라이브가 있으면 모든 드라이브가 가장 느린 속도로 인식됩니다. 이러한 요인은 스토리지 시스템의 성능과 전체 용량에 영향을 줍니다.

다양한 드라이브 기술(HDD 및 SSD 드라이브)을 혼합할 수 없습니다. RAID 3, 5 및 6은 최대 30개의 드라이브로 제한됩니다. RAID 1 및 RAID 10은 미러링을 사용하므로 이러한 볼륨 그룹에는 동일한 수의 디스크가 있어야 합니다.

장애가 발생한 드라이브 관리

볼륨 그룹은 볼륨 그룹에 포함된 RAID 1/10, RAID 3, RAID 5 또는 RAID 6 볼륨에서 드라이브에 장애가 발생할 경우 핫 스페어 드라이브를 대기 상태로 사용합니다. 핫 스페어 드라이브에는 데이터가 없으며 스토리지 어레이에 또 다른 수준의 중복성이 추가됩니다.

스토리지 배열의 드라이브에 오류가 발생하면 물리 스왑 없이 핫 스페어 드라이브가 장애가 발생한 드라이브로 자동 대체됩니다. 드라이브에 오류가 발생할 때 핫 스페어 드라이브를 사용할 수 있는 경우 컨트롤러는 중복 데이터를 사용하여 오류가 발생한 드라이브에서 핫 스페어 드라이브로 데이터를 재구성합니다.

용량 용어

스토리지 어레이에 적용되는 용량 조건에 대해 알아보십시오.

스토리지 오브젝트

다음 용어는 스토리지 어레이와 상호 작용할 수 있는 여러 유형의 스토리지 개체에 대해 설명합니다.

스토리지 객체	설명
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.

스토리지 객체	설명
LUN입니다	LUN(Logical Unit Number)은 호스트가 볼륨을 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다.
미러 정합성 보장 그룹	미러 정합성 보장 그룹은 하나 이상의 미러링된 쌍에 대한 컨테이너입니다. 비동기식 미러링 작업의 경우 미러 정합성 보장 그룹을 생성해야 합니다.
미러링된 볼륨 쌍	미러링된 쌍은 기본 볼륨 및 보조 볼륨이라는 두 개의 볼륨으로 구성됩니다.
수영장	풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)
스냅샷 정합성 보장 그룹	스냅샷 정합성 보장 그룹은 스냅샷 이미지를 생성할 때 단일 개체로 처리되는 볼륨의 모음입니다. 이러한 각 볼륨에는 고유한 스냅샷 이미지가 있지만 모든 이미지는 동시에 생성됩니다.
스냅샷 그룹	스냅샷 그룹은 단일 기본 볼륨의 스냅샷 이미지 모음입니다.
스냅샷 볼륨	스냅샷 볼륨을 사용하면 호스트가 스냅샷 이미지의 데이터에 액세스할 수 있습니다. 스냅샷 볼륨에는 원래 스냅샷 이미지에 영향을 주지 않고 기본 볼륨에 대한 수정 사항을 저장하는 자체 예약 용량이 포함되어 있습니다.
볼륨	볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다.
볼륨 그룹	볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.

스토리지 용량

다음 용어는 스토리지 배열에 사용되는 다양한 유형의 용량에 대해 설명합니다.

용량 유형입니다	설명
할당된 용량입니다	할당된 용량은 풀 또는 볼륨 그룹의 드라이브에서 할당된 물리적 용량입니다. 할당된 용량을 사용하여 볼륨을 생성하고 복제 서비스 작업을 수행할 수 있습니다.
여유 용량	여유 용량은 볼륨 생성 또는 복제 서비스 작업 및 스토리지 객체에 아직 할당되지 않은 풀 또는 볼륨 그룹에서 사용할 수 있는 용량입니다.

용량 유형입니다	설명
풀 또는 볼륨 그룹 용량입니다	풀, 볼륨 또는 볼륨 그룹 용량은 풀 또는 볼륨 그룹에 할당된 스토리지 시스템의 용량입니다. 이 용량은 볼륨을 생성하고 복사 서비스 작업 및 스토리지 오브젝트의 다양한 용량 요구사항을 지원하는 데 사용됩니다.
풀을 사용할 수 없는 용량입니다	풀 사용 불가 용량은 드라이브 크기가 일치하지 않아 사용할 수 없는 풀의 공간입니다.
보존 용량	Preservation capacity는 잠재적 드라이브 장애를 지원하기 위해 풀에 예약된 용량(드라이브 수)입니다.
보고된 용량입니다	보고된 용량은 호스트에 보고되고 호스트에서 액세스할 수 있는 용량입니다.
예약된 용량입니다	예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.
SSD 캐시	SSD Cache는 스토리지 어레이에서 논리적으로 함께 그룹화하는 SSD(Solid State Disk) 드라이브 세트입니다. SSD Cache 기능은 가장 자주 액세스되는 데이터("핫" 데이터)를 지연 시간이 짧은 SSD 드라이브에 캐싱하여 애플리케이션 워크로드를 동적으로 가속화합니다.
할당되지 않은 용량	할당되지 않은 용량은 스토리지 배열의 공간이며, 풀 또는 볼륨 그룹에 * 할당되지 않음 * 이 할당된 공간입니다.
쓰인 용량	쓰인 용량은 씬 볼륨에 할당된 예약 용량에서 기록된 용량입니다.

풀 또는 볼륨 그룹을 사용할지 여부를 결정합니다

풀 또는 볼륨 그룹을 사용하여 볼륨을 생성할 수 있습니다. 최적의 선택은 주로 예상되는 I/O 워크로드, 성능 요구 사항 및 데이터 보호 요구 사항과 같은 주요 스토리지 요구 사항에 따라 달라집니다.

풀 또는 볼륨 그룹을 선택해야 하는 이유

- 풀을 선택하십시오 *
- 더 빠른 드라이브 리빌드 및 단순화된 스토리지 관리가 필요한 경우, 씬 볼륨 또는 랜덤 워크로드가 필요합니다.
- 풀을 구성하는 드라이브 세트에 각 볼륨의 데이터를 무작위로 분산하려는 경우

  풀 또는 풀의 볼륨은 RAID 레벨을 설정하거나 변경할 수 없습니다. 풀은 RAID 레벨 6을 사용합니다.

- 볼륨 그룹을 선택합니다 *
- 최대 시스템 대역폭이 필요한 경우 스토리지 설정을 조정할 수 있고 워크로드가 매우 순차적입니다.
- RAID 레벨을 기반으로 드라이브에 데이터를 배포하려는 경우 볼륨 그룹을 생성할 때 RAID 레벨을 지정할 수 있습니다.

- 볼륨 그룹을 구성하는 드라이브 세트를 통해 각 볼륨의 데이터를 순차적으로 쓰려는 경우

> 풀은 볼륨 그룹과 함께 존재할 수 있으므로 스토리지 어레이에는 풀과 볼륨 그룹이 모두 포함될 수 있습니다.

풀과 볼륨 그룹 간의 기능 차이

다음 표에서는 볼륨 그룹과 풀을 비교하여 보여 줍니다.

사용	수영장	볼륨 그룹
워크로드 임의	더 좋습니다	좋습니다
순차 워크로드	좋습니다	더 좋습니다
드라이브 리빌드 시간	더 빠른 속도	느린 속도
성능(최적 모드)	양호: 소규모 블록, 랜덤 워크로드에 적합	좋음: 대규모 블록, 순차적 워크로드에 적합
성능(드라이브 리빌드 모드)	우수: 일반적으로 RAID 6보다 우수	성능 저하: 최대 40% 성능 저하
다중 드라이브 장애	데이터 보호 향상: 리빌드 속도 향상 및 우선순위 지정	데이터 보호 기능 저하: 느린 리빌드, 더 높은 데이터 손실 위험
드라이브 추가	빠른 속도: 즉석에서 풀에 추가	느림: 동적 용량 확장 작업이 필요합니다
씬 볼륨이 지원됩니다	예	아니요
SSD(Solid State Disk) 지원	예	예
단순한 관리	예: 구성할 핫 스페어 또는 RAID 설정이 없습니다	아니요: 핫 스페어를 할당하고 RAID를 구성해야 합니다
성능 조정 가능	아니요	예

풀 및 볼륨 그룹의 기능 비교

풀과 볼륨 그룹의 기능과 용도는 동일합니다. 두 오브젝트 모두 논리적으로 그룹화된 드라이브 세트이며 호스트가 액세스할 수 있는 볼륨을 생성하는 데 사용됩니다.

다음 표에서는 풀 또는 볼륨 그룹이 스토리지 요구 사항에 가장 적합한지 여부를 결정하는 데 도움이 됩니다.

기능	수영장	볼륨 그룹
다른 RAID 레벨이 지원됩니다	아니오. System Manager에서는 항상 RAID 6을 사용합니다.	예. RAID 0, 1, 10, 5 및 6을 사용할 수 있습니다.
씬 볼륨이 지원됩니다	예	아니요
FDE(전체 디스크 암호화)가 지원됩니다	예	예
DA(Data Assurance) 지원	예	예
쉘프 손실 보호가 지원됩니다	예	예
서랍 손실 보호가 지원됩니다	예	예
혼합 드라이브 속도가 지원됩니다	같은 것을 권장하지만 필수는 아닙니다. 가장 느린 드라이브는 모든 드라이브의 속도를 결정합니다.	같은 것을 권장하지만 필수는 아닙니다. 가장 느린 드라이브는 모든 드라이브의 속도를 결정합니다.
혼합 드라이브 용량이 지원됩니다	같은 것을 권장하지만 필수는 아닙니다. 가장 작은 드라이브는 모든 드라이브의 용량을 결정합니다.	같은 것을 권장하지만 필수는 아닙니다. 가장 작은 드라이브는 모든 드라이브의 용량을 결정합니다.
최소 드라이브 수입니다	11	RAID 레벨에 따라 다릅니다. RAID 0에는 1이 필요합니다. RAID 1 또는 10에는 2가 필요합니다(짝수 필요). 최소 RAID 5은 3입니다. 최소 RAID 6은 5입니다.
최대 드라이브 수입니다	스토리지 배열의 최대 제한입니다	RAID 1 및 10 - 스토리지 어레이 RAID 5, 6-30개 드라이브의 최대 제한입니다
볼륨을 생성할 때 개별 드라이브를 선택할 수 있습니다	아니요	예
볼륨을 생성할 때 세그먼트 크기를 지정할 수 있습니다	예. 128K가 지원됩니다.	예
볼륨을 생성할 때 입출력 특성을 지정할 수 있습니다	아니요	예. 파일 시스템, 데이터베이스, 멀티미디어 및 맞춤형 지원
드라이브 장애 방지	풀의 각 드라이브에서 보존 용량을 사용하므로 재구성 속도가 빨라집니다.	핫 스페어 드라이브를 사용합니다. 드라이브 IOP에 따라 재구성이 제한됩니다.

기능	수영장	볼륨 그룹
용량 제한에 도달할 때 경고가 표시됩니다	예. 사용된 용량이 최대 용량의 비율에 도달하면 경고를 설정할 수 있습니다.	아니요
지원되는 다른 스토리지 어레이로 마이그레이션	아니요. 먼저 볼륨 그룹으로 마이그레이션해야 합니다.	예
동적 세그먼트 크기(DSS)	아니요	예
RAID 레벨을 변경할 수 있습니다	아니요	예
볼륨 확장(용량 증가)	예	예
용량 확장(용량 추가)	예	예
용량 절감	예	아니요

혼합 드라이브 유형(HDD, SSD)은 풀 또는 볼륨 그룹에서 지원되지 않습니다.

자동 및 수동 풀 생성

풀을 자동 또는 수동으로 생성하여 물리적 스토리지를 그룹화한 다음 필요에 따라 동적으로 할당할 수 있습니다. 풀을 생성할 때 물리적 드라이브를 추가할 수 있습니다.

자동 작성

System Manager에서 스토리지 어레이에서 할당되지 않은 용량을 감지하면 자동 풀 생성이 시작됩니다. 할당되지 않은 용량이 감지되면 System Manager에서 자동으로 하나 이상의 풀을 생성하거나 할당되지 않은 용량을 기존 풀에 추가하거나 이 두 풀을 모두 추가하라는 메시지를 표시합니다.

자동 풀 생성은 다음 조건 중 하나가 참일 때 발생합니다.

- 스토리지 시스템에 풀이 없으며 새 풀을 생성할 수 있는 유사한 드라이브가 충분히 있습니다.
- 풀이 하나 이상 있는 스토리지 배열에 새 드라이브가 추가됩니다.

풀의 각 드라이브는 동일한 드라이브 유형(HDD 또는 SSD)이어야 하며 용량이 유사해야 합니다. System Manager에서 다음 작업을 완료하라는 메시지를 표시합니다.

- 이러한 유형의 드라이브 수가 충분한 경우 단일 풀을 생성합니다.
- 할당되지 않은 용량이 서로 다른 드라이브 유형으로 구성된 경우 여러 풀을 생성합니다.
- 스토리지 배열에 풀이 이미 정의되어 있는 경우 기존 풀에 드라이브를 추가하고 동일한 드라이브 유형의 새 드라이브를 풀에 추가합니다.
- 동일한 드라이브 유형의 드라이브를 기존 풀에 추가하고 다른 드라이브 유형을 사용하여 새 드라이브 유형이 다른 경우 다른 풀을 생성합니다.

수동 생성

자동 생성에서 최적의 구성을 확인할 수 없는 경우 풀을 수동으로 생성할 수 있습니다. 이 상황은 다음 이유 중 하나로 발생할 수 있습니다.

- 새 드라이브를 둘 이상의 풀에 추가할 수 있습니다.
- 하나 이상의 새 풀 후보가 셸프 손실 방지 또는 드로어 손실 방지 기능을 사용할 수 있습니다.
- 현재 풀 후보 중 하나 이상이 선반 손실 방지 또는 서랍 손실 보호 상태를 유지할 수 없습니다.

스토리지 배열에 여러 애플리케이션이 있고 동일한 드라이브 리소스에 대해 경쟁하지 않도록 하려면 풀을 수동으로 만들어야 할 수도 있습니다. 이 경우 하나 이상의 애플리케이션에 대해 더 작은 풀을 수동으로 생성하는 것이 좋습니다. 데이터를 분산할 볼륨이 많은 대규모 풀에 워크로드를 할당하는 대신 하나 또는 두 개의 볼륨만 할당할 수 있습니다. 특정 애플리케이션의 워크로드 전용으로 별도의 풀을 수동으로 생성하면 스토리지 시스템의 운영 속도가 빨라질 수 있고 경합이 줄어듭니다.

스토리지를 구성합니다

풀을 자동으로 생성합니다

풀 생성은 SANtricity 시스템 관리자가 스토리지 시스템에서 할당되지 않은 드라이브를 감지하면 자동으로 시작됩니다. 자동 풀 생성을 사용하여 스토리지 어레이에서 할당되지 않은 모든 드라이브를 하나의 풀로 쉽게 구성하고 기존 풀에 드라이브를 추가할 수 있습니다.

시작하기 전에

다음 조건 중 하나가 참일 경우 풀 자동 구성 대화 상자를 시작할 수 있습니다.

- 드라이브 유형이 유사한 기존 풀에 추가할 수 있는 할당되지 않은 드라이브가 하나 이상 감지되었습니다.
- 할당되지 않은 11개 이상의 드라이브가 감지되었습니다. 이 드라이브는 새 풀을 생성하는 데 사용할 수 있습니다 (드라이브 유형이 서로 다른 기존 풀에 추가할 수 없는 경우).

이 작업에 대해

다음 사항에 유의하십시오.

- 스토리지 어레이에 드라이브를 추가하면 System Manager에서 자동으로 드라이브를 감지하고 드라이브 유형과 현재 구성을 기준으로 단일 풀 또는 여러 풀을 생성하라는 메시지를 표시합니다.
- 이전에 풀을 정의한 경우 System Manager에서는 기존 풀에 호환되는 드라이브를 추가하는 옵션을 자동으로 프롬프트합니다. 새 드라이브를 기존 풀에 추가하면 System Manager에서 자동으로 새 용량에 데이터를 재분배하며, 여기에는 추가한 새 드라이브가 포함됩니다.
- EF600 또는 EF300 스토리지 어레이를 구성할 때는 각 컨트롤러가 처음 12개 슬롯에서 동일한 수의 드라이브와 마지막 12개 슬롯에서 동일한 수의 드라이브를 액세스할 수 있는지 확인하십시오. 이 구성을 사용하면 컨트롤러가 드라이브 측 PCIe 버스를 보다 효과적으로 사용할 수 있습니다.

다음 방법 중 하나를 사용하여 풀 자동 구성 대화 상자를 시작할 수 있습니다.

- 할당되지 않은 용량이 감지되면 알림 영역의 홈 페이지에 풀 자동 구성 권장 사항이 표시됩니다. View Pool Auto-Configuration * 을 클릭하여 대화상자를 시작합니다.
- 다음 작업에 설명된 대로 Pools and Volume Groups 페이지에서 Pool Auto-Configuration 대화 상자를 시작할 수도 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 메뉴 선택: More [Launch pool auto-configuration](추가 [풀 자동 구성 시작])

   결과 테이블에는 새 풀, 드라이브가 추가된 기존 풀 또는 둘 다 나열됩니다. 새 풀의 이름은 기본적으로 일련 번호로 지정됩니다.

   System Manager는 다음 작업을 수행합니다.

   - 동일한 드라이브 유형(HDD 또는 SSD)의 드라이브 수가 충분하고 용량이 유사한 경우 단일 풀을 생성합니다.
   - 할당되지 않은 용량이 서로 다른 드라이브 유형으로 구성된 경우 여러 풀을 생성합니다.
   - 스토리지 배열에 풀이 이미 정의되어 있는 경우 기존 풀에 드라이브를 추가하고 동일한 드라이브 유형의 새 드라이브를 풀에 추가합니다.
   - 동일한 드라이브 유형의 드라이브를 기존 풀에 추가하고 다른 드라이브 유형을 사용하여 새 드라이브 유형이 다른 경우 다른 풀을 생성합니다.
3. 새 풀의 이름을 변경하려면 * 편집 * 아이콘(연필)을 클릭합니다.
4. 풀의 추가 특성을 보려면 커서를 위에 놓거나 * Details * 아이콘(페이지)을 누릅니다.

   드라이브 유형, 보안 기능, 데이터 보증(DA) 기능, 쉘프 손실 보호, 서랍 손실 보호에 대한 정보가 나타납니다.

   EF600 및 EF300 스토리지 어레이의 경우 리소스 프로비저닝 및 볼륨 블록 크기에 대한 설정도 표시됩니다.
5. Accept * 를 클릭합니다.

풀을 수동으로 생성합니다

풀 자동 구성 기능이 요구 사항에 맞는 풀을 제공하지 않는 경우 후보 집합에서 풀을 수동으로 생성할 수 있습니다.

풀은 애플리케이션을 호스팅하는 데 사용할 수 있는 개별 볼륨을 생성하는 데 필요한 논리적 스토리지 용량을 제공합니다.

시작하기 전에

- 드라이브 유형(HDD 또는 SSD)이 동일한 드라이브가 최소 11개 이상 있어야 합니다.
- 쉘프 손실 방지 기능을 사용하려면 풀을 구성하는 드라이브가 6개 이상의 서로 다른 드라이브 쉘프에 있어야 하며, 단일 드라이브 쉘프에 드라이브가 2개 이상 없어야 합니다.
- 드로어 손실 방지 기능을 사용하려면 풀을 구성하는 드라이브가 5개 이상의 서로 다른 드로어에 있어야 하며 풀에는 각 드로어의 드라이브 셸프가 동일한 수만큼 포함되어 있어야 합니다.
- EF600 또는 EF300 스토리지 어레이를 구성할 때는 각 컨트롤러가 처음 12개 슬롯에서 동일한 수의 드라이브와 마지막 12개 슬롯에서 동일한 수의 드라이브를 액세스할 수 있는지 확인하십시오. 이 구성을 사용하면 컨트롤러가 드라이브 측 PCIe 버스를 보다 효과적으로 사용할 수 있습니다. 현재 System Manager에서는 볼륨 그룹을 생성할 때 고급 기능 아래에서 드라이브를 선택할 수 있습니다. 풀을 생성하려면 스토리지 배열의 모든 드라이브를 사용하는 것이 좋습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.

2. MENU: Create [Pool] 를 클릭합니다.

   풀 생성 대화 상자가 나타납니다.

3. 풀의 이름을 입력합니다.
4. * 선택 사항: * 스토리지 배열에 둘 이상의 드라이브 유형이 있는 경우 사용할 드라이브 유형을 선택합니다.

   결과 테이블에는 생성할 수 있는 모든 풀이 나열됩니다.

5. 다음 특성을 기준으로 사용할 풀 후보를 선택한 다음 * Create * 를 클릭합니다.

특징	사용
사용 가능한 용량	에는 GiB 단위의 풀 후보 가용 용량이 나와 있습니다. 애플리케이션의 스토리지 요구 사항에 맞는 용량이 있는 풀 후보를 선택합니다. 보존(스페어) 용량도 풀 전체에 분산되며 가용 용량에 포함되지 않습니다.
총 드라이브 수	에는 풀 후보 드라이브에서 사용 가능한 드라이브 수가 나와 있습니다. System Manager는 보존 용량을 위해 가능한 한 많은 드라이브를 자동으로 예약합니다. 시스템 관리자는 풀에 있는 6개 드라이브마다 보존 용량을 위해 하나의 드라이브를 예약합니다. 드라이브 장애가 발생하면 보존 용량이 재구성 데이터를 저장하는 데 사용됩니다.
드라이브 블록 크기(EF300 및 EF600만 해당)	에서는 풀의 드라이브가 쓸 수 있는 블록 크기(섹터 크기)를 보여 줍니다. 다음과 같은 값이 포함될 수 있습니다. • 512—512바이트 섹터 크기 • 4k—4,096바이트 섹터 크기
보안 가능	풀 대상이 전체 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있는 전체 보안 가능 드라이브로 구성되어 있는지 여부를 나타냅니다. • 드라이브 보안으로 풀을 보호할 수 있지만 이 기능을 사용하려면 모든 드라이브가 안전해야 합니다. • FDE 전용 풀을 생성하려면 Secure-Capable 열에서 * Yes-FDE * 를 찾습니다. FIPS 전용 풀을 생성하려면 * Yes-FIPS * 또는 * Yes-FIPS(Mixed) * 를 찾습니다. "혼합"은 140-3단계 드라이브와 140-3단계 드라이브의 혼합을 나타냅니다. 이러한 수준을 혼합하여 사용하는 경우 풀이 낮은 보안 수준(140-2)에서 작동할 수 있습니다. • 보안 기능이 있거나 그렇지 않거나 보안 수준이 혼합된 드라이브로 구성된 풀을 생성할 수 있습니다. 풀의 드라이브에 보안 기능이 지원되지 않는 드라이브가 포함되어 있으면 풀을 안전하게 설정할 수 없습니다.

특징	사용
보안을 활성화하시겠습니까?	에서는 보안 가능 드라이브를 사용하여 드라이브 보안 기능을 활성화하는 옵션을 제공합니다. 풀이 보안 기능이 있고 보안 키를 만든 경우 확인란을 선택하여 보안을 설정할 수 있습니다. 활성화된 후 드라이브 보안을 제거하는 유일한 방법은 풀을 삭제하고 드라이브를 지우는 것입니다.
DA를 지원합니다	이 풀 대상에 대해 DA(Data Assurance)를 사용할 수 있는지 여부를 나타냅니다. DA는 컨트롤러를 통해 드라이브로 데이터가 전송될 때 발생할 수 있는 오류를 검사하고 수정합니다. DA는 모든 드라이브가 DA를 지원하는 경우 활성화됩니다. 볼륨이 생성된 후에는 Storage [Volumes > View/Edit Settings > Advanced > Permanently Disable Data Assurance] 메뉴를 선택하여 DA를 비활성화할 수 있습니다. 볼륨에서 DA가 비활성화된 경우 다시 활성화할 수 없습니다.
리소스 프로비저닝 가능(EF300 및 EF600만 해당)	이 풀 대상에 대해 리소스 프로비저닝을 사용할 수 있는지 여부를 표시합니다. 리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.
선반 손실 방지	쉘프 손실 방지 기능이 사용 가능한지 여부를 표시합니다. 쉘프 손실 방지: 단일 드라이브 쉘프의 전체 통신 장애가 발생할 경우 풀 내의 볼륨 데이터에 액세스할 수 있도록 보장합니다.
서랍 손실 방지	드로어 손실 보호가 사용 가능한지 여부를 표시합니다. 이 보호 기능은 드로어가 포함된 드라이브 쉘프를 사용하는 경우에만 제공됩니다. 드로어 손실 방지 기능은 드라이브 쉘프의 단일 드로어에서 전체 통신 장애가 발생할 경우 풀 내의 볼륨 데이터에 액세스할 수 있도록 보장합니다.
지원되는 볼륨 블록 크기(EF300 및 EF600만 해당)	에는 풀의 볼륨에 대해 생성할 수 있는 블록 크기가 나와 있습니다. • 512n — 512바이트 네이티브 • 512e — 512바이트가 에뮬레이트됨 • 4k—4,096바이트.

볼륨 그룹을 생성합니다

볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹은 RAID 레벨 및 용량과 같은 공유 특성을 가진 볼륨의 컨테이너입니다.

대용량 드라이브를 사용하고 여러 컨트롤러에 볼륨을 분산할 수 있으므로 볼륨 그룹당 둘 이상의 볼륨을 생성하는 것이 스토리지 용량을 사용하고 데이터를 보호하는 좋은 방법입니다.

시작하기 전에

볼륨 그룹을 생성하기 전에 다음 지침을 검토하십시오.

- 할당되지 않은 드라이브가 하나 이상 필요합니다.
- 단일 볼륨 그룹에 포함할 수 있는 드라이브 수에 제한이 있습니다. 이러한 제한은 RAID 레벨에 따라 다릅니다.
- 쉘프/서랍 손실 보호를 활성화하려면 최소 3개의 쉘프 또는 서랍에 있는 드라이브를 사용하는 볼륨 그룹을 생성해야 합니다. 단, RAID 1을 사용하는 경우는 예외입니다. 여기서 두 개의 쉘프/서랍이 최소값이 됩니다.
- EF600 또는 EF300 스토리지 어레이를 사용하는 경우 볼륨 그룹을 수동으로 생성하려면 각 컨트롤러가 처음 12개 슬롯에서 동일한 수의 드라이브에 액세스하고 마지막 12개 슬롯에서 동일한 수의 드라이브에 액세스해야 합니다. 이 구성을 사용하면 컨트롤러가 드라이브 측 PCIe 버스를 보다 효과적으로 사용할 수 있습니다. 현재 System Manager에서는 볼륨 그룹을 생성할 때 고급 기능 아래에서 드라이브를 선택할 수 있습니다.
- 선택한 RAID 레벨이 볼륨 그룹의 결과 용량에 미치는 영향을 검토합니다.
  - RAID 1을 선택한 경우 미러링된 쌍이 선택되었는지 확인하기 위해 한 번에 두 개의 드라이브를 추가해야 합니다. 4개 이상의 드라이브를 선택하면 미러링 및 스트라이핑(RAID 10 또는 RAID 1+0이라고 함)이 수행됩니다.
  - RAID 5를 선택한 경우 최소 3개의 드라이브를 추가하여 볼륨 그룹을 만들어야 합니다.
  - RAID 6을 선택한 경우 최소 5개의 드라이브를 추가하여 볼륨 그룹을 생성해야 합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 메뉴 [Volume group](볼륨 그룹)을 클릭합니다.

   Create Volume Group 대화상자가 나타납니다.
3. 볼륨 그룹의 이름을 입력합니다.
4. 데이터 스토리지 및 보호 요구사항에 가장 적합한 RAID 레벨을 선택합니다.

   볼륨 그룹 후보 테이블이 나타나고 선택한 RAID 레벨을 지원하는 후보만 표시됩니다.
5. * 선택 사항: * 스토리지 배열에 둘 이상의 드라이브 유형이 있는 경우 사용할 드라이브 유형을 선택합니다.

   볼륨 그룹 후보 테이블이 나타나고 선택한 드라이브 유형과 RAID 레벨을 지원하는 후보만 표시됩니다.
6. * 선택 사항: * 자동 방법이나 수동 방법을 선택하여 볼륨 그룹에서 사용할 드라이브를 정의할 수 있습니다. 자동 방법이 기본 선택 항목입니다.

   드라이브를 수동으로 선택하려면 * Manually select drives (advanced) * 링크를 클릭합니다. 클릭하면 자동으로 드라이브 선택(고급) * 으로 변경됩니다.

   Manual(수동) 방법을 사용하면 볼륨 그룹을 구성하는 특정 드라이브를 선택할 수 있습니다. 할당되지 않은 특정 드라이브를 선택하여 필요한 용량을 확보할 수 있습니다. 스토리지 배열에 다른 미디어 유형 또는 다른 인터페이스 유형의 드라이브가 포함된 경우, 단일 드라이브 유형에 대해 구성되지 않은 용량만 선택하여 새 볼륨 그룹을 생성할 수 있습니다.

   ⓘ 드라이브 중복성과 최적의 드라이브 구성을 이해하는 전문가만 수동 방법을 사용해야 합니다.
7. 표시된 드라이브 특성에 따라 볼륨 그룹에서 사용할 드라이브를 선택한 다음 * Create * 를 클릭합니다.

표시되는 드라이브 특성은 자동 방법 또는 수동 방법을 선택했는지 여부에 따라 달라집니다.

자동 메서드 드라이브 특성

특징	사용
사용 가능한 용량	에는 사용 가능한 용량이 GiB 단위로 표시됩니다. 애플리케이션의 스토리지 요구사항에 필요한 용량을 갖춘 볼륨 그룹 후보를 선택합니다.
총 드라이브 수	이 볼륨 그룹에 사용할 수 있는 드라이브 수를 표시합니다. 원하는 드라이브 수가 있는 볼륨 그룹 대상을 선택합니다.
드라이브 블록 크기(EF300 및 EF600만 해당)	그룹의 드라이브가 쓸 수 있는 블록 크기(섹터 크기)를 표시합니다. 다음과 같은 값이 포함될 수 있습니다. • 512—512바이트 섹터 크기 • 4k—4,096바이트 섹터 크기
보안 가능	이 볼륨 그룹 대상이 전체 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있는 전체 보안 가능 드라이브로 구성되어 있는지 여부를 나타냅니다. • 드라이브 보안으로 볼륨 그룹을 보호할 수 있지만 이 기능을 사용하려면 모든 드라이브가 안전해야 합니다. • FDE 전용 볼륨 그룹을 생성하려면 Secure-Capable 열에서 * Yes-FDE * 를 찾습니다. FIPS 전용 볼륨 그룹을 생성하려면 * Yes-FIPS * 또는 * Yes-FIPS(Mixed) * 를 찾습니다. "혼합"은 140-3단계 드라이브와 140-3단계 드라이브의 혼합을 나타냅니다. 이러한 수준을 혼합하여 사용하는 경우 볼륨 그룹이 낮은 보안 수준(140-2)에서 작동합니다. • 보안이 가능하거나 보안이 가능하지 않거나 보안 수준이 혼합된 드라이브로 구성된 볼륨 그룹을 생성할 수 있습니다. 볼륨 그룹의 드라이브에 보안 기능이 지원되지 않는 드라이브가 포함되어 있으면 볼륨 그룹을 안전하게 만들 수 없습니다.
보안을 활성화하시겠습니까?	에서는 보안 가능 드라이브를 사용하여 드라이브 보안 기능을 활성화하는 옵션을 제공합니다. 볼륨 그룹이 보안 기능이 있고 보안 키를 설정한 경우 확인란을 선택하여 드라이브 보안을 활성화할 수 있습니다. 활성화된 후 Drive Security를 제거하는 유일한 방법은 볼륨 그룹을 삭제하고 드라이브를 지우는 것입니다.
DA를 지원합니다	이 그룹에 대해 DA(Data Assurance)를 사용할 수 있는지 여부를 나타냅니다. DA(Data Assurance)는 컨트롤러를 통해 드라이브로 데이터가 전송될 때 발생할 수 있는 오류를 확인하고 수정합니다. DA를 사용하려면 DA를 지원하는 볼륨 그룹을 선택합니다. (DA 지원 드라이브의 경우 풀에 생성된 볼륨에서 DA가 자동으로 활성화됩니다.) 볼륨 그룹에는 DA를 사용할 수 있거나 DA를 사용할 수 없는 드라이브가 포함될 수 있지만 모든 드라이브는 DA를 통해 이 기능을 사용할 수 있어야 합니다.

특징	사용
리소스 프로비저닝 가능(EF300 및 EF600만 해당)	이 그룹에 대해 리소스 프로비저닝을 사용할 수 있는지 여부를 표시합니다. 리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.
선반 손실 방지	쉘프 손실 방지 기능이 사용 가능한지 여부를 표시합니다. 쉘프 손실 보호는 쉘프에 대한 통신이 완전히 손실되는 경우 볼륨 그룹의 볼륨에 있는 데이터에 액세스할 수 있도록 보장합니다.
서랍 손실 방지	드로어 손실 보호가 사용 가능한지 여부를 표시합니다. 이 보호 기능은 드로어가 포함된 드라이브 쉘프를 사용하는 경우에만 제공됩니다. 드로어 손실 방지 기능은 드라이브 쉘프의 단일 드로어에서 전체 통신 장애가 발생할 경우 볼륨 그룹의 볼륨에 있는 데이터에 액세스할 수 있도록 보장합니다.
지원되는 볼륨 블록 크기(EF300 및 EF600만 해당)	에는 그룹의 볼륨에 대해 생성할 수 있는 블록 크기가 나와 있습니다. • 512n — 512바이트 네이티브 • 512e — 512바이트가 에뮬레이트됨 • 4k—4,096바이트.

수동 방식 드라이브 특성

특징	사용
미디어 유형	용지 종류를 나타냅니다. 지원되는 용지 종류는 다음과 같습니다. • 하드 드라이브 • 솔리드 스테이트 디스크(SSD) 볼륨 그룹의 모든 드라이브는 동일한 미디어 유형(모든 SSD 또는 모든 하드 드라이브)이어야 합니다. 볼륨 그룹은 미디어 유형 또는 인터페이스 유형을 혼합하여 사용할 수 없습니다.
드라이브 블록 크기(EF300 및 EF600만 해당)	그룹의 드라이브가 쓸 수 있는 블록 크기(섹터 크기)를 표시합니다. 다음과 같은 값이 포함될 수 있습니다. • 512—512바이트 섹터 크기 • 4k—4,096바이트 섹터 크기
드라이브 용량	드라이브 용량을 나타냅니다. • 가능하면 볼륨 그룹의 현재 드라이브 용량과 동일한 용량을 가진 드라이브를 선택합니다. • 용량이 더 작은 할당되지 않은 드라이브를 추가해야 하는 경우, 볼륨 그룹에 현재 있는 각 드라이브의 가용 용량이 줄어듭니다. 따라서 드라이브 용량은 볼륨 그룹 전체에서 동일합니다. • 용량이 더 큰 할당되지 않은 드라이브를 추가해야 하는 경우, 추가하는 할당되지 않은 드라이브의 가용 용량이 볼륨 그룹의 현재 드라이브 용량과 일치하도록 감소한다는 점을 유념하십시오.
용지함	드라이브의 트레이 위치를 나타냅니다.
슬롯	드라이브의 슬롯 위치를 나타냅니다.
속도(rpm)	드라이브의 속도를 나타냅니다.
논리 섹터 크기	섹터 크기 및 형식을 나타냅니다.

특징	사용
보안 가능	이 볼륨 그룹 대상이 전체 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있는 전체 보안 가능 드라이브로 구성되어 있는지 여부를 나타냅니다. • 드라이브 보안으로 볼륨 그룹을 보호할 수 있지만 이 기능을 사용하려면 모든 드라이브가 안전해야 합니다. • FDE 전용 볼륨 그룹을 생성하려면 Secure-Capable 열에서 * Yes-FDE * 를 찾습니다. FIPS 전용 볼륨 그룹을 생성하려면 * Yes-FIPS * 또는 * Yes-FIPS(Mixed) * 를 찾습니다. "혼합"은 140-3단계 드라이브와 140-3단계 드라이브의 혼합을 나타냅니다. 이러한 수준을 혼합하여 사용하는 경우 볼륨 그룹이 낮은 보안 수준(140-2)에서 작동합니다. • 보안이 가능하거나 보안이 가능하지 않거나 보안 수준이 혼합된 드라이브로 구성된 볼륨 그룹을 생성할 수 있습니다. 볼륨 그룹의 드라이브에 보안 기능이 지원되지 않는 드라이브가 포함되어 있으면 볼륨 그룹을 안전하게 만들 수 없습니다.
DA를 지원합니다	이 그룹에 대해 DA(Data Assurance)를 사용할 수 있는지 여부를 나타냅니다. DA(Data Assurance)는 컨트롤러를 통해 드라이브로 데이터가 전달될 때 발생할 수 있는 오류를 확인하고 수정합니다. DA를 사용하려면 DA를 지원하는 볼륨 그룹을 선택합니다. (DA 지원 드라이브의 경우 풀에 생성된 볼륨에서 DA가 자동으로 활성화됩니다.) 볼륨 그룹에는 DA를 사용할 수 있거나 DA를 사용할 수 없는 드라이브가 포함될 수 있지만 모든 드라이브는 DA를 통해 이 기능을 사용할 수 있어야 합니다.
지원되는 볼륨 블록 크기(EF300 및 EF600만 해당)	에는 그룹의 볼륨에 대해 생성할 수 있는 블록 크기가 나와 있습니다. • 512n — 512바이트 네이티브 • 512e — 512바이트가 에뮬레이트됨 • 4k—4,096바이트.
리소스 프로비저닝 가능(EF300 및 EF600만 해당)	이 그룹에 대해 리소스 프로비저닝을 사용할 수 있는지 여부를 표시합니다. 리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.

풀 또는 볼륨 그룹에 용량을 추가합니다

드라이브를 추가하여 기존 풀 또는 볼륨 그룹에서 사용 가능한 용량을 확장할 수 있습니다.

확장을 수행하면 사용 가능한 추가 용량이 풀 또는 볼륨 그룹에 포함됩니다. 이 여유 용량을 사용하여 추가 볼륨을 생성할 수 있습니다. 이 작업 중에 볼륨의 데이터에 액세스할 수 있습니다.

시작하기 전에

- 드라이브가 최적 상태여야 합니다.
- 드라이브는 드라이브 유형(HDD 또는 SSD)이 동일해야 합니다.
- 풀 또는 볼륨 그룹이 Optimal 상태여야 합니다.
- 볼륨 그룹에서 허용되는 최대 볼륨 수는 256개입니다.
- 풀에서 허용되는 최대 볼륨 수는 스토리지 시스템 모델에 따라 다릅니다.
  - 2,048 볼륨(EF600 및 E5700 시리즈)
  - 1,024개 볼륨(EF300)
  - 512 볼륨(E2800 시리즈)
- 풀 또는 볼륨 그룹에 모든 보안 가능 드라이브가 포함되어 있는 경우, 보안 가능 드라이브의 암호화 기능을 계속 사용할 수 있는 안전한 드라이브만 추가합니다.

  보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.

이 작업에 대해

풀의 경우 한 번에 최대 60개의 드라이브를 추가할 수 있습니다. 볼륨 그룹의 경우 한 번에 최대 2개의 드라이브를 추가할 수 있습니다. 최대 드라이브 수보다 많은 드라이브를 추가해야 하는 경우 이 절차를 반복합니다. 풀은 스토리지 시스템의 최대 제한보다 많은 드라이브를 포함할 수 없습니다.

> 드라이브를 추가하면 보존 용량을 늘려야 할 수 있습니다. 확장 작업 후 예약된 용량을 늘리는 것이 좋습니다.

> DA를 지원하지 않는 풀 또는 볼륨 그룹에 용량을 추가할 수 있는 DA(Data Assurance)를 사용하지 마십시오. 풀 또는 볼륨 그룹은 DA 가능 드라이브의 기능을 활용할 수 없습니다. 이 상황에서는 DA를 사용할 수 없는 드라이브를 사용하는 것이 좋습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 드라이브를 추가할 풀 또는 볼륨 그룹을 선택한 다음 * 용량 추가 * 를 클릭합니다.

   용량 추가 대화 상자가 나타납니다. 풀 또는 볼륨 그룹과 호환되는 할당되지 않은 드라이브만 나타납니다.

3. 용량을 추가할 드라이브 선택… * 에서 기존 풀 또는 볼륨 그룹에 추가할 드라이브를 하나 이상 선택합니다.

   컨트롤러 펌웨어는 위에 나열된 최상의 옵션을 사용하여 할당되지 않은 드라이브를 정렬합니다. 풀 또는 볼륨 그룹에 추가된 총 사용 가능 용량이 * 선택한 총 용량 * 의 목록 아래에 표시됩니다.

필드 상세정보

필드에 입력합니다	설명
쉘프	드라이브의 쉘프 위치를 나타냅니다.
베이	드라이브의 베이 위치를 나타냅니다.
용량(GiB)	드라이브 용량을 나타냅니다. • 가능하면 풀 또는 볼륨 그룹의 현재 드라이브 용량과 동일한 용량을 가진 드라이브를 선택합니다. • 용량이 더 작은 할당되지 않은 드라이브를 추가해야 하는 경우 현재 풀 또는 볼륨 그룹에 있는 각 드라이브의 가용 용량이 줄어듭니다. 따라서 드라이브 용량은 풀 또는 볼륨 그룹에서 동일합니다. • 용량이 더 큰 할당되지 않은 드라이브를 추가해야 하는 경우, 추가하는 할당되지 않은 드라이브의 가용 용량이 줄어들기 때문에 풀 또는 볼륨 그룹의 드라이브 현재 용량과 일치하게 됩니다.
보안 가능	드라이브가 안전한지 여부를 나타냅니다. • 드라이브 보안 기능을 사용하여 풀 또는 볼륨 그룹을 보호하려면 모든 드라이브가 보안 기능을 갖추고 있어야 합니다. • 보안 기능이 있는 드라이브와 비보안 가능 드라이브를 혼합하여 풀 또는 볼륨 그룹을 생성할 수 있지만 드라이브 보안 기능을 활성화할 수는 없습니다. • 모든 보안 가능 드라이브가 있는 풀 또는 볼륨 그룹은 암호화 기능을 사용하지 않는 경우에도 스페어링 또는 확장을 위한 비보안 가능 드라이브를 수락할 수 없습니다. • 보안이 가능한 드라이브로 보고된 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다. • FIPS 드라이브는 수준 140-3이고 수준 140-3은 상위 수준의 보안일 수 있습니다. 140-3단계 드라이브와 140-3단계 드라이브를 혼합하여 선택하면 풀 또는 볼륨 그룹이 더 낮은 보안 수준(140-2)에서 작동합니다.
DA를 지원합니다	드라이브가 DA(Data Assurance)를 지원하는지 여부를 나타냅니다. • DA(Data Assurance)가 지원되지 않는 드라이브를 사용하여 DA 가능 풀 또는 볼륨 그룹에 용량을 추가하는 것은 권장되지 않습니다. 풀 또는 볼륨 그룹에는 더 이상 DA 기능이 없으며 풀 또는 볼륨 그룹 내에서 새로 생성된 볼륨에 대해 DA를 활성화하는 옵션이 더 이상 제공되지 않습니다. • DA(Data Assurance)가 지원되지 않는 풀 또는 볼륨 그룹에 용량을 추가할 수 있는 드라이브를 사용하는 것은 권장되지 않습니다. 풀 또는 볼륨 그룹이 DA 가능 드라이브의 기능을 활용할 수 없기 때문입니다(드라이브 속성이 일치하지 않음). 이 상황에서는 DA를 사용할 수 없는 드라이브를 사용하는 것이 좋습니다.

필드에 입력합니다	설명
DULBE 가능	드라이브에 DULBE(Logical Block Error) 할당 해제 또는 미기록 해제 옵션이 있는지 여부를 나타냅니다. DULBE는 EF300 또는 EF600 스토리지 어레이가 리소스 프로비저닝된 볼륨을 지원할 수 있도록 NVMe 드라이브에 대한 옵션입니다.

4. 추가 * 를 클릭합니다.

   풀 또는 볼륨 그룹에 드라이브를 추가하는 경우 풀 또는 볼륨 그룹에 다음 속성 중 하나 이상이 없는 드라이브를 선택하면 확인 대화 상자가 나타납니다.

   - 선반 상실 보호
   - 서랍 분실 방지
   - 전체 디스크 암호화 기능
   - Data Assurance입니다
   - DULBE 기능

   현재는 셸프 손실 방지 또는 드로어 손실 방지 기능이 있는 풀에 드라이브를 추가할 때 확인 대화 상자가 표시되지 않습니다.

1. 계속하려면 * 예 * 를 클릭하고, 그렇지 않으면 * 취소 * 를 클릭합니다.

결과

할당되지 않은 드라이브를 풀 또는 볼륨 그룹에 추가한 후에는 추가 드라이브를 포함하기 위해 풀 또는 볼륨 그룹의 각 볼륨에 있는 데이터가 재배포됩니다.

스토리지 관리

볼륨 중복성을 확인합니다

기술 지원의 지침이나 Recovery Guru의 지시에 따라 풀 또는 볼륨 그룹의 볼륨에서 이중화를 확인하여 해당 볼륨의 데이터가 일관되는지 여부를 결정할 수 있습니다.

이중화 데이터는 풀 또는 볼륨 그룹의 드라이브 중 하나에 장애가 발생할 경우 교체 드라이브에 대한 정보를 빠르게 재구성하는 데 사용됩니다.

시작하기 전에

- 풀 또는 볼륨 그룹의 상태가 최적이어야 합니다.
- 풀 또는 볼륨 그룹에 진행 중인 볼륨 수정 작업이 없어야 합니다.
- RAID 0에는 데이터 중복성이 없으므로 RAID 0을 제외한 모든 RAID 수준에서 이중화를 확인할 수 있습니다.

Recovery Guru에서 지시하고 기술 지원의 지침에 따라 볼륨 중복성을 확인해야 합니다.

이 작업에 대해

한 번에 하나의 풀 또는 볼륨 그룹에서만 이 검사를 수행할 수 있습니다. 볼륨 중복 검사는 다음 작업을 수행합니다.

- RAID 3 볼륨, RAID 5 볼륨 또는 RAID 6 볼륨의 데이터 블록을 검사하고 각 블록의 중복 정보를 확인합니다. (RAID 3은 명령줄 인터페이스를 사용하는 볼륨 그룹에만 할당할 수 있습니다.)
- RAID 1 미러링 드라이브의 데이터 블록을 비교합니다.
- 컨트롤러 펌웨어가 데이터가 일치하지 않는 것으로 판단할 경우 중복 오류를 반환합니다.

> ⓘ 동일한 풀 또는 볼륨 그룹에서 중복 검사를 즉시 실행하면 오류가 발생할 수 있습니다. 이 문제를 방지하려면 동일한 풀 또는 볼륨 그룹에서 다른 중복 검사를 실행하기 전에 1-2분 정도 기다리십시오.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. Uncommon Tasks [Check volume redundancy] 메뉴를 선택합니다.

   Check Redundancy 대화상자가 나타납니다.
3. 확인하려는 볼륨을 선택한 다음 이 작업을 수행할 것인지 확인하려면 를 입력합니다 `check`.
4. 확인 * 을 클릭합니다.

   볼륨 중복 검사 작업이 시작됩니다. 풀 또는 볼륨 그룹의 볼륨은 대화 상자의 테이블 상단에서 시작하여 순차적으로 스캔됩니다. 이러한 작업은 각 볼륨을 스캔할 때 수행됩니다.

   - 볼륨 테이블에서 볼륨이 선택됩니다.
   - 이중화 체크 상태는 * Status * 열에 표시됩니다.
   - 미디어 또는 패리티 오류가 발생하면 검사가 중지되고 오류가 보고됩니다.

중복 검사 상태에 대한 자세한 정보

상태	설명
보류 중	이 볼륨이 스캔되는 첫 번째 볼륨이며, 시작을 클릭하여 중복 검사를 시작하지 않았습니다. 또는 풀 또는 볼륨 그룹의 다른 볼륨에서 중복 검사 작업이 수행되고 있습니다.
확인 중입니다	볼륨이 중복 검사를 진행 중입니다.
통과	볼륨이 중복 검사를 통과했습니다. 이중화 정보에서 불일치를 감지하지 못했습니다.
실패했습니다	볼륨이 중복 검사에 실패했습니다. 이중화 정보에서 불일치가 발견되었습니다.
미디어 오류입니다	드라이브 미디어에 결함이 있어 읽을 수 없습니다. Recovery Guru에 표시되는 지침을 따릅니다.
패리티 오류입니다	패리티는 데이터의 특정 부분에 대해 있어서는 안 되는 것이 아닙니다. 패리티 오류는 잠재적으로 심각하며 영구적인 데이터 손실을 일으킬 수 있습니다.

5. 풀 또는 볼륨 그룹의 마지막 볼륨을 선택한 후 * Done * 을 클릭합니다.

풀 또는 볼륨 그룹을 삭제합니다

풀 또는 볼륨 그룹을 삭제하여 할당되지 않은 용량을 더 많이 생성할 수 있습니다. 이 용량을 재구성하여 애플리케이션 스토리지의 요구사항을 충족할 수 있습니다.

시작하기 전에

- 풀 또는 볼륨 그룹에 있는 모든 볼륨의 데이터를 백업해야 합니다.
- 모든 입출력(I/O)을 중지해야 합니다.
- 볼륨에서 파일 시스템을 마운트 해제해야 합니다.
- 풀 또는 볼륨 그룹에서 미러 관계를 모두 삭제해야 합니다.
- 풀 또는 볼륨 그룹에 대해 진행 중인 볼륨 복제 작업을 중지해야 합니다.
- 풀 또는 볼륨 그룹이 비동기식 미러링 작업에 참여해서는 안 됩니다.
- 볼륨 그룹의 드라이브에 영구 예약이 없어야 합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 목록에서 풀 또는 볼륨 그룹을 하나 선택합니다.

한 번에 하나의 풀 또는 볼륨 그룹만 선택할 수 있습니다. 목록을 아래로 스크롤하여 추가 풀 또는 볼륨 그룹을 확인합니다.

3. Uncommon Tasks[삭제] 메뉴를 선택하고 확인합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 풀 또는 볼륨 그룹의 모든 데이터를 삭제합니다.
- 풀 또는 볼륨 그룹과 연결된 모든 드라이브를 삭제합니다.
- 연결된 드라이브를 할당 해제하므로 새 풀 또는 기존 풀 또는 볼륨 그룹에서 재사용할 수 있습니다.

볼륨 그룹의 여유 용량을 통합합니다

통합 가용 용량 옵션을 사용하여 선택한 볼륨 그룹에서 기존 가용 익스텐트를 통합합니다. 이 작업을 수행하면 볼륨 그룹의 최대 가용 용량에서 추가 볼륨을 생성할 수 있습니다.

시작하기 전에

- 볼륨 그룹에는 사용 가능한 용량 영역이 하나 이상 포함되어야 합니다.
- 볼륨 그룹의 모든 볼륨이 온라인 상태이고 최적 상태여야 합니다.
- 볼륨의 세그먼트 크기 변경과 같은 볼륨 수정 작업이 진행 중이지 않아야 합니다.

이 작업에 대해

작업을 시작한 후에는 취소할 수 없습니다. 통합 작업 중에도 데이터에 계속 액세스할 수 있습니다.

다음 방법 중 하나를 사용하여 통합 가용 용량 대화 상자를 시작할 수 있습니다.

- 볼륨 그룹에 대해 사용 가능한 용량 영역이 하나 이상 감지되면 알림 영역의 홈 페이지에 "사용 가능한 용량 통합" 권장 사항이 표시됩니다. 무료 용량 통합 * 링크를 클릭하여 대화 상자를 시작합니다.
- 다음 작업에 설명된 대로 Pools & Volume Groups 페이지에서 Consolidate Free Capacity 대화 상자를 시작할 수도 있습니다.

여유 용량 영역에 대해 자세히 알아보십시오

> 사용 가능한 용량 영역은 볼륨 삭제 또는 볼륨 생성 중 사용 가능한 모든 용량을 사용하지 않음으로 인해 발생할 수 있는 사용 가능한 용량입니다. 하나 이상의 사용 가능한 용량 영역이 있는 볼륨 그룹에서 볼륨을 생성할 때 볼륨의 용량은 해당 볼륨 그룹에서 가장 큰 사용 가능한 용량 영역으로 제한됩니다. 예를 들어, 볼륨 그룹의 사용 가능한 용량이 총 15GiB이고 사용 가능한 최대 용량 영역이 10GiB인 경우 생성할 수 있는 최대 볼륨은 10GiB입니다.
>
> 볼륨 그룹에 여유 용량을 통합하여 쓰기 성능을 향상할 수 있습니다. 호스트가 파일을 쓰기, 수정 및 삭제할 때 볼륨 그룹의 사용 가능한 용량이 시간 경과에 따라 조각화됩니다. 결국 가용 용량은 단일 연속 블록에 위치하지 않고 볼륨 그룹 전체에 작은 조각으로 분산됩니다. 이로 인해 호스트가 사용 가능한 무료 클러스터 범위에 맞게 새 파일을 조각으로 써야 하기 때문에 파일 조각화가 더욱 심해집니다.
>
> 선택한 볼륨 그룹에 여유 용량을 통합하면 호스트가 새 파일을 쓸 때마다 파일 시스템 성능이 향상됩니다. 또한 통합 프로세스를 통해 새 파일이 나중에 조각화되는 것을 방지할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 통합할 여유 용량이 있는 볼륨 그룹을 선택한 다음, Uncommon Tasks [Consolidate volume group free capacity] 메뉴를 선택합니다.

   여유 용량 통합 대화 상자가 나타납니다.

3. 이 작업을 수행하려면 를 입력합니다 `consolidate`.
4. 통합 * 을 클릭합니다.

   System Manager는 이후 스토리지 구성 작업을 위해 볼륨 그룹의 여유 용량 영역을 연속된 하나의 양으로 통합(조각 모음)하기 시작합니다.

작업을 마친 후

통합 가용 용량 작업의 진행률을 보려면 홈 [View Operations in Progress] 메뉴를 선택합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

볼륨 그룹 내보내기/가져오기

볼륨 그룹 마이그레이션을 사용하면 볼륨 그룹을 내보내서 볼륨 그룹을 다른 스토리지 어레이로 가져올 수 있습니다.

내보내기/가져오기 기능은 SANtricity 시스템 관리자 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

풀**,** 볼륨 그룹 또는 **SSD Cache**에서 로케이터 표시등을 켭니다

드라이브를 찾아 선택한 풀, 볼륨 그룹 또는 SSD Cache를 구성하는 모든 드라이브를 물리적으로 식별할 수 있습니다. 선택한 풀, 볼륨 그룹 또는 SSD Cache의 각 드라이브에 LED 표시등이 켜집니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 찾을 풀, 볼륨 그룹 또는 SSD Cache를 선택한 다음 menu:More [Turn on locator Lights](메뉴 켜기: 로케이터 라이트)를 클릭합니다.

   선택한 풀, 볼륨 그룹 또는 SSD Cache를 구성하는 드라이브의 표시등이 켜져 있음을 나타내는 대화 상자가 나타납니다.

3. 드라이브를 찾은 후 * 끄기 * 를 클릭합니다.

풀 또는 **SSD Cache**에서 용량을 제거합니다

드라이브를 제거하여 기존 풀 또는 SSD Cache의 용량을 줄일 수 있습니다.

드라이브를 제거한 후에는 풀 또는 SSD Cache의 각 볼륨에 있는 데이터가 나머지 드라이브에 재배포됩니다. 제거된 드라이브는 할당되지 않고 해당 용량은 스토리지 어레이의 총 사용 가능 용량의 일부가 됩니다.

이 작업에 대해

용량을 제거할 때 다음 지침을 따르십시오.

- SSD Cache를 먼저 삭제하지 않으면 SSD Cache의 마지막 드라이브를 제거할 수 없습니다.
- 풀의 드라이브 수를 11개 미만으로 줄일 수는 없습니다.
- 한 번에 최대 12개의 드라이브를 제거할 수 있습니다. 12개 이상의 드라이브를 제거해야 하는 경우 이 절차를 반복합니다.
- 데이터가 풀 또는 SSD Cache의 나머지 드라이브에 재분배된 경우, 데이터를 포함할 풀 또는 SSD Cache에 사용 가능한 용량이 충분하지 않으면 드라이브를 제거할 수 없습니다.

잠재적인 성능 영향에 대해 읽어보십시오

- 풀 또는 SSD Cache에서 드라이브를 제거하면 볼륨 성능이 저하될 수 있습니다.
- 풀 또는 SSD Cache에서 용량을 제거할 때는 보존 용량이 사용되지 않습니다. 하지만 풀 또는 SSD Cache에 남아 있는 드라이브 수에 따라 보존 용량이 줄어들 수 있습니다.

보안 가능 드라이브에 미치는 영향에 대해 알아보십시오

- 보안 기능이 없는 마지막 드라이브를 제거하면 모든 보안 가능 드라이브가 풀에 남아 있습니다. 이 경우 풀에 대한 보안을 설정할 수 있는 옵션이 제공됩니다.
- DA(Data Assurance)를 지원하지 않는 마지막 드라이브를 제거하면 모든 DA 가능 드라이브가 풀에 남아 있습니다.

> 풀에서 생성한 새 볼륨은 DA를 사용할 수 있습니다. 기존 볼륨을 DA로 사용하려면 볼륨을 삭제한 다음 다시 생성해야 합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 풀 또는 SSD Cache를 선택한 다음 MENU: More [Remove capacity]([용량 제거]) 를 클릭합니다.

   용량 제거 대화 상자가 나타납니다.
3. 목록에서 하나 이상의 드라이브를 선택합니다.

   목록에서 드라이브를 선택하거나 선택 취소하면 * 선택한 총 용량 * 필드가 업데이트됩니다. 이 필드에는 선택한 드라이브를 제거한 후 결과로 표시되는 풀 또는 SSD Cache의 총 용량이 표시됩니다.
4. 제거 * 를 클릭한 다음 드라이브 제거 여부를 확인합니다.

   풀 또는 SSD Cache에서 새로 축소된 용량이 Pools and Volume Groups 뷰에 반영됩니다.

풀 및 그룹 설정을 수정합니다

풀의 구성 설정을 변경합니다

풀의 이름, 용량 알림 설정, 수정 우선 순위 및 보존 용량을 비롯한 풀 설정을 편집할 수 있습니다.

이 작업에 대해

이 작업에서는 풀에 대한 구성 설정을 변경하는 방법을 설명합니다.

> System Manager 인터페이스를 사용하여 풀의 RAID 레벨을 변경할 수 없습니다. System Manager는 풀을 RAID 6으로 자동 구성합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 편집할 풀을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   풀 설정 대화 상자가 나타납니다.

3. Settings * 탭을 선택한 다음 필요에 따라 풀 설정을 편집합니다.

필드 상세정보

설정	설명
이름	사용자 제공 풀 이름을 변경할 수 있습니다. 풀 이름을 지정해야 합니다.
용량 알림	풀의 사용 가능한 용량이 지정된 임계값에 도달하거나 이를 초과할 경우 알림 알림을 보낼 수 있습니다. 풀에 저장된 데이터가 지정된 임계값을 초과하면 System Manager에서 메시지를 보내 스토리지 공간을 추가하거나 불필요한 개체를 삭제할 시간을 지정합니다. 경고는 대시보드의 알림 영역에 표시되며 서버에서 이메일 및 SNMP 트랩 메시지를 통해 관리자에게 보낼 수 있습니다. 다음과 같은 용량 알림을 정의할 수 있습니다. • * Critical alert * — 풀의 사용 가능한 용량이 지정된 임계값에 도달하거나 이를 초과할 때 이 중요 알림을 보냅니다. 스피너 컨트롤을 사용하여 임계값 비율을 조정합니다. 이 알림을 비활성화하려면 확인란을 선택합니다. • * Early alert * — 풀의 사용 가능한 용량이 지정된 임계값에 도달하면 이 조기 알림이 표시됩니다. 스피너 컨트롤을 사용하여 임계값 비율을 조정합니다. 이 알림을 비활성화하려면 확인란을 선택합니다.
수정 우선 순위	시스템 성능과 관련하여 풀의 수정 작업에 대한 우선 순위 수준을 지정할 수 있습니다. 풀에서 수정 작업의 우선 순위가 높을수록 작업이 더 빨리 완료되지만 호스트 입출력 성능이 저하될 수 있습니다. 우선 순위가 낮으면 작업에 더 오래 걸리지만 호스트 I/O 성능에는 영향을 덜 받습니다. 최저, 최저, 중간, 높음, 최고 등 5가지 우선 순위 수준 중에서 선택할 수 있습니다. 우선 순위 수준이 높을수록 호스트 I/O 및 시스템 성능에 미치는 영향이 커집니다. • * Critical reconstruction priority * — 이 슬라이더 막대는 여러 드라이브에 장애가 발생하여 일부 데이터에 중복성이 없고 추가적인 드라이브 장애로 인해 데이터가 손실될 경우 데이터 재구성 작업의 우선순위를 결정합니다. • * 저하된 재구성 우선순위 * — 이 슬라이더 막대는 드라이브 장애가 발생했을 때 데이터 재구성 작업의 우선순위를 결정하지만, 데이터에는 중복성이 있으며 추가적인 드라이브 장애로 인해 데이터가 손실되지 않습니다. • * 백그라운드 작업 우선 순위 * — 이 슬라이더 막대는 풀이 최적 상태인 동안 발생하는 풀 백그라운드 작업의 우선 순위를 결정합니다. 이러한 작업에는 DVE(Dynamic Volume Expansion), iaf(Instant Availability Format) 및 교체되거나 추가된 드라이브로 데이터 마이그레이션 등이 있습니다.

설정	설명
보존 용량(EF600 또는 EF300의 경우 "최적화 용량")	• Preservation capacity * — 잠재적인 드라이브 오류를 지원하기 위해 풀에 예약된 용량을 결정하기 위해 드라이브 수를 정의할 수 있습니다. 드라이브 장애가 발생하면 보존 용량이 재구성 데이터를 저장하는 데 사용됩니다. 풀은 볼륨 그룹에서 사용되는 핫 스페어 드라이브 대신 데이터 재구성 프로세스 중에 보존 용량을 사용합니다. Spinner 컨트롤을 사용하여 드라이브 수를 조정합니다. 드라이브 수에 따라 풀의 보존 용량이 spinner 상자 옆에 표시됩니다. 보존 용량에 대한 다음 정보를 염두에 두십시오. • 보존 용량은 풀의 총 가용 용량에서 차감되기 때문에 예비 용량을 예약하는 경우 볼륨을 생성하는 데 사용할 수 있는 가용 용량에 영향을 줍니다. 보존 용량에 0을 지정하면 풀의 모든 가용 용량이 볼륨 생성에 사용됩니다. • 보존 용량을 줄이면 풀 볼륨에 사용할 수 있는 용량이 증가합니다. ◦ 추가 최적화 용량 * (EF600 및 EF300 어레이만 해당) — 풀을 생성할 때 사용 가능한 용량과 성능 및 드라이브 마모 수명 간의 균형을 제공하는 권장 최적화 용량이 생성됩니다. 사용 가능한 용량 증가를 희생하여 성능 및 드라이브 마모 수명을 개선하려면 슬라이더를 오른쪽으로 이동하거나 성능 및 드라이브 마모 수명을 연장하여 사용 가능한 용량을 늘리기 위해 슬라이더를 왼쪽으로 이동하면 이러한 균형을 조정할 수 있습니다. SSD 드라이브는 용량의 일부가 할당되지 않은 경우 수명이 더 길고 쓰기 성능이 극대화됩니다. 풀과 연결된 드라이브의 경우 할당되지 않은 용량은 풀의 보존 용량, 사용 가능한 용량(볼륨에서 사용하지 않는 용량), 추가 최적화 용량으로 남겨 둔 사용 가능한 용량의 일부로 구성됩니다. 추가 최적화 용량은 사용 가능한 용량을 줄여 최적화 용량을 최소화하므로 볼륨 생성에 사용할 수 없습니다.

4. 저장 * 을 클릭합니다.

볼륨 그룹의 구성 설정을 변경합니다

이름 및 RAID 레벨을 포함하여 볼륨 그룹의 설정을 편집할 수 있습니다.

시작하기 전에

볼륨 그룹에 액세스하는 응용 프로그램의 성능 요구 사항을 수용하기 위해 RAID 레벨을 변경하는 경우 다음 필수 구성 요소를 충족해야 합니다.

- 볼륨 그룹이 Optimal(최적) 상태여야 합니다.
- 새 RAID 레벨로 변환하려면 볼륨 그룹에 충분한 용량이 있어야 합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 편집할 볼륨 그룹을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   볼륨 그룹 설정 대화 상자가 나타납니다.

3. 설정 * 탭을 선택한 다음 볼륨 그룹 설정을 적절하게 편집합니다.

필드 상세정보

설정	설명
이름	볼륨 그룹의 사용자 제공 이름을 변경할 수 있습니다. 볼륨 그룹의 이름을 지정해야 합니다.
RAID 레벨	드롭다운 메뉴에서 새 RAID 레벨을 선택합니다. • * RAID 0 스트라이핑* — 고성능을 제공하지만 데이터 중복성을 제공하지 않습니다. 볼륨 그룹에서 단일 드라이브에 장애가 발생하면 연결된 모든 볼륨이 실패하고 모든 데이터가 손실됩니다. 스트라이핑 RAID 그룹은 두 개 이상의 드라이브를 하나의 대용량 논리 드라이브로 결합합니다. • * RAID 1 미러링 * — 고성능 및 최고의 데이터 가용성을 제공하며, 기업 또는 개인 차원에서 중요한 데이터를 저장하는 데 적합합니다. 한 드라이브의 내용을 미러링된 쌍의 두 번째 드라이브에 자동으로 미러링하여 데이터를 보호합니다. 단일 드라이브 장애 시 보호 기능을 제공합니다. • * RAID 10 스트라이핑/미러링* — RAID 0(스트라이핑)과 RAID 1(미러링)의 조합을 제공하며, 4개 이상의 드라이브를 선택할 때 가능합니다. RAID 10은 고성능 및 내결함성이 필요한 데이터베이스와 같은 대용량 트랜잭션 애플리케이션에 적합합니다. • * RAID 5 * — 일반적인 I/O 크기가 작고 읽기 작업이 많은 다중 사용자 환경(예: 데이터베이스 또는 파일 시스템 스토리지)에 적합합니다. • * RAID 6 * — RAID 5 이상의 이중화 보호가 필요하지만 높은 쓰기 성능이 필요하지 않은 환경에 적합합니다. RAID 3은 CLI(Command Line Interface)를 사용하여 볼륨 그룹에만 할당할 수 있습니다. RAID 레벨을 변경하면 이 작업이 시작된 후에는 취소할 수 없습니다. 변경 중에는 데이터를 계속 사용할 수 있습니다.
용량 최적화(EF600 어레이만 해당)	볼륨 그룹이 생성되면 사용 가능한 용량과 성능 및 드라이브 마모 수명 간의 균형을 제공하는 권장 최적화 용량이 생성됩니다. 사용 가능한 용량 증가를 희생하여 성능 및 드라이브 마모 수명을 개선하려면 슬라이더를 오른쪽으로 이동하거나 성능 및 드라이브 마모 수명을 연장하여 사용 가능한 용량을 늘리기 위해 슬라이더를 왼쪽으로 이동하면 이러한 균형을 조정할 수 있습니다. SSD 드라이브는 용량의 일부가 할당되지 않은 경우 수명이 더 길고 쓰기 성능이 극대화됩니다. 볼륨 그룹과 연결된 드라이브의 경우 할당되지 않은 용량은 그룹의 여유 용량(볼륨에서 사용하지 않는 용량)과 추가 최적화 용량으로 남겨 둔 사용 가능한 용량의 일부로 구성됩니다. 추가 최적화 용량은 사용 가능한 용량을 줄여 최적화 용량을 최소화하므로 볼륨 생성에 사용할 수 없습니다.

4. 저장 * 을 클릭합니다.

RAID 레벨 변경으로 인해 용량이 줄어들거나, 볼륨 중복성이 손실되거나, 쉘프/드로어 손실 보호가 손실되면 확인 대화 상자가 나타납니다. 계속하려면 * 예 * 를 선택하고, 그렇지 않으면 * 아니요 * 를 클릭합니다.

결과

볼륨 그룹의 RAID 레벨을 변경하면 System Manager에서 볼륨 그룹을 구성하는 모든 볼륨의 RAID 레벨을 변경합니다. 작업 중에 성능이 약간 영향을 받을 수 있습니다.

기존 볼륨 그룹 및 풀에서 리소스 프로비저닝을 설정하거나 해제합니다

모든 DULBE 가능 드라이브의 경우 풀 또는 볼륨 그룹의 기존 볼륨에서 리소스 프로비저닝을 설정하거나 해제할 수 있습니다.

리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다. 볼륨에 할당된 모든 드라이브 블록이 할당 해제(매핑 해제)되어 SSD 마모 수명을 개선하고 최대 쓰기 성능을 높일 수 있습니다.

기본적으로 드라이브가 DULBE를 지원하는 시스템에서 리소스 프로비저닝이 설정됩니다. 이전에 리소스 프로비저닝을 사용하지 않도록 설정하지 않았다면 리소스 프로비저닝을 설정할 필요가 없습니다.

시작하기 전에

- EF300 또는 EF600 스토리지 어레이가 있어야 합니다.
- 모든 드라이브에서 NVMe 할당 해제 또는 DULBE(UnWritten Logical Block Error Enable) 오류 복구 기능을 지원하는 SSD 볼륨 그룹 또는 풀이 있어야 합니다. 그렇지 않으면 리소스 프로비저닝 옵션을 사용할 수 없습니다.

이 작업에 대해

기존 볼륨 그룹 및 풀에 대한 리소스 프로비저닝을 설정하면 선택한 볼륨 그룹 또는 풀에 있는 모든 볼륨을 변경하여 블록을 할당 해제할 수 있습니다. 이 프로세스에는 매핑 해제 세분화 수준에서 일관된 할당을 보장하기 위한 백그라운드 작업이 포함될 수 있습니다. 이 작업에서는 공간을 매핑 해제하지 않습니다. 백그라운드 작업이 완료되면 운영 체제에서 사용하지 않는 블록의 매핑을 해제해야 여유 공간을 만들 수 있습니다.

기존 볼륨 그룹 또는 풀에 대해 리소스 프로비저닝을 사용하지 않도록 설정하면 백그라운드 작업이 모든 볼륨의 모든 논리적 블록을 다시 기록합니다. 기존 데이터는 그대로 유지됩니다. 쓰기 작업은 볼륨 그룹 또는 풀과 연결된 드라이브의 블록을 매핑하거나 프로비저닝합니다.

새 볼륨 그룹 및 풀의 경우 Settings[System>Additional Settings>Enable/Disable Resource-provisioned Volumes] 메뉴에서 리소스 프로비저닝을 설정하거나 해제할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 목록에서 풀 또는 볼륨 그룹을 하나 선택합니다.

   한 번에 하나의 풀 또는 볼륨 그룹만 선택할 수 있습니다. 목록을 아래로 스크롤하여 추가 풀 또는 볼륨 그룹을 확인합니다.

3. Uncommon Tasks * 를 선택한 다음 * Enable resource provisioning * 또는 * Disable resource provisioning * 을 선택합니다.
4. 대화 상자에서 작업을 확인합니다.

* DULBE * 를 다시 활성화한 경우 백그라운드 작업이 완료된 후 호스트를 재부팅하여 DULBE 구성 변경 사항을 탐지한 다음 모든 파일 시스템을 다시 마운트해야 할 수 있습니다.

새 볼륨 그룹 또는 풀에 대한 리소스 프로비저닝을 설정하거나 해제합니다

이전에 리소스 프로비저닝을 위한 기본 기능을 비활성화한 경우 새로 생성한 모든 SSD 볼륨 그룹 또는 풀에 대해 다시 설정할 수 있습니다. 설정을 다시 비활성화할 수도 있습니다.

리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다. 볼륨에 할당된 모든 드라이브 블록이 할당 해제(매핑 해제)되어 SSD 마모 수명을 개선하고 최대 쓰기 성능을 높일 수 있습니다.

기본적으로 드라이브가 DULBE를 지원하는 시스템에서 리소스 프로비저닝이 설정됩니다.

시작하기 전에

- EF300 또는 EF600 스토리지 어레이가 있어야 합니다.
- 모든 드라이브에서 NVMe 할당 해제 또는 DULBE(UnWritten Logical Block Error Enable) 오류 복구 기능을 지원하는 SSD 볼륨 그룹 또는 풀이 있어야 합니다.

이 작업에 대해

새 볼륨 그룹 또는 풀에 대해 리소스 프로비저닝을 다시 설정하면 새로 생성한 볼륨 그룹 및 풀만 영향을 받습니다. 리소스 프로비저닝이 설정된 기존 볼륨 그룹 및 풀은 변경되지 않습니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 찾은 다음 * 리소스 프로비저닝된 볼륨 * 사용/사용 안 함 을 클릭합니다.

   설정 설명은 리소스 프로비저닝이 현재 활성화되어 있는지 여부를 나타냅니다.

3. 대화 상자에서 작업을 확인합니다.

결과

리소스 프로비저닝을 설정하거나 해제하면 생성한 새 SSD 풀 또는 볼륨 그룹에만 영향을 줍니다. 기존 풀 또는 볼륨 그룹은 변경되지 않습니다.

풀 또는 볼륨 그룹에 대한 보안을 설정합니다

풀 또는 볼륨 그룹에 대해 드라이브 보안을 설정하여 풀 또는 볼륨 그룹에 포함된 드라이브의 데이터에 대한 무단 액세스를 방지할 수 있습니다. 드라이브의 읽기 및 쓰기 액세스는 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다.

시작하기 전에

- 드라이브 보안 기능을 활성화해야 합니다.
- 보안 키를 만들어야 합니다.
- 풀 또는 볼륨 그룹이 Optimal 상태여야 합니다.
- 풀 또는 볼륨 그룹의 모든 드라이브는 보안이 가능한 드라이브여야 합니다.

이 작업에 대해

Drive Security를 사용하려면 보안 기능이 있는 풀 또는 볼륨 그룹을 선택합니다. 풀 또는 볼륨 그룹에는 보안이 가능한 드라이브와 비보안 가능 드라이브가 모두 포함될 수 있지만 모든 드라이브는 암호화 기능을 사용할 수 있어야 합니다.

보안을 설정한 후에는 풀 또는 볼륨 그룹을 삭제한 다음 드라이브를 삭제해야만 보안을 제거할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 보안을 설정할 풀 또는 볼륨 그룹을 선택한 다음 MENU: More [Enable security] 를 클릭합니다.

   보안 활성화 확인 대화 상자가 나타납니다.

3. 선택한 풀 또는 볼륨 그룹에 대해 보안을 설정할지 확인한 다음 * 사용 * 을 클릭합니다.

SSD 캐시를 관리합니다

SSD Cache의 작동 방식

SSD Cache 기능은 컨트롤러 기반 솔루션으로, 가장 자주 액세스하는 데이터("핫" 데이터)를 지연 시간이 짧은 SSD(Solid State Drive)에 캐싱하여 시스템 성능을 동적으로 향상합니다. SSD Cache는 호스트 읽기에만 사용됩니다.

SSD Cache와 운영 캐시 비교

SSD Cache는 컨트롤러의 동적 DRAM(Random Access Memory)의 기본 캐시와 함께 사용되는 보조 캐시입니다.

SSD Cache는 운영 캐시와 다르게 작동합니다.

- 운영 캐시의 경우 각 I/O 작업에서 캐시를 통해 데이터를 스테이징해야 작업을 수행할 수 있습니다.

  운영 캐시에서 데이터는 호스트 읽기 후 DRAM에 저장됩니다.

- SSD Cache는 데이터를 캐시에 저장하여 전체 시스템 성능을 향상하는 경우에만 사용됩니다.

  SSD Cache에서는 데이터가 볼륨에서 복사되어 두 개의 내부 RAID 볼륨(컨트롤러당 1개)에 저장됩니다. SSD Cache는 사용자가 SSD Cache를 생성할 때 자동으로 생성됩니다.

내부 RAID 볼륨은 내부 캐시 처리를 위해 사용됩니다. 이러한 볼륨은 사용자 인터페이스에 액세스하거나 표시할 수 없습니다. 그러나 이러한 두 볼륨은 스토리지 어레이에서 허용되는 총 볼륨 수에 대해 계산됩니다.

SSD Cache의 사용 방법

지능형 캐싱은 데이터를 지연 시간이 짧은 드라이브에 배치하므로 향후 데이터 요청에 더욱 빠르게 대응할 수 있습니다. 프로그램이 캐시에 있는 데이터("캐시 적중"이라고 함)를 요청하면 지연 시간이 낮은 드라이브에서 해당 트랜잭션을 처리할 수 있습니다. 그렇지 않으면 ""캐시 누락""이 발생하고 데이터는 속도가 느린 원래 드라이브에서 액세스해야 합니다. 캐시 적중률이 높아질수록 전반적인 성능이 향상됩니다.

호스트 프로그램이 스토리지 어레이의 드라이브에 액세스하면 데이터가 SSD Cache에 저장됩니다. 호스트 프로그램에서 동일한 데이터에 다시 액세스할 때 하드 드라이브 대신 SSD Cache에서 데이터를 읽습니다. 일반적으로 액세스하는 데이터는 SSD Cache에 저장됩니다. 하드 드라이브는 SSD Cache에서 데이터를 읽을 수 없는 경우에만

액세스할 수 있습니다.

SSD Cache는 데이터를 캐시에 저장하여 전체 시스템 성능을 향상하는 경우에만 사용됩니다.

CPU가 읽기 데이터를 처리해야 하는 경우 다음 단계를 따릅니다.

1. DRAM 캐시를 확인합니다.
2. DRAM 캐시에서 발견되지 않으면 SSD Cache를 확인합니다.
3. SSD Cache에서 찾을 수 없는 경우 하드 드라이브에서 가져옵니다. 데이터를 캐싱할 가치가 있는 것으로 판단되면 SSD Cache로 복사하십시오.

향상된 성능

액세스 빈도가 가장 높은 데이터(핫 스폿)를 SSD Cache에 복사하면 하드 디스크의 작동 효율성이 증가하고, 지연 시간이 단축되고, 읽기 및 쓰기 속도가 빨라집니다. 고성능 SSD를 사용하여 HDD 볼륨의 데이터를 캐싱하면 I/O 성능과 응답 시간이 향상됩니다.

간단한 볼륨 I/O 메커니즘을 사용하여 데이터를 SSD Cache로 이동하거나 SSD Cache에서 이동할 수 있습니다. 데이터를 SSD에 캐싱하고 저장한 후에는 SSD Cache에서 해당 데이터의 후속 읽기가 수행되므로 HDD 볼륨에 액세스할 필요가 없습니다.

SSD Cache 및 드라이브 보안 기능

또한 Drive Security(보안 활성화)를 사용하는 볼륨에서 SSD Cache를 사용하려면 볼륨과 SSD Cache의 드라이브 보안 기능이 일치해야 합니다. 일치하지 않으면 볼륨이 보안 활성화되지 않습니다.

SSD Cache 구축

SSD Cache를 구현하려면 다음을 수행합니다.

1. SSD Cache를 생성합니다.
2. SSD Cache를 SSD 읽기 캐싱을 구현할 볼륨과 연결합니다.

> 컨트롤러의 SSD Cache를 사용하도록 할당된 볼륨은 자동 로드 밸런싱 전송을 지원하지 않습니다.

SSD 캐시 제한 사항

스토리지 어레이에서 SSD Cache를 사용할 때의 제한 사항에 대해 알아보십시오.

제한 사항

- 컨트롤러의 SSD Cache를 사용하도록 할당된 볼륨은 자동 로드 밸런싱 전송을 지원하지 않습니다.
- 현재 스토리지 어레이당 하나의 SSD Cache만 지원됩니다.
- 스토리지 어레이에서 사용할 수 있는 최대 SSD Cache 용량은 10TB입니다.
- SSD Cache는 스냅샷 이미지에서 지원되지 않습니다.
- SSD Cache가 활성화 또는 비활성화된 볼륨을 가져오거나 내보내면 캐시된 데이터를 가져오거나 내보낼 수 없습니다.
- SSD Cache를 먼저 삭제하지 않으면 SSD Cache의 마지막 드라이브를 제거할 수 없습니다.

- SSD Cache는 SSD Cache를 생성할 때만 보안을 설정할 수 있습니다. 나중에 볼륨에 대해 가능한 한 보안을 설정할 수 없습니다.
- SSD Cache에서 보안이 불가능한 드라이브와 보안 기능을 함께 사용하는 경우 이러한 드라이브에 대해 드라이브 보안을 설정할 수 없습니다.
- 보안이 설정된 볼륨에는 보안이 설정된 SSD Cache가 있어야 합니다.

SSD Cache 생성

시스템 성능을 동적으로 가속하기 위해 SSD Cache 기능을 사용하여 가장 자주 액세스하는 데이터("핫" 데이터)를 지연 시간이 짧은 SSD(Solid State Drive)에 캐싱할 수 있습니다. SSD Cache는 호스트 읽기에만 사용됩니다.

시작하기 전에

스토리지 배열에 일부 SSD 드라이브가 포함되어 있어야 합니다.

이 작업에 대해

새 SSD Cache를 생성할 때 단일 드라이브 또는 여러 드라이브를 사용할 수 있습니다. 읽기 캐시가 스토리지 배열에 있기 때문에, 캐시는 스토리지 배열을 사용하는 모든 응용 프로그램에서 공유됩니다. 캐시할 볼륨을 선택한 다음 캐싱은 자동으로 이루어지며 동적 볼륨입니다.

새 SSD Cache를 생성할 때 다음 지침을 따르십시오.

- SSD Cache는 나중에 생성하지 않을 때만 보안을 설정할 수 있습니다.
- 스토리지 어레이당 하나의 SSD Cache만 지원됩니다.
- 하나의 볼륨에만 SSD 캐시가 활성화된 경우 전체 SSD 캐시가 해당 볼륨을 소유하는 컨트롤러에 할당됩니다.
- 스토리지 어레이에서 사용 가능한 최대 SSD Cache 용량은 컨트롤러의 기본 캐시 용량에 따라 달라집니다.
- SSD Cache는 스냅샷 이미지에서 지원되지 않습니다.
- SSD Cache가 활성화 또는 비활성화된 볼륨을 가져오거나 내보내면 캐시된 데이터를 가져오거나 내보낼 수 없습니다.
- 컨트롤러의 SSD Cache를 사용하도록 할당된 볼륨은 자동 로드 밸런싱 전송을 지원하지 않습니다.
- 연결된 볼륨이 보안 설정된 경우 보안 설정된 SSD Cache를 생성합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 메뉴: 생성 [SSD Cache] 를 클릭합니다.

   SSD 캐시 생성 대화 상자가 나타납니다.

3. SSD Cache의 이름을 입력합니다.
4. 다음 특성을 기준으로 사용할 SSD Cache 대상을 선택합니다.

특징	사용
용량	에는 사용 가능한 용량이 GiB 단위로 표시됩니다. 애플리케이션의 스토리지 요구사항에 맞는 용량을 선택합니다. SSD Cache의 최대 용량은 컨트롤러의 기본 캐시 용량에 따라 다릅니다. SSD Cache에 최대 용량을 초과하여 할당하는 경우 추가 용량을 사용할 수 없습니다. SSD Cache 용량은 할당된 전체 용량에 반영됩니다.
총 드라이브 수	에는 이 SSD 캐시에 사용할 수 있는 드라이브 수가 나와 있습니다. 원하는 드라이브 수가 들어 있는 SSD 대상을 선택합니다.
보안 가능	SSD 캐시 대상이 전체 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있는 전체 보안 가능 드라이브로 구성되어 있는지 여부를 나타냅니다. 보안이 설정된 SSD 캐시를 생성하려면 Secure-Capable 열에서 * Yes-FDE * 또는 * Yes-FIPS * 를 찾습니다.
보안을 설정하시겠습니까?	에서는 보안 가능 드라이브를 사용하여 드라이브 보안 기능을 활성화하는 옵션을 제공합니다. 보안이 설정된 SSD Cache를 생성하려면 보안 활성화 확인란을 선택합니다. 일단 활성화되면 보안을 비활성화할 수 없습니다. SSD Cache는 나중에 생성하지 않을 때만 보안을 설정할 수 있습니다.
DA를 지원합니다	이 SSD Cache 대상에 대해 DA(Data Assurance)를 사용할 수 있는지 여부를 나타냅니다. DA(Data Assurance)는 컨트롤러를 통해 드라이브로 데이터가 전송될 때 발생할 수 있는 오류를 확인하고 수정합니다. DA를 사용하려면 DA를 지원하는 SSD Cache 대상을 선택합니다. 이 옵션은 DA 기능이 활성화된 경우에만 사용할 수 있습니다. SSD Cache에는 DA 지원 드라이브와 비 DA 지원 드라이브가 모두 포함될 수 있지만 DA를 사용하려면 모든 드라이브가 DA 지원 가능해야 합니다.

5. SSD Cache를 SSD 읽기 캐싱을 구현할 볼륨과 연결합니다. 호환 볼륨에서 SSD 캐시를 즉시 활성화하려면 * 호스트에 매핑된 기존 호환 볼륨에서 SSD 캐시 사용 * 확인란을 선택합니다.

   볼륨은 동일한 드라이브 보안 및 DA 기능을 공유하는 경우 호환됩니다.

6. Create * 를 클릭합니다.

SSD 캐시 설정을 변경합니다

SSD Cache의 이름을 편집하고 해당 상태, 최대 및 현재 용량, Drive Security 및 Data Assurance 상태, 관련 볼륨 및 드라이브를 확인할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 편집할 SSD Cache를 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   SSD Cache Settings 대화상자가 나타납니다.
3. SSD Cache 설정을 적절하게 검토 또는 편집합니다.

필드 상세정보

설정	설명
이름	변경할 수 있는 SSD Cache의 이름을 표시합니다. SSD Cache의 이름은 필수입니다.
특징	SSD Cache의 상태를 표시합니다. 가능한 상태는 다음과 같습니다. • 최적 • 알 수 없음 • 성능 저하 • 실패(실패 상태로 인해 심각한 MEL 이벤트가 발생합니다.) • 일시 중단됨
용량	에는 SSD Cache에 허용되는 현재 용량과 최대 용량이 나와 있습니다. SSD Cache에 허용되는 최대 용량은 컨트롤러의 기본 캐시 크기에 따라 다릅니다. • 최대 1GiB • 1GiB에서 2GiB까지 • 2GiB에서 4GiB까지 • 4GiB 초과
보안 및 DA	에서는 SSD Cache의 드라이브 보안 및 Data Assurance 상태를 보여 줍니다. • * 보안 가능 * — SSD 캐시가 완전히 보안 가능 드라이브로 구성되어 있는지 여부를 나타냅니다. 보안 가능 드라이브는 자체 암호화 드라이브로 무단 액세스로부터 데이터를 보호할 수 있습니다. • * Secure-enabled * — SSD Cache에서 보안이 설정되었는지 여부를 나타냅니다. • * DA 가능 * — SSD 캐시가 완전히 DA 가능 드라이브로 구성되는지 여부를 나타냅니다. DA 지원 드라이브는 호스트와 스토리지 시스템 간에 데이터가 전달될 때 발생할 수 있는 오류를 확인하고 수정할 수 있습니다.
연관된 개체	에는 SSD Cache와 연결된 볼륨 및 드라이브가 나와 있습니다.

4. 저장 * 을 클릭합니다.

SSD Cache 통계를 확인합니다

SSD Cache의 통계(예: 읽기, 쓰기, 캐시 적중, 캐시 할당 백분율)를 볼 수 있습니다. 캐시 활용률입니다.

상세 통계의 하위 집합인 공칭 통계가 SSD 캐시 통계 보기 대화 상자에 표시됩니다. 모든 SSD 통계를 파일로 엑스포트하는 경우에만 SSD Cache에 대한 상세 통계를 볼 수 `.csv` 있습니다.

통계를 검토 및 해석할 때는 통계의 조합을 통해 일부 해석이 파생된다는 점을 염두에 두십시오.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 통계를 보려는 SSD Cache를 선택하고 메뉴: 자세히 [SSD Cache 통계 보기]를 클릭합니다.

   SSD Cache 통계 보기 대화 상자가 나타나고 선택한 SSD 캐시에 대한 공칭 통계가 표시됩니다.

   필드 상세정보

설정	설명
읽기	에는 SSD Cache 지원 볼륨의 총 호스트 읽기 수가 나와 있습니다. 읽기-쓰기의 비율이 클수록 캐시의 작업이 더 낫습니다.
쓰기	SSD Cache가 활성화된 볼륨에 대한 총 호스트 쓰기 수입니다. 읽기-쓰기의 비율이 클수록 캐시의 작업이 더 낫습니다.
캐시 적중 횟수	캐시 적중 수를 표시합니다.
캐시 적중률	캐시 적중률을 표시합니다. 이 숫자는 캐시 적중 횟수/(읽기+쓰기)에서 파생됩니다. 효과적인 SSD Cache 작업을 위해서는 캐시 적중률이 50%를 초과해야 합니다.
캐시 할당 %	할당된 SSD Cache 스토리지의 비율을 표시합니다. 이 스토리지는 이 컨트롤러에서 사용할 수 있으며 할당된 바이트/사용 가능 바이트에서 파생되는 SSD Cache 스토리지의 백분율로 표시됩니다.
캐시 활용률	에는 할당된 SSD Cache 스토리지의 백분율로 표시된 활성화된 볼륨의 데이터가 포함된 SSD Cache 스토리지의 백분율이 나와 있습니다. 이 양은 SSD Cache의 사용률 또는 밀도를 나타냅니다. 할당된 바이트/사용 가능한 바이트에서 파생됩니다.
모두 내보내기	모든 SSD Cache 통계를 CSV 형식으로 내보냅니다. 내보낸 파일에는 SSD Cache에 대해 사용 가능한 모든 통계(공칭 및 세부 정보)가 포함됩니다.

3. 대화 상자를 닫으려면 * 취소 * 를 클릭합니다.

예약된 용량을 관리합니다

예약 용량 작동 방식

볼륨에 대해 스냅샷 또는 비동기식 미러링 작업과 같은 복제 서비스 작업이 제공되면 예약된

용량이 자동으로 생성됩니다.

예약된 용량의 목적은 문제가 발생할 경우 이러한 볼륨에 데이터 변경 사항을 저장하는 것입니다. 볼륨과 마찬가지로 예약된 용량은 풀 또는 볼륨 그룹에서 생성됩니다.

예약 용량을 사용하는 서비스 객체를 복사합니다

예약 용량은 다음과 같은 복사본 서비스 개체에서 사용하는 기본 스토리지 메커니즘입니다.

- 스냅샷 그룹
- 스냅샷 볼륨 읽기/쓰기
- 정합성 보장 그룹 구성원 볼륨입니다
- 미러링 쌍 볼륨

이러한 복제 서비스 객체를 생성하거나 확장하는 경우 풀 또는 볼륨 그룹에서 새 예약 용량을 생성해야 합니다. 예약된 용량은 일반적으로 스냅샷 작업을 위한 기본 볼륨의 40%와 비동기식 미러링 작업을 위한 기본 볼륨의 20%입니다. 그러나 예약된 용량은 원래 데이터의 변경 횟수에 따라 달라집니다.

씬 볼륨 및 예약된 용량입니다

씬 볼륨의 경우 보고된 최대 256TiB에 도달한 경우 용량을 늘릴 수 없습니다. 씬 볼륨의 예약된 용량이 보고된 최대 용량보다 큰 크기로 설정되었는지 확인합니다. 씬 볼륨은 항상 씬 프로비저닝되므로 볼륨에 데이터를 쓸 때 용량이 할당됩니다.

풀의 씬 볼륨을 사용하여 예약된 용량을 생성하는 경우 다음 작업과 예약된 용량에 대한 결과를 검토하십시오.

- 씬 볼륨의 예약된 용량에 장애가 발생하면 씬 볼륨 자체가 Failed(실패) 상태로 자동 전환되지 않습니다. 그러나 씬 볼륨의 모든 I/O 작업은 예약된 용량 볼륨에 대한 액세스를 요구하기 때문에 입출력 작업은 항상 확인 조건을 요청 호스트로 반환합니다. 예약된 용량 볼륨의 기본 문제를 해결할 수 있는 경우 예약된 용량 볼륨이 최적의 상태로 반환되고 씬 볼륨이 다시 작동합니다.
- 기존 씬 볼륨을 사용하여 비동기식 미러링 쌍을 완료하는 경우 해당 씬 볼륨은 새로 예약된 용량 볼륨으로 다시 초기화됩니다. 초기 동기화 프로세스 중에는 운영 측의 프로비저닝된 블록만 전송됩니다.

용량 알림

복제 서비스 개체에는 구성 가능한 용량 경고 및 경고 임계값과 예약된 용량이 가득 찬 경우 구성 가능한 응답이 있습니다.

복제 서비스 개체 볼륨의 예약된 용량이 가득 찰 수준에 이르면 사용자에게 경고가 표시됩니다. 기본적으로 이 알림은 예약된 용량 볼륨이 75% 찼을 때 발생하지만 필요에 따라 이 알림 지점을 위 또는 아래로 조정할 수 있습니다. 이 경고가 표시되면 해당 시점에 예약된 용량 볼륨의 용량을 늘릴 수 있습니다. 이러한 관점에서 각 복제 서비스 개체를 독립적으로 구성할 수 있습니다.

분리된 예약 용량 볼륨

분리된 예약 용량 볼륨은 연결된 복사본 서비스 개체가 삭제되어 복사 서비스 작업을 위해 더 이상 데이터를 저장하지 않는 볼륨입니다. 복제 서비스 객체가 삭제되면 예약된 용량 볼륨도 삭제해야 합니다. 그러나 예약된 용량 볼륨을 삭제하지 못했습니다.

분리된 예약된 용량 볼륨은 호스트에서 액세스하지 않으므로 재확보할 수 있습니다. 분리된 예약 용량 볼륨을 수동으로 삭제하여 해당 용량을 다른 작업에 사용할 수 있습니다.

System Manager는 홈 페이지의 알림 영역에 "사용되지 않는 용량 재확보" 메시지와 함께 고립된 예약된 용량 볼륨에 대한 알림을 표시합니다. 사용되지 않는 용량 재확보 * 를 클릭하면 사용되지 않는 용량 재확보 대화 상자가 표시되어 고립된 예약된 용량 볼륨을 삭제할 수 있습니다.

예약된 용량의 특성

- 여유 용량을 충분히 확보하기 위해 볼륨 생성 중에 예약된 용량에 할당된 용량을 고려해야 합니다.
- 예약된 용량은 기본 볼륨보다 작을 수 있습니다(최소 크기는 8MiB).
- 일부 공간은 메타데이터에서 소비되지만 192KiB는 매우 작기 때문에 예약된 용량 볼륨의 크기를 결정할 때 고려하지 않아도 됩니다.
- 예약된 용량은 호스트에서 직접 읽거나 쓸 수 없습니다.
- 각 읽기/쓰기 스냅샷 볼륨, 스냅샷 그룹, 정합성 보장 그룹 구성원 볼륨 및 미러링된 쌍 볼륨에 대해 예약된 용량이 있습니다.

예약된 용량을 늘립니다

스토리지 오브젝트의 모든 복제 서비스 작업에 사용되는 물리적으로 할당된 용량인 예약 용량을 늘릴 수 있습니다.

스냅샷 작업의 경우 일반적으로 기본 볼륨의 40%이며, 비동기식 미러링 작업의 경우 일반적으로 기본 볼륨의 20%입니다. 일반적으로 스토리지 객체의 예약된 용량이 가득 차고 있다는 경고가 표시되면 예약 용량을 늘립니다.

시작하기 전에

- 풀 또는 볼륨 그룹의 볼륨은 최적 상태여야 하며 수정 상태가 아니어야 합니다.
- 용량을 늘리기 위해 사용할 풀 또는 볼륨 그룹에 사용 가능한 용량이 있어야 합니다.

  풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우, 할당되지 않은 용량을 미사용 드라이브 형식으로 풀 또는 볼륨 그룹에 추가할 수 있습니다.

이 작업에 대해

다음과 같은 스토리지 객체에 대해 예약 용량을 8GiB씩 늘릴 수 있습니다.

- 스냅샷 그룹
- 스냅샷 볼륨
- 정합성 보장 그룹 구성원 볼륨입니다
- 미러링 쌍 볼륨

운영 볼륨에 많은 변경이 있을 것으로 생각되거나 특정 복사 서비스 작업의 수명이 매우 길 경우 높은 비율을 사용하십시오.

읽기 전용인 스냅샷 볼륨에 대해 예약된 용량을 늘릴 수 없습니다. 읽기-쓰기의 스냅샷 볼륨에만 예약된 용량이 필요합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.

2. Reserved Capacity * 탭을 선택합니다.
3. 예약된 용량을 늘릴 스토리지 객체를 선택한 다음 * 용량 증가 * 를 클릭합니다.

   예약된 용량 증가 대화 상자가 나타납니다.

4. 스피너 상자를 사용하여 용량 비율을 조정합니다.

   선택한 스토리지 객체가 포함된 풀 또는 볼륨 그룹에 사용 가능한 용량이 없고 스토리지 배열에 할당되지 않은 용량이 있는 경우 새 풀 또는 볼륨 그룹을 생성할 수 있습니다. 그런 다음 해당 풀 또는 볼륨 그룹의 새 가용 용량을 사용하여 이 작업을 다시 시도할 수 있습니다.

5. 증가 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스토리지 객체에 대한 예약 용량을 늘립니다.
- 새로 추가된 예약된 용량을 표시합니다.

예약 용량을 줄입니다

용량 감소 옵션을 사용하면 스냅샷 그룹, 스냅샷 볼륨 및 정합성 보장 그룹 구성원 볼륨과 같은 스토리지 객체에 대해 예약된 용량을 줄일 수 있습니다. 예약된 용량을 늘리는 데 사용한 양으로만 감소시킬 수 있습니다.

시작하기 전에

- 스토리지 객체에는 둘 이상의 예약된 용량 볼륨이 포함되어야 합니다.
- 스토리지 객체는 미러링된 쌍 볼륨이 아니어야 합니다.
- 스토리지 객체가 스냅샷 볼륨인 경우 비활성화된 스냅샷 볼륨이어야 합니다.
- 스토리지 객체가 스냅샷 그룹인 경우 연결된 스냅샷 이미지를 포함해서는 안 됩니다.

이 작업에 대해

다음 지침을 검토하십시오.

- 예약된 용량 볼륨은 추가된 역순으로 제거할 수 있습니다.
- 연결된 예약 용량이 없기 때문에 읽기 전용인 스냅샷 볼륨에 대해 예약된 용량을 줄일 수 없습니다. 읽기-쓰기의 스냅샷 볼륨에만 예약된 용량이 필요합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 예약된 용량을 줄일 스토리지 객체를 선택한 다음 * 용량 감소 * 를 클릭합니다.

   예약된 용량 감소 대화 상자가 나타납니다.

4. 예약된 용량을 줄일 용량을 선택한 다음 * 감소 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스토리지 객체의 용량을 업데이트합니다.
- 스토리지 객체에 대해 새로 업데이트된 예약 용량을 표시합니다.
- 스냅샷 볼륨의 용량을 줄이면 System Manager는 자동으로 스냅샷 볼륨을 사용 안 함 상태로 전환합니다. Disabled는 스냅샷 볼륨이 현재 스냅샷 이미지와 연결되어 있지 않으므로 입출력을 위해 호스트에 할당할 수 없음을 의미합니다

스냅샷 그룹에 대한 예약된 용량 설정을 변경합니다

스냅샷 그룹의 설정을 변경하여 이름, 자동 삭제 설정, 허용되는 최대 스냅샷 이미지 수, SANtricity System Manager에서 예약된 용량 알림 알림을 보내는 백분율 지점 또는 예약된 용량이 정의된 최대 백분율에 도달할 때 사용할 정책을 변경할 수 있습니다.

스냅샷 그룹을 생성하는 동안 그룹에 포함된 모든 스냅샷 이미지에 대한 데이터를 저장하기 위해 예약된 용량이 생성됩니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 편집할 스냅샷 그룹을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   스냅샷 그룹 설정 대화 상자가 나타납니다.

4. 스냅샷 그룹의 설정을 적절하게 변경합니다.

필드 상세정보

설정	설명
• 스냅샷 그룹 설정 *	이름
스냅샷 그룹의 이름입니다. 스냅샷 그룹의 이름을 지정해야 합니다.	자동 삭제
그룹에 있는 총 스냅샷 이미지 수를 사용자 정의 최대치 이하로 유지하는 설정입니다. 이 옵션을 설정하면 새 스냅샷이 생성될 때마다 System Manager가 그룹에서 가장 오래된 스냅샷 이미지를 자동으로 삭제하여 그룹에 허용되는 최대 스냅샷 이미지 수를 준수합니다.	스냅샷 이미지 제한
스냅샷 그룹에 허용되는 최대 스냅샷 이미지 수를 지정하는 구성 가능한 값입니다.	스냅샷 스케줄입니다
예 인 경우 스냅샷을 자동으로 생성하도록 스케줄이 설정됩니다.	• 예약된 용량 설정 *
다음 경우에 알림:	spinner 상자를 사용하여 스냅샷 그룹의 예약된 용량이 거의 꽉 찰 때 System Manager에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스냅샷 그룹의 예약 용량이 지정된 임계값을 초과하면 System Manager에서 경고를 보내, 예약된 용량을 늘리거나 불필요한 개체를 삭제할 수 있습니다.
전체 예약 용량에 대한 정책입니다	다음 정책 중 하나를 선택할 수 있습니다. • * 가장 오래된 스냅샷 이미지 제거 * — System Manager는 스냅샷 그룹에서 가장 오래된 스냅샷 이미지를 자동으로 제거합니다. 그러면 스냅샷 이미지 예약 용량이 그룹 내에서 재사용될 수 있습니다. • * 기본 볼륨에 대한 쓰기 거부 * — 예약된 용량이 최대 정의 비율에 도달하면 System Manager가 예약된 용량 액세스를 트리거한 기본 볼륨에 대한 모든 I/O 쓰기 요청을 거부합니다.
• 관련 개체 *	기본 볼륨

설정	설명
그룹에 사용된 기본 볼륨의 이름입니다. 기본 볼륨은 스냅샷 이미지가 생성되는 원본입니다. 일반 볼륨이거나 씬 볼륨일 수 있으며 일반적으로 호스트에 할당됩니다. 기본 볼륨은 볼륨 그룹 또는 디스크 풀에 상주할 수 있습니다.	스냅샷 이미지

5. 변경 사항을 스냅샷 그룹 설정에 적용하려면 * 저장 * 을 클릭합니다.

스냅샷 볼륨에 대한 예약된 용량 설정을 변경합니다

스냅샷 볼륨에 대한 설정을 변경하여 스냅샷 볼륨에 대한 예약된 용량이 거의 꽉 찼을 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 편집할 스냅샷 볼륨을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   Snapshot Volume Reserved Capacity Settings(스냅샷 볼륨 예비 용량 설정) 대화 상자가 나타납니다.

4. 스냅샷 볼륨에 대한 예약된 용량 설정을 적절하게 변경합니다.

   필드 상세정보

설정	설명
다음 경우에 알림:	스피너 상자를 사용하여 구성원 볼륨의 예약된 용량이 거의 가득 찰 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스냅샷 볼륨에 대한 예약된 용량이 지정된 임계값을 초과하면 예약된 용량을 늘리거나 불필요한 객체를 삭제할 수 있는 알림이 시스템에 전송됩니다.

5. Save * 를 클릭하여 스냅샷 볼륨의 예약된 용량 설정에 변경 사항을 적용합니다.

정합성 보장 그룹 구성원 볼륨에 대한 예약된 용량 설정을 변경합니다

정합성 보장 그룹 구성원 볼륨의 설정을 변경하여 구성원 볼륨의 예약된 용량이 거의 가득 차면 SANtricity 시스템 관리자가 알림 알림을 보내는 백분율 지점을 조정하고 예약된 용량이 정의된 최대 비율에 도달할 때 사용할 정책을 변경할 수 있습니다.

이 작업에 대해

개별 구성원 볼륨에 대한 예약된 용량 설정을 변경하면 정합성 보장 그룹에 연결된 모든 구성원 볼륨에 대한 예약된 용량 설정도 변경됩니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 편집할 일관성 그룹 구성원 볼륨을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   구성원 볼륨 예약 용량 설정 대화 상자가 나타납니다.

4. 구성원 볼륨에 대한 예약된 용량 설정을 적절하게 변경합니다.

   필드 상세정보

설정	설명
다음 경우에 알림:	스피너 상자를 사용하여 멤버 볼륨에 대한 예약된 용량이 거의 가득 찰 때 System Manager에서 경고 알림을 보내는 백분율 지점을 조정합니다. 구성원 볼륨의 예약된 용량이 지정된 임계값을 초과하면 System Manager에서 경고를 보내 예약된 용량을 늘리거나 불필요한 개체를 삭제할 수 있습니다. 하나의 구성원 볼륨에 대한 경고 설정을 변경하면 동일한 정합성 보장 그룹에 속한 _ALL_구성원 볼륨에 대해 이 설정이 변경됩니다.
전체 예약 용량에 대한 정책입니다	다음 정책 중 하나를 선택할 수 있습니다. • * 가장 오래된 스냅샷 이미지 제거 * — System Manager는 정합성 보장 그룹에서 가장 오래된 스냅샷 이미지를 자동으로 제거합니다. 그러면 그룹 내에서 재사용하기 위해 구성원의 예약된 용량이 해제됩니다. • * 기본 볼륨에 대한 쓰기 거부 * — 예약된 용량이 최대 정의 비율에 도달하면 System Manager가 예약된 용량 액세스를 트리거한 기본 볼륨에 대한 모든 I/O 쓰기 요청을 거부합니다.

5. 변경 사항을 적용하려면 * 저장 * 을 클릭합니다.

결과

System Manager에서는 구성원 볼륨에 대한 예약된 용량 설정과 정합성 보장 그룹의 모든 구성원 볼륨에 대한 예약된 용량 설정을 변경합니다.

미러링된 페어 볼륨에 대한 예약된 용량 설정을 변경합니다

미러링된 페어 볼륨의 설정을 변경하여 미러링된 페어 볼륨의 예약된 용량이 거의 꽉 찼을 때 SANtricity 시스템 관리자가 알림 메시지를 보내는 백분율 지점을 조정할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. Reserved Capacity * 탭을 선택합니다.
3. 편집할 미러링된 쌍 볼륨을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   Mirrored Pair Volume Reserved Capacity Settings(미러링된 볼륨 예비 용량 설정) 대화 상자가 나타납니다.

4. 미러링된 페어 볼륨에 대한 예약된 용량 설정을 적절하게 변경합니다.

   필드 상세정보

설정	설명
다음 경우에 알림:	미러링 쌍의 예약된 용량이 거의 꽉 찼을 때 System Manager에서 경고 알림을 보내는 백분율 지점을 Spinner 상자를 사용하여 조정합니다. 미러링된 쌍의 예약된 용량이 지정된 임계값을 초과하면 System Manager에서 경고를 보내, 예약된 용량을 늘릴 수 있도록 합니다. 미러링된 한 쌍의 경고 설정을 변경하면 동일한 미러 정합성 보장 그룹에 속한 모든 미러링된 쌍에 대한 경고 설정이 변경됩니다.

5. 변경 사항을 적용하려면 * 저장 * 을 클릭합니다.

보류 중인 스냅샷 이미지를 취소합니다

대기 중인 스냅샷 이미지가 완료되기 전에 취소할 수 있습니다. 스냅샷은 비동기적으로 발생하고 스냅샷이 완료될 때까지 스냅샷 상태가 보류 중입니다. 동기화 작업이 완료되는 즉시 스냅샷 이미지가 완료됩니다.

이 작업에 대해

스냅샷 이미지는 다음과 같은 동시 조건으로 인해 보류 상태입니다.

- 스냅샷 그룹의 기본 볼륨이나 이 스냅샷 이미지가 포함된 정합성 보장 그룹의 구성원 볼륨이 비동기식 미러 그룹의 구성원입니다.
- 현재 볼륨 또는 볼륨이 비동기식 미러링 동기화 작업에 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 보류 중인 스냅샷 이미지를 취소할 스냅샷 그룹을 선택한 다음, 메뉴를 클릭합니다: Uncommon Tasks [Cancel pending snapshot image].
4. 보류 중인 스냅샷 이미지를 취소하려면 * 예 * 를 클릭합니다.

스냅샷 그룹을 삭제합니다

스냅샷 그룹은 해당 데이터를 영구적으로 삭제하고 시스템에서 제거하려는 경우 삭제됩니다. 스냅샷 그룹을 삭제하면 풀 또는 볼륨 그룹에서 재사용하기 위해 예약된 용량이 재확보됩니다.

이 작업에 대해

스냅샷 그룹이 삭제되면 그룹의 모든 스냅샷 이미지도 삭제됩니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. 예약된 용량 * 탭을 클릭합니다.
3. 삭제할 스냅샷 그룹을 선택한 다음 메뉴(Uncommon Tasks[Delete snapshot group])를 클릭합니다.

   스냅샷 그룹 삭제 확인 대화 상자가 나타납니다.

4. 를 `delete` 입력하여 확인합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스냅샷 그룹과 연결된 모든 스냅샷 이미지를 삭제합니다.
- 스냅샷 그룹의 이미지와 연결된 스냅샷 볼륨을 비활성화합니다.
- 스냅샷 그룹에 대해 존재하는 예약된 용량을 삭제합니다.

FAQ 를 참조하십시오

볼륨 그룹이란 무엇입니까?

볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.

풀이란?

풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)

관리자는 풀을 통해 각 호스트의 사용량을 모니터링하여 스토리지 공간이 부족해질 가능성이 있는지 확인하고 기존의 디스크 크기 조정 중단을 방지할 수 있습니다. 풀이 고갈될 경우 운영 중단 없이 풀에 드라이브를 추가할 수 있으며 용량 증가는 호스트에 투명합니다.

풀을 사용하면 균형 상태를 유지하기 위해 데이터가 자동으로 재배포됩니다. 풀 전체에 패리티 정보 및 여유 용량을 분산하여 풀의 모든 드라이브를 장애가 발생한 드라이브를 재구축하는 데 사용할 수 있습니다. 이 방식에서는 전용 핫 스페어 드라이브를 사용하지 않으며 풀 전체에 보존(스페어) 용량이 예약됩니다. 드라이브 장애가 발생하면 다른 드라이브의 세그먼트를 읽어서 데이터를 다시 생성합니다. 그런 다음 새 드라이브를 선택하여 장애 발생 드라이브에 있던 각 세그먼트를 작성함으로써 드라이브 전체의 데이터 분배를 유지합니다.

예약 용량이란?

예약된 용량은 스냅샷 이미지, 정합성 보장 그룹 구성원 볼륨 및 미러링된 쌍 볼륨과 같은 복제 서비스 개체에 대한 데이터를 저장하는 물리적으로 할당된 용량입니다.

복제 서비스 작업과 연결된 예약된 용량 볼륨은 풀 또는 볼륨 그룹에 상주합니다. 풀 또는 볼륨 그룹에서 예약된 용량을 생성합니다.

FDE/FIPS 보안이란 무엇입니까?

FDE/FIPS 보안이란 읽기 중에 고유 암호화 키를 사용하여 데이터를 암호화하고 해독하는 동안 데이터를 보호하는 보안 가능 드라이브를 말합니다. 이러한 보안 가능 드라이브는 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스를 방지합니다.

보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다. FIPS 드라이브는 인증 테스트를 거쳤습니다.

> FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.

중복 검사란?

중복 검사는 풀 또는 볼륨 그룹의 볼륨에 있는 데이터가 일관되는지 여부를 확인합니다. 이중화 데이터는 풀 또는 볼륨 그룹의 드라이브 중 하나에 장애가 발생할 경우 교체 드라이브에 대한 정보를 빠르게 재구성하는 데 사용됩니다.

한 번에 하나의 풀 또는 볼륨 그룹에서만 이 검사를 수행할 수 있습니다. 볼륨 중복 검사는 다음 작업을 수행합니다.

- RAID 3 볼륨, RAID 5 볼륨 또는 RAID 6 볼륨의 데이터 블록을 검색한 다음 각 블록의 중복 정보를 확인합니다. (RAID 3은 명령줄 인터페이스를 사용하는 볼륨 그룹에만 할당할 수 있습니다.)
- RAID 1 미러링 드라이브의 데이터 블록을 비교합니다.
- 데이터가 컨트롤러 펌웨어와 일치하지 않는 것으로 확인되면 중복 오류를 반환합니다.

> 동일한 풀 또는 볼륨 그룹에서 중복 검사를 즉시 실행하면 오류가 발생할 수 있습니다. 이 문제를 방지하려면 동일한 풀 또는 볼륨 그룹에서 다른 중복 검사를 실행하기 전에 1-2분 정도 기다리십시오.

풀과 볼륨 그룹의 차이점은 무엇입니까?

풀은 볼륨 그룹과 유사하며 다음과 같은 차이점이 있습니다.

- 풀의 데이터는 동일한 드라이브 세트에 저장되는 볼륨 그룹의 데이터와 달리 풀의 모든 드라이브에 무작위로 저장됩니다.
- 드라이브 장애가 발생할 경우 풀의 성능 저하가 줄어들고 재구성 시간이 단축됩니다.
- 풀에는 보존 용량이 내장되어 있으므로 전용 핫 스페어 드라이브가 필요하지 않습니다.
- 풀을 사용하면 많은 수의 드라이브를 그룹화할 수 있습니다.

- 풀은 지정된 RAID 레벨이 필요하지 않습니다.

풀을 수동으로 구성하는 이유는 무엇입니까**?**

다음 예에서는 풀을 수동으로 구성하려는 이유를 설명합니다.

- 스토리지 배열에 여러 애플리케이션이 있고 동일한 드라이브 리소스에 대해 경쟁하지 않으려는 경우 하나 이상의 애플리케이션에 대해 더 작은 풀을 수동으로 생성하는 것이 좋습니다.

  데이터를 분산할 볼륨이 많은 대규모 풀에 워크로드를 할당하는 대신 하나 또는 두 개의 볼륨만 할당할 수 있습니다. 특정 애플리케이션의 워크로드 전용으로 별도의 풀을 수동으로 생성하면 스토리지 시스템의 운영 속도가 빨라질 수 있고 경합이 줄어듭니다.

  풀을 수동으로 생성하려면 * 스토리지 * 를 선택한 다음 * 풀 및 볼륨 그룹 * 을 선택합니다. All Capacity 탭에서 Create [Pool] 메뉴를 클릭합니다.

- 동일한 드라이브 유형의 풀이 여러 개 있는 경우 System Manager에서 풀에 대한 드라이브를 자동으로 추천할 수 없다는 메시지가 나타납니다. 그러나 기존 풀에 드라이브를 수동으로 추가할 수 있습니다.

  기존 풀에 드라이브를 수동으로 추가하려면 풀 및 볼륨 그룹 페이지에서 풀을 선택한 다음 * 용량 추가 * 를 클릭합니다.

용량 알림이 중요한 이유는 무엇입니까**?**

용량 알림은 풀에 드라이브를 추가할 시점을 나타냅니다. 스토리지 배열 작업을 성공적으로 수행하려면 풀에 충분한 가용 용량이 필요합니다. 풀의 사용 가능한 용량이 지정된 비율에 도달하거나 초과될 때 알림을 보내도록 SANtricity 시스템 관리자를 구성하여 이러한 작업이 중단되지 않도록 할 수 있습니다.

풀 자동 구성 * 옵션 또는 * 풀 생성 * 옵션을 사용하여 풀을 생성할 때 이 비율을 설정합니다. 자동 옵션을 선택하면 기본 설정에 따라 알림 수신 시기를 자동으로 결정합니다. 풀을 수동으로 생성하기로 선택한 경우 알림 알림 설정을 확인하거나, 원하는 경우 기본 설정을 적용할 수 있습니다. 이 설정은 나중에 메뉴에서 설정 [알림]을 조정할 수 있습니다.

> ⓘ 풀의 사용 가능한 용량이 지정된 비율에 도달하면 알림 구성에 지정된 방법을 사용하여 알림 알림이 전송됩니다.

보존 용량을 늘릴 수 없는 이유는 무엇입니까**?**

사용 가능한 모든 용량에 볼륨을 생성한 경우 보존 용량을 늘릴 수 없습니다.

Preservation capacity는 잠재적 드라이브 장애를 지원하기 위해 풀에 예약된 용량(드라이브 수)입니다. 풀이 생성되면 시스템은 풀의 드라이브 수에 따라 기본 보존 용량을 자동으로 예약합니다. 사용 가능한 모든 용량에 볼륨을 생성한 경우 드라이브를 추가하거나 볼륨을 삭제하여 풀에 용량을 추가하지 않으면 보존 용량을 늘릴 수 없습니다.

풀 및 볼륨 그룹 * 에서 보존 용량을 변경할 수 있습니다. 편집할 풀을 선택합니다. 설정 보기/편집 * 을 클릭한 다음 * 설정 * 탭을 선택합니다.

> ⓘ 보존 용량은 풀의 드라이브에 실제 보존 용량이 분산되어 있더라도 여러 드라이브로 지정됩니다.

풀에서 제거할 수 있는 드라이브 수에 제한이 있습니까**?**

SANtricity System Manager는 풀에서 제거할 수 있는 드라이브 수에 대한 제한을 설정합니다.

- 풀의 드라이브 수를 11개 미만으로 줄일 수는 없습니다.
- 풀의 남은 드라이브에 데이터가 재분배될 때 제거된 드라이브의 데이터를 포함할 여유 용량이 충분하지 않으면 드라이브를 제거할 수 없습니다.
- 한 번에 최대 60개의 드라이브를 제거할 수 있습니다. 60개 이상의 드라이브를 선택하면 드라이브 제거 옵션이 비활성화됩니다. 60개 이상의 드라이브를 제거해야 하는 경우 드라이브 제거 작업을 반복합니다.

드라이브에 지원되는 미디어 유형은 무엇입니까**?**

지원되는 미디어 유형은 하드 디스크 드라이브(HDD) 및 솔리드 스테이트 디스크(SSD)입니다.

일부 드라이브가 표시되지 않는 이유는 무엇입니까**?**

Add Capacity 대화 상자에서 기존 풀 또는 볼륨 그룹에 용량을 추가하는 데 일부 드라이브를 사용할 수 없습니다.

드라이브는 다음과 같은 이유로 적합하지 않습니다.

- 드라이브를 할당하지 않고 안전하게 사용할 수 없어야 합니다. 다른 풀, 다른 볼륨 그룹에 이미 속해 있거나 핫 스페어로 구성된 드라이브는 사용할 수 없습니다. 드라이브 할당이 취소되었지만 보안이 설정된 경우 해당 드라이브를 수동으로 지워야 사용할 수 있습니다.
- 최적화되지 않은 상태의 드라이브는 해당되지 않습니다.
- 드라이브 용량이 너무 작으면 대상에서 제외됩니다.
- 드라이브 미디어 유형은 풀 또는 볼륨 그룹 내에서 일치해야 합니다. 다음을 혼합할 수 없습니다.
  - 솔리드 스테이트 디스크(SSD)가 장착된 하드 디스크 드라이브(HDD)
  - SAS 드라이브를 포함한 NVMe
  - 512바이트 및 4KiB 볼륨 블록 크기의 드라이브
- 풀 또는 볼륨 그룹에 모든 보안 가능 드라이브가 포함되어 있는 경우 비보안 가능 드라이브가 표시되지 않습니다.
- 풀 또는 볼륨 그룹에 모든 FIPS(Federal Information Processing Standards) 드라이브가 포함되어 있는 경우 비 FIPS 드라이브가 나열되지 않습니다.
- 풀 또는 볼륨 그룹에 모든 DA(Data Assurance) 가능 드라이브가 포함되어 있고 풀 또는 볼륨 그룹에 하나 이상의 DA 지원 볼륨이 있는 경우, DA를 사용할 수 없는 드라이브는 사용할 수 없으므로 해당 풀 또는 볼륨 그룹에 추가할 수 없습니다. 그러나 풀 또는 볼륨 그룹에 DA 지원 볼륨이 없는 경우 DA를 사용할 수 없는 드라이브를 해당 풀 또는 볼륨 그룹에 추가할 수 있습니다. 이러한 드라이브를 혼합하려는 경우 DA 지원 볼륨을 생성할 수 없습니다.

> 새 드라이브를 추가하거나 풀 또는 볼륨 그룹을 삭제하여 스토리지 시스템에서 용량을 늘릴 수 있습니다.

선반/서랍 손실 방지 기능을 어떻게 유지합니까**?**

풀 또는 볼륨 그룹에 대한 쉘프/드로어 손실 보호를 유지하려면 다음 표에 나와 있는 기준을 사용하십시오.

레벨	선반/서랍 손실 방지 기준	필요한 최소 쉘프/서랍 수
수영장	쉘프의 경우 풀에는 단일 쉘프에 2개 이상의 드라이브가 없어야 합니다. 드로어의 경우 풀에는 각 드로어의 드라이브 수가 동일해야 합니다.	선반용 6개 5 서랍용
RAID 6 를 참조하십시오	볼륨 그룹은 단일 쉘프 또는 서랍에 2개 이상의 드라이브를 포함하지 않습니다.	3
RAID 3 또는 RAID 5	볼륨 그룹의 각 드라이브는 별도의 쉘프 또는 드로어에 있습니다.	3
RAID 1 를 참조하십시오	미러링된 쌍의 각 드라이브는 별도의 쉘프 또는 드로어에 위치해야 합니다.	2
RAID 0 를 참조하십시오	선반/서랍 손실 방지를 달성할 수 없습니다.	해당 없음

풀 또는 볼륨 그룹에서 드라이브가 이미 장애가 발생한 경우에는 쉘프/드로어 손실 보호가 유지되지 않습니다. 이 경우, 드라이브 쉘프 또는 드로어에 액세스하지 못하게 되고 결과적으로 풀 또는 볼륨 그룹의 다른 드라이브가 데이터 손실을 유발합니다.

풀 및 볼륨 그룹에 가장 적합한 드라이브 포지셔닝은 무엇입니까**?**

풀 및 볼륨 그룹을 생성할 때는 드라이브 선택 항목의 균형을 상단 및 하단 드라이브 슬롯 사이에서 조정해야 합니다.

EF600 및 EF300 컨트롤러의 경우 드라이브 슬롯 0-11은 하나의 PCI 브리지에 연결되고 슬롯 12-23은 다른 PCI 브리지에 연결됩니다. 최적의 성능을 얻으려면 드라이브 선택 항목의 균형을 조정하여 위쪽 및 아래쪽 슬롯의 드라이브 수가 대략적으로 같아야 합니다. 이러한 포지셔닝을 통해 볼륨이 필요한 것보다 더 빠르게 대역폭 제한을 넘지 않도록 할 수 있습니다.

애플리케이션에 가장 적합한 **RAID** 레벨은 무엇입니까**?**

볼륨 그룹의 성능을 최대화하려면 적절한 RAID 레벨을 선택해야 합니다. 볼륨 그룹에 액세스하는 응용 프로그램의 읽기 및 쓰기 비율을 알면 적절한 RAID 레벨을 결정할 수 있습니다. 성능 페이지를 사용하여 이러한 비율을 얻습니다.

RAID 레벨 및 애플리케이션 성능

RAID는 _levels_라는 일련의 구성을 사용하여 드라이브에서 사용자 및 중복 데이터를 기록하고 검색하는 방법을 결정합니다. 각 RAID 레벨은 서로 다른 성능 기능을 제공합니다. RAID 5 및 RAID 6 구성의 탁월한 읽기 성능 때문에 읽기 비율이 높은 응용 프로그램은 RAID 5 볼륨 또는 RAID 6 볼륨을 사용하여 잘 수행됩니다.

읽기 백분율(쓰기 집약적)이 낮은 응용 프로그램은 RAID 5 볼륨 또는 RAID 6 볼륨에서 제대로 작동하지 않습니다. 성능

저하는 컨트롤러가 RAID 5 볼륨 그룹 또는 RAID 6 볼륨 그룹의 드라이브에 데이터 및 중복 데이터를 기록하는 방식으로 인해 발생합니다.

다음 정보를 기반으로 RAID 레벨을 선택합니다.

- RAID 0 *
- * 설명 *
  - 비중복, 스트라이핑 모드
- * 작동 방식 *
  - RAID 0은 볼륨 그룹의 모든 드라이브에 데이터를 스트라이핑합니다.
- * 데이터 보호 기능 *
  - 고가용성 요구 사항에 대해서는 RAID 0을 권장하지 않습니다. RAID 0은 중요하지 않은 데이터에 적합합니다.
  - 볼륨 그룹에서 단일 드라이브에 장애가 발생하면 연결된 모든 볼륨이 실패하고 모든 데이터가 손실됩니다.
- * 드라이브 번호 요구 사항 *
  - RAID 레벨 0에는 최소 하나의 드라이브가 필요합니다.
  - RAID 0 볼륨 그룹은 30개 이상의 드라이브를 가질 수 있습니다.
  - 스토리지 배열의 모든 드라이브를 포함하는 볼륨 그룹을 생성할 수 있습니다.
- RAID 1 또는 RAID 10 *
- * 설명 *
  - 스트라이핑/미러 모드
- * 작동 방식 *
  - RAID 1은 디스크 미러링을 사용하여 두 개의 중복 디스크에 동시에 데이터를 씁니다.
  - RAID 10은 드라이브 스트라이핑을 사용하여 미러링된 드라이브 쌍의 집합에 걸쳐 데이터를 스트라이핑합니다.
- * 데이터 보호 기능 *
  - RAID 1 및 RAID 10은 고성능과 최상의 데이터 가용성을 제공합니다.
  - RAID 1 및 RAID 10은 드라이브 미러링을 사용하여 한 드라이브에서 다른 드라이브로 정확하게 복사합니다.
  - 드라이브 쌍의 드라이브 중 하나에 장애가 발생하면 스토리지 어레이가 데이터 또는 서비스의 손실 없이 다른 드라이브로 즉시 전환할 수 있습니다.
  - 단일 드라이브 장애로 인해 관련 볼륨의 성능이 저하됩니다. 미러 드라이브를 통해 데이터에 액세스할 수 있습니다.
  - 볼륨 그룹의 드라이브 쌍 장애로 인해 연결된 모든 볼륨이 장애가 발생하고 데이터 손실이 발생할 수 있습니다.
- * 드라이브 번호 요구 사항 *
  - RAID 1에는 사용자 데이터용 드라이브 1개와 미러링된 데이터용 드라이브 1개 등 최소 2개의 드라이브가 필요합니다.
  - 드라이브를 4개 이상 선택하면 사용자 데이터를 위한 드라이브 2개와 미러링된 데이터를 위한 드라이브 2개 등 RAID 10이 볼륨 그룹 전체에 자동으로 구성됩니다.
  - 볼륨 그룹에 짝수의 드라이브가 있어야 합니다. 드라이브 수가 짝수이고 할당되지 않은 드라이브가 일부 있는 경우 * Pools & Volume Groups * 로 이동하여 볼륨 그룹에 드라이브를 추가하고 작업을 재시도하십시오.

◦ RAID 1 및 RAID 10 볼륨 그룹은 30개 이상의 드라이브를 가질 수 있습니다. 스토리지 배열의 모든 드라이브를 포함하는 볼륨 그룹을 생성할 수 있습니다.

- RAID 5 *
- * 설명 *
  - 높은 I/O 모드.
- * 작동 방식 *
  - 사용자 데이터 및 중복 정보(패리티)는 드라이브에 스트라이핑됩니다.
  - 하나의 드라이브에 해당하는 용량이 중복 정보에 사용됩니다.
- * 데이터 보호 기능 *
  - RAID 5 볼륨 그룹에서 단일 드라이브에 장애가 발생하면 연결된 모든 볼륨의 성능이 저하됩니다. 중복 정보를 통해 데이터에 계속 액세스할 수 있습니다.
  - RAID 5 볼륨 그룹에서 두 개 이상의 드라이브에 장애가 발생하면 연결된 모든 볼륨에 장애가 발생하고 모든 데이터가 손실됩니다.
- * 드라이브 번호 요구 사항 *
  - 볼륨 그룹에 최소 3개의 드라이브가 있어야 합니다.
  - 일반적으로 볼륨 그룹에서 최대 30개의 드라이브로 제한됩니다.
- RAID 6 *
- * 설명 *
  - 높은 I/O 모드.
- * 작동 방식 *
  - 사용자 데이터 및 중복 정보(이중 패리티)는 드라이브에 스트라이핑됩니다.
  - 두 드라이브의 동일한 용량이 중복 정보에 사용됩니다.
- * 데이터 보호 기능 *
  - RAID 6 볼륨 그룹에서 하나 또는 두 개의 드라이브에 장애가 발생하면 연결된 모든 볼륨의 성능이 저하되지만 중복 정보를 통해 데이터에 계속 액세스할 수 있습니다.
  - RAID 6 볼륨 그룹에서 3개 이상의 드라이브에 장애가 발생하면 연결된 모든 볼륨에 장애가 발생하고 모든 데이터가 손실됩니다.
- * 드라이브 번호 요구 사항 *
  - 볼륨 그룹에 최소 5개의 드라이브가 있어야 합니다.
  - 일반적으로 볼륨 그룹에서 최대 30개의 드라이브로 제한됩니다.

풀의 RAID 레벨은 변경할 수 없습니다. 사용자 인터페이스는 풀을 RAID 6으로 자동 구성합니다.

RAID 레벨 및 데이터 보호

RAID 1, RAID 5 및 RAID 6은 드라이브 미디어에 중복 데이터를 기록하여 내결함성을 제공합니다. 중복 데이터는 데이터 사본(미러링)이거나 데이터에서 파생된 오류 정정 코드일 수 있습니다. 드라이브 장애가 발생할 경우 중복 데이터를 사용하여 교체 드라이브에 대한 정보를 빠르게 재구성할 수 있습니다.

단일 볼륨 그룹에서 단일 RAID 레벨을 구성합니다. 해당 볼륨 그룹의 모든 중복 데이터는 볼륨 그룹 내에 저장됩니다.

볼륨 그룹의 용량은 구성원 드라이브의 총 용량에서 중복 데이터를 위해 예약된 용량을 뺀 값입니다. 중복성에 필요한 용량은 사용된 RAID 레벨에 따라 다릅니다.

Data Assurance란 무엇입니까**?**

DA(Data Assurance)는 T10 PI(보호 정보) 표준을 구현하여 I/O 경로를 통해 데이터가 전송될 때 발생할 수 있는 오류를 확인하고 수정하여 데이터 무결성을 향상합니다.

일반적으로 Data Assurance 기능을 사용하면 컨트롤러와 드라이브 사이의 입출력 경로 부분을 확인할 수 있습니다. DA 기능은 풀 및 볼륨 그룹 레벨에서 제공됩니다.

이 기능을 활성화하면 스토리지 배열은 볼륨의 각 데이터 블록에 오류 검사 코드(순환 중복 검사 또는 CRC라고도 함)를 추가합니다. 데이터 블록이 이동된 후 스토리지 배열은 이러한 CRC 코드를 사용하여 전송 중에 오류가 발생했는지 확인합니다. 잠재적으로 손상된 데이터는 디스크에 기록되거나 호스트에 반환되지 않습니다. DA 기능을 사용하려면 새 볼륨을 생성할 때 DA를 지원하는 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "DA" 옆에 있는 "예"를 확인합니다).

DA가 가능한 입출력 인터페이스를 사용하여 이러한 DA 지원 볼륨을 호스트에 할당해야 합니다. DA를 지원할 수 있는 I/O 인터페이스로는 파이버 채널, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, InfiniBand를 통한 NVMe/RoCE 및 iSER(RDMA/IB용 iSCSI 확장) DA는 InfiniBand를 통한 SRP에서 지원되지 않습니다.

보안 기능**(**드라이브 보안**)**이란 무엇입니까**?**

드라이브 보안은 스토리지 어레이에서 제거할 때 보안이 설정된 드라이브의 데이터에 대한 무단 액세스를 방지하는 기능입니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.

예약된 용량 증가에 대해 알아야 할 사항은 무엇입니까**?**

일반적으로 예약된 용량이 가득 찰 위험이 있다는 경고가 나타나면 용량을 늘려야 합니다. 예약 용량은 8GiB의 증분으로 늘릴 수 있습니다.

- 필요한 경우 확장할 수 있도록 풀 또는 볼륨 그룹에 충분한 가용 용량이 있어야 합니다.

  풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우, 할당되지 않은 용량을 미사용 드라이브 형식으로 풀 또는 볼륨 그룹에 추가할 수 있습니다.

- 풀 또는 볼륨 그룹의 볼륨은 최적 상태여야 하며 수정 상태가 아니어야 합니다.
- 용량을 늘리기 위해 사용할 풀 또는 볼륨 그룹에 사용 가능한 용량이 있어야 합니다.
- 읽기 전용인 스냅샷 볼륨에 대해 예약된 용량을 늘릴 수 없습니다. 읽기-쓰기의 스냅샷 볼륨에만 예약된 용량이 필요합니다.

스냅샷 작업의 경우 예약된 용량은 일반적으로 기본 볼륨의 40%입니다. 비동기식 미러링 작업의 경우 예약된 용량은 일반적으로 기본 볼륨의 20%입니다. 기본 볼륨에 많은 변경이 있을 것으로 예상되거나 스토리지 오브젝트의 복사 서비스 작업 예상 수명이 매우 길 경우 더 높은 비율을 사용하십시오.

감량할 다른 금액을 선택할 수 없는 이유는 무엇입니까**?**

예약된 용량을 늘리기 위해 사용한 양으로만 줄일 수 있습니다. 구성원 볼륨에 대해 예약된 용량은 추가된 역순으로 제거할 수 있습니다.

다음 조건 중 하나가 존재할 경우 스토리지 객체에 대한 예약 용량을 줄일 수 없습니다.

- 스토리지 객체가 미러링된 페어 볼륨인 경우
- 스토리지 객체에 예약된 용량에 대해 하나의 볼륨만 포함된 경우 스토리지 객체에는 예약된 용량을 위한 볼륨이 2개 이상 있어야 합니다.
- 스토리지 객체가 비활성화된 스냅샷 볼륨인 경우
- 스토리지 객체에 하나 이상의 연결된 스냅샷 이미지가 포함되어 있는 경우

예약된 용량에 대한 볼륨은 추가된 역순으로 제거할 수 있습니다.

연결된 예약 용량이 없기 때문에 읽기 전용인 스냅샷 볼륨에 대해 예약된 용량을 줄일 수 없습니다. 읽기-쓰기의 스냅샷 볼륨에만 예약된 용량이 필요합니다.

각 구성원 볼륨에 대해 예약된 용량이 필요한 이유는 무엇입니까**?**

스냅샷 정합성 보장 그룹의 각 구성원 볼륨은 호스트 애플리케이션이 수정한 내용을 참조된 정합성 보장 그룹 스냅샷 이미지에 영향을 주지 않고 기본 볼륨에 저장하려면 고유한 예약 용량을 가져야 합니다. 예약된 용량은 읽기-쓰기로 지정된 구성원 볼륨에 포함된 데이터의 복제본에 대한 쓰기 액세스 권한을 호스트 애플리케이션에 제공합니다.

정합성 보장 그룹 스냅샷 이미지는 호스트에서 직접 읽거나 쓸 수 없습니다. 대신, 스냅샷 이미지는 기본 볼륨에서 캡처된 데이터만 저장하는 데 사용됩니다.

읽기-쓰기로 지정된 일관성 그룹 스냅샷 볼륨을 생성하는 동안 System Manager는 일관성 그룹의 각 구성원 볼륨에 대해 예약된 용량을 생성합니다. 이 예약된 용량은 호스트 애플리케이션에서 정합성 보장 그룹 스냅샷 이미지에 포함된 데이터 복제본에 대한 쓰기 액세스를 제공합니다.

모든 **SSD Cache** 통계를 보고 해석하려면 어떻게 해야 합니까**?**

SSD Cache에 대한 공칭 통계 및 세부 통계를 볼 수 있습니다. 공칭 통계는 상세 통계의 하위 집합입니다.

자세한 통계는 모든 SSD 통계를 파일로 내보낼 때만 볼 수 `.csv` 있습니다. 통계를 검토 및 해석할 때는 통계의 조합을 통해 일부 해석이 파생된다는 점을 염두에 두십시오.

공칭 통계

SSD Cache 통계를 보려면 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다. 통계를 보려는 SSD Cache를 선택한 다음 menu:More [View Statistics](추가 [통계 보기])를 선택합니다. 공칭 통계는 SSD 캐시 통계 보기 대화 상자에 표시됩니다.

다음 목록에는 상세 통계의 하위 집합인 공칭 통계가 나와 있습니다.

공칭 통계	설명
읽기/쓰기	SSD Cache 지원 볼륨에서 또는 호스트에서 데이터를 쓸 수 있는 총 호스트 읽기 수입니다. 쓰기에 상대적인 읽기를 비교합니다. 유효 SSD 캐시 작업을 위해서는 읽기 작업이 쓰기 보다 커야 합니다. 읽기-쓰기의 비율이 클수록 캐시 작업이 향상됩니다.

공칭 통계	설명
캐시 적중 횟수	캐시 적중 횟수
캐시 적중 횟수(%)	캐시 적중 횟수/(읽기+쓰기)에서 파생됩니다. 유효 SSD 캐시 작업의 캐시 적중률은 50%보다 커야 합니다. 작은 숫자는 다음과 같은 몇 가지 사항을 나타낼 수 있습니다. • 읽기-쓰기의 비율이 너무 작습니다 • 읽기는 반복되지 않습니다 • 캐시 용량이 너무 작습니다
캐시 할당(%)	할당된 SSD Cache 스토리지의 양으로, 이 컨트롤러에서 사용할 수 있는 SSD Cache 스토리지의 백분율로 표시됩니다. 할당된 바이트/사용 가능한 바이트에서 파생됩니다. 캐시 할당 비율은 일반적으로 100%로 표시됩니다. 이 수치가 100% 미만일 경우 캐시가 워밍업되지 않았거나 SSD Cache 용량이 액세스하는 모든 데이터에 비해 크기 초과임을 의미합니다. 후자의 경우, SSD Cache 용량이 작으면 동일한 수준의 성능을 제공할 수 있습니다. 이는 캐싱된 데이터가 SSD Cache에 배치되었음을 나타내는 것이 아니라 SSD Cache에 데이터를 저장하기 위한 준비 단계일 뿐입니다.
캐시 활용률(%)	SSD Cache 스토리지에 할당된 SSD Cache 스토리지의 백분율로, 활성화된 볼륨의 데이터가 포함된 SSD Cache 스토리지의 양입니다. 이 값은 사용자 데이터 바이트 /할당된 바이트에서 파생된 SSD Cache의 사용률 또는 밀도를 나타냅니다. 일반적으로 캐시 활용률 백분율은 100%보다 낮으며, 이보다 훨씬 낮을 수 있습니다. 이 수치는 캐시 데이터로 채워진 SSD Cache 용량의 비율을 나타냅니다. SSD Cache의 각 할당 유닛인 SSD Cache 블록이 약간 독립적인 서브블록이라는 작은 유닛으로 분리되기 때문에 이 수치는 100%보다 낮습니다. 일반적으로 숫자가 클수록 좋지만 숫자가 적더라도 성능이 크게 향상될 수 있습니다.

자세한 통계

세부 통계는 공칭 통계와 추가 통계로 구성됩니다. 이러한 추가 통계는 공칭 통계와 함께 저장되지만, 공칭 통계와 달리 SSD 캐시 통계 보기 대화 상자에 표시되지 않습니다. 통계를 파일로 내보낸 후에만 상세 통계를 볼 수 `.csv` 있습니다.

파일을 볼 때 `.csv`, 상세 통계는 명목 통계 다음에 나열됩니다.

자세한 통계	설명
블럭 읽기	호스트 읽기의 블록 수입니다.
블럭 쓰기	호스트 쓰기의 블록 수입니다.
전체 적중 블록	캐시 적중의 블록 수입니다. 전체 적중 블록은 SSD Cache에서 완전히 읽은 블록 수를 나타냅니다. SSD Cache는 전체 캐시 적중률이 높은 작업의 성능에만 도움이 됩니다.
부분 조회수	SSD Cache에서 하나 이상의 블록이 있지만 모든 블록이 있는 호스트 읽기 수입니다. 부분 적중은 기본 볼륨에서 읽기가 처리된 SSD Cache * Miss * 입니다.

자세한 통계	설명
부분 조회수 - 블록	부분 조회수(Partial Hits)의 블록 수입니다. 부분 캐시 적중 및 부분 캐시 적중 블록은 SSD Cache에 일부 데이터만 있는 작업으로 인해 발생합니다. 이 경우 작업은 캐시된 하드 디스크 드라이브(HDD) 볼륨에서 데이터를 받아야 합니다. SSD Cache는 이러한 유형의 적중에는 성능 이점이 없습니다. 부분 캐시 적중 블록 수가 전체 캐시 적중 블록보다 많을 경우 다른 I/O 특성 유형(파일 시스템, 데이터베이스 또는 웹 서버)을 사용하면 성능이 향상될 수 있습니다. SSD 캐시가 워밍업 중일 때는 캐시 적중 횟수와 비교하여 부분 적중 횟수 및 실패 횟수가 더 많은 것으로 예상됩니다.
실패	SSD Cache에 블록이 없는 호스트 읽기 수입니다. SSD Cache 누락은 기본 볼륨에서 읽기가 만족스러우면 발생합니다. SSD 캐시가 워밍업 중일 때는 캐시 적중 횟수와 비교하여 부분 적중 횟수 및 실패 횟수가 더 많은 것으로 예상됩니다.
비적중 - 블록	비적중 블록 수입니다.
작업 채우기(호스트 읽기)	기본 볼륨에서 SSD Cache로 데이터가 복사된 호스트 읽기 수입니다.
작업 채우기(호스트 읽기) - 블록	작업 채우기(호스트 읽기)의 블록 수입니다.
작업 채우기(호스트 쓰기)	기본 볼륨에서 SSD Cache로 데이터가 복사된 호스트 쓰기 수입니다. 쓰기 입출력 작업의 결과로 캐시를 채우지 않는 캐시 구성 설정의 경우 작업 채우기(호스트 쓰기) 수가 0일 수 있습니다.
작업 채우기(호스트 쓰기) - 블록	작업 채우기(호스트 쓰기)의 블록 수입니다.
작업을 무효화합니다	데이터가 SSD Cache에서 무효화되거나 제거된 횟수입니다. 캐시 무효화 작업은 각 호스트 쓰기 요청, FUA(Forced Unit Access)가 포함된 각 호스트 읽기 요청, 각 확인 요청 및 기타 일부 상황에 대해 수행됩니다.
작업 재활용	SSD Cache 블록이 다른 기본 볼륨 및/또는 다른 LBA(논리 블록 주소 지정) 범위에 다시 사용된 횟수 효과적인 캐시 작업을 위해서는 읽기 및 쓰기 작업의 조합 수에 비해 재활용 횟수가 적어야 합니다. 재활용 작업 수가 결합된 읽기 및 쓰기 수에 근접하면 SSD 캐시는 스래싱(thrashing)입니다. 캐시 용량을 늘려야 하거나 워크로드를 SSD Cache와 함께 사용하는 것이 적합하지 않습니다.
사용 가능한 바이트	이 컨트롤러에서 SSD Cache에서 사용할 수 있는 바이트 수입니다.
할당된 바이트	이 컨트롤러가 SSD Cache에서 할당한 바이트 수입니다. SSD Cache에서 할당된 바이트가 비어 있거나 기본 볼륨의 데이터가 포함되어 있을 수 있습니다.
사용자 데이터 바이트	SSD Cache에서 기본 볼륨의 데이터를 포함하는 할당된 바이트 수입니다. 사용 가능한 바이트, 할당된 바이트 및 사용자 데이터 바이트는 캐시 할당 백분율 및 캐시 사용률 비율을 계산하는 데 사용됩니다.

풀의 최적화 용량은 얼마입니까**?**

SSD 드라이브는 용량의 일부가 할당되지 않은 경우 수명이 더 길고 쓰기 성능이 극대화됩니다.

풀과 연결된 드라이브의 경우 할당되지 않은 용량은 풀의 보존 용량, 사용 가능한 용량(볼륨에서 사용하지 않는 용량), 추가 최적화 용량으로 남겨 둔 사용 가능한 용량의 일부로 구성됩니다. 추가 최적화 용량은 사용 가능한 용량을 줄여 최적화 용량을 최소화하므로 볼륨 생성에 사용할 수 없습니다.

풀을 생성할 때 성능, 드라이브 마모 수명 및 가용 용량의 균형을 제공하는 권장 최적화 용량이 생성됩니다. Pool Settings(풀 설정) 대화 상자에 있는 Additional Optimization Capacity(추가 최적화 용량) 슬라이더를 사용하여 풀의 최적화 용량을 조정할 수 있습니다. 슬라이더를 조정하면 사용 가능한 용량을 희생하여 더 나은 성능과 드라이브 마모 수명을 얻을 수 있고, 성능과 드라이브 마모 수명을 희생하여 사용 가능한 추가 용량을 확보할 수 있습니다.

추가 최적화 용량 슬라이더는 EF600 및 EF300 스토리지 시스템에서만 사용할 수 있습니다.

볼륨 그룹의 최적화 용량은 무엇입니까**?**

SSD 드라이브는 용량의 일부가 할당되지 않은 경우 수명이 더 길고 쓰기 성능이 극대화됩니다.

볼륨 그룹과 연결된 드라이브의 경우 할당되지 않은 용량은 볼륨 그룹의 여유 용량(볼륨에서 사용하지 않는 용량)과 최적화 용량으로 남겨 둔 사용 가능한 용량의 일부로 구성됩니다. 추가 최적화 용량은 사용 가능한 용량을 줄여 최적화 용량을 최소화하므로 볼륨 생성에 사용할 수 없습니다.

볼륨 그룹이 생성되면 성능, 드라이브 마모 수명 및 가용 용량의 균형을 제공하는 권장 최적화 용량이 생성됩니다. 볼륨 그룹 설정 대화 상자의 추가 최적화 용량 슬라이더를 사용하여 볼륨 그룹의 최적화 용량을 조정할 수 있습니다. 슬라이더를 조정하면 사용 가능한 용량을 희생하여 더 나은 성능과 드라이브 마모 수명을 얻을 수 있고, 성능과 드라이브 마모 수명을 희생하여 사용 가능한 추가 용량을 확보할 수 있습니다.

추가 최적화 용량 슬라이더는 EF600 및 EF300 스토리지 시스템에서만 사용할 수 있습니다.

리소스 프로비저닝 기능은 무엇입니까**?**

리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.

리소스 프로비저닝된 볼륨은 SSD 볼륨 그룹 또는 풀의 일반 볼륨으로, 볼륨이 생성될 때 드라이브 용량이 할당되지만 드라이브 블록이 할당 해제(매핑 해제)됩니다. 이에 비해 기존의 일반 볼륨에서는 Data Assurance 보호 정보 필드를 초기화하고 각 RAID 스트라이프에서 데이터 및 RAID 패리티를 일관되게 만들기 위해 백그라운드 볼륨 초기화 작업 중에 모든 드라이브 블록이 매핑되거나 할당됩니다. 리소스 프로비저닝된 볼륨에서는 시간 제한이 없는 백그라운드 초기화가 없습니다. 대신 각 RAID 스트라이프는 스트라이프의 볼륨 블록에 처음으로 쓸 때 초기화됩니다.

리소스 프로비저닝된 볼륨은 SSD 볼륨 그룹 및 풀에서만 지원되며, 그룹 또는 풀의 모든 드라이브에서 DULBE(Logical Block Error Enable) 오류 복구 기능을 지원합니다. 리소스 프로비저닝된 볼륨이 생성되면 볼륨에 할당된 모든 드라이브 블록의 할당 해제(매핑 해제)가 발생합니다. 또한 호스트는 NVMe 데이터 세트 관리 명령 또는 SCSI Unmap 명령을 사용하여 볼륨에서 논리적 블록을 할당 해제할 수 있습니다. 블록을 할당 해제하면 SSD 마모 수명을 개선하고 최대 쓰기 성능을 높일 수 있습니다. 개선 정도는 드라이브 모델 및 용량에 따라 다릅니다.

리소스 프로비저닝된 볼륨 기능에 대해 알아야 할 내용은 무엇입니까**?**

리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드

초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.

리소스 프로비저닝된 볼륨은 SSD 볼륨 그룹 또는 풀의 일반 볼륨으로, 볼륨이 생성될 때 드라이브 용량이 할당되지만 드라이브 블록이 할당 해제(매핑 해제)됩니다. 이에 비해 기존의 일반 볼륨에서는 Data Assurance 보호 정보 필드를 초기화하고 각 RAID 스트라이프에서 데이터 및 RAID 패리티를 일관되게 만들기 위해 백그라운드 볼륨 초기화 작업 중에 모든 드라이브 블록이 매핑되거나 할당됩니다. 리소스 프로비저닝된 볼륨에서는 시간 제한이 없는 백그라운드 초기화가 없습니다. 대신 각 RAID 스트라이프는 스트라이프의 볼륨 블록에 처음으로 쓸 때 초기화됩니다.

리소스 프로비저닝된 볼륨은 SSD 볼륨 그룹 및 풀에서만 지원되며, 그룹 또는 풀의 모든 드라이브에서 DULBE(Logical Block Error Enable) 오류 복구 기능을 지원합니다. 리소스 프로비저닝된 볼륨이 생성되면 볼륨에 할당된 모든 드라이브 블록의 할당 해제(매핑 해제)가 발생합니다. 또한 호스트는 NVMe 데이터 세트 관리 명령 또는 SCSI Unmap 명령을 사용하여 볼륨에서 논리적 블록을 할당 해제할 수 있습니다. 블록을 할당 해제하면 SSD 마모 수명을 개선하고 최대 쓰기 성능을 높일 수 있습니다. 개선 정도는 드라이브 모델 및 용량에 따라 다릅니다.

드라이브가 DULBE를 지원하는 시스템에서는 리소스 프로비저닝이 기본적으로 사용됩니다. 풀 및 볼륨 그룹 * 에서 기본 설정을 비활성화할 수 있습니다.

볼륨 및 워크로드

볼륨 및 워크로드 개요

애플리케이션, 데이터베이스 및 파일 시스템에서 데이터를 저장하는 컨테이너로 볼륨을 생성할 수 있습니다. 볼륨을 생성할 때 특정 애플리케이션의 스토리지 어레이 구성을 사용자 지정할 워크로드도 선택합니다.

볼륨 및 워크로드란**?**

a_volume_은 호스트가 액세스할 수 있도록 특정 용량으로 생성된 논리적 구성 요소입니다. 볼륨이 두 개 이상의 드라이브로 구성될 수 있지만 볼륨은 호스트에 하나의 논리적 구성 요소로 나타납니다. 볼륨이 정의되면 워크로드에 추가할 수 있습니다. 워크로드 _ 는 SQL Server 또는 Exchange와 같은 애플리케이션을 지원하는 스토리지 오브젝트로서, 이 스토리지 객체를 사용하여 해당 애플리케이션에 대한 스토리지를 최적화할 수 있습니다.

자세한 내용:

- "볼륨 작동 방식"
- "작업 부하 작동 방식"
- "볼륨 용어"
- "볼륨에 용량을 할당하는 방법입니다"
- "볼륨에 대해 수행할 수 있는 작업입니다"

볼륨 및 워크로드를 어떻게 생성합니까**?**

먼저, 워크로드를 생성합니다. 메뉴: 스토리지 [볼륨] 으로 이동하여 단계를 안내하는 마법사를 엽니다. 그런 다음 풀 또는 볼륨 그룹에서 사용할 수 있는 용량으로 볼륨을 생성한 다음 생성한 워크로드를 할당합니다.

자세한 내용:

- "볼륨 생성을 위한 워크플로우"

- "워크로드 생성"
- "볼륨 생성"
- "워크로드에 볼륨 추가"

관련 정보

볼륨과 관련된 개념에 대해 자세히 알아보기:

- "볼륨에 대한 데이터 무결성 및 데이터 보안"
- "SSD Cache 및 볼륨"
- "씬 볼륨 모니터링"

개념

볼륨 작동 방식

볼륨은 스토리지 어레이에서 스토리지 공간을 관리하고 구성하는 데이터 컨테이너입니다.

스토리지 어레이에서 사용 가능한 스토리지 용량에서 볼륨을 생성하여 시스템 리소스를 쉽게 구성 및 사용할 수 있습니다. 이 개념은 컴퓨터에서 폴더/디렉터리를 사용하여 쉽고 빠르게 액세스할 수 있도록 파일을 구성하는 것과 비슷합니다.

볼륨은 호스트에서 볼 수 있는 유일한 데이터 계층입니다. SAN 환경에서 볼륨은 호스트에 표시되는 LUN(Logical Unit Number)에 매핑됩니다. LUN은 FC, iSCSI 및 SAS를 비롯하여 스토리지 어레이에서 지원하는 하나 이상의 호스트 액세스 프로토콜을 사용하여 액세스할 수 있는 사용자 데이터를 저장합니다.

풀 및 볼륨 그룹에서 생성할 수 있는 볼륨 유형입니다

볼륨은 풀 또는 볼륨 그룹에서 용량을 그립니다. 스토리지 시스템에 있는 풀 또는 볼륨 그룹에서 다음 유형의 볼륨을 생성할 수 있습니다.

- * from pool * — 풀에서 _fully-provisioned(thick) volumes_or_thin-provisioned(thin) volumes. _ 로 볼륨을 생성할 수 있습니다

> System Manager 인터페이스에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

- * 볼륨 그룹에서 * — 볼륨 그룹에서 _완전히 프로비저닝된(일반) 볼륨으로만 볼륨을 생성할 수 있습니다.

일반 볼륨 및 씬 볼륨은 스토리지 배열에서 다음과 같은 다양한 방식으로 용량을 그립니다.

- 볼륨을 생성할 때 일반 볼륨의 용량이 할당됩니다.
- 씬 볼륨의 용량은 볼륨에 쓸 때 데이터로 할당됩니다.

씬 프로비저닝은 낭비되는 할당 용량을 방지하고 초기 스토리지 비용을 줄여 줍니다. 그러나 일반 볼륨이 생성될 때 모든 스토리지가 한 번에 할당되므로 전체 프로비저닝의 이점은 지연 시간이 줄어듭니다.

> EF600 및 EF300 스토리지 시스템은 씬 프로비저닝을 지원하지 않습니다.

볼륨의 특성

풀 또는 볼륨 그룹의 각 볼륨은 어떤 유형의 데이터가 저장되어 있는지 기준으로 고유한 개별 특성을 가질 수 있습니다. 이러한 특징에는 다음이 포함됩니다.

- * 세그먼트 크기 * — 세그먼트는 스토리지 어레이가 스트라이프의 다음 드라이브(RAID 그룹)로 이동하기 전에 드라이브에 저장되는 데이터의 양(KB)입니다. 세그먼트 크기는 볼륨 그룹의 용량과 같거나 그보다 작습니다. 세그먼트 크기가 고정되어 풀의 경우 변경할 수 없습니다.
- * 용량 * — 풀 또는 볼륨 그룹에서 사용 가능한 용량을 사용하여 볼륨을 생성합니다. 볼륨을 생성하기 전에 풀 또는 볼륨 그룹이 이미 있어야 하며 볼륨을 생성할 수 있는 충분한 가용 용량이 있어야 합니다.
- * 컨트롤러 소유권 * — 모든 스토리지 어레이에는 하나 또는 두 개의 컨트롤러가 있을 수 있습니다. 단일 컨트롤러 어레이에서 볼륨 워크로드는 단일 컨트롤러에서 관리합니다. 듀얼 컨트롤러 어레이에서 볼륨은 볼륨을 "소유"하는 기본 컨트롤러(A 또는 B)를 갖게 됩니다. 이중 컨트롤러 구성에서는 컨트롤러 간에 워크로드가 이동할 때 자동 로드 밸런싱 기능을 사용하여 볼륨 소유권을 자동으로 조정하여 로드 밸런싱 문제를 해결합니다. 자동 로드 밸런싱은 자동화된 I/O 워크로드 밸런싱을 제공하고 호스트에서 들어오는 I/O 트래픽을 두 컨트롤러 간에 동적으로 관리 및 밸런싱합니다.
- * 볼륨 할당 * — 볼륨을 생성할 때 또는 나중에 호스트에 볼륨에 대한 액세스를 제공할 수 있습니다. 모든 호스트 액세스는 LUN(Logical Unit Number)을 통해 관리됩니다. 호스트는 다시 볼륨에 할당된 LUN을 감지합니다. 여러 호스트에 볼륨을 할당하는 경우 클러스터링 소프트웨어를 사용하여 모든 호스트에서 볼륨을 사용할 수 있는지 확인합니다.

  호스트 유형에는 호스트가 액세스할 수 있는 볼륨 수에 대한 특정 제한이 있을 수 있습니다. 특정 호스트에서 사용할 볼륨을 생성할 때 이 제한 사항을 염두에 두십시오.

- * 설명적 이름 * - - - 어떤 이름을 원하든 볼륨의 이름을 지정할 수 있지만 이름을 설명하는 것이 좋습니다.

볼륨 생성 중에 각 볼륨에 용량이 할당되며 이름, 세그먼트 크기(볼륨 그룹만 해당), 컨트롤러 소유권 및 볼륨-호스트 할당이 할당됩니다. 볼륨 데이터는 필요에 따라 컨트롤러 전체에서 자동으로 로드 밸런싱됩니다.

작업 부하 작동 방식

볼륨을 생성할 때 특정 애플리케이션에 대한 스토리지 어레이 구성을 사용자 지정할 워크로드를 선택합니다.

워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.

볼륨을 생성하는 동안 시스템에서 워크로드 사용에 대한 질문에 답하라는 메시지를 표시합니다. 예를 들어 Microsoft Exchange용 볼륨을 만드는 경우 필요한 메일박스 수, 평균 메일박스 용량 요구 사항, 원하는 데이터베이스 복제본 수를 묻는 메시지가 표시됩니다. 시스템에서는 이 정보를 사용하여 최적의 볼륨 구성을 생성합니다. 이 구성은 필요에 따라 편집할 수 있습니다. 선택적으로 볼륨 생성 순서에서 이 단계를 건너뛸 수 있습니다.

워크로드의 유형입니다

두 가지 유형의 워크로드, 즉 애플리케이션별 워크로드와 기타 워크로드를 생성할 수 있습니다.

- * 응용 프로그램별 *. 애플리케이션별 워크로드를 사용하여 볼륨을 생성하는 경우, 애플리케이션 워크로드 I/O와 애플리케이션 인스턴스의 기타 트래픽 간의 경합을 최소화하기 위해 최적화된 볼륨 구성을 권장할 수 있습니다. I/O 유형, 세그먼트 크기, 컨트롤러 소유권, 읽기 및 쓰기 캐시와 같은 볼륨 특성은 자동으로 권장 사항이며 다음과 같은

애플리케이션 유형에 대해 생성되는 워크로드에 최적화되어 있습니다.

- Microsoft ® SQL Server ™ 를 참조하십시오
- Microsoft ® Exchange Server ™ 를 참조하십시오
- 비디오 감시 애플리케이션
- VMware ESXi ™ (가상 머신 파일 시스템과 함께 사용할 볼륨용)

  볼륨 추가/편집 대화 상자를 사용하여 권장 볼륨 구성을 검토하고 시스템 권장 볼륨 및 특성을 편집, 추가 또는 삭제할 수 있습니다.

- * 기타 * (또는 특정 볼륨 생성을 지원하지 않는 애플리케이션). 다른 워크로드는 볼륨 구성을 사용하며, 특정 애플리케이션과 연결되지 않은 워크로드를 생성하려는 경우 또는 스토리지 어레이에서 사용하려는 애플리케이션에 대한 최적화 기능이 시스템에 내장되어 있지 않은 경우 수동으로 지정해야 합니다. 볼륨 추가/편집 대화 상자를 사용하여 볼륨 구성을 수동으로 지정해야 합니다.

애플리케이션 및 워크로드 뷰

애플리케이션 및 워크로드를 보려면 SANtricity 시스템 관리자를 시작하십시오. 이 인터페이스를 통해 다음과 같은 몇 가지 방법으로 애플리케이션별 워크로드와 관련된 정보를 볼 수 있습니다.

- 볼륨 타일에서 * 애플리케이션 및 워크로드 * 탭을 선택하여 스토리지 어레이의 볼륨을 워크로드별로 그룹화하고 워크로드가 연결된 애플리케이션 유형을 볼 수 있습니다.
- 성능 타일에서 * 애플리케이션 및 워크로드 * 탭을 선택하여 논리적 객체에 대한 성능 메트릭(지연 시간, IOPS 및 MBs)을 볼 수 있습니다. 오브젝트는 애플리케이션 및 관련 워크로드별로 그룹화됩니다. 이 성능 데이터를 정기적으로 수집하면 기준 측정을 설정하고 추세를 분석할 수 있습니다. 이렇게 하면 I/O 성능과 관련된 문제를 조사하는 데 도움이 됩니다.

볼륨 용어

볼륨 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

모든 볼륨 유형

기간	설명
할당된 용량입니다	할당된 용량을 사용하여 볼륨을 생성하고 복제 서비스 작업을 수행할 수 있습니다. 할당된 용량과 보고된 용량은 일반 볼륨에 대해 동일하지만 씬 볼륨에 대해서는 다릅니다. 일반 볼륨의 경우 물리적으로 할당된 공간은 호스트에 보고된 공간과 같습니다. 씬 볼륨의 경우 보고된 용량은 호스트에 보고된 용량이고, 할당된 용량은 데이터 쓰기에 현재 할당된 드라이브 공간의 양입니다.
공유합니다	애플리케이션은 SQL Server 또는 Exchange와 같은 소프트웨어입니다. 각 애플리케이션을 지원할 워크로드를 하나 이상 정의합니다. 일부 애플리케이션의 경우, 시스템은 스토리지를 최적화하는 볼륨 구성을 자동으로 권장합니다. 볼륨 구성에는 I/O 유형, 세그먼트 크기, 컨트롤러 소유권, 읽기 및 쓰기 캐시 같은 특성이 포함됩니다.
용량	용량은 볼륨에 저장할 수 있는 데이터의 양입니다.

기간	설명
컨트롤러 소유권	컨트롤러 소유권은 볼륨의 소유 또는 기본 컨트롤러로 지정된 컨트롤러를 정의합니다. 볼륨은 볼륨을 "소유"하는 기본 컨트롤러(A 또는 B)를 가질 수 있습니다. 컨트롤러 간에 워크로드가 이동할 때 로드 밸런싱 문제를 해결하려면 자동 로드 밸런싱 기능을 사용하여 볼륨 소유권을 자동으로 조정합니다. 자동 로드 밸런싱은 자동화된 I/O 워크로드 밸런싱을 제공하고 호스트에서 들어오는 I/O 트래픽이 두 컨트롤러 간에 동적으로 관리 및 균형 조정되도록 합니다.
동적 캐시 읽기 프리페치	동적 캐시 읽기 프리페치를 사용하면 컨트롤러에서 드라이브에서 캐시로 데이터 블록을 읽는 동안 순차적 데이터 블록을 추가로 캐시에 복사할 수 있습니다. 이 캐싱은 향후 캐시에서 데이터 요청을 채울 수 있는 기회를 높여줍니다. 동적 캐시 읽기 프리페치는 순차적 I/O를 사용하는 멀티미디어 애플리케이션에 중요합니다 캐시로 프리페치되는 데이터의 속도와 양은 호스트 읽기의 속도 및 요청 크기에 따라 자동으로 조정됩니다. 랜덤 액세스로 인해 데이터를 캐시로 프리페치하지 않습니다. 이 기능은 읽기 캐시를 사용하지 않는 경우 적용되지 않습니다. 씬 볼륨의 경우 동적 캐시 읽기 프리페치는 항상 비활성화되어 변경할 수 없습니다.
가용 용량 영역	사용 가능한 용량 영역은 볼륨 삭제 또는 볼륨 생성 중 사용 가능한 모든 용량을 사용하지 않음으로 인해 발생할 수 있는 사용 가능한 용량입니다. 하나 이상의 사용 가능한 용량 영역이 있는 볼륨 그룹에서 볼륨을 생성할 때 볼륨의 용량은 해당 볼륨 그룹에서 가장 큰 사용 가능한 용량 영역으로 제한됩니다. 예를 들어, 볼륨 그룹의 사용 가능한 용량이 총 15GiB이고 사용 가능한 최대 용량 영역이 10GiB인 경우 생성할 수 있는 최대 볼륨은 10GiB입니다. 여유 용량을 통합하면 볼륨 그룹의 최대 사용 가능 용량에서 추가 볼륨을 생성할 수 있습니다.
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.
호스트 클러스터	호스트 클러스터는 호스트 그룹입니다. 호스트 클러스터를 생성하여 동일한 볼륨을 여러 호스트에 쉽게 할당할 수 있습니다.
핫 스페어 드라이브	핫 스페어 드라이브는 볼륨 그룹에서만 지원됩니다. 핫 스페어 드라이브에는 데이터가 없으며 볼륨 그룹에 포함된 RAID 1, RAID 3, RAID 5 또는 RAID 6 볼륨에서 드라이브 장애가 발생할 경우 대기 상태로 작동합니다. 핫 스페어 드라이브는 스토리지 배열에 또 다른 수준의 중복성을 추가합니다.
LUN입니다	LUN(Logical Unit Number)은 호스트가 볼륨을 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다.
미디어 스캔	미디어 검사를 통해 드라이브에서 읽거나 쓰는 동안 드라이브 미디어 오류가 발견되기 전에 이를 감지할 수 있습니다. 미디어 검사는 백그라운드 작업으로 수행되고 정의된 사용자 볼륨에서 모든 데이터 및 중복 정보를 검사합니다.

기간	설명
네임스페이스	네임스페이스는 블록 액세스를 위해 포맷된 NVM 스토리지입니다. 스토리지 배열의 볼륨과 관련된 SCSI의 논리 유닛과 유사합니다.
수영장	풀은 논리적으로 그룹화된 드라이브 집합입니다. 풀을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. (풀 또는 볼륨 그룹에서 볼륨을 생성하는 경우)
풀 또는 볼륨 그룹 용량입니다	풀, 볼륨 또는 볼륨 그룹 용량은 풀 또는 볼륨 그룹에 할당된 스토리지 시스템의 용량입니다. 이 용량은 볼륨을 생성하고 복사 서비스 작업 및 스토리지 오브젝트의 다양한 용량 요구사항을 지원하는 데 사용됩니다.
읽기 캐시	읽기 캐시는 드라이브에서 읽은 데이터를 저장하는 버퍼입니다. 읽기 작업의 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브에 액세스할 필요가 없습니다. 데이터가 플러시될 때까지 읽기 캐시에 남아 있습니다.
보고된 용량입니다	보고된 용량은 호스트에 보고되고 호스트에서 액세스할 수 있는 용량입니다. 보고된 용량과 할당된 용량은 일반 볼륨에서 동일하지만 씬 볼륨에서는 다릅니다. 일반 볼륨의 경우 물리적으로 할당된 공간은 호스트에 보고된 공간과 같습니다. 씬 볼륨의 경우 보고된 용량은 호스트에 보고된 용량이고, 할당된 용량은 데이터 쓰기에 현재 할당된 드라이브 공간의 양입니다.
세그먼트 크기	세그먼트는 스토리지 어레이가 스트라이프의 다음 드라이브(RAID 그룹)로 이동하기 전에 드라이브에 저장되는 데이터의 양(KB)입니다. 세그먼트 크기는 볼륨 그룹의 용량과 같거나 그보다 작습니다. 세그먼트 크기가 고정되어 풀의 경우 변경할 수 없습니다.
스트라이핑	스트라이핑은 스토리지 배열에 데이터를 저장하는 방식입니다. 스트라이핑은 데이터 흐름을 특정 크기의 블록("블록 크기")으로 분할한 다음 이러한 블록을 드라이브에 하나씩 씁니다. 이러한 데이터 저장 방식은 여러 물리적 드라이브에 데이터를 배포하고 저장하는 데 사용됩니다. 스트라이핑은 RAID 0과 동의어이며 패리티를 사용하지 않고 RAID 그룹의 모든 드라이브에 데이터를 분산합니다.
볼륨	볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다.
볼륨 할당	볼륨 할당은 호스트 LUN이 볼륨에 할당되는 방법입니다.
볼륨 이름입니다	볼륨 이름은 볼륨 생성 시 볼륨에 할당된 문자열, 기본 이름을 그대로 사용하거나 볼륨에 저장된 데이터의 유형을 나타내는 보다 설명이 포함된 이름을 제공할 수 있습니다.
볼륨 그룹	볼륨 그룹은 공유 특성을 가진 볼륨의 컨테이너입니다. 볼륨 그룹의 용량과 RAID 레벨이 정의되어 있습니다. 볼륨 그룹을 사용하여 호스트에서 액세스할 수 있는 볼륨을 하나 이상 생성할 수 있습니다. 볼륨 그룹 또는 풀에서 볼륨을 생성합니다.

기간	설명
워크로드	워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.
쓰기 캐시	쓰기 캐시는 드라이브에 아직 기록되지 않은 호스트의 데이터를 저장하는 버퍼입니다. 데이터는 드라이브에 기록될 때까지 쓰기 캐시에 유지됩니다. 쓰기 캐싱은 I/O 성능을 높일 수 있습니다.
미러링을 통한 쓰기 캐싱	미러링으로 쓰기 캐싱은 한 컨트롤러의 캐시 메모리에 기록된 데이터가 다른 컨트롤러의 캐시 메모리에도 기록될 때 발생합니다. 따라서 한 컨트롤러에 장애가 발생하면 다른 컨트롤러가 처리되지 않은 모든 쓰기 작업을 완료할 수 있습니다. 쓰기 캐시 미러링은 쓰기 캐시가 설정되고 두 개의 컨트롤러가 있는 경우에만 사용할 수 있습니다. 볼륨 생성 시 기본 설정은 미러링을 사용한 쓰기 캐시입니다.
배터리 없이 쓰기 캐싱	배터리가 없는 쓰기 캐싱 설정을 사용하면 배터리가 없거나 고장, 완전히 방전되었거나 완전히 충전되지 않은 경우에도 쓰기 캐시가 계속 유지됩니다. 일반적으로 배터리 없이 쓰기 캐시를 선택하는 것은 권장되지 않습니다. 전원이 끊길 경우 데이터가 손실될 수 있기 때문입니다. 일반적으로 쓰기 캐시는 배터리가 충전되거나 장애가 발생한 배터리를 교체할 때까지 컨트롤러에 의해 일시적으로 꺼집니다.

씬 볼륨에만 적용됩니다

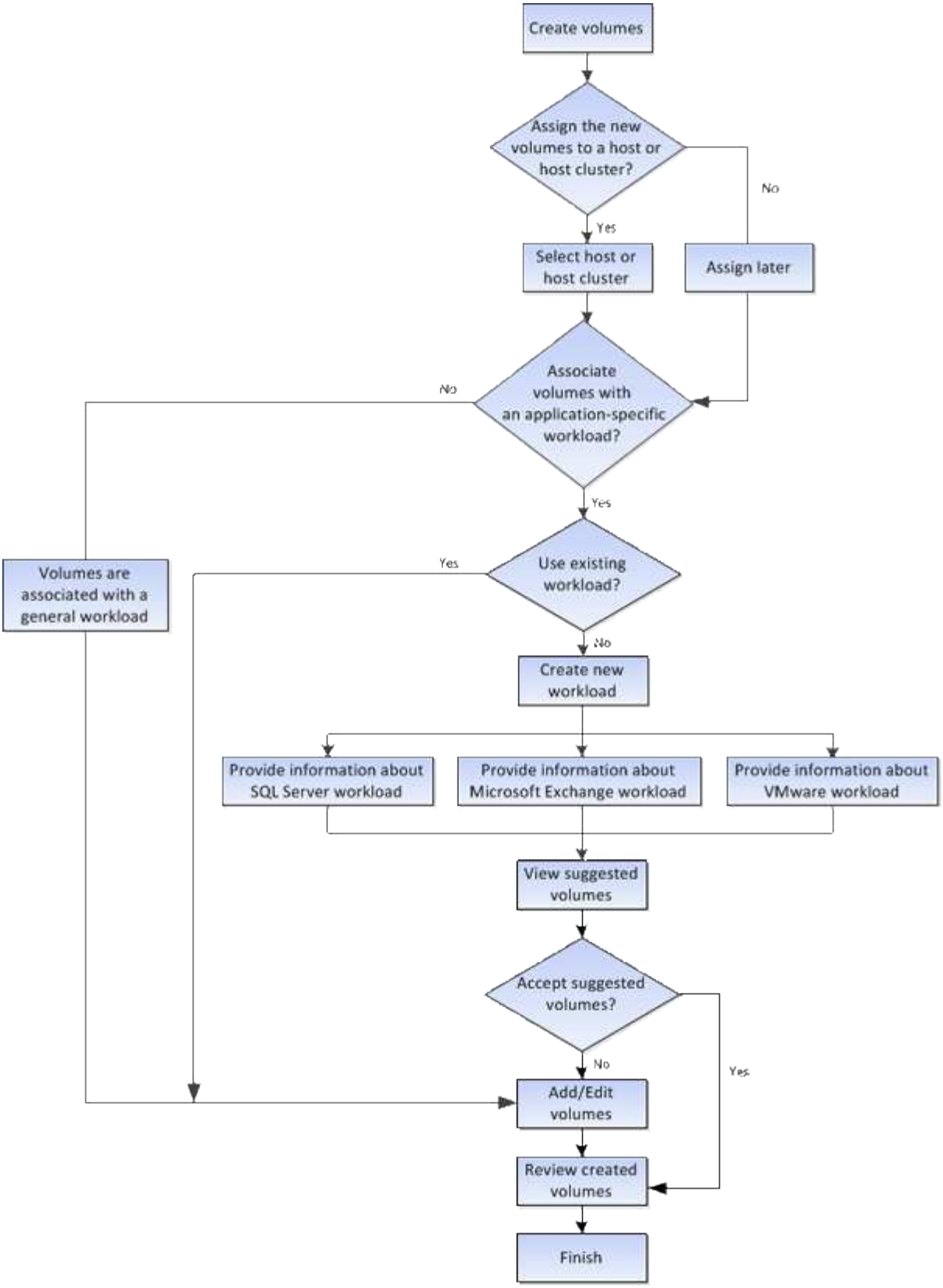
System Manager에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

EF600 또는 EF300 스토리지 시스템에서는 씬 볼륨을 사용할 수 없습니다.

기간	설명
할당된 용량 제한입니다	할당된 용량 제한은 씬 볼륨에 할당된 물리적 용량을 확장할 수 있는 용량의 한도를 나타냅니다.
쓰인 용량	쓰인 용량은 씬 볼륨에 할당된 예약 용량에서 기록된 용량입니다.
경고 임계값	씬 볼륨에 할당된 용량이 최대 백분율(경고 임계값)에 도달하면 경고 임계값 알림이 발생하도록 설정할 수 있습니다.

볼륨 생성을 위한 워크플로우

SANtricity 시스템 관리자에서 다음 단계를 수행하여 볼륨을 생성할 수 있습니다.



볼륨에 대한 데이터 무결성 및 데이터 보안

볼륨에서 DA(Data Assurance) 기능 및 드라이브 보안 기능을 사용하도록 설정할 수 있습니다. 이러한 기능은 풀 및 볼륨 그룹 레벨에서 제공됩니다.

데이터 무결성 보장

DA(Data Assurance)는 T10 PI(보호 정보) 표준을 구현하여 I/O 경로를 통해 데이터가 전송될 때 발생할 수 있는 오류를 확인하고 수정하여 데이터 무결성을 향상합니다. 일반적으로 Data Assurance 기능을 사용하면 컨트롤러와 드라이브 사이의 입출력 경로 부분을 확인할 수 있습니다. DA 기능은 풀 및 볼륨 그룹 레벨에서 제공됩니다.

이 기능을 활성화하면 스토리지 배열은 볼륨의 각 데이터 블록에 오류 검사 코드(순환 중복 검사 또는 CRC라고도 함)를 추가합니다. 데이터 블록이 이동된 후 스토리지 배열은 이러한 CRC 코드를 사용하여 전송 중에 오류가 발생했는지 확인합니다. 잠재적으로 손상된 데이터는 디스크에 기록되거나 호스트에 반환되지 않습니다. DA 기능을 사용하려면 새 볼륨을 생성할 때 DA를 지원하는 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "DA" 옆에 있는 "예"를 확인합니다).

드라이브 보안

드라이브 보안은 스토리지 어레이에서 제거할 때 보안이 설정된 드라이브의 데이터에 대한 무단 액세스를 방지하는 기능입니다. 이러한 드라이브는 연방 정보 처리 표준 140-2 레벨 2(FIPS 드라이브)를 충족하도록 인증된 전체 디스크 암호화(FDE) 드라이브 또는 드라이브일 수 있습니다.

드라이브 보안 작동 방식

FDE 또는 FIPS 중 어떤 보안 가능 드라이브도 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이 암호화 및 암호 해독은 성능 또는 사용자 워크플로에 영향을 주지 않습니다. 각 드라이브에는 드라이브에서 전송할 수 없는 고유한 암호화 키가 있습니다.

드라이브 보안이 볼륨 수준에서 작동하는 방식

보안 가능 드라이브에서 풀 또는 볼륨 그룹을 생성할 때 해당 풀 또는 볼륨 그룹에 대해 드라이브 보안을 설정할 수도 있습니다. Drive Security 옵션을 사용하면 드라이브 및 관련 볼륨 그룹과 풀의 보안이 __enabled_로 설정됩니다. 풀 또는 볼륨 그룹에는 보안이 가능한 드라이브와 비보안 가능 드라이브가 모두 포함될 수 있지만 모든 드라이브는 암호화 기능을 사용할 수 있어야 합니다.

드라이브 보안을 구현하는 방법

드라이브 보안을 구현하려면 다음 단계를 수행하십시오.

1. 스토리지 어레이에 FDE 드라이브 또는 FIPS 드라이브와 같은 보안 지원 드라이브를 제공합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
2. 컨트롤러 및 드라이브에서 읽기/쓰기 액세스를 위해 공유하는 일련의 문자인 보안 키를 생성합니다. 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 외부 키 관리의 경우 키 관리 서버를 사용하여 인증을 설정해야 합니다.
3. 풀 및 볼륨 그룹에 대해 드라이브 보안 설정:
   - 풀 또는 볼륨 그룹을 생성합니다(후보 테이블의 * Secure-Capable * 열에서 * Yes * 를 찾습니다).
   - 새 볼륨을 생성할 때 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 * 보안 가능 * 옆에 * 예 * 가 표시됨).

     드라이브 보안 기능을 사용하면 스토리지 배열의 보안 지원 드라이브와 컨트롤러 간에 공유되는 보안 키를 만들 수 있습니다. 드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다.

SSD Cache 및 볼륨

읽기 전용 성능을 개선하기 위해 SSD Cache에 볼륨을 추가할 수 있습니다. SSD Cache는 스토리지 어레이에서 논리적으로 함께 그룹화하는 SSD(Solid State Disk) 드라이브 세트로 구성됩니다.

볼륨

간단한 볼륨 I/O 메커니즘을 사용하여 데이터를 SSD Cache로 이동하거나 SSD Cache에서 이동할 수 있습니다. 데이터를 SSD에 캐싱하고 저장한 후에는 SSD Cache에서 해당 데이터의 후속 읽기가 수행되므로 HDD 볼륨에 액세스할 필요가 없습니다.

SSD Cache는 컨트롤러의 동적 DRAM(Random Access Memory)의 기본 캐시와 함께 사용되는 보조 캐시입니다.

- 운영 캐시에서 데이터는 호스트 읽기 후 DRAM에 저장됩니다.
- SSD Cache에서는 데이터가 볼륨에서 복사되어 두 개의 내부 RAID 볼륨(컨트롤러당 1개)에 저장됩니다. SSD Cache는 사용자가 SSD Cache를 생성할 때 자동으로 생성됩니다.

내부 RAID 볼륨은 내부 캐시 처리를 위해 사용됩니다. 이러한 볼륨은 사용자 인터페이스에 액세스하거나 표시할 수 없습니다. 그러나 이러한 두 볼륨은 스토리지 어레이에서 허용되는 총 볼륨 수에 대해 계산됩니다.

컨트롤러의 SSD Cache를 사용하도록 할당된 볼륨은 자동 로드 밸런싱 전송을 지원하지 않습니다.

드라이브 보안 기능

또한 Drive Security(보안 활성화)를 사용하는 볼륨에서 SSD Cache를 사용하려면 볼륨과 SSD Cache의 드라이브 보안 기능이 일치해야 합니다. 일치하지 않으면 볼륨이 보안 활성화되지 않습니다.

볼륨에 대해 수행할 수 있는 작업입니다

볼륨에 대해 용량 증가, 삭제, 복사, 초기화, 재배포 등의 다양한 작업을 수행할 수 있습니다. 소유권 변경, 캐시 설정 변경 및 미디어 스캔 설정 변경

용량 증가

다음과 같은 두 가지 방법으로 볼륨의 용량을 확장할 수 있습니다.

- 풀 또는 볼륨 그룹에서 사용할 수 있는 가용 용량을 사용합니다.

  Storage[Pools and Volume Groups > Add Capacity] 메뉴를 선택하여 볼륨에 용량을 추가합니다.

- 할당되지 않은 용량(미사용 드라이브 형태)을 볼륨의 풀 또는 볼륨 그룹에 추가합니다. 풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우 이 옵션을 사용합니다.

  스토리지 [풀 및 볼륨 그룹 > 용량 추가] 메뉴를 선택하여 풀 또는 볼륨 그룹에 할당되지 않은 용량을 추가합니다.

  풀 또는 볼륨 그룹에서 사용 가능한 용량을 사용할 수 없는 경우 볼륨의 용량을 늘릴 수 없습니다. 먼저 풀 또는 볼륨 그룹의 크기를 늘리거나 미사용 볼륨을 삭제해야 합니다.

볼륨 용량을 확장한 후에는 파일 시스템 크기를 수동으로 늘려야 합니다. 이 방법은 사용 중인 파일 시스템에 따라

다릅니다. 자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

삭제

일반적으로 볼륨이 잘못된 매개 변수 또는 용량으로 생성되었거나, 스토리지 구성 요구 사항을 더 이상 충족하지 않거나, 백업 또는 애플리케이션 테스트에 더 이상 필요하지 않은 스냅샷 이미지일 경우 볼륨을 삭제합니다. 볼륨을 삭제하면 풀 또는 볼륨 그룹의 사용 가능한 용량이 증가합니다.

볼륨을 삭제하면 해당 볼륨의 모든 데이터가 손실됩니다. 볼륨을 삭제하면 연결된 스냅샷 이미지, 스케줄 및 스냅샷 볼륨도 삭제되고 모든 미러링 관계가 제거됩니다.

복사

볼륨을 복사할 때 동일한 스토리지 배열에서 두 개의 개별 볼륨, 즉 소스 볼륨과 타겟 볼륨의 시점 복제본을 생성합니다. 스토리지 [볼륨 > 복사본 서비스 > 볼륨 복사] 메뉴를 선택하여 볼륨을 복사할 수 있습니다.

초기화

볼륨을 초기화하면 볼륨의 모든 데이터가 지워집니다. 볼륨이 처음 생성될 때 자동으로 초기화됩니다. 그러나 Recovery Guru는 특정 장애 조건에서 복구하기 위해 볼륨을 수동으로 초기화하도록 조언할 수 있습니다. 볼륨을 초기화할 때 볼륨은 WWN, 호스트 할당, 할당된 용량 및 예약된 용량 설정을 유지합니다. 또한 동일한 DA(Data Assurance) 설정 및 보안 설정을 유지합니다.

Storage [Volumes > More > Initialize volumes] 메뉴를 선택하여 볼륨을 초기화할 수 있습니다.

재분포

볼륨을 재배포하여 볼륨을 기본 컨트롤러 소유자에게 다시 옮깁니다. 일반적으로 다중 경로 드라이버는 호스트 및 스토리지 어레이 사이의 데이터 경로에 문제가 발생할 경우 원하는 컨트롤러 소유자로부터 볼륨을 이동합니다.

대부분의 호스트 다중 경로 드라이버는 기본 컨트롤러 소유자에 대한 경로의 각 볼륨에 액세스를 시도합니다. 그러나 이 기본 경로를 사용할 수 없게 되면 호스트의 다중 경로 드라이버가 대체 경로로 페일오버됩니다. 이 페일오버로 볼륨 소유권이 대체 컨트롤러로 변경될 수 있습니다. 페일오버를 발생시키는 조건을 해결한 후 일부 호스트는 자동으로 볼륨 소유권을 기본 컨트롤러 소유자로 다시 이동하지만 경우에 따라 볼륨을 수동으로 재분산해야 할 수 있습니다.

Storage [Volumes > More > Redistribute volumes] 메뉴를 선택하여 볼륨을 재배포할 수 있습니다.

볼륨 소유권을 변경합니다

볼륨의 소유권을 변경하면 볼륨의 기본 컨트롤러 소유권이 변경됩니다. 볼륨의 기본 컨트롤러 소유자가 Storage [Volumes > View/Edit Settings > Advanced Tab] 메뉴에 나열됩니다.

스토리지 [볼륨 > 자세히 > 소유권 변경] 메뉴를 선택하여 볼륨의 소유권을 변경할 수 있습니다.

미러링 및 볼륨 소유권

미러링된 쌍의 운영 볼륨이 컨트롤러 A에 의해 소유되는 경우, 보조 볼륨은 원격 스토리지 어레이의 컨트롤러 A에 의해 소유됩니다. 운영 볼륨의 소유자를 변경하면 보조 볼륨의 소유자가 자동으로 변경되어 두 볼륨이 동일한 컨트롤러에 의해 소유되도록 합니다. 기본 면의 현재 소유권 변경 사항은 보조 면의 해당 현재 소유권 변경 사항에 자동으로 적용됩니다.

미러 정합성 보장 그룹에 로컬 보조 볼륨이 포함되어 있고 컨트롤러 소유권이 변경된 경우 첫 번째 쓰기 작업에서 보조 볼륨이 자동으로 원래 컨트롤러 소유자에게 다시 전송됩니다. 소유권 변경 * 옵션을 사용하면 보조 볼륨의 컨트롤러

소유권을 변경할 수 없습니다.

볼륨 및 볼륨 소유권을 복사합니다

볼륨 복사 작업 중에 동일한 컨트롤러가 소스 볼륨과 타겟 볼륨을 모두 소유해야 합니다. 복사 볼륨 작업이 시작될 때 두 볼륨에 동일한 기본 컨트롤러가 없는 경우가 있습니다. 따라서 타겟 볼륨의 소유권이 소스 볼륨의 기본 컨트롤러로 자동 전송됩니다. 볼륨 복사가 완료되거나 중지되면 대상 볼륨의 소유권이 기본 컨트롤러로 복원됩니다.

복제 볼륨 작업 중에 소스 볼륨의 소유권이 변경되면 타겟 볼륨의 소유도 변경됩니다. 특정 운영 체제 환경에서는 I/O 경로를 사용하기 전에 다중 경로 호스트 드라이버를 재구성해야 할 수 있습니다. (일부 다중 경로 드라이버는 I/O 경로를 인식하기 위해 편집이 필요합니다. 자세한 내용은 드라이버 설명서를 참조하십시오.)

캐시 설정을 변경합니다

캐시 메모리는 드라이브 미디어보다 액세스 시간이 빠른 컨트롤러의 임시 휘발성 저장 장치(RAM)의 영역입니다. 캐시 메모리를 사용하는 경우 다음과 같은 이유로 전반적인 I/O 성능을 높일 수 있습니다.

- 읽기를 위해 호스트에서 요청된 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브 액세스가 필요하지 않습니다.
- 쓰기 데이터는 처음에는 캐시에 기록되기 때문에 데이터가 드라이브에 기록될 때까지 기다리지 않고 애플리케이션을 계속 사용할 수 있습니다.

메뉴: 스토리지 [볼륨 > 자세히 > 캐시 설정 변경]을 선택하여 다음 캐시 설정을 변경합니다.

- * 읽기 및 쓰기 캐싱 * — 읽기 캐시는 드라이브에서 읽은 데이터를 저장하는 버퍼입니다. 읽기 작업의 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브에 액세스할 필요가 없습니다. 데이터가 플러시될 때까지 읽기 캐시에 남아 있습니다.

  쓰기 캐시는 드라이브에 아직 기록되지 않은 호스트의 데이터를 저장하는 버퍼입니다. 데이터는 드라이브에 기록될 때까지 쓰기 캐시에 유지됩니다. 쓰기 캐싱은 I/O 성능을 높일 수 있습니다.

- * 미러링으로 쓰기 캐싱 * — 한 컨트롤러의 캐시 메모리에 기록된 데이터가 다른 컨트롤러의 캐시 메모리에도 쓰일 때 미러링을 사용하는 쓰기 캐시가 발생합니다. 따라서 한 컨트롤러에 장애가 발생하면 다른 컨트롤러가 처리되지 않은 모든 쓰기 작업을 완료할 수 있습니다. 쓰기 캐시 미러링은 쓰기 캐시가 설정되고 두 개의 컨트롤러가 있는 경우에만 사용할 수 있습니다. 볼륨 생성 시 기본 설정은 미러링을 사용한 쓰기 캐시입니다.
- * 배터리 없는 쓰기 캐싱 * — 배터리 없는 쓰기 캐싱 설정을 사용하면 배터리가 없거나, 고장, 방전되거나, 완전히 충전되지 않았더라도 쓰기 캐싱을 계속할 수 있습니다. 일반적으로 배터리 없이 쓰기 캐시를 선택하는 것은 권장되지 않습니다. 전원이 끊길 경우 데이터가 손실될 수 있기 때문입니다. 일반적으로 쓰기 캐시는 배터리가 충전되거나 장애가 발생한 배터리를 교체할 때까지 컨트롤러에 의해 일시적으로 꺼집니다.

  이 설정은 쓰기 캐시를 설정한 경우에만 사용할 수 있습니다. 씬 볼륨에는 이 설정을 사용할 수 없습니다.

- * 동적 읽기 캐시 프리페치 * — 동적 캐시 읽기 프리페치를 사용하면 컨트롤러에서 드라이브에서 캐시로 데이터 블록을 읽는 동안 순차적 데이터 블록을 추가로 캐시에 복사할 수 있습니다. 이 캐싱은 향후 캐시에서 데이터 요청을 채울 수 있는 기회를 높여줍니다. 동적 캐시 읽기 프리페치는 순차적 I/O를 사용하는 멀티미디어 애플리케이션에 중요합니다 캐시로 프리페치되는 데이터의 속도와 양은 호스트 읽기의 속도 및 요청 크기에 따라 자동으로 조정됩니다. 랜덤 액세스로 인해 데이터를 캐시로 프리페치하지 않습니다. 이 기능은 읽기 캐시를 사용하지 않는 경우 적용되지 않습니다.

  씬 볼륨의 경우 동적 캐시 읽기 프리페치는 항상 비활성화되어 변경할 수 없습니다.

미디어 스캔 설정을 변경합니다

미디어 검사는 애플리케이션에서 자주 읽지 않는 디스크 블록의 미디어 오류를 감지하고 복구합니다. 이 검사는 장애가 발생한 드라이브의 데이터가 풀 또는 볼륨 그룹의 다른 드라이브의 중복 정보와 데이터를 사용하여 재구성되므로 풀 또는 볼륨 그룹의 다른 드라이브에 장애가 발생할 경우 데이터 손실을 방지할 수 있습니다.

미디어 스캔은 스캔 용량 및 스캔 기간에 따라 일정한 속도로 계속 실행됩니다. 백그라운드 스캔은 우선 순위가 더 높은 백그라운드 작업(예: 재구성)에 의해 일시적으로 중단될 수 있지만 동일한 일정한 속도로 재개됩니다.

Storage [Volumes > More > Change media scan settings] 메뉴를 선택하여 미디어 검사가 실행되는 기간을 설정하고 설정할 수 있습니다.

스토리지 배열 및 해당 볼륨에 대해 미디어 검사 옵션이 활성화된 경우에만 볼륨이 스캔됩니다. 해당 볼륨에 대해서도 중복 검사가 활성화된 경우 볼륨에 중복성이 있는 경우 볼륨의 중복 정보가 데이터와 일관되는지 검사합니다. 중복성 검사를 통한 미디어 검사는 각 볼륨을 만들 때 기본적으로 활성화됩니다.

스캔 중에 복구할 수 없는 매체 오류가 발생하면 중복 정보를 사용하여 데이터가 복구됩니다(가능한 경우). 예를 들어, 이중화 정보는 최적의 RAID 5 볼륨 또는 최적의 RAID 6 볼륨에서 사용할 수 있으며 하나의 드라이브에만 장애가 있습니다. 복구 불가능한 오류가 중복 정보를 사용하여 복구할 수 없는 경우 데이터 블록이 읽을 수 없는 섹터 로그에 추가됩니다. 수정 가능한 미디어 오류와 수정 불가능한 미디어 오류가 모두 이벤트 로그에 보고됩니다.

중복 검사가 데이터와 중복 정보 간의 불일치를 발견하면 이벤트 로그에 보고됩니다.

볼륨에 용량을 할당하는 방법입니다

스토리지 배열의 드라이브는 데이터의 물리적 스토리지 용량을 제공합니다. 데이터 저장을 시작하려면 먼저 할당된 용량을 풀 또는 볼륨 그룹이라고 하는 논리적 구성 요소로 구성해야 합니다. 이러한 스토리지 객체를 사용하여 스토리지 배열의 데이터를 구성, 저장, 유지 및 보존할 수 있습니다.

용량을 사용하여 볼륨 생성 및 확장

풀 또는 볼륨 그룹의 할당되지 않은 용량 또는 사용 가능한 용량에서 볼륨을 생성할 수 있습니다.

- 할당되지 않은 용량에서 볼륨을 생성할 경우 풀 또는 볼륨 그룹과 볼륨을 동시에 생성할 수 있습니다.
- 사용 가능한 용량에서 볼륨을 생성할 때 이미 존재하는 풀 또는 볼륨 그룹에 추가 볼륨을 생성하는 것입니다.

볼륨 용량을 확장한 후에는 파일 시스템 크기를 수동으로 늘려야 합니다. 이 방법은 사용 중인 파일 시스템에 따라 다릅니다. 자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

일반 볼륨 및 씬 볼륨의 용량 유형입니다

일반 볼륨이나 씬 볼륨을 생성할 수 있습니다. 보고된 용량과 할당된 용량은 일반 볼륨에서 동일하지만 씬 볼륨에서는 다릅니다.

- 일반 볼륨의 경우 보고된 볼륨 용량은 할당된 물리적 스토리지 용량과 같습니다. 물리적 스토리지 용량의 전체 양이 있어야 합니다. 물리적으로 할당된 공간은 호스트에 보고된 공간과 같습니다.

  일반적으로 일반 볼륨의 보고된 용량을 볼륨이 커질 것으로 생각되는 최대 용량으로 설정합니다. 일반 볼륨은 애플리케이션이 생성할 때 모든 가용 용량이 예약되고 할당되기 때문에 애플리케이션에 예측 가능하고 우수한 성능을 제공합니다.

- 씬 볼륨의 경우 보고된 용량은 호스트에 보고된 용량이고, 할당된 용량은 데이터 쓰기에 현재 할당된 드라이브 공간의 양입니다.

  보고된 용량은 스토리지 배열에 할당된 용량보다 클 수 있습니다. 씬 볼륨은 현재 사용 가능한 자산에 관계없이 성장에 맞게 크기를 조정할 수 있습니다.

> SANtricity System Manager에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

일반 볼륨에 대한 용량 제한입니다

일반 볼륨의 최소 용량은 1MiB이고 최대 용량은 풀 또는 볼륨 그룹의 드라이브 수와 용량에 따라 결정됩니다.

일반 볼륨에 대해 보고된 용량을 늘릴 때는 다음 지침을 염두에 두십시오.

- 최대 3개의 소수 자릿수(예: 65.375GiB)를 지정할 수 있습니다.
- 용량은 볼륨 그룹에서 사용할 수 있는 최대값보다 작거나 같아야 합니다.

  볼륨을 생성할 때 DSS(동적 세그먼트 크기) 마이그레이션에 일부 추가 용량이 사전 할당됩니다. DSS 마이그레이션은 볼륨의 세그먼트 크기를 변경할 수 있는 소프트웨어의 기능입니다.

- 2TiB보다 큰 볼륨은 일부 호스트 운영 체제에서 지원됩니다(보고된 최대 용량은 호스트 운영 체제에 의해 결정됨). 실제로 일부 호스트 운영 체제는 최대 128TiB 볼륨을 지원합니다. 자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

씬 볼륨의 용량 제한입니다

보고된 용량이 크고 할당된 용량이 상대적으로 적은 씬 볼륨을 생성할 수 있으므로 스토리지 활용도와 효율성을 높이는 데 도움이 됩니다. 애플리케이션을 중단하지 않고 할당된 용량을 늘릴 수 있으므로 씬 볼륨을 사용하면 스토리지 관리를 간소화할 수 있습니다.

씬 볼륨은 보고된 용량 및 할당된 용량 외에 쓰기 용량도 포함합니다. 쓰인 용량은 씬 볼륨에 할당된 예약 용량에서 기록된 용량입니다.

다음 표에는 씬 볼륨의 용량 제한이 나와 있습니다.

용량 유형입니다	최소 크기	최대 크기
보고됨	32MiB	256TiB
할당됨	4MiB	64TiB

씬 볼륨의 경우 보고된 최대 256TiB에 도달한 경우 용량을 늘릴 수 없습니다. 씬 볼륨의 예약된 용량이 보고된 최대 용량보다 큰 크기로 설정되었는지 확인합니다.

할당된 용량 제한에 따라 할당된 용량이 자동으로 확장됩니다. 할당된 용량 제한을 사용하면 씬 볼륨의 자동 증가를 보고된 용량 이하로 제한할 수 있습니다. 기록된 데이터의 양이 할당된 용량에 근접하면 할당된 용량 제한을 변경할 수 있습니다.

할당된 용량 제한을 변경하려면 Storage [Volumes > Thin Volume Monitoring 탭 > Change Limit] 메뉴를

선택합니다.

System Manager에서는 씬 볼륨을 생성할 때 전체 용량을 할당하지 않기 때문에 풀에 사용 가능한 용량이 부족할 수 있습니다. 공간이 부족하면 씬 볼륨뿐 아니라 풀에서 용량이 필요한 다른 작업(예: 스냅샷 이미지 또는 스냅샷 볼륨)에 대해서도 풀에 대한 쓰기를 차단할 수 있습니다. 그러나 풀에서 읽기 작업은 계속 수행할 수 있습니다. 이 상황이 발생하면 경고 임계값 경고가 표시됩니다.

씬 볼륨 모니터링

씬 볼륨의 공간을 모니터링하고 용량 부족 상태를 방지하기 위해 적절한 경고를 생성할 수 있습니다.

씬 프로비저닝된 환경은 기본 물리적 스토리지보다 더 많은 논리적 공간을 할당할 수 있습니다. 스토리지 [볼륨 > 씬 볼륨 모니터링] 탭을 선택하여 씬 볼륨이 할당된 최대 한도에 도달하기 전에 얼마나 많은 증가하는지 모니터링할 수 있습니다.

Thin Monitoring 뷰를 사용하여 다음 작업을 수행할 수 있습니다.

- 씬 볼륨이 자동으로 확장될 수 있는 할당된 용량을 제한하는 한도를 정의합니다.
- 씬 볼륨이 할당된 최대 용량 제한에 근접할 때 홈 페이지의 알림 영역에 경고(경고 임계값 초과)가 전송되는 백분율 지점을 설정합니다.

씬 볼륨의 용량을 늘리려면 보고된 용량을 늘리십시오.

> System Manager에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

> EF600 또는 EF300 스토리지 시스템에서는 씬 볼륨을 사용할 수 없습니다.

일반 볼륨과 씬 볼륨 비교

일반 볼륨은 항상 완전히 프로비저닝되므로 볼륨을 생성할 때 모든 용량이 할당됩니다. 씬 볼륨은 항상 씬 프로비저닝됩니다. 즉, 데이터가 볼륨에 쓰일 때 용량이 할당됩니다.

> System Manager에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

볼륨 유형입니다	설명
일반 볼륨	• 일반 볼륨은 풀 또는 볼륨 그룹에서 생성됩니다. • 일반 볼륨의 경우 향후 스토리지 요구 사항을 예상하여 많은 양의 스토리지 공간이 사전에 제공됩니다. • 일반 볼륨은 볼륨을 생성할 때 물리적 스토리지에 사전 할당된 볼륨의 전체 크기로 생성됩니다. 이 사전 할당은 100GiB 볼륨을 생성하는 것이 실제로 드라이브에서 할당된 용량을 100GiB로 사용한다는 것을 의미합니다. 그러나 공간이 계속 사용되지 않아 스토리지 용량의 활용률이 부족할 수 있습니다. • 일반 볼륨을 생성할 때 단일 볼륨에 용량을 초과 할당하지 않도록 합니다. 단일 볼륨에 용량을 초과 할당하면 시스템의 모든 물리적 스토리지를 빠르게 사용할 수 있습니다. • 복제 서비스(스냅샷 이미지, 스냅샷 볼륨, 볼륨 복사본, 비동기식 미러링)에는 스토리지 용량도 필요하므로 일반 볼륨에 모든 용량을 할당하지 마십시오. 공간이 부족하면 풀 또는 볼륨 그룹에 대한 쓰기가 차단될 수 있습니다. 이 상황이 발생하면 여유 용량 경고 임계값 경고가 표시됩니다.
씬 볼륨	• 씬 볼륨은 볼륨 그룹이 아니라 풀에서만 생성됩니다. • 씬 볼륨은 RAID 6이어야 합니다. • EF600 또는 EF300 스토리지 시스템에서는 씬 볼륨을 사용할 수 없습니다. • 씬 볼륨을 생성하려면 CLI를 사용해야 합니다. • 일반 볼륨과 달리 씬 볼륨에 필요한 공간은 생성 중에 할당되지 않고 나중에 필요할 때 제공됩니다. • 씬 볼륨을 사용하면 크기를 초과 할당할 수 있습니다. 즉, 볼륨 크기보다 큰 LUN 크기를 할당할 수 있습니다. 그런 다음 필요에 따라 LUN의 크기를 확장하지 않고 (필요한 경우 프로세스에 드라이브 추가) 사용자를 분리하지 않고 볼륨을 확장할 수 있습니다. • 씬 프로비저닝 블록 공간 재확보(UNMAP)를 사용하여 호스트에서 실행한 SCSI UNMAP 명령을 통해 스토리지 어레이에서 씬 프로비저닝된 볼륨의 블록을 재확보할 수 있습니다. 씬 프로비저닝을 지원하는 스토리지 어레이는 재확보된 공간을 재사용하여 동일한 스토리지 시스템 내에서 다른 씬 프로비저닝된 볼륨에 대한 할당 요청을 충족시킬 수 있으므로 디스크 공간 소비를 더욱 효율적으로 보고하고 리소스를 더욱 효율적으로 사용할 수 있습니다.

씬 볼륨 제한 사항

씬 볼륨은 다음 경우를 제외하고 일반 볼륨으로 모든 작업을 지원합니다.

- 씬 볼륨의 세그먼트 크기는 변경할 수 없습니다.
- 씬 볼륨에 대한 사전 읽기 이중화 검사는 활성화할 수 없습니다.
- 볼륨 복사 작업에서는 씬 볼륨을 타겟 볼륨으로 사용할 수 없습니다.
- 씬 볼륨의 할당된 용량 한도 및 경고 임계값은 비동기 미러링된 쌍의 운영 측면에서만 변경할 수 있습니다. 기본 측에서 이러한 매개 변수를 변경하면 자동으로 보조 측으로 전파됩니다.

스토리지를 구성합니다

워크로드 생성

모든 유형의 애플리케이션에 대한 워크로드를 생성할 수 있습니다.

이 작업에 대해

워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 메뉴: Create [Workload](워크로드 생성)를 선택합니다.

   애플리케이션 워크로드 생성 대화 상자가 나타납니다.

3. 드롭다운 목록을 사용하여 워크로드를 생성할 애플리케이션 유형을 선택한 다음 워크로드 이름을 입력합니다.
4. Create * 를 클릭합니다.

작업을 마친 후

생성한 워크로드에 스토리지 용량을 추가할 준비가 되었습니다. 볼륨 생성 * 옵션을 사용하여 응용 프로그램에 대해 하나 이상의 볼륨을 생성하고 각 볼륨에 특정 양의 용량을 할당할 수 있습니다.

볼륨 생성

볼륨을 생성하여 애플리케이션별 워크로드에 스토리지 용량을 추가하고 생성된 볼륨을 특정 호스트 또는 호스트 클러스터에 표시할 수 있습니다. 또한 볼륨 생성 시퀀스에서는 생성하려는 각 볼륨에 특정 용량을 할당하는 옵션을 제공합니다.

이 작업에 대해

대부분의 애플리케이션 유형은 사용자 정의 볼륨 구성으로 기본 설정됩니다. 일부 애플리케이션 유형에서는 볼륨 생성 시 스마트 구성이 적용됩니다. 예를 들어 Microsoft Exchange 애플리케이션용 볼륨을 만드는 경우 필요한 메일박스 수, 평균 메일박스 용량 요구 사항, 원하는 데이터베이스 복제본 수를 묻는 메시지가 표시됩니다. System Manager는 이 정보를 사용하여 최적의 볼륨 구성을 생성하므로 필요에 따라 편집할 수 있습니다.

볼륨을 생성하는 프로세스는 여러 단계로 이루어집니다.

1단계**:** 볼륨의 호스트를 선택합니다

볼륨을 생성하여 애플리케이션별 워크로드에 스토리지 용량을 추가하고 생성된 볼륨을 특정 호스트 또는 호스트 클러스터에 표시할 수 있습니다. 또한 볼륨 생성 시퀀스에서는 생성하려는 각 볼륨에 특정 용량을 할당하는 옵션을 제공합니다.

시작하기 전에

- 호스트 타일 아래에 유효한 호스트 또는 호스트 클러스터가 있습니다.
- 호스트에 대한 호스트 포트 식별자가 정의되었습니다.
- DA 지원 볼륨을 생성하기 전에 사용하려는 호스트 연결이 DA를 지원해야 합니다. 스토리지 시스템의 컨트롤러에 있는 호스트 접속 중 하나라도 DA를 지원하지 않으면 연결된 호스트가 DA 지원 볼륨의 데이터에 액세스할 수

없습니다.

이 작업에 대해

볼륨을 할당할 때 다음 지침을 염두에 두십시오.

- 호스트의 운영 체제에는 호스트가 액세스할 수 있는 볼륨 수에 대한 특정 제한이 있을 수 있습니다. 특정 호스트에서 사용할 볼륨을 생성할 때 이 제한 사항을 염두에 두십시오.
- 스토리지 배열의 각 볼륨에 대해 하나의 할당을 정의할 수 있습니다.
- 할당된 볼륨은 스토리지 배열의 컨트롤러 간에 공유됩니다.
- 동일한 LUN(Logical Unit Number)을 호스트 또는 호스트 클러스터에서 볼륨에 액세스하는 데 두 번 사용할 수 없습니다. 고유한 LUN을 사용해야 합니다.
- 볼륨 생성 프로세스의 속도를 높이려면 새로 생성된 볼륨이 오프라인으로 초기화되도록 호스트 할당 단계를 건너뛸 수 있습니다.

호스트 클러스터의 호스트에 대해 설정된 할당과 충돌하는 호스트 클러스터에 볼륨을 할당하려고 하면 호스트에 볼륨을 할당할 수 없습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 메뉴 선택: Create [Volume](체적 생성)

   Create Volumes 대화상자가 나타납니다.

3. 드롭다운 목록에서 볼륨을 할당할 특정 호스트 또는 호스트 클러스터를 선택하거나 나중에 호스트 또는 호스트 클러스터를 할당하도록 선택합니다.
4. 선택한 호스트 또는 호스트 클러스터에 대한 볼륨 생성 시퀀스를 계속하려면 * Next * 를 클릭하고 로 이동합니다 2단계: 볼륨에 대한 워크로드를 선택합니다.

   워크로드 선택 대화 상자가 나타납니다.

2단계**:** 볼륨에 대한 워크로드를 선택합니다

Microsoft SQL Server, Microsoft Exchange, Video Surveillance 애플리케이션 또는 VMware와 같은 특정 애플리케이션에 맞게 스토리지 어레이 구성을 사용자 지정할 워크로드를 선택합니다. 이 스토리지 배열에서 사용하려는 애플리케이션이 목록에 없으면 "기타 애플리케이션"을 선택할 수 있습니다.

이 작업에 대해

이 작업에서는 기존 워크로드에 대한 볼륨을 생성하는 방법에 대해 설명합니다.

- _애플리케이션별 워크로드를 사용하여 볼륨을 생성하는 경우, 시스템은 애플리케이션 워크로드 I/O와 애플리케이션 인스턴스의 기타 트래픽 간의 경합을 최소화하기 위해 최적화된 볼륨 구성을 권장할 수 있습니다. 볼륨 추가/편집 대화 상자를 사용하여 권장 볼륨 구성을 검토하고 시스템 권장 볼륨 및 특성을 편집, 추가 또는 삭제할 수 있습니다.
- _ "기타"_응용 프로그램(또는 특정 볼륨 생성이 지원되지 않는 응용 프로그램)을 사용하여 볼륨을 생성하는 경우 볼륨 추가/편집 대화 상자를 사용하여 볼륨 구성을 수동으로 지정합니다.

단계

1. 다음 중 하나를 수행합니다.

- 기존 워크로드에 대한 볼륨을 생성하려면 * 기존 워크로드에 대한 볼륨 생성 * 옵션을 선택합니다.
- 지원되는 애플리케이션 또는 "기타" 애플리케이션의 새 워크로드를 정의하려면 * 새 워크로드 생성 * 옵션을 선택합니다.
  - 드롭다운 목록에서 새 워크로드를 생성할 애플리케이션의 이름을 선택합니다.

    이 스토리지 배열에서 사용하려는 애플리케이션이 목록에 없는 경우 "기타" 항목 중 하나를 선택합니다.
  - 생성할 워크로드의 이름을 입력합니다.

2. 다음 * 을 클릭합니다.
3. 워크로드가 지원되는 애플리케이션 유형과 연결되어 있는 경우 요청된 정보를 입력하고, 그렇지 않은 경우 로 이동합니다.3단계: 볼륨 추가 또는 편집

3단계**:** 볼륨 추가 또는 편집

System Manager에서는 선택한 애플리케이션 또는 워크로드를 기준으로 볼륨 구성을 제안할 수 있습니다. 이 볼륨 구성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 권장 볼륨 구성을 적용하거나 필요에 따라 편집할 수 있습니다. "기타" 애플리케이션 중 하나를 선택한 경우 생성할 볼륨과 특성을 수동으로 지정해야 합니다.

시작하기 전에

- 풀 또는 볼륨 그룹에 충분한 가용 용량이 있어야 합니다.
- 볼륨 그룹에서 허용되는 최대 볼륨 수는 256개입니다.
- 풀에서 허용되는 최대 볼륨 수는 스토리지 시스템 모델에 따라 다릅니다.
  - 2,048 볼륨(EF600 및 E5700 시리즈)
  - 1,024개 볼륨(EF300)
  - 512 볼륨(E2800 시리즈)
- DA(Data Assurance) 지원 볼륨을 생성하려면 사용하려는 호스트 연결이 DA를 지원해야 합니다.

  보안 가능 풀 또는 볼륨 그룹 선택

  DA 지원 볼륨을 생성하려면 DA를 지원하는 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "DA" 옆에 * Yes * 가 표시됨).

  DA 기능은 System Manager의 풀 및 볼륨 그룹 레벨에서 제공됩니다. DA 보호 기능은 컨트롤러를 통해 드라이브로 데이터가 전송될 때 발생할 수 있는 오류를 검사하고 수정합니다. 새 볼륨에 대해 DA 가능 풀 또는 볼륨 그룹을 선택하면 오류가 감지되고 수정됩니다.

  스토리지 시스템의 컨트롤러에 있는 호스트 접속 중 하나라도 DA를 지원하지 않으면 연결된 호스트가 DA 지원 볼륨의 데이터에 액세스할 수 없습니다.
- 보안이 설정된 볼륨을 생성하려면 스토리지 배열에 대한 보안 키를 생성해야 합니다.

보안 가능 풀 또는 볼륨 그룹 선택

보안이 설정된 볼륨을 생성하려면 보안이 가능한 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "보안 가능" 옆에 * 예 * 가 표시됨).

드라이브 보안 기능은 System Manager의 풀 및 볼륨 그룹 레벨에서 제공됩니다. 보안 가능 드라이브는 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스를 방지합니다. 보안이 설정된 드라이브는 쓰기 중에 데이터를 암호화하고, 읽을 때 unique_encryption key_를 사용하여 데이터를 해독합니다.

풀 또는 볼륨 그룹에는 보안이 가능한 드라이브와 비보안 가능 드라이브가 모두 포함될 수 있지만 모든 드라이브는 암호화 기능을 사용할 수 있어야 합니다.

- 리소스 프로비저닝된 볼륨을 만들려면 모든 드라이브가 DULBE(할당 취소 또는 기록되지 않은 논리적 블록 오류) 옵션이 있는 NVMe 드라이브여야 합니다.

이 작업에 대해

풀 또는 볼륨 그룹에서 볼륨을 생성합니다. Add/Edit Volumes 대화 상자에는 스토리지 시스템의 모든 적합한 풀 및 볼륨 그룹이 표시됩니다. 해당하는 각 풀 및 볼륨 그룹에 사용 가능한 드라이브 수와 총 사용 가능한 용량이 나타납니다.

일부 애플리케이션별 워크로드의 경우, 해당되는 각 풀 또는 볼륨 그룹은 제안된 볼륨 구성을 기준으로 제안된 용량을 표시하고 남은 사용 가능 용량을 GiB 단위로 표시합니다. 다른 워크로드의 경우 제안된 용량은 풀 또는 볼륨 그룹에 볼륨을 추가하고 보고된 용량을 지정할 때 나타납니다.

단계

1. 다른 워크로드를 선택했는지와 애플리케이션별 워크로드를 기준으로 다음 작업 중 하나를 선택하십시오.
   - * 기타 * — 하나 이상의 볼륨을 생성하는 데 사용할 각 풀 또는 볼륨 그룹에서 * 새 볼륨 추가 * 를 클릭합니다.

필드 상세정보

필드에 입력합니다	설명
볼륨 이름	볼륨을 생성하는 동안 System Manager에서 볼륨에 기본 이름을 할당합니다. 기본 이름을 그대로 사용하거나 볼륨에 저장된 데이터의 유형을 나타내는 추가 설명을 제공할 수 있습니다.
보고된 용량	새 볼륨의 용량과 사용할 용량 단위(MiB, GiB 또는 TiB)를 정의합니다. 일반 볼륨의 경우 최소 용량은 1MiB이고 최대 용량은 풀 또는 볼륨 그룹에 있는 드라이브의 수와 용량에 따라 결정됩니다. 복제 서비스(스냅샷 이미지, 스냅샷 볼륨, 볼륨 복사본, 원격 미러)에도 스토리지 용량이 필요하므로 표준 볼륨에 모든 용량을 할당하지 마십시오. 풀의 용량은 드라이브 유형에 따라 4GiB 또는 8GiB 단위로 할당됩니다. 4GiB 또는 8GiB의 배수에 포함되지 않은 용량은 할당되지만 사용할 수 없습니다. 전체 용량을 사용할 수 있도록 용량을 4GiB 또는 8GiB 단위로 지정합니다. 사용할 수 없는 용량이 있는 경우, 볼륨을 다시 얻을 수 있는 유일한 방법은 볼륨의 용량을 늘리는 것입니다.
볼륨 블록 크기(EF300 및 EF600만 해당)	볼륨에 대해 생성할 수 있는 블록 크기를 표시합니다. • 512 — 512바이트 • 4k—4,096바이트

필드에 입력합니다	설명
세그먼트 크기	에는 볼륨 그룹의 볼륨에만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. • 허용되는 세그먼트 크기 전환 * — System Manager는 허용되는 세그먼트 크기 전환을 결정합니다. 현재 세그먼트 크기에서 잘못 전환되는 세그먼트 크기는 드롭다운 목록에서 사용할 수 없습니다. 허용되는 전이는 일반적으로 현재 세그먼트 크기의 두 배 또는 절반입니다. 예를 들어 현재 볼륨 세그먼트 크기가 32KiB인 경우 16KiB 또는 64KiB의 새 볼륨 세그먼트 크기가 허용됩니다. • SSD 캐시 사용 볼륨 * — SSD 캐시 사용 볼륨에 대해 4KiB 세그먼트 크기를 지정할 수 있습니다. 작은 블록 입출력 작업을 처리하는 SSD Cache 지원 볼륨(예: 16KiB 입출력 블록 크기 이하)에 대해서만 4KiB 세그먼트 크기를 선택해야 합니다. 대규모 블록 순차적 작업을 처리하는 SSD Cache 지원 볼륨의 세그먼트 크기로 4KiB를 선택하면 성능에 영향을 미칠 수 있습니다. • 세그먼트 크기를 변경하는 시간 * — 볼륨의 세그먼트 크기를 변경하는 시간은 다음 변수에 따라 다릅니다. ◦ 호스트로부터의 I/O 로드 ◦ 볼륨의 수정 우선 순위입니다 ◦ 볼륨 그룹의 드라이브 수입니다 ◦ 드라이브 채널 수입니다 ◦ 스토리지 어레이 컨트롤러의 처리 능력 볼륨의 세그먼트 크기를 변경하면 I/O 성능에 영향을 미치지만 데이터를 계속 사용할 수 있습니다.
보안 가능	• 예 * 는 풀 또는 볼륨 그룹의 드라이브가 보안 가능한 경우에만 "보안 가능" 옆에 표시됩니다. 드라이브 보안은 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스를 방지합니다. 이 옵션은 드라이브 보안 기능이 설정되어 있고 스토리지 배열에 대한 보안 키가 설정된 경우에만 사용할 수 있습니다. 풀 또는 볼륨 그룹에는 보안이 가능한 드라이브와 비보안 가능 드라이브가 모두 포함될 수 있지만 모든 드라이브는 암호화 기능을 사용할 수 있어야 합니다.
DA	• 예 * 는 풀 또는 볼륨 그룹의 드라이브가 DA(Data Assurance)를 지원하는 경우에만 "DA" 옆에 표시됩니다. DA는 전체 스토리지 시스템에서 데이터 무결성을 높입니다. DA를 사용하면 데이터를 컨트롤러를 통해 드라이브로 전송할 때 발생할 수 있는 오류를 스토리지 어레이에서 확인할 수 있습니다. 새 볼륨에 DA를 사용하면 오류가 감지됩니다.

필드에 입력합니다	설명
리소스 프로비저닝(EF300 및 EF600만 해당)	드라이브가 이 옵션을 지원하는 경우에만 * 예 * 가 "리소스 프로비저닝" 옆에 표시됩니다. 리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.

◦ * 애플리케이션별 워크로드 * — * 다음 * 을 클릭하여 선택한 워크로드에 대해 시스템 권장 볼륨 및 특성을 수락하거나 * 볼륨 편집 * 을 클릭하여 선택한 워크로드에 대해 시스템 권장 볼륨 및 특성을 변경, 추가 또는 삭제합니다.

필드 상세정보

필드에 입력합니다	설명
볼륨 이름	볼륨을 생성하는 동안 System Manager에서 볼륨에 기본 이름을 할당합니다. 기본 이름을 그대로 사용하거나 볼륨에 저장된 데이터의 유형을 나타내는 추가 설명을 제공할 수 있습니다.
보고된 용량	새 볼륨의 용량과 사용할 용량 단위(MiB, GiB 또는 TiB)를 정의합니다. 일반 볼륨의 경우 최소 용량은 1MiB이고 최대 용량은 풀 또는 볼륨 그룹에 있는 드라이브의 수와 용량에 따라 결정됩니다. 복제 서비스(스냅샷 이미지, 스냅샷 볼륨, 볼륨 복사본, 원격 미러)에도 스토리지 용량이 필요하므로 표준 볼륨에 모든 용량을 할당하지 마십시오. 풀의 용량은 드라이브 유형에 따라 4GiB 또는 8GiB 단위로 할당됩니다. 4GiB 또는 8GiB의 배수에 포함되지 않은 용량은 할당되지만 사용할 수 없습니다. 전체 용량을 사용할 수 있도록 용량을 4GiB 또는 8GiB 단위로 지정합니다. 사용할 수 없는 용량이 있는 경우, 볼륨을 다시 얻을 수 있는 유일한 방법은 볼륨의 용량을 늘리는 것입니다.
볼륨 유형	볼륨 유형은 애플리케이션별 워크로드에 대해 생성한 볼륨 유형을 나타냅니다.
볼륨 블록 크기(EF300 및 EF600만 해당)	볼륨에 대해 생성할 수 있는 블록 크기를 표시합니다. • 512 — 512바이트 • 4k—4,096바이트

필드에 입력합니다	설명
세그먼트 크기	에는 볼륨 그룹의 볼륨에만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. • 허용되는 세그먼트 크기 전환 * — System Manager는 허용되는 세그먼트 크기 전환을 결정합니다. 현재 세그먼트 크기에서 잘못 전환되는 세그먼트 크기는 드롭다운 목록에서 사용할 수 없습니다. 허용되는 전이는 일반적으로 현재 세그먼트 크기의 두 배 또는 절반입니다. 예를 들어 현재 볼륨 세그먼트 크기가 32KiB인 경우 16KiB 또는 64KiB의 새 볼륨 세그먼트 크기가 허용됩니다. • SSD 캐시 사용 볼륨 * — SSD 캐시 사용 볼륨에 대해 4KiB 세그먼트 크기를 지정할 수 있습니다. 작은 블록 입출력 작업을 처리하는 SSD Cache 지원 볼륨(예: 16KiB 입출력 블록 크기 이하)에 대해서만 4KiB 세그먼트 크기를 선택해야 합니다. 대규모 블록 순차적 작업을 처리하는 SSD Cache 지원 볼륨의 세그먼트 크기로 4KiB를 선택하면 성능에 영향을 미칠 수 있습니다. • 세그먼트 크기를 변경하는 시간 * — 볼륨의 세그먼트 크기를 변경하는 시간은 다음 변수에 따라 다릅니다. ◦ 호스트로부터의 I/O 로드 ◦ 볼륨의 수정 우선 순위입니다 ◦ 볼륨 그룹의 드라이브 수입니다 ◦ 드라이브 채널 수입니다 ◦ 스토리지 어레이 컨트롤러의 처리 능력 볼륨의 세그먼트 크기를 변경하면 I/O 성능에 영향을 미치지만 데이터를 계속 사용할 수 있습니다.

필드에 입력합니다	설명
보안 가능	• 예 * 는 풀 또는 볼륨 그룹의 드라이브가 보안 가능한 경우에만 "보안 가능" 옆에 표시됩니다. 드라이브 보안은 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스를 방지합니다. 이 옵션은 드라이브 보안 기능이 설정되어 있고 스토리지 배열에 대한 보안 키가 설정된 경우에만 사용할 수 있습니다. 풀 또는 볼륨 그룹에는 보안이 가능한 드라이브와 비보안 가능 드라이브가 모두 포함될 수 있지만 모든 드라이브는 암호화 기능을 사용할 수 있어야 합니다.
DA	• 예 * 는 풀 또는 볼륨 그룹의 드라이브가 DA(Data Assurance)를 지원하는 경우에만 "DA" 옆에 표시됩니다. DA는 전체 스토리지 시스템에서 데이터 무결성을 높입니다. DA를 사용하면 데이터를 컨트롤러를 통해 드라이브로 전송할 때 발생할 수 있는 오류를 스토리지 어레이에서 확인할 수 있습니다. 새 볼륨에 DA를 사용하면 오류가 감지됩니다.
리소스 프로비저닝(EF300 및 EF600만 해당)	드라이브가 이 옵션을 지원하는 경우에만 * 예 * 가 "리소스 프로비저닝" 옆에 표시됩니다. 리소스 프로비저닝은 EF300 및 EF600 스토리지 어레이에서 사용 가능한 기능으로, 백그라운드 초기화 프로세스 없이 볼륨을 즉시 사용할 수 있도록 지원합니다.

2. 선택한 응용 프로그램에 대해 볼륨 생성 시퀀스를 계속하려면 * 다음 * 을 클릭하고 로 이동합니다4단계: 볼륨 구성을 검토합니다.

4단계**:** 볼륨 구성을 검토합니다

생성하려는 볼륨의 요약을 검토하고 필요한 사항을 변경합니다.

단계

1. 생성할 볼륨을 검토합니다. 변경하려면 * 뒤로 * 를 클릭합니다.
2. 볼륨 구성이 만족스러우면 * 마침 * 을 클릭합니다.

결과

System Manager는 선택한 풀 및 볼륨 그룹에 새 볼륨을 생성한 다음 All Volumes 테이블에 새 볼륨을 표시합니다.

작업을 마친 후

- 응용 프로그램이 볼륨을 사용할 수 있도록 응용 프로그램 호스트에서 필요한 모든 운영 체제 수정을 수행합니다.

- 타사 공급업체에서 제공하는 운영 체제별 유틸리티를 실행한 다음 SMcli 명령을 `-identifyDevices` 실행하여 볼륨 이름과 호스트 스토리지 배열 이름을 서로 연관시킵니다.

  SMcli는 SANtricity System Manager를 통해 직접 사용할 수 있습니다. SMcli의 다운로드 가능한 버전은 EF600, EF300, E5700, EF570, E2800에서 사용할 수 있습니다. EF280 컨트롤러: SANtricity 시스템 관리자 내에서 SMcli를 다운로드하려면 * 설정 * > * 시스템 * 및 * 추가 기능 * > * 명령줄 인터페이스 * 를 선택합니다.

워크로드에 볼륨 추가

현재 워크로드에 연결되지 않은 볼륨에 대해 기존 또는 새 워크로드에 하나 이상의 볼륨을 추가할 수 있습니다.

이 작업에 대해

CLI(Command Line Interface)를 사용하여 볼륨을 생성했거나 다른 스토리지 어레이에서 마이그레이션(가져오기/내보내기)한 경우 볼륨은 워크로드에 연결되지 않습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 애플리케이션 및 워크로드 * 탭을 선택합니다.

   애플리케이션 및 워크로드 보기가 나타납니다.

3. 워크로드에 추가 * 를 선택합니다.

   워크로드 선택 대화 상자가 나타납니다.

4. 다음 작업 중 하나를 수행합니다.
   - * 기존 워크로드에 볼륨 추가 * — 기존 워크로드에 볼륨을 추가하려면 이 옵션을 선택합니다.

     드롭다운 목록을 사용하여 워크로드를 선택합니다. 이 워크로드에 추가하는 볼륨에 워크로드의 관련 애플리케이션 유형이 할당됩니다.

   - * 새 워크로드에 볼륨 추가 * — 애플리케이션 유형에 대한 새 워크로드를 정의하고 새 워크로드에 볼륨을 추가하려면 이 옵션을 선택합니다.
5. 작업 순서에 추가를 계속하려면 * 다음 * 을 선택합니다.

   볼륨 선택 대화 상자가 나타납니다.

6. 워크로드에 추가할 볼륨을 선택합니다.
7. 선택한 워크로드에 추가할 볼륨을 검토합니다.
8. 워크로드 구성이 만족스러우면 * 마침 * 을 클릭합니다.

볼륨 관리

볼륨의 용량을 늘립니다

풀 또는 볼륨 그룹에서 사용할 수 있는 가용 용량을 사용하여 볼륨의 보고된 용량(호스트에 보고된 용량)을 늘릴 수 있습니다.

시작하기 전에

- 볼륨의 연결된 풀 또는 볼륨 그룹에서 충분한 가용 용량을 사용할 수 있습니다.
- 볼륨은 최적이며 수정 상태가 아닙니다.
- 씬 볼륨의 보고된 최대 용량 256TiB에 도달하지 않았습니다.
- 볼륨에서 사용 중인 핫 스페어 드라이브가 없습니다. (볼륨 그룹의 볼륨에만 적용됩니다.)

한 번에 볼륨 용량을 최대 128TiB까지만 확장할 수 있습니다.

이 작업에 대해

이 풀 또는 볼륨 그룹의 다른 볼륨에 대해서는 향후 용량 요구 사항을 염두에 두십시오. 스냅샷 이미지, 스냅샷 볼륨 또는 원격 미러를 생성할 수 있는 여유 용량을 충분히 확보하십시오.

볼륨 용량 증가는 특정 운영 체제에서만 지원됩니다. 지원되지 않는 호스트 운영 체제에서 볼륨 용량을 늘릴 경우 확장된 용량을 사용할 수 없으며 원래 볼륨 용량을 복원할 수 없습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 용량을 늘릴 볼륨을 선택한 다음 * 용량 증가 * 를 선택합니다.

   용량 증가 확인 대화 상자가 나타납니다.

3. 계속하려면 * 예 * 를 선택하십시오.

   보고된 용량 증가 대화 상자가 나타납니다.

   이 대화 상자에는 볼륨의 현재 보고된 용량과 볼륨의 연결된 풀 또는 볼륨 그룹에서 사용 가능한 가용 용량이 표시됩니다.

4. 보고된 용량을 현재 사용 가능한 보고된 용량에 추가하려면 * 보고 용량 증가… * 상자를 사용합니다. 용량 값을 변경하여 메비바이트(MiB), 기비바이트(GiB) 또는 테비바이트(TiB)로 표시할 수 있습니다.
5. 증가 * 를 클릭합니다.

결과

- System Manager는 선택에 따라 볼륨의 용량을 늘립니다.
- Home[View Operations in Progress] 메뉴를 선택하여 선택한 볼륨에 대해 현재 실행 중인 용량 증가 작업의 진행률을 확인합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

작업을 마친 후

볼륨 용량을 확장한 후에는 파일 시스템 크기를 수동으로 늘려야 합니다. 이 방법은 사용 중인 파일 시스템에 따라 다릅니다. 자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

볼륨 초기화

볼륨이 처음 생성될 때 자동으로 초기화됩니다. 그러나 Recovery Guru는 특정 장애 조건에서 복구하기 위해 볼륨을 수동으로 초기화하도록 조언할 수 있습니다. 이 옵션은 기술 지원 부서의 안내에 따라서만 사용할 수 있습니다. 초기화할 볼륨을 하나 이상 선택할 수 있습니다.

시작하기 전에

- 모든 I/O 작업이 중지되었습니다.
- 초기화하려는 볼륨의 모든 디바이스 또는 파일 시스템은 마운트 해제해야 합니다.
- 볼륨이 Optimal(최적) 상태이며 볼륨에서 수정 작업이 진행 중있지 않습니다.

> 작업을 시작한 후에는 취소할 수 없습니다. 모든 볼륨 데이터가 지워집니다. Recovery Guru에서 그렇게 하도록 조언하지 않는 한 이 작업을 수행하지 마십시오. 이 절차를 시작하기 전에 기술 지원 부서에 문의하십시오.

이 작업에 대해

볼륨을 초기화할 때 볼륨은 WWN, 호스트 할당, 할당된 용량 및 예약된 용량 설정을 유지합니다. 또한 동일한 DA(Data Assurance) 설정 및 보안 설정을 유지합니다.

다음과 같은 유형의 볼륨을 초기화할 수 없습니다.

- 스냅샷 볼륨의 기본 볼륨입니다
- 미러 관계의 운영 볼륨입니다
- 미러 관계의 보조 볼륨입니다
- 볼륨 복사본의 소스 볼륨입니다
- 볼륨 복사본의 타겟 볼륨입니다
- 이미 초기화가 진행 중인 볼륨입니다

이 항목은 풀 또는 볼륨 그룹에서 생성된 표준 볼륨에만 적용됩니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 임의의 볼륨을 선택한 다음 menu:More [Initialize volumes](추가 [볼륨 초기화])를 선택합니다.

   볼륨 초기화 대화 상자가 나타납니다. 스토리지 배열의 모든 볼륨이 이 대화 상자에 나타납니다.

3. 초기화하려는 볼륨을 하나 이상 선택하고 작업을 수행할지 확인합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 초기화된 볼륨에서 모든 데이터를 지웁니다.
- 블록 인덱스를 지웁니다. 이로 인해 기록되지 않은 블록이 0으로 채워진 것처럼 읽힙니다(볼륨이 완전히 비어 있는 것처럼 보임).

Home [View Operations in Progress] 메뉴를 선택하여 선택한 볼륨에 대해 현재 실행 중인 초기화 작업의 진행률을 확인합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

볼륨을 재배포합니다

볼륨을 재배포하여 볼륨을 기본 컨트롤러 소유자에게 다시 옮깁니다. 일반적으로 다중 경로

드라이버는 호스트 및 스토리지 어레이 사이의 데이터 경로에 문제가 발생할 경우 원하는 컨트롤러 소유자로부터 볼륨을 이동합니다.

시작하기 전에

- 재배포하려는 볼륨이 사용 중이 아니거나 입출력 오류가 발생합니다.
- 재배포하려는 볼륨을 사용하는 모든 호스트에 다중 경로 드라이버가 설치되어 있거나 I/O 오류가 발생합니다.

  호스트에 다중 경로 드라이버 없이 볼륨을 재배포하려는 경우, 재분배 작업이 진행 중인 동안 볼륨에 대한 모든 I/O 작업을 중지하여 애플리케이션 오류를 방지해야 합니다.

이 작업에 대해

대부분의 호스트 다중 경로 드라이버는 기본 컨트롤러 소유자에 대한 경로의 각 볼륨에 액세스를 시도합니다. 그러나 이 기본 경로를 사용할 수 없게 되면 호스트의 다중 경로 드라이버가 대체 경로로 페일오버됩니다. 이 페일오버로 볼륨 소유권이 대체 컨트롤러로 변경될 수 있습니다. 페일오버를 발생시키는 조건을 해결한 후 일부 호스트는 자동으로 볼륨 소유권을 기본 컨트롤러 소유자로 다시 이동하지만 경우에 따라 볼륨을 수동으로 재분산해야 할 수 있습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 메뉴 선택: More [Redistribute volumes](추가 [볼륨 재배포])

   Redistribute Volumes 대화상자가 나타납니다. 기본 컨트롤러 소유자가 현재 소유자와 일치하지 않는 스토리지 배열의 모든 볼륨이 이 대화 상자에 나타납니다.

3. 재배포할 볼륨을 하나 이상 선택하고 작업을 수행할지 확인합니다.

결과

System Manager에서 선택한 볼륨을 기본 컨트롤러 소유자로 이동하거나 Redistribute Volumes Unnessary 대화 상자가 나타날 수 있습니다.

볼륨의 컨트롤러 소유권을 변경합니다

호스트 애플리케이션의 입출력이 새 경로를 통해 진행되도록 볼륨의 기본 컨트롤러 소유권을 변경할 수 있습니다.

시작하기 전에

다중 경로 드라이버를 사용하지 않는 경우, 현재 볼륨을 사용 중인 모든 호스트 응용 프로그램을 종료해야 합니다. 이렇게 하면 입출력 경로가 변경될 때 응용 프로그램 오류가 발생하지 않습니다.

이 작업에 대해

풀 또는 볼륨 그룹에서 하나 이상의 볼륨에 대한 컨트롤러 소유권을 변경할 수 있습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 볼륨을 선택한 다음 메뉴 추가 [소유권 변경]을 선택합니다.

   볼륨 소유권 변경 대화 상자가 나타납니다. 스토리지 배열의 모든 볼륨이 이 대화 상자에 나타납니다.

3. Preferred Owner * 드롭다운 목록을 사용하여 변경하려는 각 볼륨의 기본 컨트롤러를 변경하고 작업을 수행할지

확인합니다.

결과

- System Manager는 볼륨의 컨트롤러 소유권을 변경합니다. 이제 이 I/O 경로를 통해 볼륨에 대한 I/O가 전달됩니다.
- 다중 경로 드라이버가 새 경로를 인식하도록 다시 구성하기 전까지 볼륨은 새 I/O 경로를 사용하지 않을 수 있습니다. 이 작업은 일반적으로 5분 이내에 완료됩니다.

볼륨을 삭제합니다

일반적으로 볼륨이 잘못된 매개 변수 또는 용량으로 생성되었거나, 스토리지 구성 요구 사항을 더 이상 충족하지 않거나, 백업 또는 애플리케이션 테스트에 더 이상 필요하지 않은 스냅샷 이미지일 경우 볼륨을 삭제합니다.

볼륨을 삭제하면 풀 또는 볼륨 그룹의 사용 가능한 용량이 증가합니다. 삭제할 볼륨을 하나 이상 선택할 수 있습니다.

시작하기 전에

삭제하려는 볼륨에서 다음 사항을 확인합니다.

- 모든 데이터가 백업됩니다.
- 모든 입출력(I/O)이 중지됩니다.
- 모든 디바이스 및 파일 시스템이 마운트 해제되었습니다.

이 작업에 대해

다음 조건 중 하나가 있는 볼륨은 삭제할 수 없습니다.

- 볼륨을 초기화하는 중입니다.
- 볼륨을 재구성하는 중입니다.
- 볼륨은 카피백 작업을 진행 중인 드라이브가 포함된 볼륨 그룹의 일부입니다.
- 볼륨이 이제 실패 상태가 아닌 경우, 볼륨이 세그먼트 크기 변경과 같은 수정 작업을 진행 중입니다.
- 볼륨에 모든 유형의 영구 예약이 있습니다.
- 볼륨은 복사 볼륨의 소스 볼륨 또는 대상 볼륨이며 보류 중, 진행 중 또는 실패 상태입니다.

볼륨을 삭제하면 해당 볼륨의 모든 데이터가 손실됩니다.

볼륨이 지정된 크기(현재 128TB)를 초과할 경우 백그라운드에서 삭제가 수행되고 있으며 확보된 공간을 즉시 사용할 수 없습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 삭제 * 를 클릭합니다.

   Delete Volumes(볼륨 삭제) 대화 상자가 나타납니다.

3. 삭제할 볼륨을 하나 이상 선택하고 작업을 수행할지 확인합니다.

4. 삭제 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 연결된 스냅샷 이미지, 스케줄 및 스냅샷 볼륨을 삭제합니다.
- 미러링 관계를 제거합니다.
- 풀 또는 볼륨 그룹의 사용 가능한 용량을 늘립니다.

씬 볼륨에 할당된 용량 제한을 변경합니다

필요 시 공간을 할당할 수 있는 씬 볼륨의 경우 씬 볼륨이 자동으로 확장될 수 있는 할당된 용량을 제한하는 제한을 변경할 수 있습니다.

씬 볼륨이 할당된 용량 제한에 근접하면 홈 페이지의 알림 영역으로 알림(경고 임계값 초과)이 전송되는 백분율 지점을 변경할 수도 있습니다. 이 경고 알림을 활성화 또는 비활성화할 수 있습니다.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

할당된 용량 제한에 따라 할당된 용량이 자동으로 확장됩니다. 할당된 용량 제한을 사용하면 씬 볼륨의 자동 증가를 보고된 용량 이하로 제한할 수 있습니다. 기록된 데이터의 양이 할당된 용량에 근접하면 할당된 용량 제한을 변경할 수 있습니다.

씬 볼륨의 할당된 용량 한도 및 경고 임계값을 변경할 때는 볼륨의 사용자 데이터와 복제 서비스 데이터 모두에서 사용할 공간을 고려해야 합니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. Thin Volume Monitoring * 탭을 선택합니다.

   Thin Volume Monitoring(씬 볼륨 모니터링) 보기가 나타납니다.

3. 변경할 씬 볼륨을 선택한 다음 * Change Limit * 를 선택합니다.

   변경 한도 대화 상자가 나타납니다. 이 대화 상자에 선택한 씬 볼륨의 할당된 용량 제한 및 경고 임계값 설정이 표시됩니다.

4. 필요에 따라 할당된 용량 한도 및 경고 임계값을 변경합니다.

필드 상세정보

설정	설명
할당된 용량 제한을 다음으로 변경…	쓰기가 실패하는 임계값으로, 씬 볼륨에서 추가 리소스를 사용할 수 없습니다. 이 임계값은 볼륨에서 보고된 용량 크기의 백분율입니다.
다음 경우에 알림: (경고 임계값)	씬 볼륨이 할당된 용량 제한에 근접할 때 시스템에서 알림을 생성하도록 하려면 확인란을 선택합니다. 이 알림은 홈 페이지의 알림 영역으로 전송됩니다. 이 임계값은 볼륨에서 보고된 용량 크기의 백분율입니다. 경고 임계값 경고 알림을 비활성화하려면 이 확인란의 선택을 취소합니다.

5. 저장 * 을 클릭합니다.

설정을 관리합니다

볼륨의 설정을 변경합니다

이름, 호스트 할당, 세그먼트 크기, 수정 우선순위, 캐싱 등과 같은 볼륨 설정을 변경할 수 있습니다. 등.

시작하기 전에

변경하려는 볼륨이 최적 상태입니다.

볼륨 설정을 변경하는 동안 일부 작업을 사용할 수 없습니다

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 변경할 볼륨을 선택한 다음 * 설정 보기/편집 * 을 선택합니다.

   볼륨 설정 대화 상자가 나타납니다. 선택한 볼륨의 구성 설정이 이 대화 상자에 나타납니다.

3. 볼륨의 이름과 호스트 할당을 변경하려면 * Basic * 탭을 선택합니다.

필드 상세정보

설정	설명
이름	볼륨의 이름을 표시합니다. 현재 이름이 더 이상 의미가 없거나 적용할 수 없는 경우 볼륨의 이름을 변경합니다.
용량	선택한 볼륨에 대해 보고되고 할당된 용량을 표시합니다. 보고된 용량과 할당된 용량은 일반 볼륨에서 동일하지만 씬 볼륨에서는 다릅니다. 일반 볼륨의 경우 물리적으로 할당된 공간은 호스트에 보고된 공간과 같습니다. 씬 볼륨의 경우 보고된 용량은 호스트에 보고된 용량이고, 할당된 용량은 데이터 쓰기에 현재 할당된 드라이브 공간의 양입니다.
풀/볼륨 그룹입니다	풀 또는 볼륨 그룹의 이름과 RAID 레벨을 표시합니다. 풀 또는 볼륨 그룹이 보안이 가능하고 보안이 설정된 상태인지 여부를 나타냅니다.
호스트	볼륨 할당을 표시합니다. I/O 작업을 위해 액세스할 수 있도록 볼륨을 호스트 또는 호스트 클러스터에 할당합니다. 이 할당은 호스트 또는 호스트 클러스터에 특정 볼륨 또는 스토리지 배열의 여러 볼륨에 대한 액세스 권한을 부여합니다. • * Assigned to * — 선택한 볼륨에 대한 액세스 권한이 있는 호스트 또는 호스트 클러스터를 식별합니다. • * LUN * — 논리 단위 번호(LUN)는 호스트가 볼륨에 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다. NVMe 인터페이스의 경우 이 열에는 네임스페이스 ID가 표시됩니다. 네임스페이스는 블록 액세스를 위해 포맷된 NVM 스토리지입니다. 스토리지 배열의 볼륨과 관련된 SCSI의 논리 유닛과 유사합니다. 네임스페이스 ID는 네임스페이스에 대한 NVMe 컨트롤러의 고유 식별자이며 1에서 255 사이의 값으로 설정할 수 있습니다. SCSI의 LUN(Logical Unit Number)과 유사합니다.
식별자	선택한 볼륨의 식별자를 표시합니다. • * WWID(World Wide Identifier) * — 볼륨의 고유 16진수 식별자입니다. • * EUI(Extended Unique Identifier) * — EUI-64 볼륨 식별자입니다. • * 하위 시스템 식별자(SSID) * — 볼륨의 스토리지 어레이 하위 시스템 식별자입니다.

4. 풀 또는 볼륨 그룹의 볼륨에 대한 추가 구성 설정을 변경하려면 * 고급 * 탭을 선택합니다.

필드 상세정보

설정	설명
애플리케이션 및 워크로드 정보	볼륨 생성 중에 애플리케이션별 워크로드 또는 기타 워크로드를 생성할 수 있습니다. 해당하는 경우 선택한 볼륨에 대한 워크로드 이름, 애플리케이션 유형 및 볼륨 유형이 표시됩니다. 필요한 경우 워크로드 이름을 변경할 수 있습니다.
서비스 품질 설정	• 영구적으로 데이터 무결성 보장 * 사용 안 함 — 이 설정은 볼륨이 DA(Data Assurance)를 사용하는 경우에만 나타납니다. DA는 컨트롤러를 통해 드라이브로 데이터가 전송될 때 발생할 수 있는 오류를 검사하고 수정합니다. 선택한 볼륨에서 DA를 영구적으로 비활성화하려면 이 옵션을 사용합니다. 비활성화하면 이 볼륨에서 DA를 다시 활성화할 수 없습니다. • 사전 읽기 중복 검사 활성화 * — 이 설정은 볼륨이 일반 볼륨인 경우에만 나타납니다. 사전 읽기 이중화 검사는 읽기 수행 시 볼륨의 데이터가 일관되는지 여부를 결정합니다. 이 기능이 활성화된 볼륨은 컨트롤러 펌웨어에 의해 데이터가 일치하지 않는 것으로 확인되면 읽기 오류를 반환합니다.
컨트롤러 소유권	볼륨의 소유 또는 기본 컨트롤러로 지정된 컨트롤러를 정의합니다. 컨트롤러 소유권은 매우 중요하며 신중하게 계획해야 합니다. 전체 I/O에 대해 컨트롤러를 최대한 균형 조정해야 합니다.

설정	설명
세그먼트 크기 조정	에는 볼륨 그룹의 볼륨에 대해서만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. • 허용되는 세그먼트 크기 전환 * — System Manager는 허용되는 세그먼트 크기 전환을 결정합니다. 현재 세그먼트 크기에서 잘못 전환되는 세그먼트 크기는 드롭다운 목록에서 사용할 수 없습니다. 허용되는 전이는 일반적으로 현재 세그먼트 크기의 두 배 또는 절반입니다. 예를 들어 현재 볼륨 세그먼트 크기가 32KiB인 경우 16KiB 또는 64KiB의 새 볼륨 세그먼트 크기가 허용됩니다. • SSD 캐시 사용 볼륨 * — SSD 캐시 사용 볼륨에 대해 4KiB 세그먼트 크기를 지정할 수 있습니다. 작은 블록 입출력 작업을 처리하는 SSD Cache 지원 볼륨(예: 16KiB 입출력 블록 크기 이하)에 대해서만 4KiB 세그먼트 크기를 선택해야 합니다. 대규모 블록 순차적 작업을 처리하는 SSD Cache 지원 볼륨의 세그먼트 크기로 4KiB를 선택하면 성능에 영향을 미칠 수 있습니다. • 세그먼트 크기를 변경하는 시간 * — 볼륨의 세그먼트 크기를 변경하는 시간은 다음 변수에 따라 다릅니다. ◦ 호스트로부터의 I/O 로드 ◦ 볼륨의 수정 우선 순위입니다 ◦ 볼륨 그룹의 드라이브 수입니다 ◦ 드라이브 채널 수입니다 ◦ 스토리지 어레이 컨트롤러의 처리 능력 볼륨의 세그먼트 크기를 변경하면 I/O 성능에 영향을 미치지만 데이터를 계속 사용할 수 있습니다.
수정 우선 순위	에는 볼륨 그룹의 볼륨에 대해서만 표시되는 수정 우선 순위 설정이 나와 있습니다. 수정 우선순위는 시스템 성능과 관련하여 볼륨 수정 작업에 할당되는 처리 시간을 정의합니다. 시스템 성능에 영향을 미칠 수 있지만 볼륨 수정 우선 순위를 높일 수 있습니다. 슬라이더 막대를 이동하여 우선 순위 수준을 선택합니다. • 수정 우선 순위 비율 * - 최저 우선 순위 비율은 시스템 성능에 도움이 되지만 수정 작업은 더 오래 걸립니다. 가장 높은 우선 순위의 경우 수정 작업에 도움이 되지만 시스템 성능이 저하될 수 있습니다.
캐싱	에는 볼륨의 전체 I/O 성능에 영향을 미치기 위해 변경할 수 있는 캐싱 설정이 나와 있습니다.

설정	설명
SSD 캐시	에는 SSD 캐시 설정이 나와 있습니다. 이 설정은 호환 볼륨에서 읽기 전용 성능을 향상하는 방법으로 활성화할 수 있습니다. 동일한 드라이브 보안 및 Data Assurance 기능을 공유하는 볼륨은 호환됩니다. • SSD 캐시 기능은 하나 또는 여러 개의 SSD(Solid State Disk)를 사용하여 읽기 캐시를 구현합니다 *. SSD의 읽기 시간이 더 빨라지므로 애플리케이션 성능이 향상됩니다. 읽기 캐시가 스토리지 배열에 있기 때문에, 캐시는 스토리지 배열을 사용하는 모든 응용 프로그램에서 공유됩니다. 캐시하려는 볼륨을 선택한 다음 캐싱은 자동으로 이루어지며 동적 볼륨입니다.

5. 저장 * 을 클릭합니다.

   System Manager는 선택에 따라 볼륨 설정을 변경합니다.

작업을 마친 후

Home[View Operations in Progress] 메뉴를 선택하여 선택한 볼륨에 대해 현재 실행 중인 변경 작업의 진행 상황을 봅니다.

워크로드 설정을 변경합니다

워크로드의 이름을 변경하고 관련 애플리케이션 유형을 볼 수 있습니다. 현재 이름이 더 이상 의미가 없거나 적용할 수 없는 경우 워크로드의 이름을 변경합니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 애플리케이션 및 워크로드 * 탭을 선택합니다.

   애플리케이션 및 워크로드 보기가 나타납니다.

3. 변경할 워크로드를 선택한 다음 * 설정 보기/편집 * 을 선택합니다.

   애플리케이션 및 워크로드 설정 대화 상자가 나타납니다.

4. * 선택 사항: * 사용자가 제공한 워크로드 이름을 변경합니다.
5. 저장 * 을 클릭합니다.

볼륨의 캐시 설정을 변경합니다

읽기 캐시 및 쓰기 캐시 설정을 변경하여 볼륨의 전체 I/O 성능에 영향을 줄 수 있습니다.

이 작업에 대해

볼륨에 대한 캐시 설정을 변경할 때 다음 지침을 염두에 두십시오.

- 캐시 설정 변경 대화 상자를 연 후 선택한 캐시 속성 옆에 아이콘이 표시될 수 있습니다. 이 아이콘은 컨트롤러의 캐싱 작업이 일시적으로 중단되었음을 나타냅니다.

이 동작은 새 배터리가 충전 중이거나 컨트롤러가 분리되었거나 컨트롤러에서 캐시 크기가 일치하지 않는 경우 발생할 수 있습니다. 조건이 지워지면 대화 상자에서 선택한 캐시 속성이 활성화됩니다. 선택한 캐시 속성이 활성화되지 않으면 기술 지원 부서에 문의하십시오.

- 단일 볼륨 또는 스토리지 배열의 여러 볼륨에 대한 캐시 설정을 변경할 수 있습니다. 모든 표준 볼륨 또는 모든 씬 볼륨에 대한 캐시 설정을 동시에 변경할 수 있습니다.

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 임의의 볼륨을 선택한 다음 MENU: More [Change cache settings](추가 [캐시 설정 변경])를 선택합니다.

   캐시 설정 변경 대화 상자가 나타납니다. 스토리지 배열의 모든 볼륨이 이 대화 상자에 나타납니다.

3. 기본 * 탭을 선택하여 읽기 캐싱 및 쓰기 캐싱 설정을 변경합니다.

   필드 상세정보

캐시 설정	설명
읽기 캐싱	읽기 캐시는 드라이브에서 읽은 데이터를 저장하는 버퍼입니다. 읽기 작업의 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브에 액세스할 필요가 없습니다. 데이터가 플러시될 때까지 읽기 캐시에 남아 있습니다.
쓰기 캐싱	쓰기 캐시는 드라이브에 아직 기록되지 않은 호스트의 데이터를 저장하는 버퍼입니다. 데이터는 드라이브에 기록될 때까지 쓰기 캐시에 유지됩니다. 쓰기 캐싱은 I/O 성능을 높일 수 있습니다. 볼륨에 대해 * Write caching * 을 사용하지 않도록 설정하면 캐시가 자동으로 플러시됩니다.

4. 고급 * 탭을 선택하여 일반 볼륨의 고급 설정을 변경합니다. 고급 캐시 설정은 일반 볼륨에만 사용할 수 있습니다.

필드 상세정보

캐시 설정	설명
동적 읽기 캐시 미리 가져오기	동적 캐시 읽기 프리페치를 사용하면 컨트롤러에서 드라이브에서 캐시로 데이터 블록을 읽는 동안 순차적 데이터 블록을 추가로 캐시에 복사할 수 있습니다. 이 캐싱은 향후 캐시에서 데이터 요청을 채울 수 있는 기회를 높여줍니다. 동적 캐시 읽기 프리페치는 순차적 I/O를 사용하는 멀티미디어 애플리케이션에 중요합니다 캐시로 프리페치되는 데이터의 속도와 양은 호스트 읽기의 속도 및 요청 크기에 따라 자동으로 조정됩니다. 랜덤 액세스로 인해 데이터를 캐시로 프리페치하지 않습니다. 이 기능은 읽기 캐시를 사용하지 않는 경우 적용되지 않습니다. 씬 볼륨의 경우 동적 캐시 읽기 프리페치는 항상 비활성화되어 변경할 수 없습니다.
배터리가 없는 쓰기 캐싱	배터리가 없는 쓰기 캐싱 설정을 사용하면 배터리가 없거나 고장, 완전히 방전되었거나 완전히 충전되지 않은 경우에도 쓰기 캐시가 계속 유지됩니다. 일반적으로 배터리 없이 쓰기 캐시를 선택하는 것은 권장되지 않습니다. 전원이 끊길 경우 데이터가 손실될 수 있기 때문입니다. 일반적으로 쓰기 캐시는 배터리가 충전되거나 장애가 발생한 배터리를 교체할 때까지 컨트롤러에 의해 일시적으로 꺼집니다. * 데이터 손실 가능성 * — 이 옵션을 선택하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다. 이 설정은 쓰기 캐시를 설정한 경우에만 사용할 수 있습니다. 씬 볼륨에는 이 설정을 사용할 수 없습니다.
미러링을 사용한 쓰기 캐싱	미러링으로 쓰기 캐싱은 한 컨트롤러의 캐시 메모리에 기록된 데이터가 다른 컨트롤러의 캐시 메모리에도 기록될 때 발생합니다. 따라서 한 컨트롤러에 장애가 발생하면 다른 컨트롤러가 처리되지 않은 모든 쓰기 작업을 완료할 수 있습니다. 쓰기 캐시 미러링은 쓰기 캐시가 설정되고 두 개의 컨트롤러가 있는 경우에만 사용할 수 있습니다. 볼륨 생성 시 기본 설정은 미러링을 사용한 쓰기 캐시입니다. 이 설정은 쓰기 캐시를 설정한 경우에만 사용할 수 있습니다. 씬 볼륨에는 이 설정을 사용할 수 없습니다.

5. 캐시 설정을 변경하려면 * 저장 * 을 클릭합니다.

볼륨에 대한 미디어 스캔 설정을 변경합니다

미디어 검사는 볼륨의 모든 데이터 및 중복 정보를 검사하는 백그라운드 작업입니다. 하나 이상의 볼륨에 대한 미디어 스캔 설정을 활성화 또는 비활성화하거나 스캔 기간을 변경하려면 이 옵션을 사용합니다.

시작하기 전에

다음 사항을 이해합니다.

- 미디어 스캔은 스캔 용량 및 스캔 기간에 따라 일정한 속도로 계속 실행됩니다. 백그라운드 스캔은 우선 순위가 더 높은 백그라운드 작업(예: 재구성)에 의해 일시적으로 중단될 수 있지만 동일한 일정한 속도로 재개됩니다.
- 스토리지 배열 및 해당 볼륨에 대해 미디어 검사 옵션이 활성화된 경우에만 볼륨이 스캔됩니다. 해당 볼륨에 대해서도 중복 검사가 활성화된 경우 볼륨에 중복성이 있는 경우 볼륨의 중복 정보가 데이터와 일관되는지 검사합니다. 중복성 검사를 통한 미디어 검사는 각 볼륨을 만들 때 기본적으로 활성화됩니다.
- 스캔 중에 복구할 수 없는 매체 오류가 발생하면 중복 정보를 사용하여 데이터가 복구됩니다(가능한 경우).

  예를 들어, 이중화 정보는 최적의 RAID 5 볼륨 또는 최적의 RAID 6 볼륨에서 사용할 수 있으며 하나의 드라이브에만 장애가 있습니다. 복구 불가능한 오류가 중복 정보를 사용하여 복구할 수 없는 경우 데이터 블록이 읽을 수 없는 섹터 로그에 추가됩니다. 수정 가능한 미디어 오류와 수정 불가능한 미디어 오류가 모두 이벤트 로그에 보고됩니다.

  중복 검사가 데이터와 중복 정보 간의 불일치를 발견하면 이벤트 로그에 보고됩니다.

이 작업에 대해

미디어 검사는 애플리케이션에서 자주 읽지 않는 디스크 블록의 미디어 오류를 감지하고 복구합니다. 따라서 드라이브 장애가 발생할 경우 볼륨 그룹 또는 풀에 있는 다른 드라이브의 데이터 및 이중화 정보를 사용하여 장애가 발생한 드라이브의 데이터가 재구성되므로 데이터 손실을 방지할 수 있습니다.

다음 작업을 수행할 수 있습니다.

- 전체 스토리지 어레이에 대한 백그라운드 미디어 검사를 설정하거나 해제합니다
- 전체 스토리지 배열의 스캔 기간을 변경합니다
- 하나 이상의 볼륨에 대한 미디어 스캔을 활성화 또는 비활성화합니다
- 하나 이상의 볼륨에 대한 중복 검사를 활성화 또는 비활성화합니다

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 임의의 볼륨을 선택한 다음 MENU: More [Change media scan settings](메뉴: 추가 [미디어 스캔 설정 변경])를 선택합니다.

   드라이브 미디어 검색 설정 변경 대화 상자가 나타납니다. 스토리지 배열의 모든 볼륨이 이 대화 상자에 나타납니다.

3. 미디어 스캔을 활성화하려면 * 다음 과정을 통해 미디어 스캔 * 확인란을 선택합니다.

   미디어 스캔 확인란을 비활성화하면 모든 미디어 스캔 설정이 일시 중단됩니다.

4. 미디어 검사를 실행할 일 수를 지정합니다.
5. 미디어 스캔을 수행하려는 각 볼륨에 대해 * Media Scan * (미디어 스캔 *) 확인란을 선택합니다.

   System Manager에서는 미디어 검사를 실행하도록 선택한 각 볼륨에 대해 Redundancy Check(이중화 확인) 옵션을 활성화합니다. 중복성 검사를 수행하지 않을 개별 볼륨이 있는 경우 * Redundancy Check *(중복성 검사 *) 확인란을 선택 취소합니다.

6. 저장 * 을 클릭합니다.

   System Manager는 선택에 따라 백그라운드 미디어 검사에 변경 사항을 적용합니다.

복사 서비스를 사용합니다

볼륨 복사 개요

볼륨 복사 기능을 사용하면 동일한 스토리지 배열에 소스 볼륨과 타겟 볼륨이라는 두 개의 개별 볼륨을 생성하여 볼륨의 시점 복제본을 생성할 수 있습니다.

이 기능은 소스 볼륨에서 타겟 볼륨으로 바이트 단위 복제를 수행하여 타겟 볼륨의 데이터를 소스 볼륨의 데이터와 동일하게 만듭니다.

데이터 복사로 액세스 향상

볼륨 변경에 대한 스토리지 요구 사항으로 볼륨 복사 기능을 사용하면 용량이 작은 드라이브를 사용하는 풀 또는 볼륨 그룹에서 용량이 큰 드라이브를 사용하는 풀 또는 볼륨 그룹으로 데이터를 복사할 수 있습니다. 예를 들어, 볼륨 복사 기능을 사용하여 다음을 수행할 수 있습니다.

- 데이터를 더 큰 드라이브로 이동:
- 데이터 전송 속도가 더 빠른 드라이브로 변경합니다.
- 새로운 기술을 사용하여 드라이브로 변경하여 성능을 높일 수 있습니다.
- 씬 볼륨을 일반 볼륨으로 변경합니다.

복제 소스 볼륨과 타겟 볼륨의 호스트 주소 지정 가능/논리적 블록 크기(섹터 크기)가 동일해야 합니다.

보고된 볼륨 블록 크기:

- * 기본 블록 크기 * – 볼륨의 블록 크기와 드라이브 블록 크기(512 또는 4K)가 일치합니다.
- * Emulated 512 블록 크기 * - 드라이브는 4K이지만 보고된 블록 크기는 512입니다.

씬 볼륨을 일반 볼륨으로 변경합니다

씬 볼륨을 일반 볼륨으로 변경하려면 볼륨 복사 작업을 사용하여 씬 볼륨의 복사본을 만듭니다. 볼륨 복사 작업의 대상은 항상 일반 볼륨입니다.

> System Manager에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다. 씬 볼륨을 생성하려면 CLI(Command Line Interface)를 사용합니다.

데이터 백업

볼륨 복사 기능을 사용하면 동일한 스토리지 배열의 한 볼륨에서 다른 볼륨으로 데이터를 복사하여 볼륨을 백업할 수 있습니다. 타겟 볼륨을 소스 볼륨의 백업, 시스템 테스트 또는 테이프 드라이브와 같은 다른 디바이스에 백업할 수 있습니다.

스냅샷 볼륨 데이터를 기본 볼륨으로 복원합니다

연결된 스냅샷 볼륨에서 기본 볼륨으로 데이터를 복원해야 하는 경우 볼륨 복사 기능을 사용하여 스냅샷 볼륨에서 기본 볼륨으로 데이터를 복사할 수 있습니다. 스냅샷 볼륨에 데이터의 볼륨 복사본을 생성한 다음 데이터를 기본 볼륨으로 복사할 수 있습니다.

소스 및 타겟 볼륨

다음 표에는 Copy Volume(볼륨 복사) 기능을 사용하여 소스 및 타겟 볼륨에 사용할 수 있는 볼륨 유형이 나와 있습니다.

볼륨 유형입니다	오프라인 볼륨 복사본 소스 볼륨	온라인 볼륨 복사본 소스 볼륨	온라인 및 오프라인 대상 볼륨
풀의 일반 볼륨입니다	예	예	예
볼륨 그룹의 일반 볼륨입니다	예	예	예
씬 볼륨	예 [1]	예	아니요
스냅샷 볼륨	예 [2]	아니요	아니요
Snapshot 기본 볼륨	예	예	아니요
원격 미러 운영 볼륨	예 [3]	예	아니요

[1] 타겟 볼륨의 용량이 씬 볼륨에서 보고된 용량과 같거나 커야 합니다.

[2] 온라인 복사 작업이 완료될 때까지 스냅샷 볼륨 복사본을 사용할 수 없습니다.

[3] 소스 볼륨이 기본 볼륨인 경우 타겟 볼륨의 용량은 소스 볼륨의 사용 가능한 용량과 같거나 커야 합니다.

볼륨 복사 작업의 유형입니다

offline_Copy Volume 작업 또는 _online_Copy Volume 작업을 수행할 수 있습니다. 오프라인 작업은 소스 볼륨에서 데이터를 읽고 타겟 볼륨에 복사합니다. 온라인 작업에서는 스냅샷 볼륨을 소스로 사용하고 해당 데이터를 타겟 볼륨에 복사합니다.

데이터 무결성을 보장하기 위해 타겟 볼륨에 대한 모든 입출력 작업은 볼륨 복사 작업 중 어느 유형이든 일시 중단됩니다. 이 서스펜션은 절차가 완료될 때까지 타겟 볼륨의 데이터 상태가 일관되지 않기 때문에 발생합니다.

오프라인 및 온라인 볼륨 복사 작업은 아래에 설명되어 있습니다.

오프라인 복사본 볼륨 작업입니다

오프라인 복사본 볼륨 관계는 소스 볼륨과 타겟 볼륨 사이에 있습니다. 오프라인 복제는 소스 볼륨에서 데이터를 읽고 타겟 볼륨에 복사하는 한편, 진행 중인 복제본으로 소스 볼륨에 대한 모든 업데이트를 일시 중지시킵니다. 소스 볼륨에 대한 모든 업데이트가 일시 중지되어 타겟 볼륨에 시간 정합성이 보장되지 않는 항목이 생성되는 것을 방지합니다.

오프라인 복사 작업에 대해 알아야 할 사항	
읽기 및 쓰기 요청	• 오프라인 복사본에 사용 중인 소스 볼륨은 볼륨 복사 작업의 상태가 진행 중 또는 보류 중 인 동안 읽기 전용 입출력 작업에 사용할 수 있습니다. • 오프라인 복제가 완료된 후에는 쓰기 요청이 허용됩니다. • 쓰기 방지 오류 메시지를 방지하려면 볼륨 복사 작업에 참여하고 있는 소스 볼륨에 진행 중 상태로 액세스하지 마십시오.
저널링 파일 시스템	• 소스 볼륨이 저널링 파일 시스템으로 포맷된 경우, 소스 볼륨에 대한 읽기 요청을 발급하려는 시도는 스토리지 어레이 컨트롤러에 의해 거부될 수 있으며 오류 메시지가 나타날 수 있습니다. • 저널링 파일 시스템 드라이버는 읽기 요청을 발급하기 전에 쓰기 요청을 발행합니다. 컨트롤러가 쓰기 요청을 거부하면 쓰기 요청이 거부되어 읽기 요청이 실행되지 않을 수 있습니다. 이 경우 소스 볼륨이 쓰기 보호되어 있음을 나타내는 오류 메시지가 나타날 수 있습니다. • 이 문제가 발생하지 않도록 하려면 볼륨 복사 작업의 상태가 진행 중인 동안에는 오프라인 복사본에 참여하고 있는 소스 볼륨에 액세스하지 마십시오.

온라인 볼륨 복사 작업입니다

온라인 볼륨 복사 관계는 스냅샷 볼륨과 타겟 볼륨 사이에 있습니다. 소스 볼륨이 온라인 상태이고 데이터 쓰기에 사용할 수 있는 동안 볼륨 복사 작업을 시작할 수 있습니다. 이 기능은 볼륨의 스냅샷을 생성하고 스냅샷을 복제본의 실제 소스 볼륨으로 사용하여 수행합니다.

소스 볼륨에 대해 볼륨 복사 작업을 시작하면 System Manager에서 기본 볼륨의 스냅샷 이미지와 기본 볼륨의 스냅샷 이미지와 타겟 볼륨 간의 복제 관계를 생성합니다. 스냅샷 이미지를 소스 볼륨으로 사용하면 복제가 진행되는 동안 스토리지 어레이가 소스 볼륨에 계속 쓸 수 있습니다.

온라인 복사 작업 중에 COW(Copy-On-Write) 절차로 인해 성능에 영향을 줍니다. 온라인 복사가 완료되면 기본 볼륨 성능이 복원됩니다.

온라인 복사 작업에 대해 알아야 할 사항	
어떤 종류의 볼륨을 사용할 수 있습니까?	• 시점 이미지가 생성되는 볼륨을 기본 볼륨이라고 하며 스토리지 배열의 표준 볼륨 또는 씬 볼륨이어야 합니다. • 타겟 볼륨은 볼륨 그룹의 표준 볼륨이거나 풀의 표준 볼륨일 수 있습니다. 타겟 볼륨은 씬 볼륨이거나 스냅샷 그룹의 기본 볼륨일 수 없습니다. • 온라인 볼륨 복사 기능을 사용하여 씬 볼륨의 데이터를 동일한 스토리지 시스템 내에 있는 풀의 표준 볼륨으로 복사할 수 있습니다. 그러나 Copy Volume(볼륨 복사) 기능을 사용하여 표준 볼륨에서 씬 볼륨으로 데이터를 복사할 수는 없습니다.
기본 볼륨 성능	• 복사 소스로 사용되는 스냅샷 볼륨이 활성 상태이면 COW(Copy-On-Write) 작업으로 인해 기본 볼륨 성능이 저하됩니다. 복제가 완료되면 스냅샷이 비활성화되고 기본 볼륨 성능이 복원됩니다. 스냅샷이 해제되더라도 예약된 용량 볼륨 및 복제 관계는 그대로 유지됩니다.

온라인 복사 작업에 대해 알아야 할 사항	
생성된 볼륨의 유형입니다	• 온라인 복제 작업 중에 스냅샷 볼륨 및 예약된 용량 볼륨이 생성됩니다. • 스냅샷 볼륨은 데이터가 포함된 실제 볼륨이 아니라 특정 시간에 볼륨에 포함된 데이터에 대한 참조입니다. • 생성된 각 스냅샷에 대해 예약된 용량 볼륨이 생성되어 스냅샷에 대한 데이터를 보유합니다. 예약된 용량 볼륨은 스냅샷 이미지를 관리하는 데만 사용됩니다.
예약된 용량 볼륨입니다	• 소스 볼륨의 데이터 블록이 수정되기 전에 수정할 블록의 내용이 보호되도록 예약된 용량 볼륨에 복사됩니다. • 예약된 용량 볼륨에 원래 데이터의 복사본이 이러한 데이터 블록에 저장되기 때문에 이러한 데이터 블록에 대한 추가 변경 사항은 소스 볼륨에만 기록됩니다. • 예약된 용량 볼륨에 저장된 데이터 블록만이 스냅샷 시간 이후에 변경된 데이터 블록이므로 온라인 복제 작업에서는 전체 물리적 복사본보다 디스크 공간이 적게 사용됩니다.

볼륨 복사

동일한 스토리지 배열의 한 볼륨에서 다른 볼륨으로 데이터를 복사하고 소스 볼륨의 물리적 시점 중복(클론)을 생성할 수 있습니다.

시작하기 전에

- 소스 볼륨과 타겟 볼륨에 대한 모든 입출력 작업을 중지해야 합니다.
- 소스 볼륨과 타겟 볼륨의 모든 파일 시스템은 마운트 해제해야 합니다.
- 이전에 볼륨 복사 작업에서 타겟 볼륨을 사용한 경우 해당 데이터가 더 이상 필요하지 않거나 데이터를 백업한 것입니다.

이 작업에 대해

소스 볼륨은 호스트 입출력을 수락하고 애플리케이션 데이터를 저장하는 볼륨입니다. Copy Volume(볼륨 복사)이 시작되면 소스 볼륨의 데이터가 전체 대상 볼륨에 복사됩니다.

타겟 볼륨은 소스 볼륨의 데이터 복제본을 유지하는 표준 볼륨입니다. 볼륨 복사 작업이 완료된 후 타겟 볼륨이 소스 볼륨과 동일합니다. 타겟 볼륨의 용량이 소스 볼륨과 같거나 커야 하지만 RAID 레벨이 다를 수 있습니다.

온라인 및 오프라인 복사본에 대한 자세한 정보

- 온라인 사본 *

온라인 복사본은 스토리지 어레이 내의 모든 볼륨에 대한 시점 복사본을 생성하지만, 복제가 진행 중인 볼륨에 쓸 수는 있습니다. 이 기능은 볼륨의 스냅샷을 생성하고 스냅샷을 복제본의 실제 소스 볼륨으로 사용하여 수행합니다. 시점 이미지가 생성되는 볼륨을 기본 볼륨이라고 하며 표준 볼륨이거나 스토리지 어레이의 씬 볼륨일 수 있습니다.

- 오프라인 복사 *

오프라인 복제는 소스 볼륨에서 데이터를 읽고 타겟 볼륨에 복사하는 한편, 진행 중인 복제본으로 소스 볼륨에 대한 모든 업데이트를 일시 중지시킵니다. 소스 볼륨에 대한 모든 업데이트가 일시 중지되어 타겟 볼륨에 시간 정합성이 보장되지 않는 항목이 생성되는 것을 방지합니다. 오프라인 볼륨 복사본 관계는 소스 볼륨과 타겟 볼륨 사이에 있습니다.

볼륨 복사 작업은 타겟 볼륨의 데이터를 덮어쓰고 타겟 볼륨과 연결된 모든 스냅샷 볼륨에 실패합니다(있는 경우).

단계

1. Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.
2. 볼륨 복사 작업의 소스로 사용할 볼륨을 선택한 다음 메뉴: 서비스 복사 [볼륨 복사] 를 선택합니다.

   Copy Volume - Select Target(볼륨 복사 - 대상 선택) 대화 상자가 나타납니다.

3. 데이터를 복사할 대상 볼륨을 선택합니다.

   이 대화 상자에 표시된 표에는 모든 대상 볼륨이 나열됩니다.

4. 볼륨 복사 작업의 복사 우선 순위를 설정하려면 슬라이더 막대를 사용합니다.

   복제 우선 순위는 서비스 입출력 요청과 비교하여 볼륨 복사 작업을 완료하는 데 사용되는 시스템 리소스의 양을 결정합니다.

   복사 우선 순위 속도에 대해 자세히 알아보세요

   복사 우선 순위 비율은 5가지입니다.

   - 최저
   - 낮음
   - 중간
   - 높음
   - 최고

   복사 우선 순위가 가장 낮은 속도로 설정된 경우 입출력 작업의 우선 순위가 지정되고 볼륨 복사 작업이 더 오래 걸립니다. 복사 우선 순위가 가장 높은 속도로 설정된 경우 볼륨 복사 작업의 우선 순위가 지정되지만 스토리지 배열의 입출력 작업에 영향을 줄 수 있습니다.

5. 온라인 복사본을 만들지, 아니면 오프라인 복사본을 만들지 선택합니다. 온라인 복사본을 만들려면 복사 작업 중** 소스 볼륨을 온라인으로 유지 확인란을 선택합니다.
6. 다음 중 하나를 수행합니다.
   - online_copy 작업을 수행하려면 * 다음 * 을 클릭하여 * 용량 예약 * 대화 상자로 계속 진행합니다.
   - offline_copy 작업을 수행하려면 * Finish * 를 클릭하여 오프라인 복사를 시작합니다.
7. 온라인 복사본을 만들도록 선택한 경우 온라인 복사본에 대한 데이터 및 기타 정보를 저장하는 데 필요한 예약 용량을 설정한 다음 * 마침 * 을 클릭하여 온라인 복사본을 시작합니다.

   지정된 예약 용량을 지원하는 후보만 볼륨 후보 테이블에 표시됩니다. 예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

   다음 지침에 따라 예약된 용량을 할당합니다.

   - 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%이며 일반적으로 이 용량이면 충분합니다.
   - 그러나 예약된 용량은 원래 데이터의 변경 횟수에 따라 달라집니다. 스토리지 객체가 활성 상태가 길수록 예약된 용량이 커야 합니다.

결과

System Manager는 소스 볼륨의 모든 데이터를 타겟 볼륨으로 복사합니다. 볼륨 복사 작업이 완료되면 타겟 볼륨은 호스트에 대해 자동으로 읽기 전용이 됩니다.

작업을 마친 후

Copy Volume(볼륨 복사) 작업의 진행률을 보려면 Home(홈) [View Operations in Progress(진행 중인 작업 보기)] 메뉴를 선택합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

볼륨 복사 작업에 대한 작업을 수행합니다

진행 중인 볼륨 복사 작업을 보거나, 중지하고, 우선 순위를 변경하거나, 다시 복사하거나, 볼륨 복사 작업을 지울 수 있습니다.

단계

1. Home[View Operations in Progress] 메뉴를 선택합니다.

   작업 진행 중 대화 상자가 나타납니다.

2. 수행할 볼륨 복사 작업을 찾은 다음 * Actions * 열의 링크를 클릭하여 다음 작업 중 하나를 수행합니다.

   특히 작업을 중지할 때 대화 상자에 제공된 모든 주의 텍스트를 읽습니다.

조치	설명
중지	작업의 상태가 진행 중, 보류 중 또는 실패인 경우 볼륨 복사 작업을 중지할 수 있습니다. Copy Volume(볼륨 복사)이 중지되면 매핑된 모든 호스트가 소스 볼륨에 대한 쓰기 권한을 갖습니다. 데이터가 소스 볼륨에 기록되면 타겟 볼륨의 데이터가 더 이상 소스 볼륨의 데이터와 일치하지 않습니다.

조치	설명
우선 순위를 변경합니다	작업 상태가 진행 중 인 상태에서 볼륨 복사 작업의 우선 순위를 변경하여 볼륨 복사 작업이 완료되는 속도를 선택할 수 있습니다.
다시 복사합니다	볼륨 복사 작업을 중지했다가 다시 시작하거나 볼륨 복사 작업이 실패하거나 중지되면 볼륨을 다시 복사할 수 있습니다. 볼륨 복사 작업은 처음부터 다시 시작됩니다. 재복사 작업은 타겟 볼륨의 기존 데이터를 덮어쓰며 대상 볼륨과 연결된 모든 스냅샷 볼륨에 실패합니다(있는 경우).
지우기	작업 상태가 진행 중, 보류 중 또는 실패인 경우 볼륨 복사 작업을 제거할 수 있습니다. Clear * 를 선택하기 전에 이 작업을 수행해야 합니다. 확인 대화 상자가 없습니다.

FAQ 를 참조하십시오

볼륨이란 무엇입니까?

볼륨은 애플리케이션, 데이터베이스 및 파일 시스템이 데이터를 저장하는 컨테이너입니다. 호스트가 스토리지의 스토리지를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다.

볼륨은 풀 또는 볼륨 그룹에서 사용할 수 있는 용량에서 생성됩니다. 볼륨에 정의된 용량이 있습니다. 볼륨이 두 개 이상의 드라이브로 구성될 수 있지만 볼륨은 호스트에 하나의 논리적 구성 요소로 나타납니다.

볼륨 그룹에 볼륨을 생성할 충분한 가용 용량이 있는 경우 용량 초과 할당 오류가 발생하는 이유는 무엇입니까?

선택한 볼륨 그룹에 하나 이상의 사용 가능한 용량 영역이 있을 수 있습니다. 사용 가능한 용량 영역은 볼륨 삭제 또는 볼륨 생성 중 사용 가능한 모든 용량을 사용하지 않음으로 인해 발생할 수 있는 사용 가능한 용량입니다.

하나 이상의 사용 가능한 용량 영역이 있는 볼륨 그룹에서 볼륨을 생성할 때 볼륨의 용량은 해당 볼륨 그룹에서 가장 큰 사용 가능한 용량 영역으로 제한됩니다. 예를 들어, 볼륨 그룹의 사용 가능한 용량이 총 15GiB이고 사용 가능한 최대 용량 영역이 10GiB인 경우 생성할 수 있는 최대 볼륨은 10GiB입니다.

볼륨 그룹에 사용 가능한 용량 영역이 있는 경우 볼륨 그룹 그래프에는 기존 사용 가능한 용량 영역의 수를 나타내는 링크가 포함되어 있습니다. 링크를 선택하면 각 영역의 용량을 나타내는 팝업 창이 표시됩니다.

여유 용량을 통합하면 볼륨 그룹의 최대 사용 가능 용량에서 추가 볼륨을 생성할 수 있습니다. 다음 방법 중 하나를 사용하여 선택한 볼륨 그룹에서 기존 사용 가능한 용량을 통합할 수 있습니다.

- 볼륨 그룹에 대해 사용 가능한 용량 영역이 하나 이상 감지되면 알림 영역의 홈 페이지에 "사용 가능한 용량 통합" 권장 사항이 표시됩니다. 무료 용량 통합 * 링크를 클릭하여 대화 상자를 시작합니다.
- Pools & Volume Groups [Uncommon Tasks > Consolidate volume group free capacity] 메뉴를 선택하여 대화 상자를 시작할 수도 있습니다.

최대 가용 용량 영역이 아닌 특정 가용 용량 영역을 사용하려면 CLI(Command Line Interface)를 사용합니다.

선택한 워크로드가 볼륨 생성에 어떤 영향을 미칩니까**?**

볼륨 생성 중에 워크로드 사용에 대한 정보를 묻는 메시지가 표시됩니다. 시스템에서는 이 정보를 사용하여 최적의 볼륨 구성을 생성합니다. 이 구성은 필요에 따라 편집할 수 있습니다. 선택적으로 볼륨 생성 순서에서 이 단계를 건너뛸 수 있습니다.

워크로드는 애플리케이션을 지원하는 스토리지 객체입니다. 애플리케이션별로 하나 이상의 워크로드 또는 인스턴스를 정의할 수 있습니다. 일부 애플리케이션의 경우 시스템에서 기본 볼륨 특성이 비슷한 볼륨을 포함하도록 워크로드를 구성합니다. 이러한 볼륨 특성은 워크로드가 지원하는 애플리케이션 유형에 따라 최적화됩니다. 예를 들어, Microsoft SQL Server 애플리케이션을 지원하는 워크로드를 생성한 다음 해당 워크로드에 대한 볼륨을 생성하는 경우 기본 볼륨 특성은 Microsoft SQL Server를 지원하도록 최적화되어 있습니다.

- * 응용 프로그램별 * — 응용 프로그램별 작업 부하를 사용하여 볼륨을 생성할 때 응용 프로그램 작업 부하 I/O와 응용 프로그램 인스턴스의 다른 트래픽 간의 경합을 최소화하기 위해 최적화된 볼륨 구성을 권장할 수 있습니다. I/O 유형, 세그먼트 크기, 컨트롤러 소유권, 읽기 및 쓰기 캐시와 같은 볼륨 특성은 자동으로 권장 사항이며 다음과 같은 애플리케이션 유형에 대해 생성되는 워크로드에 최적화되어 있습니다.
  - Microsoft ® SQL Server ™ 를 참조하십시오
  - Microsoft ® Exchange Server ™ 를 참조하십시오
  - 비디오 감시 애플리케이션
  - VMware ESXi ™ (가상 머신 파일 시스템과 함께 사용할 볼륨용)

    볼륨 추가/편집 대화 상자를 사용하여 권장 볼륨 구성을 검토하고 시스템 권장 볼륨 및 특성을 편집, 추가 또는 삭제할 수 있습니다.
- * 기타 * (또는 특정 볼륨 생성을 지원하지 않는 애플리케이션) — 다른 워크로드는 볼륨 구성을 사용하며, 특정 애플리케이션과 연결되지 않은 워크로드를 생성하려는 경우 또는 스토리지 어레이에서 사용하려는 애플리케이션에 대한 내장 최적화가 없는 경우 수동으로 지정해야 합니다. 볼륨 추가/편집 대화 상자를 사용하여 볼륨 구성을 수동으로 지정해야 합니다.

이러한 볼륨이 워크로드와 관련이 없는 이유는 무엇입니까**?**

CLI(Command Line Interface)를 사용하여 볼륨을 생성했거나 다른 스토리지 어레이에서 마이그레이션(가져오기/내보내기)한 경우 볼륨은 워크로드에 연결되지 않습니다.

선택한 워크로드를 삭제할 수 없는 이유는 무엇입니까**?**

이 워크로드는 CLI(Command Line Interface)를 사용하여 생성되거나 다른 스토리지 어레이에서 마이그레이션(가져오기/내보내기)된 볼륨 그룹으로 구성됩니다. 따라서 이 워크로드의 볼륨은 애플리케이션별 워크로드와 연결되지 않으므로 워크로드를 삭제할 수 없습니다.

애플리케이션별 워크로드를 사용하면 스토리지 어레이를 관리하는 데 어떤 도움이 됩니까**?**

애플리케이션별 워크로드의 볼륨 특성에 따라 스토리지 어레이의 구성 요소와 워크로드가 상호 작용하는 방식이 결정되며, 지정된 구성에서 환경의 성능을 파악하는 데 도움이 됩니다.

애플리케이션은 SQL Server 또는 Exchange와 같은 소프트웨어입니다. 각 애플리케이션을 지원할 워크로드를 하나 이상 정의합니다.

이 정보를 제공하면 스토리지를 생성하는 데 어떤 도움이 됩니까**?**

워크로드 정보는 선택한 워크로드에 대한 I/O 유형, 세그먼트 크기, 읽기/쓰기 캐시 등과 같은 볼륨 특성을 최적화하는 데 사용됩니다. 이처럼 최적화된 특성을 바탕으로 워크로드가 스토리지 어레이 구성요소와 상호 작용하는 방식이 결정됩니다.

제공하는 워크로드 정보를 기반으로 System Manager에서 적절한 볼륨을 생성하여 현재 시스템에 존재하는 사용 가능한 풀 또는 볼륨 그룹에 배치합니다. 시스템이 볼륨을 생성하고 선택한 워크로드에 대한 현재 모범 사례를 기반으로 해당 특성을 최적화합니다.

특정 워크로드에 대한 볼륨 생성을 완료하기 전에 볼륨 추가/편집 대화 상자를 사용하여 권장 볼륨 구성을 검토하고 시스템 권장 볼륨 및 특성을 편집, 추가 또는 삭제할 수 있습니다.

모범 사례 정보는 응용 프로그램별 설명서를 참조하십시오.

확장된 용량을 인식하려면 어떻게 해야 합니까**?**

볼륨의 용량을 늘릴 경우 호스트에서 즉시 볼륨 용량 증가를 인식하지 못할 수 있습니다.

대부분의 운영 체제는 볼륨 확장이 시작된 후 확장된 볼륨 용량을 인식하고 자동으로 확장합니다. 그러나 일부는 그렇지 않을 수도 있습니다. OS에서 확장된 볼륨 용량을 자동으로 인식하지 못하는 경우 디스크 재검색 또는 재부팅을 수행해야 할 수 있습니다.

볼륨 용량을 확장한 후에는 파일 시스템 크기를 수동으로 늘려야 합니다. 이 방법은 사용 중인 파일 시스템에 따라 다릅니다.

자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

내 풀 및/또는 볼륨 그룹이 모두 표시되지 않는 이유는 무엇입니까**?**

볼륨을 이동할 수 없는 풀 또는 볼륨 그룹이 목록에 표시되지 않습니다.

풀 또는 볼륨 그룹은 다음과 같은 이유로 적합하지 않습니다.

- 풀 또는 볼륨 그룹 풀의 DA(Data Assurance) 기능이 일치하지 않습니다.
- 풀 또는 볼륨 그룹이 최적화되지 않은 상태입니다.
- 풀 또는 볼륨 그룹의 용량이 너무 작습니다.

세그먼트 크기란**?**

세그먼트는 스토리지 어레이가 스트라이프의 다음 드라이브(RAID 그룹)로 이동하기 전에 드라이브에 저장되는 데이터의 양(KB)입니다. 세그먼트 크기는 풀이 아닌 볼륨 그룹에만 적용됩니다.

세그먼트 크기는 포함된 데이터 블록 수로 정의됩니다. 세그먼트 크기를 결정할 때 볼륨에 저장할 데이터 유형을 알아야 합니다. 일반적으로 애플리케이션에서 작은 랜덤 읽기/쓰기(IOPS)를 사용하는 경우, 작은 세그먼트 크기가 더 작을수록 더 우수한 성능을 얻을 수 있습니다. 또는 애플리케이션에 대규모 순차 읽기 및 쓰기(처리량)가 있는 경우 일반적으로 큰

세그먼트 크기가 더 좋습니다.

애플리케이션에서 작은 랜덤 읽기 및 쓰기를 사용하든, 대규모 순차 읽기 및 쓰기를 사용하든, 세그먼트 크기가 일반적인 데이터 블록 청크 크기보다 클 경우 스토리지 어레이가 더 뛰어난 성능을 발휘합니다. 따라서 일반적으로 드라이브에서 데이터에 더 쉽고 빠르게 액세스할 수 있으며, 이는 스토리지 어레이 성능 향상을 위해 중요합니다.

IOPS 성능이 중요한 환경

IOPS(초당 입출력 작업) 환경에서 드라이브에 읽기/쓰기가 수행되는 일반 데이터 블록 크기(""청크")보다 큰 세그먼트 크기를 사용하면 스토리지 시스템의 성능이 향상됩니다. 이렇게 하면 각 청크가 단일 드라이브에 기록됩니다.

처리량이 중요한 환경

처리량 환경에서 세그먼트 크기는 데이터의 총 드라이브 수와 일반적인 데이터 청크 크기(I/O 크기)의 짝수 부분이 되어야 합니다. 이렇게 하면 데이터가 볼륨 그룹의 드라이브에 단일 스트라이프로 분산되므로 읽기 및 쓰기 속도가 빨라집니다.

선호하는 컨트롤러 소유권은 무엇입니까**?**

선호 컨트롤러 소유권은 볼륨의 소유 또는 주 컨트롤러로 지정된 컨트롤러를 정의합니다.

컨트롤러 소유권은 매우 중요하며 신중하게 계획해야 합니다. 전체 I/O에 대해 컨트롤러를 최대한 균형 조정해야 합니다.

예를 들어, 하나의 컨트롤러가 주로 대규모 순차 데이터 블록을 읽고 다른 컨트롤러에 빈번한 읽기 및 쓰기 작업을 수행하는 작은 데이터 블록이 있으면 로드가 매우 달라집니다. 어떤 볼륨에 어떤 데이터 유형이 포함되어 있는지 이해하면 두 컨트롤러 모두에서 I/O 전송 균형을 동일하게 유지할 수 있습니다.

나중에 호스트 할당 선택 항목을 언제 사용하시겠습니까**?**

볼륨 생성 프로세스의 속도를 높이려면 새로 생성된 볼륨이 오프라인으로 초기화되도록 호스트 할당 단계를 건너뛸 수 있습니다.

새로 생성된 볼륨을 초기화해야 합니다. 시스템은 두 가지 모드(즉시 사용 가능한 형식(iaf) 백그라운드 초기화 프로세스 또는 오프라인 프로세스) 중 하나를 사용하여 이러한 모드를 초기화할 수 있습니다.

볼륨을 호스트에 매핑하면 해당 그룹의 초기화 볼륨이 백그라운드 초기화로 강제로 전환됩니다. 이 백그라운드 초기화 프로세스를 사용하면 동시 호스트 입출력이 허용되므로 시간이 오래 걸릴 수 있습니다.

볼륨 그룹의 볼륨 중 어느 것도 매핑되지 않은 경우 오프라인 초기화가 수행됩니다. 오프라인 프로세스는 백그라운드 프로세스보다 훨씬 빠릅니다.

호스트 블록 크기 요구 사항에 대해 알아야 할 내용은 무엇입니까**?**

EF300 및 EF600 시스템의 경우 512바이트 또는 4KiB 블록 크기("섹터 크기"라고도 함)를 지원하도록 볼륨을 설정할 수 있습니다. 볼륨을 생성하는 동안 올바른 값을 설정해야 합니다. 가능한 경우 시스템은 적절한 기본값을 제안합니다.

볼륨 블록 크기를 설정하기 전에 다음 제한 사항 및 지침을 읽으십시오.

- 일부 운영 체제와 가상 머신(현재 VMware 등)에는 512바이트 블록 크기가 필요하며 4KiB를 지원하지 않으므로 볼륨을 생성하기 전에 호스트 요구 사항을 알아야 합니다. 일반적으로 볼륨을 4KiB 블록 크기로 설정하여 최상의

성능을 얻을 수 있지만 호스트에서 4KiB(""4Kn") 블록을 허용하는지 확인합니다.

- 풀 또는 볼륨 그룹에 대해 선택하는 드라이브 유형에 따라 지원되는 볼륨 블록 크기가 다음과 같이 결정됩니다.
  - 512바이트 블록에 쓰는 드라이브를 사용하여 볼륨 그룹을 생성하는 경우 512바이트 블록의 볼륨만 생성할 수 있습니다.
  - 4KiB 블록에 쓰는 드라이브를 사용하여 볼륨 그룹을 생성하는 경우 512바이트 또는 4KiB 블록으로 볼륨을 생성할 수 있습니다.
- 어레이에 iSCSI 호스트 인터페이스 카드가 있는 경우 모든 볼륨은 볼륨 그룹 블록 크기와 관계없이 512바이트 블록으로 제한됩니다. 이는 특정 하드웨어 구현 때문입니다.
- 블록 크기를 설정한 후에는 변경할 수 없습니다. 블록 크기를 변경해야 하는 경우 볼륨을 삭제하고 다시 생성해야 합니다.

호스트 및 호스트 클러스터

호스트 및 호스트 클러스터 개요

스토리지 시스템과 데이터 서버 간의 접속을 정의하는 호스트 및 호스트 클러스터를 구성할 수 있습니다.

호스트 및 호스트 클러스터란 무엇입니까?

a_host_는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다. host cluster_는 동일한 볼륨을 여러 호스트에 할당하기 위해 생성할 수 있는 호스트 그룹입니다.

자세한 내용:

- "호스트 용어"
- "볼륨에 액세스합니다"
- "최대 LUN 수입니다"

호스트 및 호스트 클러스터를 구성하려면 어떻게 합니까?

호스트 접속을 정의하려면 Storage [Hosts] 메뉴로 이동하여 호스트를 수동으로 구성할 수 있습니다. 두 개 이상의 호스트가 동일한 볼륨 세트에 대한 액세스를 공유하도록 하려면 클러스터를 정의하고 해당 클러스터에 볼륨을 할당할 수 있습니다.

자세한 내용:

- "수동 호스트 생성"
- "호스트 및 호스트 클러스터에 볼륨을 할당하는 방법"
- "호스트 생성 및 볼륨 할당을 위한 워크플로우"
- "호스트를 수동으로 생성합니다"
- "호스트 클러스터를 생성합니다"
- "호스트에 볼륨을 할당합니다"

관련 정보

호스트 관련 작업에 대해 자세히 알아보기:

- "자동 로드 밸런싱을 설정합니다"
- "호스트 연결 보고를 설정합니다"
- "기본 호스트 유형을 변경합니다"

개념

호스트 용어

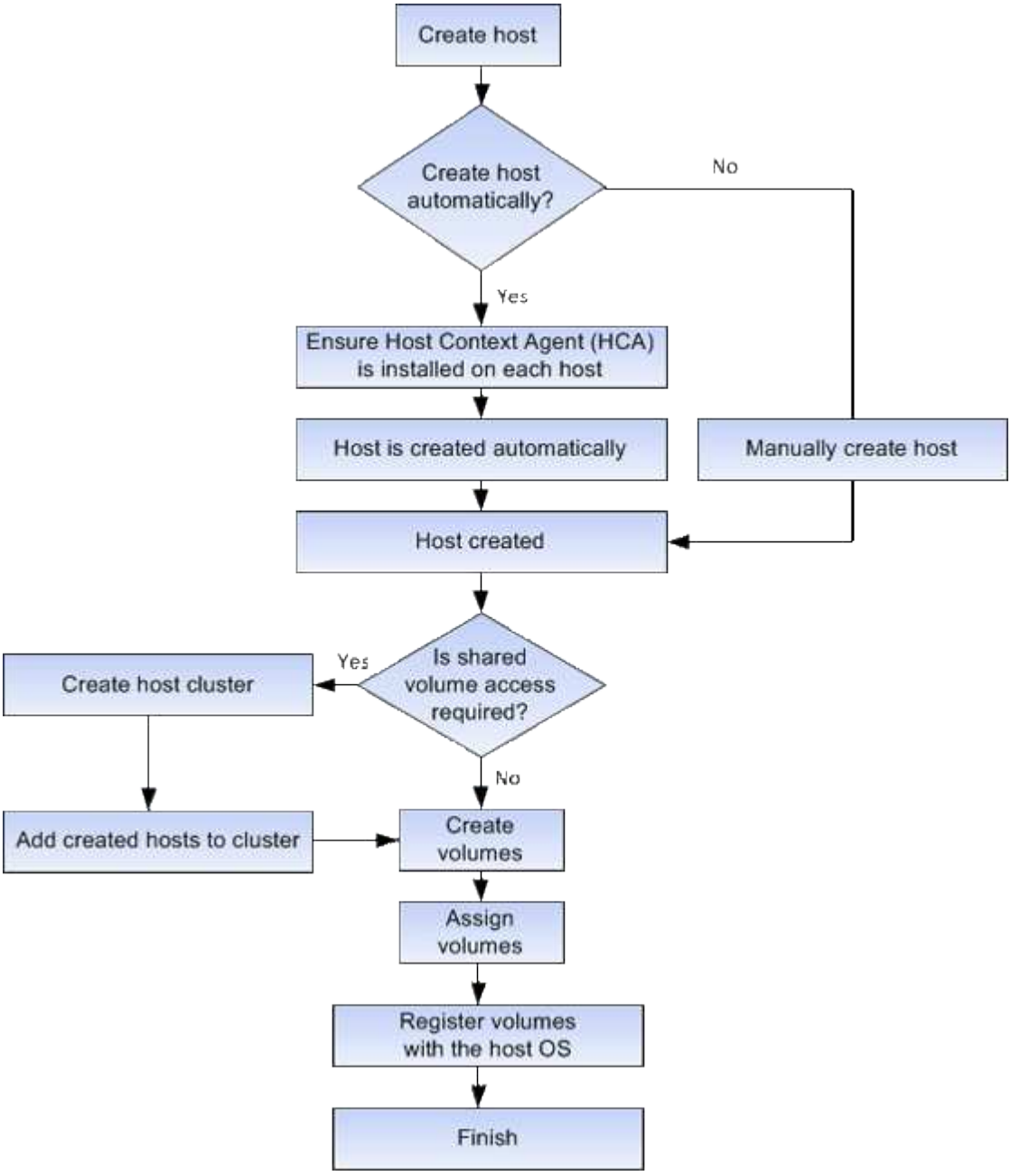
호스트 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

구성 요소	정의
호스트	호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.
호스트 이름입니다	호스트 이름은 호스트의 시스템 이름과 같아야 합니다.
호스트 클러스터	호스트 클러스터는 호스트 그룹입니다. 호스트 클러스터를 생성하여 동일한 볼륨을 여러 호스트에 쉽게 할당할 수 있습니다.
호스트 인터페이스 프로토콜입니다	호스트 인터페이스 프로토콜은 컨트롤러와 호스트 간의 연결(예: 파이버 채널, iSCSI 등)입니다.
HBA 또는 네트워크 인터페이스 카드(NIC)	HBA(호스트 버스 어댑터)는 호스트에 상주하며 하나 이상의 호스트 포트를 포함하는 보드입니다.
호스트 포트	호스트 포트는 컨트롤러에 대한 물리적 연결을 제공하고 I/O 작업에 사용되는 호스트 버스 어댑터(HBA)의 포트입니다.
호스트 포트 식별자입니다	호스트 포트 식별자는 HBA(호스트 버스 어댑터)의 각 호스트 포트와 연결된 고유한 전역 이름입니다. • iSCSI(Internet Small Computer System Interface) 호스트 포트 식별자는 1자에서 233자 사이여야 합니다. iSCSI 호스트 포트 식별자는 표준 IQN 형식(예:)으로 표시됩니다 `iqn.xxx.com.xxx:8b3ad`. • Fibre Channel 및 SAS(Serial Attached SCSI)와 같은 비 iSCSI 호스트 포트 식별자는 두 문자마다 콜론으로 구분됩니다(예: `xx:yy:zz`). Fibre Channel 호스트 포트 식별자는 16자여야 합니다.
호스트 운영 체제 유형입니다	호스트 운영 체제 유형은 스토리지 배열의 컨트롤러가 호스트의 운영 체제(또는 버전)에 따라 I/O에 반응하는 방식을 정의하는 구성 설정입니다. 이 이름은 간단한 경우 _host type_이라고도 합니다.

구성 요소	정의
컨트롤러 호스트 포트입니다	컨트롤러 호스트 포트는 호스트에 대한 물리적 연결을 제공하고 I/O 작업에 사용되는 컨트롤러의 포트입니다.
LUN입니다	LUN(Logical Unit Number)은 호스트가 볼륨을 액세스하는 데 사용하는 주소 공간에 할당된 번호입니다. 볼륨은 LUN 형태의 용량으로 호스트에 표시됩니다. 각 호스트에는 고유한 LUN 주소 공간이 있습니다. 따라서 서로 다른 호스트에서 동일한 LUN을 사용하여 서로 다른 볼륨에 액세스할 수 있습니다.

호스트 생성 및 볼륨 할당을 위한 워크플로우

다음 그림에서는 호스트 액세스를 구성하는 방법을 보여 줍니다.



수동 호스트 생성

호스트를 생성하는 것은 스토리지 어레이가 호스트에 연결된 호스트를 파악하고 볼륨에 대한 I/O 액세스를 허용하는 데 필요한 단계 중 하나입니다. 호스트는 수동으로만 생성할 수 있습니다.

수동 생성

수동 호스트 생성을 사용하면 스토리지 배열 컨트롤러에서 감지한 호스트 포트 식별자가 호스트와 올바르게 연결되도록 할 수 있습니다.

수동 호스트 생성 중에 호스트 포트 식별자를 목록에서 선택하거나 직접 입력하여 연결합니다. 호스트를 생성한 후 볼륨에 대한 액세스를 공유하려는 경우 호스트에 볼륨을 할당하거나 호스트 클러스터에 추가할 수 있습니다.

호스트 및 호스트 클러스터에 볼륨을 할당하는 방법

호스트 또는 호스트 클러스터에서 볼륨에 I/O를 보내려면 볼륨을 호스트 또는 호스트 클러스터에 할당해야 합니다.

볼륨을 생성할 때 호스트 또는 호스트 클러스터를 선택하거나 나중에 호스트 또는 호스트 클러스터에 볼륨을 할당할 수 있습니다. 호스트 클러스터는 호스트 그룹입니다. 호스트 클러스터를 생성하여 동일한 볼륨을 여러 호스트에 쉽게 할당할 수 있습니다.

호스트에 볼륨을 할당할 수 있는 유연성이 있으므로 특정 스토리지 요구 사항을 충족할 수 있습니다.

- * 호스트 클러스터의 일부가 아닌 독립 실행형 호스트 * — 개별 호스트에 볼륨을 할당할 수 있습니다. 볼륨은 한 호스트에서만 액세스할 수 있습니다.
- * 호스트 클러스터 * — 호스트 클러스터에 볼륨을 할당할 수 있습니다. 호스트 클러스터의 모든 호스트에서 볼륨에 액세스할 수 있습니다.
- * 호스트 클러스터 내의 호스트 * — 호스트 클러스터의 일부인 개별 호스트에 볼륨을 할당할 수 있습니다. 호스트가 호스트 클러스터의 일부이더라도 호스트 클러스터의 다른 호스트가 아닌 개별 호스트에서만 볼륨에 액세스할 수 있습니다.

볼륨이 생성되면 LUN(논리 유닛 번호)이 자동으로 할당됩니다. LUN은 I/O 작업 중에 호스트와 컨트롤러 사이의 "주소" 역할을 합니다. 볼륨이 생성된 후 LUN을 변경할 수 있습니다.

볼륨에 액세스합니다

액세스 볼륨은 스토리지 어레이에서 호스트 I/O 연결을 통해 스토리지 어레이 및 호스트와 통신하는 데 사용되는 공장 구성 볼륨입니다. 액세스 볼륨에는 LUN(Logical Unit Number)이 필요합니다.

액세스 볼륨은 다음과 같은 경우에 사용됩니다.

- * 대역내 관리 * — 스토리지 배열을 관리하기 위해 대역내 연결에 액세스 볼륨을 사용합니다. CLI(Command Line Interface)를 사용하여 스토리지 어레이를 관리하는 경우에만 이 작업을 수행할 수 있습니다.

  EF600 또는 EF300 스토리지 시스템에서는 대역 내 관리를 사용할 수 없습니다.

볼륨을 호스트에 처음 할당할 때 액세스 볼륨이 자동으로 생성됩니다. 예를 들어, 호스트에 Volume_1 및 Volume_2를

할당할 경우 해당 할당 결과를 볼 때 세 개의 볼륨(Volume_1, Volume_2 및 Access)이 표시됩니다.

CLI를 사용하여 호스트를 자동으로 생성하거나 스토리지 배열을 대역 내에서 관리하지 않는 경우, 액세스 볼륨이 필요하지 않으며 액세스 볼륨을 삭제하여 LUN을 확보할 수 있습니다. 이렇게 하면 볼륨 대 LUN 할당과 호스트에 대한 대역 내 관리 연결이 제거됩니다.

최대 **LUN** 수입니다

스토리지 어레이에는 각 호스트에 사용할 수 있는 최대 LUN(Logical Unit Number)이 있습니다.

최대 수는 호스트의 운영 체제에 따라 다릅니다. 스토리지 시스템은 사용된 LUN 수를 추적합니다. 최대 LUN 수를 초과하는 호스트에 볼륨을 할당하려고 하면 호스트가 볼륨을 액세스할 수 없습니다.

기본 호스트 운영 체제 유형입니다

호스트가 처음 접속될 때 스토리지 시스템에서 기본 호스트 유형을 사용합니다. 볼륨에 액세스할 때 스토리지 배열의 컨트롤러가 호스트의 운영 체제에서 작동하는 방식을 정의합니다.

접속된 호스트를 기준으로 스토리지 시스템의 작동 방식을 변경해야 하는 경우 호스트 유형을 변경할 수 있습니다. 일반적으로 호스트를 스토리지 어레이에 접속하거나 추가 호스트를 접속할 때 기본 호스트 유형을 변경합니다.

다음 지침을 염두에 두십시오.

- 스토리지 시스템에 접속하려는 모든 호스트의 운영 체제가 동일한 경우(호스트 환경 균질성) 호스트 유형을 운영 체제와 일치하도록 변경합니다.
- 스토리지 시스템에 접속하려는 운영 체제가 다른 호스트(이기종 호스트 환경)가 있는 경우 호스트 유형을 호스트 운영 체제의 대부분과 일치하도록 변경합니다.

  예를 들어 8개의 서로 다른 호스트를 스토리지 배열에 연결하고 그 중 6개의 호스트가 Windows 운영 체제를 실행 중인 경우, Windows를 기본 호스트 운영 체제 유형으로 선택해야 합니다.

- 연결된 호스트의 대부분이 서로 다른 운영 체제를 사용하는 경우 호스트 유형을 공장 출하시 기본값으로 변경합니다.

  예를 들어, 8개의 서로 다른 호스트를 스토리지 시스템에 접속하고 있고 이 중 2개의 호스트가 Windows 운영 체제를 실행 중인 경우 3개는 VMware 운영 체제를 실행하고, 또 다른 3개는 Linux 운영 체제를 실행하고 있으므로 기본 호스트 운영 체제 유형으로 공장 기본값을 선택해야 합니다.

호스트 액세스를 구성합니다

호스트를 수동으로 생성합니다

자동으로 검색할 수 없는 호스트의 경우 호스트를 수동으로 생성할 수 있습니다. 호스트를 생성하는 것은 스토리지 어레이가 호스트에 연결된 호스트를 파악하고 볼륨에 대한 I/O 액세스를 허용하는 데 필요한 단계 중 하나입니다.

이 작업에 대해

호스트를 생성할 때 다음 지침을 염두에 두십시오.

- 호스트와 연결된 호스트 식별자 포트를 정의해야 합니다.
- 호스트에 할당된 시스템 이름과 동일한 이름을 제공해야 합니다.
- 선택한 이름이 이미 사용 중인 경우에는 이 작업이 성공하지 않습니다.
- 이름의 길이는 30자를 초과할 수 없습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. MENU: Create [Host] 를 클릭합니다.

   Create Host 대화 상자가 나타납니다.

3. 필요에 따라 호스트 설정을 선택합니다.

필드 상세정보

설정	설명
이름	새 호스트의 이름을 입력합니다.
호스트 운영 체제 유형입니다	드롭다운 목록에서 새 호스트에서 실행 중인 운영 체제를 선택합니다.
호스트 인터페이스 유형입니다	(선택 사항) 스토리지 배열에서 지원되는 호스트 인터페이스 유형이 두 개 이상인 경우 사용할 호스트 인터페이스 유형을 선택합니다.
호스트 포트	다음 중 하나를 수행합니다. • * I/O 인터페이스 * 를 선택합니다 일반적으로 호스트 포트는 로그인한 상태여야 하며 드롭다운 목록에서 사용할 수 있습니다. 목록에서 호스트 포트 식별자를 선택할 수 있습니다. • * 수동 추가 * 호스트 포트 식별자가 목록에 표시되지 않으면 호스트 포트가 로그인되어 있지 않은 것입니다. 호스트 포트 식별자를 찾아 호스트에 연결하는 데 HBA 유틸리티 또는 iSCSI Initiator 유틸리티를 사용할 수 있습니다. 호스트 포트 식별자를 수동으로 입력하거나 유틸리티에서(한 번에 하나씩) * 호스트 포트 * 필드로 복사/붙여넣을 수 있습니다. 호스트와 연결하려면 한 번에 하나의 호스트 포트 식별자를 선택해야 하지만 호스트와 연결된 식별자를 계속 선택할 수 있습니다. 각 식별자는 * 호스트 포트 * 필드에 표시됩니다. 필요한 경우 옆에 있는 * X * 를 선택하여 식별자를 제거할 수도 있습니다.
CHAP 이니시에이터입니다	(선택 사항) iSCSI IQN을 사용하여 호스트 포트를 선택하거나 수동으로 입력한 경우, CHAP(Challenge Handshake Authentication Protocol)를 사용하여 인증하기 위해 스토리지 배열에 액세스를 시도하는 호스트가 필요한 경우 * CHAP initiator * 확인란을 선택합니다. 선택하거나 수동으로 입력한 각 iSCSI 호스트 포트에 대해 다음을 수행합니다. • CHAP 인증을 위해 각 iSCSI 호스트 이니시에이터에 설정된 것과 동일한 CHAP 암호를 입력합니다. 상호 CHAP 인증(호스트가 스토리지 어레이에서 자체적으로 유효성을 검사할 수 있도록 하는 양방향 인증)을 사용하는 경우, 초기 설정 시 또는 설정을 변경하여 스토리지 배열에 대한 CHAP 암호를 설정해야 합니다. • 호스트 인증이 필요하지 않은 경우 필드를 비워 둡니다. 현재 System Manager에서 사용하는 유일한 iSCSI 인증 방법은 CHAP입니다.

4. Create * 를 클릭합니다.

결과

호스트가 성공적으로 생성된 후 시스템은 호스트에 대해 구성된 각 호스트 포트(사용자 레이블)의 기본 이름을 생성합니다.

기본 별칭은 <Hostname_Port Number> 입니다. 예를 들어 에 대해 생성된 첫 번째 포트의 기본 별칭입니다. host IPT is IPT_1

호스트 클러스터를 생성합니다

두 개 이상의 호스트에서 동일한 볼륨에 대한 I/O 액세스가 필요한 경우 호스트 클러스터를 생성합니다.

이 작업에 대해

호스트 클러스터를 생성할 때는 다음 지침을 염두에 두십시오.

- 클러스터를 생성하는 데 사용할 수 있는 호스트가 두 개 이상 없으면 이 작업이 시작되지 않습니다.
- 호스트 클러스터의 호스트는 서로 다른 운영 체제(이기종)를 가질 수 있습니다.
- 호스트 클러스터의 NVMe 호스트는 비 NVMe 호스트와 혼합하여 사용할 수 없습니다.
- DA(Data Assurance) 지원 볼륨을 생성하려면 사용하려는 호스트 연결이 DA를 지원해야 합니다.

  스토리지 시스템의 컨트롤러에 있는 호스트 접속 중 하나라도 DA를 지원하지 않으면 연결된 호스트가 DA 지원 볼륨의 데이터에 액세스할 수 없습니다.

- 선택한 이름이 이미 사용 중인 경우에는 이 작업이 성공하지 않습니다.
- 이름의 길이는 30자를 초과할 수 없습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 메뉴 선택: Create [Host Cluster](호스트 클러스터 생성)를 선택합니다.

   Create Host Cluster 대화상자가 나타납니다.

3. 호스트 클러스터에 대한 설정을 적절히 선택합니다.

   필드 상세정보

설정	설명
이름	새 호스트 클러스터의 이름을 입력합니다.
볼륨 액세스를 공유할 호스트를 선택합니다	드롭다운 목록에서 두 개 이상의 호스트를 선택합니다. 호스트 클러스터에 아직 포함되지 않은 호스트만 목록에 표시됩니다.

4. Create * 를 클릭합니다.

선택한 호스트가 서로 다른 DA(Data Assurance) 기능을 가진 인터페이스 유형에 연결된 경우 호스트 클러스터에서 DA를 사용할 수 없다는 메시지가 포함된 대화 상자가 나타납니다. 이 비가용성은 DA 지원 볼륨을 호스트 클러스터에 추가하지 못하도록 합니다. 계속하려면 * 예 * 를 선택하고 취소하려면 * 아니요 * 를 선택합니다.

DA는 전체 스토리지 시스템에서 데이터 무결성을 높입니다. DA를 사용하면 호스트와 드라이브 간에 데이터가 이동할 때 발생할 수 있는 오류를 스토리지 시스템에서 확인할 수 있습니다. 새 볼륨에 DA를 사용하면 오류가 감지됩니다.

결과

새 호스트 클러스터가 아래 행에 할당된 호스트와 함께 테이블에 나타납니다.

호스트에 볼륨을 할당합니다

I/O 작업에 사용할 수 있도록 호스트 또는 호스트 클러스터에 볼륨을 할당해야 합니다. 이 할당은 스토리지 배열에 있는 하나 이상의 볼륨에 호스트 또는 호스트 클러스터 액세스 권한을 부여합니다.

이 작업에 대해

호스트에 볼륨을 할당할 때는 다음 지침을 염두에 두십시오.

- 한 번에 하나의 호스트 또는 호스트 클러스터에만 볼륨을 할당할 수 있습니다.
- 할당된 볼륨은 스토리지 배열의 컨트롤러 간에 공유됩니다.
- 동일한 LUN(Logical Unit Number)을 호스트 또는 호스트 클러스터에서 볼륨에 액세스하는 데 두 번 사용할 수 없습니다. 고유한 LUN을 사용해야 합니다.
- 새 볼륨 그룹의 경우 모든 볼륨이 생성되어 초기화될 때까지 기다린 후 호스트에 할당하면 볼륨 초기화 시간이 줄어듭니다. 볼륨 그룹에 연결된 볼륨이 매핑되면 _ALL_VOLUME가 느린 초기화로 돌아갑니다. 홈 [작업 진행 중] 메뉴에서 초기화 진행률을 확인할 수 있습니다.

다음과 같은 조건에서는 볼륨을 할당할 수 없습니다.

- 모든 볼륨이 할당됩니다.
- 볼륨이 이미 다른 호스트 또는 호스트 클러스터에 할당되어 있습니다.

다음과 같은 조건에서는 볼륨을 할당할 수 없습니다.

- 유효한 호스트 또는 호스트 클러스터가 없습니다.
- 호스트에 대해 정의된 호스트 포트 식별자가 없습니다.
- 모든 볼륨 할당이 정의되었습니다.

이 작업 중에는 할당되지 않은 모든 볼륨이 표시되지만 DA(Data Assurance)를 사용하거나 사용하지 않는 호스트의 기능은 다음과 같습니다.

- DA 지원 호스트의 경우 DA 사용 또는 DA 사용 안 함 볼륨을 선택할 수 있습니다.
- DA를 사용할 수 없는 호스트의 경우 DA를 사용할 수 있는 볼륨을 선택하면 호스트에 볼륨을 할당하기 전에 시스템에서 자동으로 볼륨의 DA를 해제해야 한다는 경고가 표시됩니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 볼륨을 할당할 호스트 또는 호스트 클러스터를 선택한 다음 * 볼륨 할당 * 을 클릭합니다.

   할당할 수 있는 모든 볼륨이 나열된 대화 상자가 나타납니다. 특정 볼륨을 쉽게 찾을 수 있도록 모든 열을 정렬하거나 * Filter * (필터 *) 상자에 원하는 항목을 입력할 수 있습니다.

3. 할당할 각 볼륨 옆의 확인란을 선택하거나 표 머리글에서 확인란을 선택하여 모든 볼륨을 선택합니다.
4. 작업을 완료하려면 * 배정 * 을 클릭하십시오.

결과

볼륨이나 볼륨을 호스트 또는 호스트 클러스터에 성공적으로 할당한 후 시스템은 다음 작업을 수행합니다.

- 할당된 볼륨은 다음으로 사용 가능한 LUN 번호를 받습니다. 호스트는 LUN 번호를 사용하여 볼륨을 액세스합니다.
- 사용자 제공 볼륨 이름이 호스트에 연결된 볼륨 목록에 나타납니다. 해당하는 경우 공장 구성 액세스 볼륨이 호스트와 연결된 볼륨 목록에도 표시됩니다.

호스트 및 클러스터 관리

기본 호스트 유형을 변경합니다

기본 호스트 운영 체제 변경 설정을 사용하여 스토리지 어레이 레벨에서 기본 호스트 유형을 변경합니다. 일반적으로 호스트를 스토리지 어레이에 접속하거나 추가 호스트를 접속할 때 기본 호스트 유형을 변경합니다.

이 작업에 대해

다음 지침을 염두에 두십시오.

- 스토리지 시스템에 접속하려는 모든 호스트의 운영 체제가 동일한 경우(호스트 환경 균질성) 호스트 유형을 운영 체제와 일치하도록 변경합니다.
- 스토리지 시스템에 접속하려는 운영 체제가 다른 호스트(이기종 호스트 환경)가 있는 경우 호스트 유형을 호스트 운영 체제의 대부분과 일치하도록 변경합니다.

  예를 들어 8개의 서로 다른 호스트를 스토리지 배열에 연결하고 그 중 6개의 호스트가 Windows 운영 체제를 실행 중인 경우, Windows를 기본 호스트 운영 체제 유형으로 선택해야 합니다.

- 연결된 호스트의 대부분이 서로 다른 운영 체제를 사용하는 경우 호스트 유형을 공장 출하시 기본값으로 변경합니다.

  예를 들어, 8개의 서로 다른 호스트를 스토리지 시스템에 접속하고 있고 이 중 2개의 호스트가 Windows 운영 체제를 실행 중인 경우 3개는 VMware 운영 체제를 실행하고, 또 다른 3개는 Linux 운영 체제를 실행하고 있으므로 기본 호스트 운영 체제 유형으로 공장 기본값을 선택해야 합니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 찾은 다음 * 기본 호스트 운영 체제 유형 변경 * 을 클릭합니다.
3. 기본값으로 사용할 호스트 운영 체제 유형을 선택합니다.

4. 변경 * 을 클릭합니다.

볼륨 할당 해제

호스트 또는 호스트 클러스터에서 해당 볼륨에 대한 I/O 액세스가 더 이상 필요하지 않은 경우 호스트 또는 호스트 클러스터에서 볼륨을 할당 해제합니다.

이 작업에 대해

볼륨을 할당 해제할 때 다음 지침을 염두에 두십시오.

- 호스트 클러스터에서 마지막으로 할당된 볼륨을 제거하고 호스트 클러스터에도 특정 볼륨이 할당된 호스트가 있는 경우 호스트 클러스터의 마지막 할당을 제거하기 전에 해당 할당을 제거하거나 이동해야 합니다.
- 운영 체제에 등록된 볼륨에 호스트 클러스터, 호스트 또는 호스트 포트가 할당된 경우 이러한 노드를 제거하기 전에 이 등록을 해제해야 합니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 편집할 호스트 또는 호스트 클러스터를 선택하고 * 볼륨 할당 해제 * 를 클릭합니다.

   현재 할당된 모든 볼륨이 표시된 대화 상자가 나타납니다.
3. 할당 취소할 각 볼륨 옆의 확인란을 선택하거나 표 머리글에서 확인란을 선택하여 모든 볼륨을 선택합니다.
4. 할당 취소 * 를 클릭합니다.

결과

- 할당되지 않은 볼륨은 새 할당에 사용할 수 있습니다.
- 호스트에서 변경 사항이 구성될 때까지 호스트 운영 체제에서 볼륨을 인식합니다.

호스트 또는 호스트 클러스터를 삭제합니다

호스트 또는 호스트 클러스터를 삭제할 수 있습니다.

이 작업에 대해

호스트 또는 호스트 클러스터를 삭제할 때는 다음 지침을 염두에 두십시오.

- 특정 볼륨 할당이 삭제되고 연결된 볼륨을 새 할당에 사용할 수 있습니다.
- 호스트가 고유한 특정 할당이 있는 호스트 클러스터의 일부인 경우 호스트 클러스터에는 영향이 없습니다. 그러나 호스트가 다른 할당이 없는 호스트 클러스터의 일부인 경우 호스트 클러스터와 기타 연결된 호스트 또는 호스트 포트 식별자는 기본 할당을 상속합니다.
- 호스트와 연결된 모든 호스트 포트 식별자는 정의되지 않습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 삭제할 호스트 또는 호스트 클러스터를 선택하고 * Delete * 를 클릭합니다.

   확인 대화 상자가 나타납니다.

3. 작업을 수행할지 확인한 다음 * 삭제 * 를 클릭합니다.

결과

호스트를 삭제한 경우 시스템은 다음 작업을 수행합니다.

- 호스트를 삭제하고 해당하는 경우 호스트 클러스터에서 제거합니다.
- 할당된 볼륨에 대한 액세스를 제거합니다.
- 연결된 볼륨을 할당되지 않은 상태로 반환합니다.
- 호스트와 연결된 모든 호스트 포트 식별자를 연결되지 않은 상태로 반환합니다.

호스트 클러스터를 삭제한 경우 시스템은 다음 작업을 수행합니다.

- 호스트 클러스터와 관련 호스트(있는 경우)를 삭제합니다.
- 할당된 볼륨에 대한 액세스를 제거합니다.
- 연결된 볼륨을 할당되지 않은 상태로 반환합니다.
- 호스트와 연결된 모든 호스트 포트 식별자를 연결되지 않은 상태로 반환합니다.

호스트 연결 보고를 설정합니다

스토리지 어레이가 컨트롤러와 구성된 호스트 간의 연결을 지속적으로 모니터링하도록 호스트 연결 보고를 설정한 다음 연결이 중단되면 경고를 표시합니다. 이 기능은 기본적으로 활성화되어 있습니다.

이 작업에 대해

호스트 접속 보고 기능을 해제하면 시스템이 더 이상 스토리지 배열에 연결된 호스트의 접속 또는 다중 경로 드라이버 문제를 모니터링하지 않습니다.

> 호스트 연결 보고를 비활성화하면 컨트롤러 리소스 활용률을 모니터링 및 밸런싱하는 자동 로드 밸런싱도 비활성화됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 호스트 연결 보고 활성화/비활성화 * 를 클릭합니다.

   이 옵션 아래의 텍스트는 현재 활성화 또는 비활성화 여부를 나타냅니다.

   확인 대화 상자가 열립니다.

3. 계속하려면 * 예 * 를 클릭하십시오.

   이 옵션을 선택하면 기능을 활성화/비활성화 상태로 전환할 수 있습니다.

설정을 관리합니다

호스트의 설정을 변경합니다

호스트의 이름, 호스트 운영 체제 유형 및 관련 호스트 클러스터를 변경할 수 있습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 편집할 호스트를 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   현재 호스트 설정을 보여주는 대화 상자가 나타납니다.

3. 아직 선택하지 않은 경우 * 속성 * 탭을 클릭합니다.
4. 필요에 따라 설정을 변경합니다.

   필드 상세정보

설정	설명
이름	사용자가 제공한 호스트 이름을 변경할 수 있습니다. 호스트 이름을 지정해야 합니다.
연결된 호스트 클러스터입니다	다음 옵션 중 하나를 선택할 수 있습니다. • * 없음 * — 호스트가 독립 실행형 호스트로 유지됩니다. 호스트가 호스트 클러스터에 연결되어 있는 경우 시스템은 클러스터에서 호스트를 제거합니다. • * <호스트 클러스터> * — 시스템이 호스트를 선택한 클러스터에 연결합니다.
호스트 운영 체제 유형입니다	정의한 호스트에서 실행 중인 운영 체제의 유형을 변경할 수 있습니다.

5. 저장 * 을 클릭합니다.

호스트 클러스터의 설정을 변경합니다

호스트 클러스터 이름을 변경하거나 호스트 클러스터에서 호스트를 추가 또는 제거할 수 있습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 편집할 호스트 클러스터를 선택하고 * 설정 보기/편집 * 을 클릭합니다.

   현재 호스트 클러스터 설정을 보여 주는 대화 상자가 나타납니다.

3. 호스트 클러스터에 대한 설정을 적절히 변경합니다.

필드 상세정보

설정	설명
이름	호스트 클러스터의 사용자 제공 이름을 지정할 수 있습니다. 클러스터 이름을 지정해야 합니다.
연결된 호스트	호스트를 추가하려면 * Associated Hosts * 상자를 클릭한 다음 드롭다운 목록에서 호스트 이름을 선택합니다. 호스트 이름을 수동으로 입력할 수 없습니다. 호스트를 삭제하려면 호스트 이름 옆의 * X * 를 클릭합니다.

4. 저장 * 을 클릭합니다.

호스트의 호스트 포트 식별자를 변경합니다

호스트 포트 식별자의 사용자 레이블을 변경하거나, 호스트에 새 호스트 포트 식별자를 추가하거나, 호스트에서 호스트 포트 식별자를 삭제하려면 호스트 포트 식별자를 변경합니다.

이 작업에 대해

호스트 포트 식별자를 변경할 때 다음 지침을 염두에 두십시오.

- * 추가 * — 호스트 포트를 추가하면 스토리지 배열에 연결하기 위해 생성한 호스트에 호스트 포트 식별자를 연결합니다. HBA(호스트 버스 어댑터) 유틸리티를 사용하여 포트 정보를 수동으로 입력할 수 있습니다.
- * 편집 * — 호스트 포트를 편집하여 호스트 포트를 다른 호스트로 이동(연결)할 수 있습니다. 호스트 버스 어댑터 또는 iSCSI 이니시에이터를 다른 호스트로 이동했을 수 있으므로 호스트 포트를 새 호스트로 이동(연결)해야 합니다.
- * 삭제 * — 호스트 포트를 삭제하여 호스트에서 호스트 포트를 제거(연결 해제)할 수 있습니다.

단계

1. 스토리지 [호스트] 메뉴를 선택합니다.
2. 포트를 연결할 호스트를 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   호스트 클러스터의 호스트에 포트를 추가하려면 호스트 클러스터를 확장하고 원하는 호스트를 선택합니다. 호스트 클러스터 수준에서는 포트를 추가할 수 없습니다.

   현재 호스트 설정을 보여주는 대화 상자가 나타납니다.

3. 호스트 포트 * 탭을 클릭합니다.

   대화 상자에 현재 호스트 포트 식별자가 표시됩니다.

4. 호스트 포트 식별자 설정을 적절하게 변경합니다.

설정	설명
호스트 포트	다음 옵션 중 하나를 선택할 수 있습니다. • * Add * — Add를 사용하여 새 호스트 포트 식별자를 호스트에 연결합니다. 호스트 포트 식별자 이름의 길이는 호스트 인터페이스 기술에 의해 결정됩니다. 파이버 채널 및 Infiniband 호스트 포트 식별자 이름은 16자여야 합니다. iSCSI 호스트 포트 식별자 이름은 최대 223자까지 지정할 수 있습니다. 포트는 고유해야 합니다. 이미 구성된 포트 번호는 허용되지 않습니다. • * 삭제 * — 호스트 포트 식별자를 제거(연결 해제)하려면 삭제를 사용합니다. 삭제 옵션은 호스트 포트를 물리적으로 제거하지 않습니다. 이 옵션은 호스트 포트와 호스트 간의 연결을 제거합니다. 호스트 버스 어댑터 또는 iSCSI 이니시에이터를 제거하지 않는 한, 호스트 포트는 컨트롤러에서 계속 인식됩니다. ⓘ 호스트 포트 식별자를 삭제하면 이 호스트와 더 이상 연결되지 않습니다. 또한 호스트는 이 호스트 포트 식별자를 통해 할당된 볼륨에 대한 액세스 권한을 상실합니다.
라벨	포트 레이블 이름을 변경하려면 * 편집 * 아이콘(연필)을 클릭합니다. 포트 레이블 이름은 고유해야 합니다. 이미 구성된 레이블 이름은 허용되지 않습니다.
CHAP 암호	iSCSI 호스트에만 표시됩니다. 이니시에이터(iSCSI 호스트)의 CHAP 암호를 설정하거나 변경할 수 있습니다. System Manager에서는 CHAP(Challenge Handshake Authentication Protocol) 방법을 사용하여 초기 링크 중에 대상 및 초기자의 ID를 확인합니다. 인증은 CHAP 암호라는 공유 보안 키를 기반으로 합니다.

5. 저장 * 을 클릭합니다.

FAQ 를 참조하십시오

호스트 및 호스트 클러스터란 무엇입니까?

호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다. 호스트 클러스터는 호스트 그룹입니다. 호스트 클러스터를 생성하여 동일한 볼륨을 여러 호스트에 쉽게 할당할 수 있습니다.

호스트를 별도로 정의합니다. 독립적인 엔티티이거나 호스트 클러스터에 추가할 수 있습니다. 개별 호스트에 볼륨을 할당하거나 호스트 클러스터의 다른 호스트와 하나 이상의 볼륨에 대한 액세스를 공유하는 호스트 클러스터의 일부가 될 수 있습니다.

호스트 클러스터는 SANtricity System Manager에서 생성한 논리적 엔터티입니다. 볼륨을 할당하려면 먼저 호스트를 호스트 클러스터에 추가해야 합니다.

호스트 클러스터를 생성해야 하는 이유는 무엇입니까?

동일한 볼륨 세트에 대한 액세스를 공유하는 호스트가 2개 이상인 경우 호스트 클러스터를 생성해야 합니다. 일반적으로 개별 호스트에는 볼륨 액세스를 조정하기 위해 클러스터링

소프트웨어가 설치되어 있습니다.

어떤 호스트 운영 체제 유형이 올바른지 어떻게 알 수 있습니까?

호스트 운영 체제 유형 필드에는 호스트의 운영 체제가 들어 있습니다. 드롭다운 목록에서 권장 호스트 유형을 선택할 수 있습니다.

드롭다운 목록에 표시되는 호스트 유형은 스토리지 어레이 모델 및 펌웨어 버전에 따라 다릅니다. 가장 최신 버전은 가장 일반적인 옵션을 먼저 표시하며, 이 옵션이 가장 적절할 가능성이 높습니다. 이 목록의 모양은 옵션이 완전히 지원됨을 의미하지는 않습니다.

호스트 지원에 대한 자세한 내용은 를 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

다음 호스트 유형 중 일부가 목록에 나타날 수 있습니다.

호스트 운영 체제 유형입니다	운영 체제**(OS)** 및 다중 경로 드라이버
Linux DM-MP(커널 3.10 이상)	3.10 이상의 커널과 함께 장치 매퍼 다중 경로 페일오버 솔루션을 사용하여 Linux 운영 체제를 지원합니다.
VMware ESXi	VMware 기본 제공 스토리지 어레이 유형 정책 모듈 SATP_ALUA를 사용하여 NMP(Native Multipathing Plug-in) 아키텍처를 실행하는 VMware ESXi 운영 체제를 지원합니다.
Windows(클러스터형 또는 비클러스터형)	ATTO 다중 경로 드라이버를 실행하지 않는 Windows 클러스터 또는 클러스터링되지 않은 구성을 지원합니다.
ATTO 클러스터(모든 운영 체제)	ATTO Technology, Inc., 다중 경로 드라이버를 사용하는 모든 클러스터 구성을 지원합니다.
Linux(Veritas DMP)	Veritas DMP 다중 경로 솔루션을 사용하여 Linux 운영 체제를 지원합니다.
Linux(ATTO)	ATTO Technology, Inc., 다중 경로 드라이버를 사용하는 Linux 운영 체제를 지원합니다.
Mac OS(ATTO)	ATTO Technology, Inc., 다중 경로 드라이버를 사용하는 Mac OS 버전을 지원합니다.
Windows(ATTO)	ATTO Technology, Inc., 다중 경로 드라이버를 사용하는 Windows 운영 체제를 지원합니다.
FlexArray(ALUA)	다중 경로에 대해 ALUA를 사용하여 NetApp FlexArray 시스템을 지원합니다.
IBM SVC	IBM SAN Volume Controller 구성을 지원합니다.

호스트 운영 체제 유형입니다	운영 체제**(OS)** 및 다중 경로 드라이버
공장 출하 시 기본값	스토리지 배열의 초기 시작용으로 예약되어 있습니다. 호스트 운영 체제 유형이 출하 시 기본값으로 설정되어 있는 경우 연결된 호스트에서 실행 중인 호스트 운영 체제 및 다중 경로 드라이버에 맞게 변경합니다.
Linux DM-MP(커널 3.9 이상)	3.9 이하의 커널과 함께 장치 매퍼 다중 경로 장애 조치 솔루션을 사용하여 Linux 운영 체제를 지원합니다.
Window Clustered(더 이상 사용되지 않음)	호스트 운영 체제 유형이 이 값으로 설정되어 있으면 Windows(클러스터형 또는 비클러스터형) 설정을 대신 사용합니다.

HBA와 어댑터 포트란 무엇입니까**?**

HBA(호스트 버스 어댑터)는 호스트에 상주하며 하나 이상의 호스트 포트를 포함하는 보드입니다. 호스트 포트는 컨트롤러에 대한 물리적 연결을 제공하고 I/O 작업에 사용되는 호스트 버스 어댑터(HBA)의 포트입니다.

HBA의 어댑터 포트를 호스트 포트라고 합니다. 대부분의 HBA에는 하나 또는 두 개의 호스트 포트가 있습니다. HBA에는 고유한 WWID(World Wide Identifier)가 있으며 각 HBA 호스트 포트에는 고유한 WWID가 있습니다. 호스트 포트 식별자는 SANtricity System Manager를 통해 호스트를 수동으로 생성할 때 적절한 HBA를 물리적 호스트와 연결하는 데 사용됩니다.

호스트 포트를 호스트에 일치시키려면 어떻게 해야 합니까**?**

호스트를 수동으로 생성하는 경우 먼저 호스트에서 사용할 수 있는 적절한 HBA(호스트 버스 어댑터) 유틸리티를 사용하여 호스트에 설치된 각 HBA와 연결된 호스트 포트 식별자를 확인해야 합니다.

이 정보가 있는 경우 Create Host 대화 상자에 제공된 목록에서 스토리지 배열에 로그인한 호스트 포트 식별자를 선택합니다.

생성 중인 호스트에 대해 적절한 호스트 포트 식별자를 선택해야 합니다. 잘못된 호스트 포트 식별자를 연결하면 다른 호스트에서 이 데이터에 의도하지 않은 액세스가 발생할 수 있습니다.

CHAP 암호를 생성하려면 어떻게 해야 합니까**?**

스토리지 배열에 연결된 iSCSI 호스트에서 CHAP(Challenge Handshake Authentication Protocol) 인증을 설정하는 경우 각 iSCSI 호스트에 대해 해당 초기자 CHAP 암호를 다시 입력해야 합니다.

이렇게 하려면 호스트 생성 작업의 일부로 또는 설정 보기/편집 옵션을 통해 System Manager를 사용할 수 있습니다.

CHAP 상호 인증을 사용하는 경우 설정 페이지에서 스토리지 배열에 대한 대상 CHAP 암호도 정의하고 각 iSCSI 호스트에서 해당 대상 CHAP 암호를 다시 입력해야 합니다.

기본 클러스터는 무엇입니까?

기본 클러스터는 기본 클러스터에 할당된 볼륨에 대한 액세스 권한을 얻기 위해 스토리지 배열에 로그인한 연결되지 않은 호스트 포트 식별자를 허용하는 시스템 정의 엔티티입니다. 연결되지 않은 호스트 포트 식별자는 특정 호스트와 논리적으로 연결되지 않지만 호스트에 물리적으로 설치되어 스토리지 배열에 로그인하는 호스트 포트입니다.

> 호스트가 스토리지 배열의 특정 볼륨에 특정 액세스를 가지도록 하려면 기본 클러스터를 _사용하지 _않아야 합니다. 대신 호스트 포트 식별자를 해당 호스트에 연결해야 합니다. 이 작업은 Create Host(호스트 생성) 작업 중에 수동으로 수행할 수 있습니다. 그런 다음 개별 호스트 또는 호스트 클러스터에 볼륨을 할당합니다.

외부 스토리지 환경이 모든 호스트 및 스토리지 배열에 연결된 모든 로그인 호스트 포트 식별자를 모든 볼륨에 액세스할 수 있도록 허용하는 특수한 상황에서는 _ 전용 _ 기본 클러스터를 사용해야 합니다(모든 액세스 모드). 호스트를 스토리지 시스템 또는 사용자 인터페이스에 특별히 알려주지 않습니다.

처음에는 CLI(Command Line Interface)를 통해 기본 클러스터에만 볼륨을 할당할 수 있습니다. 그러나 기본 클러스터에 볼륨을 한 개 이상 할당한 후에는 이 개체(기본 클러스터라고 함)가 사용자 인터페이스에 표시되며, 여기에서 이 엔터티를 관리할 수 있습니다.

호스트 연결 보고란 무엇입니까?

호스트 연결 보고가 설정되면 스토리지 어레이는 컨트롤러와 구성된 호스트 간의 연결을 지속적으로 모니터링한 다음 연결이 중단되면 경고를 표시합니다.

느슨하거나 손상되거나 누락된 케이블이 있거나 호스트에 다른 문제가 있는 경우 연결이 중단될 수 있습니다. 이러한 경우, 시스템이 Recovery Guru 메시지를 열 수 있습니다.

- * 호스트 중복성 손실* — 두 컨트롤러가 호스트와 통신할 수 없는 경우 열립니다.
- * 잘못된 호스트 유형 * — 호스트 유형이 스토리지 배열에 잘못 지정되어 장애 조치 문제가 발생할 경우 열립니다.

컨트롤러를 재부팅하면 연결 시간 초과보다 오래 걸릴 수 있는 상황에서 호스트 연결 보고를 사용하지 않도록 설정할 수 있습니다. 이 기능을 사용하지 않도록 설정하면 복구 Gurus 메시지가 표시되지 않습니다.

> 호스트 연결 보고를 비활성화하면 컨트롤러 리소스 사용을 모니터링 및 밸런싱하는 자동 로드 밸런싱도 비활성화됩니다. 그러나 호스트 연결 보고를 다시 활성화하면 자동 로드 밸런싱 기능이 자동으로 다시 활성화되지 않습니다.

스냅샷 수

스냅샷 개요

스냅샷 기능을 사용하면 백업 또는 테스트에 사용할 스토리지 어레이 볼륨의 시점 이미지를 생성할 수 있습니다.

스냅샷 이미지란 무엇입니까?

스냅샷 image_는 특정 시점에 캡처된 볼륨 데이터의 논리적 복사본입니다. 복원 지점과 마찬가지로 스냅샷 이미지를

통해 알려진 양호한 데이터 집합으로 롤백할 수 있습니다. 호스트가 스냅샷 이미지를 액세스할 수는 있지만 해당 이미지를 직접 읽거나 쓸 수는 없습니다.

자세한 내용:

- "스냅샷 스토리지의 작동 방식"
- "스냅샷 용어"
- "기본 볼륨, 예약 용량 및 스냅샷 그룹"
- "Snapshot 일정 및 정합성 보장 그룹"
- "Snapshot 볼륨"

스냅샷을 생성하려면 어떻게 해야 합니까**?**

기본 볼륨 또는 스냅샷 정합성 보장 그룹에서 스냅샷 이미지를 수동으로 생성할 수 있습니다. 이 절차는 스토리지 [스냅샷] 메뉴에서 사용할 수 있습니다.

자세한 내용:

- "스냅샷 요구 사항 및 지침"
- "스냅샷 이미지 및 볼륨 생성을 위한 워크플로우"
- "스냅샷 이미지를 생성합니다"
- "스냅샷 이미지를 예약합니다"
- "스냅샷 정합성 보장 그룹을 생성합니다"
- "스냅샷 볼륨을 생성합니다"

스냅샷에서 데이터를 롤백하려면 어떻게 해야 합니까**?**

롤백_은 기본 볼륨의 데이터를 이전 시점으로 되돌리는 프로세스입니다. 스토리지 [스냅샷] 메뉴에서 스냅샷 데이터를 롤백할 수 있습니다.

자세한 내용:

- "스냅샷 롤백"
- "기본 볼륨에 대한 스냅샷 이미지 롤백을 시작합니다"
- "정합성 보장 그룹 구성원에 대한 스냅샷 이미지 롤백을 시작합니다"

관련 정보

스냅샷과 관련된 작업에 대해 자세히 알아보기:

- "스냅샷 볼륨에 대한 예약 용량을 변경합니다"
- "스냅샷 그룹의 예약된 용량을 변경합니다"

개념

스냅샷 스토리지의 작동 방식

스냅샷 기능은 COW(Copy-on-Write) 기술을 사용하여 스냅샷 이미지를 저장하고 할당된 예약 용량을 사용합니다.

스냅샷 이미지 사용 방법

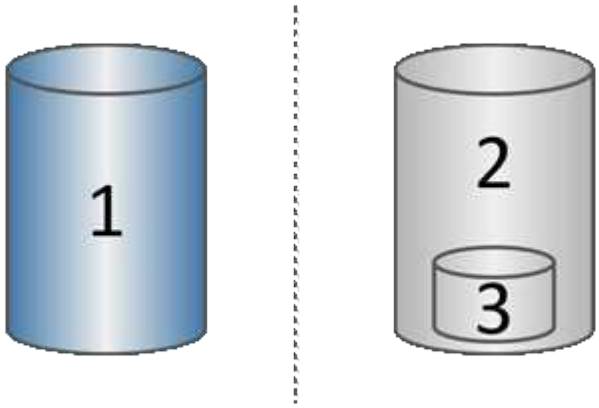
스냅샷 이미지는 특정 시점에 캡처된 볼륨 내용의 논리적 읽기 전용 복사본입니다. 스냅샷을 사용하여 데이터 손실을 방지할 수 있습니다.

스냅샷 이미지는 테스트 환경에도 유용합니다. 데이터의 가상 복제본을 생성하여 실제 볼륨 자체를 변경하지 않고 스냅샷을 사용하여 데이터를 테스트할 수 있습니다. 또한 호스트는 스냅샷 이미지에 대한 쓰기 액세스 권한이 없으므로 스냅샷은 항상 안전한 백업 리소스입니다.

스냅샷 생성

스냅샷이 생성될 때 스냅샷 기능은 다음과 같이 이미지 데이터를 저장합니다.

- 스냅샷 이미지가 생성되면 기본 볼륨과 정확히 일치합니다. 스냅샷 기능은 쓰기 시 복사 기술을 사용합니다. 스냅샷을 생성한 후 기본 볼륨의 블록 또는 블록 세트에 처음으로 데이터를 쓰게 되면 새 데이터를 기본 볼륨에 쓰기 전에 원래 데이터가 예약된 용량으로 복제됩니다.
- 후속 스냅샷에는 변경된 데이터 블록만 포함됩니다. 기본 볼륨에서 데이터를 덮어쓰기 전에 스냅샷 기능은 copy-on-write 기술을 사용하여 영향을 받는 섹터의 필요한 이미지를 스냅샷 예약 용량에 저장합니다.



[1]기본 볼륨(물리 디스크 용량);[2]스냅샷(논리적 디스크 용량);[3]예약된 용량(물리 디스크 용량)

- 예약된 용량에는 스냅샷을 생성한 후 변경된 기본 볼륨의 일부에 대한 원본 데이터 블록이 저장되며 변경 내용 추적을 위한 인덱스가 포함됩니다. 일반적으로 예약된 용량의 크기는 기본 볼륨의 40%로 기본 설정됩니다. (예약된 용량이 더 필요한 경우 예약된 용량을 늘릴 수 있습니다.)
- 스냅샷 이미지는 타임 스탬프를 기준으로 특정 순서로 저장됩니다. 기본 볼륨의 가장 오래된 스냅샷 이미지만 수동으로 삭제할 수 있습니다.

스냅샷 복원

데이터를 기본 볼륨으로 복원하려면 스냅샷 볼륨 또는 스냅샷 이미지를 사용할 수 있습니다.

- * 스냅샷 볼륨 * — 삭제된 파일을 검색해야 하는 경우, 알려진 양호한 스냅샷 이미지에서 스냅샷 볼륨을 생성한 다음 호스트에 할당합니다.
- * 스냅샷 이미지 * — 기본 볼륨을 특정 시점으로 복원해야 하는 경우 이전 스냅샷 이미지를 사용하여 데이터를 기본 볼륨으로 롤백합니다.

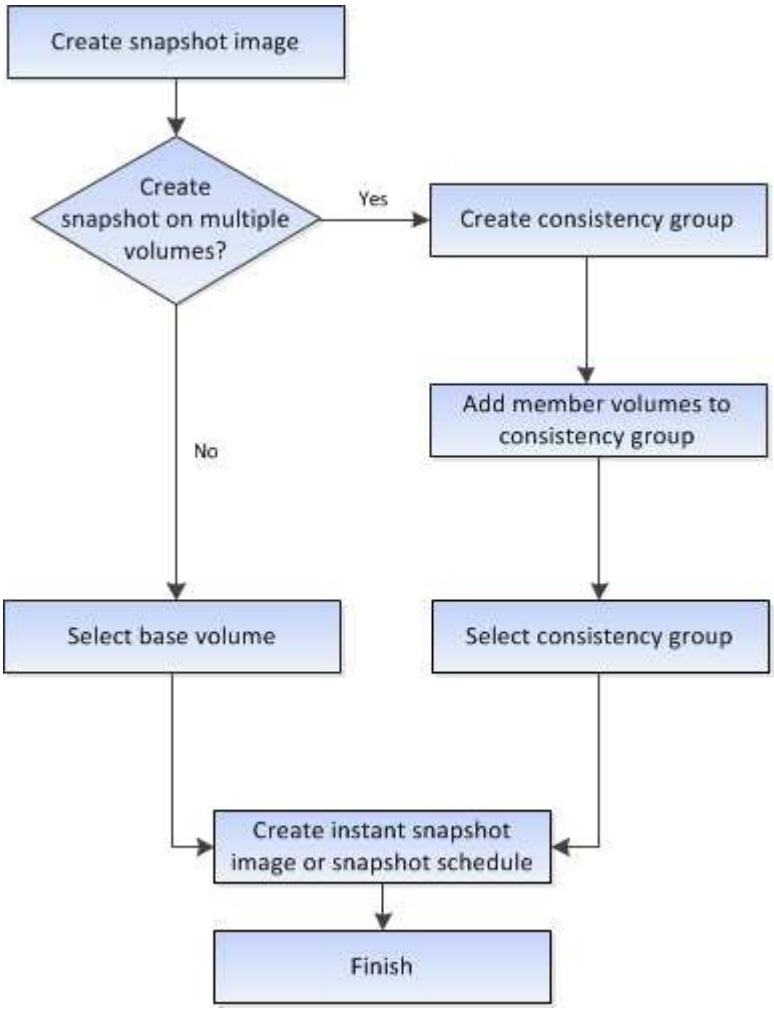
스냅샷 용어

스냅샷 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

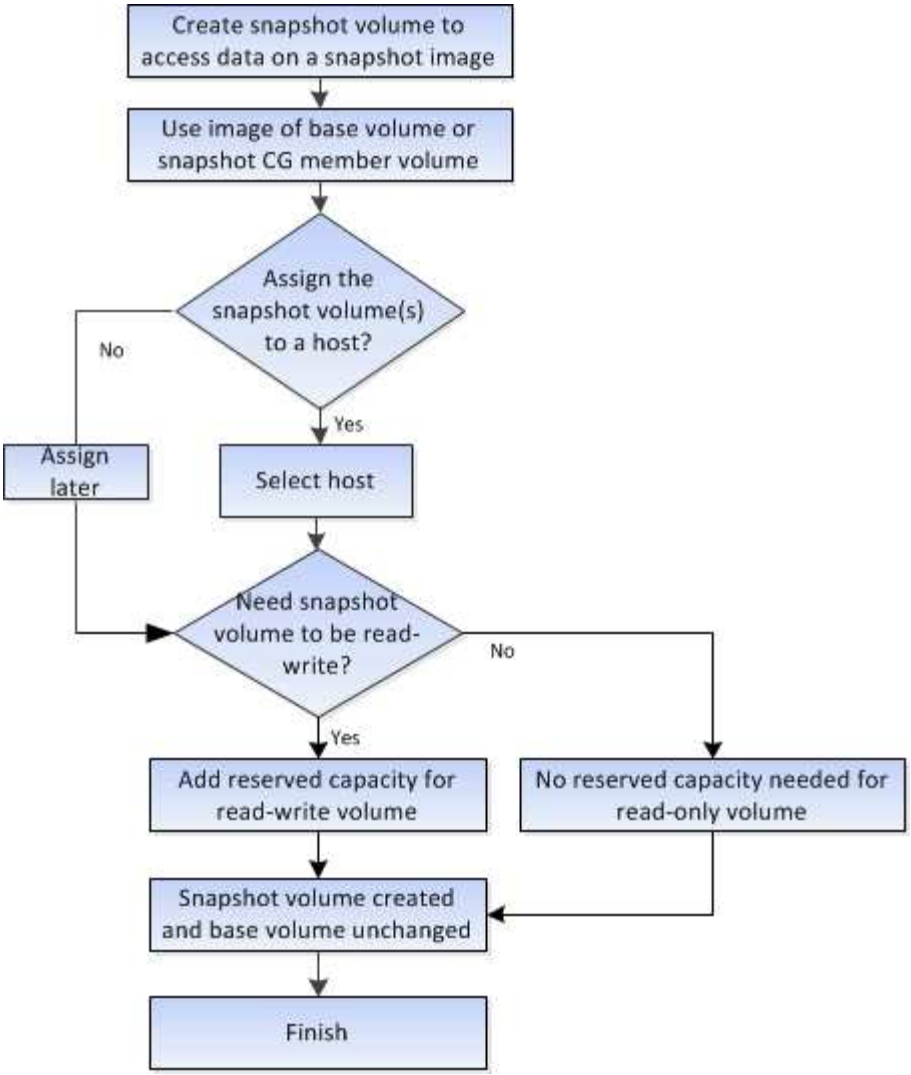
기간	설명
스냅샷 기능	스냅샷 기능은 볼륨의 이미지를 생성하고 관리하는 데 사용됩니다.
스냅샷 이미지	스냅샷 이미지는 특정 시점에 캡처된 볼륨 데이터의 논리적 복사본입니다. 복원 지점과 마찬가지로 스냅샷 이미지를 통해 알려진 양호한 데이터 집합으로 롤백할 수 있습니다. 호스트가 스냅샷 이미지를 액세스할 수는 있지만 해당 이미지를 직접 읽거나 쓸 수는 없습니다.
기본 볼륨	기본 볼륨은 스냅샷 이미지가 생성되는 원본입니다. 일반 볼륨이거나 씬 볼륨일 수 있으며 일반적으로 호스트에 할당됩니다. 기본 볼륨은 볼륨 그룹 또는 디스크 풀에 상주할 수 있습니다.
스냅샷 볼륨	스냅샷 볼륨을 사용하면 호스트가 스냅샷 이미지의 데이터에 액세스할 수 있습니다. 스냅샷 볼륨에는 원래 스냅샷 이미지에 영향을 주지 않고 기본 볼륨에 대한 수정 사항을 저장하는 자체 예약 용량이 포함되어 있습니다.
스냅샷 그룹	스냅샷 그룹은 단일 기본 볼륨의 스냅샷 이미지 모음입니다.
예약된 용량 볼륨입니다	예약된 용량 볼륨은 기본 볼륨의 데이터 블록 및 해당 블록의 보존된 콘텐츠를 추적합니다.
스냅샷 스케줄입니다	스냅샷 스케줄은 자동화된 스냅샷 이미지를 생성하는 시간표입니다. 일정을 통해 이미지 생성 빈도를 제어할 수 있습니다.
스냅샷 정합성 보장 그룹	스냅샷 정합성 보장 그룹은 스냅샷 이미지를 생성할 때 단일 개체로 처리되는 볼륨의 모음입니다. 이러한 각 볼륨에는 고유한 스냅샷 이미지가 있지만 모든 이미지는 동시에 생성됩니다.
스냅샷 정합성 보장 그룹 구성원 볼륨입니다	스냅샷 정합성 보장 그룹에 속한 각 볼륨을 구성원 볼륨이라고 합니다. 스냅샷 정합성 보장 그룹에 볼륨을 추가하면 System Manager에서 이 구성원 볼륨에 해당하는 새 스냅샷 그룹을 자동으로 생성합니다.
롤백	롤백은 기본 볼륨의 데이터를 이전 시점으로 되돌리는 프로세스입니다.
예약된 용량입니다	예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

SANtricity 시스템 관리자에서 다음 단계를 수행하여 스냅샷 이미지 및 스냅샷 볼륨을 생성할 수 있습니다.

스냅샷 이미지 생성 워크플로



스냅샷 볼륨 생성 워크플로우입니다



스냅샷 요구 사항 및 지침

스냅샷을 생성 및 사용할 때는 다음 요구 사항 및 지침을 검토하십시오.

스냅샷 이미지 및 스냅샷 그룹

- 각 스냅샷 이미지는 정확히 하나의 스냅샷 그룹에 연결됩니다.
- 연결된 객체에 대해 예약된 스냅샷 또는 인스턴트 스냅샷 이미지를 처음 생성할 때 스냅샷 그룹이 생성됩니다. 이렇게 하면 예약된 용량이 생성됩니다.

  풀 및 볼륨 그룹 페이지에서 스냅샷 그룹을 볼 수 있습니다.

- 스토리지 배열이 오프라인이거나 전원이 꺼진 경우에는 예약된 스냅샷 이미지가 발생하지 않습니다.
- 스냅샷 스케줄이 있는 스냅샷 그룹을 삭제하면 스냅샷 스케줄도 삭제됩니다.
- 더 이상 필요하지 않은 스냅샷 볼륨이 있는 경우 이를 삭제하는 대신 연결된 예약된 용량과 함께 다시 사용할 수 있습니다. 이렇게 하면 동일한 기본 볼륨의 다른 스냅샷 볼륨이 생성됩니다. 스냅샷 이미지가 동일한 기본 볼륨에 있는 경우 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 동일한 스냅샷 이미지 또는 다른 스냅샷 이미지와 다시 연결할 수 있습니다.

스냅샷 정합성 보장 그룹

- 스냅샷 정합성 보장 그룹은 스냅샷 정합성 보장 그룹의 구성원인 각 볼륨에 대해 하나의 스냅샷 그룹을 포함합니다.
- 스냅샷 정합성 보장 그룹을 하나의 스케줄에만 연결할 수 있습니다.
- 스냅샷 스케줄이 있는 스냅샷 정합성 보장 그룹을 삭제하면 스냅샷 스케줄도 삭제됩니다.
- 스냅샷 정합성 보장 그룹에 연결된 스냅샷 그룹은 개별적으로 관리할 수 없습니다. 대신 스냅샷 정합성 보장 그룹 레벨에서 관리 작업(스냅샷 이미지 생성, 스냅샷 이미지 또는 스냅샷 그룹 삭제, 스냅샷 이미지 롤백)을 수행해야 합니다.

기본 볼륨

- 스냅샷 볼륨은 연결된 기본 볼륨과 동일한 DA(Data Assurance) 및 보안 설정을 가져야 합니다.
- 장애가 발생한 기본 볼륨의 스냅샷 볼륨은 생성할 수 없습니다.
- 기본 볼륨이 볼륨 그룹에 있는 경우 연결된 스냅샷 정합성 보장 그룹의 구성원 볼륨은 풀 또는 볼륨 그룹에 상주할 수 있습니다.
- 기본 볼륨이 풀에 있는 경우 연결된 스냅샷 정합성 보장 그룹의 모든 구성원 볼륨은 기본 볼륨과 동일한 풀에 상주해야 합니다.

예약된 용량입니다

- 예약 용량은 하나의 기본 볼륨에만 연결됩니다.
- 스케줄을 사용하면 많은 수의 스냅샷 이미지가 생성될 수 있습니다. 예약된 스냅샷에 대한 예약된 용량이 충분한지 확인합니다.
- 스냅샷 정합성 보장 그룹에 대해 예약된 용량 볼륨은 스냅샷 정합성 보장 그룹 구성원 볼륨에 대해 연결된 기본 볼륨과 동일한 DA(Data Assurance) 및 보안 설정을 가져야 합니다.

보류 중인 스냅샷 이미지

스냅샷 이미지 생성은 다음과 같은 조건에서 보류 상태로 유지될 수 있습니다.

- 이 스냅샷 이미지가 포함된 기본 볼륨은 비동기식 미러 그룹의 구성원입니다.
- 기본 볼륨이 현재 동기화 작업 중입니다. 동기화 작업이 완료되는 즉시 스냅샷 이미지 생성이 완료됩니다.

최대 스냅샷 이미지 수입니다

- 볼륨이 스냅샷 정합성 보장 그룹의 구성원인 경우 System Manager는 해당 구성원 볼륨에 대한 스냅샷 그룹을 생성합니다. 이 스냅샷 그룹은 기본 볼륨당 허용되는 최대 스냅샷 그룹 수에 대해 계산됩니다.
- 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹에 스냅샷 이미지를 생성하려고 하지만 연결된 그룹이 최대 스냅샷 이미지 수에 도달했을 경우 다음 두 가지 옵션을 사용할 수 있습니다.
  - 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹에 대해 자동 삭제를 설정합니다.
  - 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹에서 하나 이상의 스냅샷 이미지를 수동으로 삭제하고 작업을 다시 시도하십시오.

자동 삭제

스냅샷 그룹 또는 스냅샷 정합성 보장 그룹이 자동 삭제되도록 설정된 경우 시스템이 그룹에 대한 새 스냅샷 이미지를 생성할 때 가장 오래된 스냅샷 이미지가 삭제됩니다.

롤백 작업

- 롤백 작업이 진행 중일 때는 다음 작업을 수행할 수 없습니다.
  - 롤백에 사용 중인 스냅샷 이미지를 삭제합니다.
  - 롤백 작업에 참여하고 있는 기본 볼륨에 대한 새 스냅샷 이미지를 생성합니다.
  - 연결된 스냅샷 그룹의 리포지토리 - 전체 정책을 변경합니다.
- 다음 작업 중 하나라도 진행 중인 경우에는 롤백 작업을 시작할 수 없습니다.
  - 용량 확장(풀 또는 볼륨 그룹에 용량 추가)
  - 볼륨 확장(볼륨 용량 증가)
  - 볼륨 그룹의 RAID 레벨 변경
  - 볼륨의 세그먼트 크기 변경
- 기본 볼륨이 볼륨 복사본에 참여하고 있는 경우에는 롤백 작업을 시작할 수 없습니다.
- 기본 볼륨이 원격 미러의 2차 볼륨인 경우에는 롤백 작업을 시작할 수 없습니다.
- 연결된 스냅샷 저장소 볼륨에서 사용된 용량 중 읽을 수 없는 섹터가 있는 경우 롤백 작업이 실패합니다.

기본 볼륨, 예약 용량 및 스냅샷 그룹

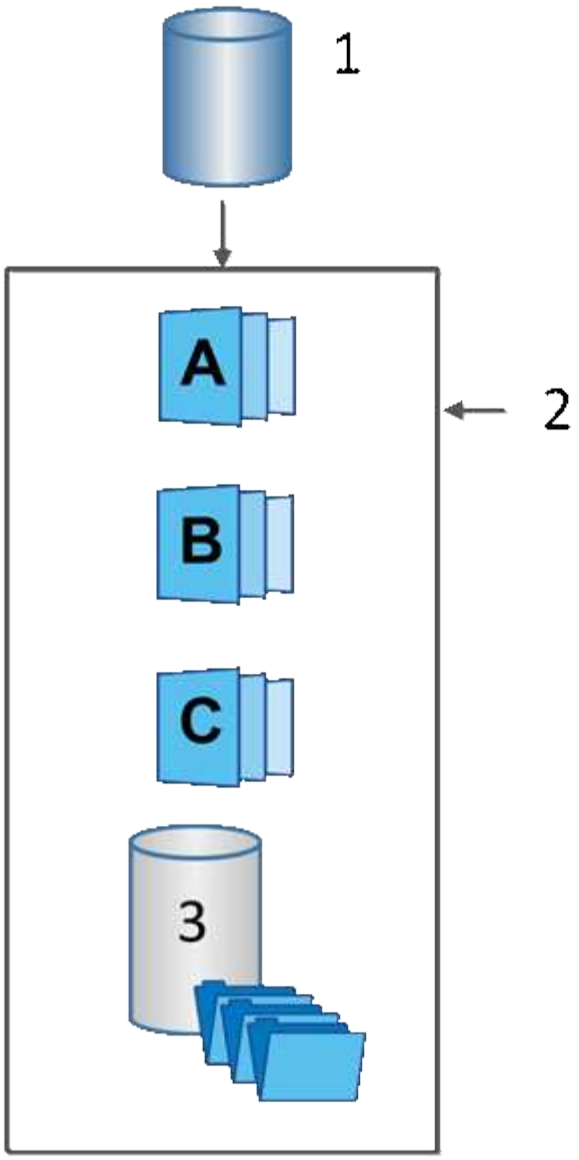
스냅샷 기능은 기본 볼륨, 예약된 용량 및 스냅샷 그룹을 사용합니다.

기본 볼륨

a_base volume_은 스냅샷 이미지의 소스로 사용되는 볼륨입니다. 기본 볼륨은 일반 볼륨이거나 씬 볼륨일 수 있으며 풀 또는 볼륨 그룹에 상주할 수 있습니다.

기본 볼륨의 스냅샷을 생성하려면 언제든지 인스턴트 이미지를 생성하거나 스냅샷에 대한 정기적인 스케줄을 정의하여 프로세스를 자동화할 수 있습니다.

다음 그림에서는 스냅샷 개체와 기본 볼륨 간의 관계를 보여 줍니다.



[1]기본 볼륨;[2]그룹의 스냅샷 개체(이미지 및 예약된 용량);[3]스냅샷 그룹에 예약된 용량입니다.

예약된 용량 및 스냅샷 그룹

System Manager는 스냅샷 이미지를 _ 스냅샷 그룹 _ 으로 구성합니다. System Manager에서 스냅샷 그룹을 설정하면 해당 그룹에 대한 스냅샷 이미지를 유지하고 추가 스냅샷에 대한 후속 변경 사항을 추적하기 위해 associated_reserved capacity_를 자동으로 생성합니다.

기본 볼륨이 볼륨 그룹에 있는 경우 예약된 용량을 풀 또는 볼륨 그룹에 배치할 수 있습니다. 기본 볼륨이 풀에 있는 경우 예약된 용량은 기본 볼륨과 동일한 풀에 있어야 합니다.

스냅샷 그룹은 사용자 작업이 필요하지 않지만 언제든지 스냅샷 그룹의 예약된 용량을 조정할 수 있습니다. 또한 다음 조건이 충족되면 예약된 용량을 생성하라는 메시지가 표시될 수 있습니다.

- 아직 스냅샷 그룹이 없는 기본 볼륨의 스냅샷을 생성할 때마다 System Manager는 자동으로 스냅샷 그룹을 생성합니다. 이 작업을 수행하면 후속 스냅샷 이미지를 저장하는 데 사용되는 기본 볼륨에 예약된 용량도 생성됩니다.

- 기본 볼륨에 대한 스냅샷 스케줄을 생성할 때마다 System Manager가 자동으로 스냅샷 그룹을 생성합니다.

자동 삭제

스냅샷 작업 시 기본 옵션을 사용하여 자동 삭제를 설정합니다. 자동 삭제는 스냅샷 그룹이 32개 이미지의 스냅샷 그룹 제한에 도달하면 가장 오래된 스냅샷 이미지를 자동으로 삭제합니다. 자동 삭제를 해제하면 스냅샷 그룹 제한이 결국 초과되고 수동으로 스냅샷 그룹 설정을 구성하고 예약된 용량을 관리해야 합니다.

스냅샷 스케줄 및 스냅샷 정합성 보장 그룹

스냅샷 이미지 수집에 스케줄을 사용하고 스냅샷 정합성 보장 그룹을 사용하여 여러 기본 볼륨을 관리합니다.

기본 볼륨의 스냅샷 작업을 쉽게 관리하려면 다음 기능을 사용할 수 있습니다.

- * 스냅샷 일정 * — 단일 기본 볼륨에 대한 스냅샷을 자동화합니다.
- * 스냅샷 일관성 그룹 * — 여러 기본 볼륨을 하나의 엔터티로 관리

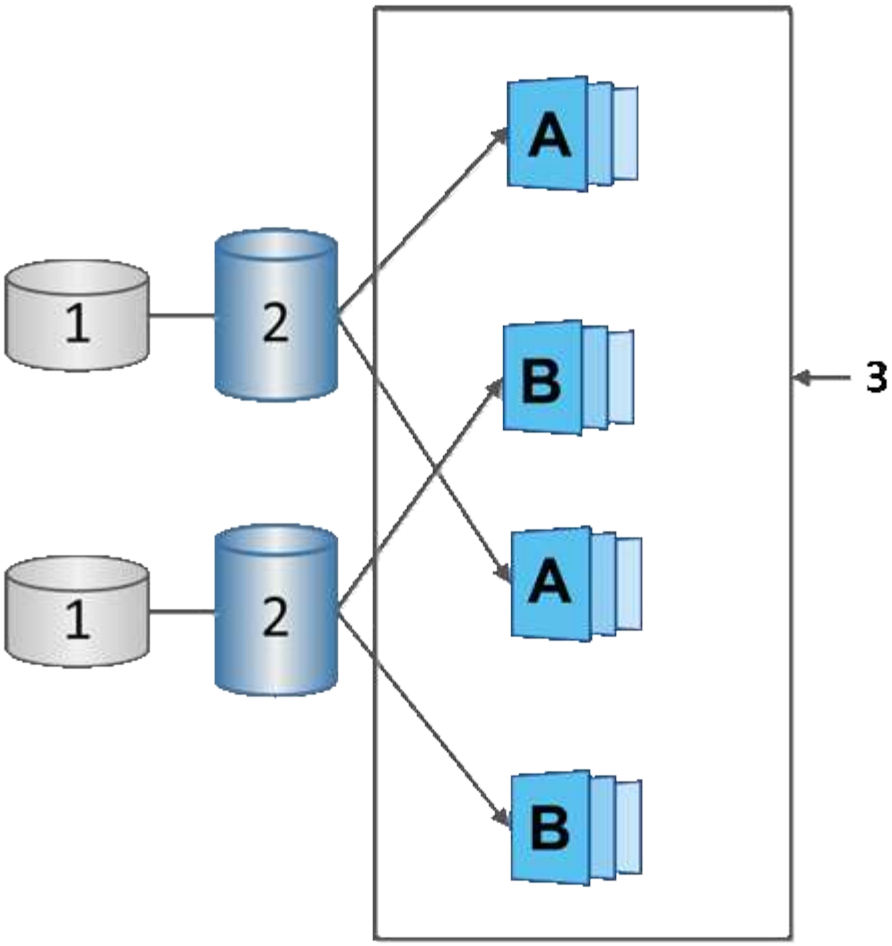
스냅샷 스케줄입니다

기본 볼륨에 대한 스냅샷을 자동으로 생성하려는 경우 스케줄을 생성할 수 있습니다. 예를 들어 매주 토요일 자정, 매월 첫째 날 또는 원하는 날짜 및 시간에 스냅샷 이미지를 생성하는 일정을 정의할 수 있습니다. 단일 스케줄에 대해 최대 32개의 스냅샷이 도달하면 예약된 스냅샷을 일시 중지하거나, 예약된 용량을 더 많이 생성하거나, 스냅샷을 삭제할 수 있습니다. 스냅샷은 수동으로 삭제하거나 삭제 프로세스를 자동화하여 삭제할 수 있습니다. 스냅샷 이미지가 삭제된 후에는 재사용을 위해 추가 예약 용량을 사용할 수 있습니다.

스냅샷 정합성 보장 그룹

스냅샷 정합성 보장 그룹은 여러 볼륨에서 동시에 스냅샷 이미지를 생성하려는 경우에 생성됩니다. 스냅샷 이미지 작업은 스냅샷 정합성 보장 그룹 전체에서 수행됩니다. 예를 들어 모든 볼륨의 동기화된 스냅샷을 동일한 타임스탬프로 예약할 수 있습니다. 스냅샷 정합성 보장 그룹은 한 볼륨에 로그를 저장하는 데이터베이스 애플리케이션, 다른 볼륨에 있는 데이터베이스 파일 등 여러 볼륨에 걸쳐 있는 애플리케이션에 이상적입니다.

스냅샷 정합성 보장 그룹에 포함된 볼륨을 구성원 볼륨이라고 합니다. 볼륨을 일관성 그룹에 추가하면 System Manager에서 해당 구성원 볼륨에 해당하는 예약된 새 용량을 자동으로 생성합니다. 각 구성원 볼륨의 스냅샷 이미지를 자동으로 생성하도록 일정을 정의할 수 있습니다.



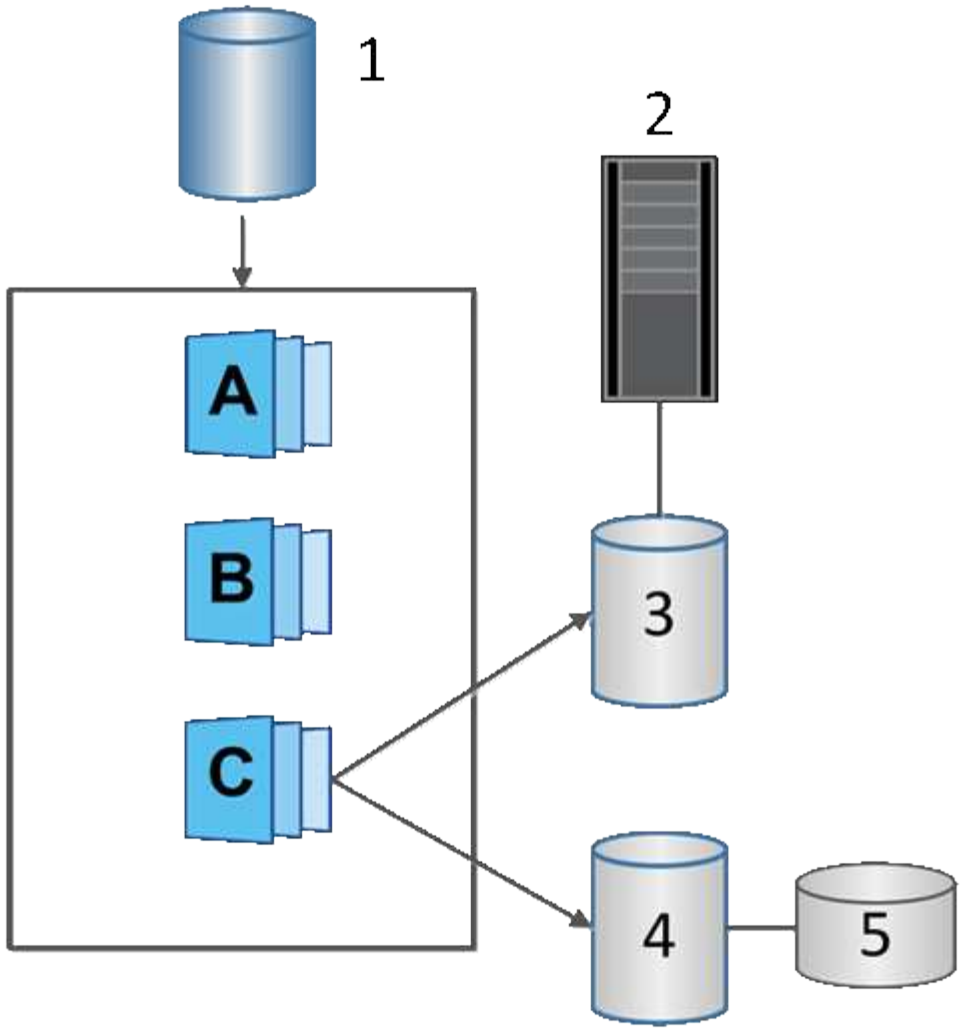
[1] 예약된 용량;[2] 멤버 볼륨;[3] 정합성 보장 그룹 스냅샷 이미지

Snapshot 볼륨

스냅샷 데이터를 읽거나 쓰려면 스냅샷 볼륨을 생성하여 호스트에 할당할 수 있습니다. 스냅샷 볼륨은 기본 볼륨(RAID 레벨, I/O 특성 등)과 동일한 특성을 공유합니다.

스냅샷 볼륨을 생성할 때 해당 볼륨을 *read-only* 또는 _read-write Accessible_로 지정할 수 있습니다.

읽기 전용 스냅샷 볼륨을 생성할 때 예약된 용량을 추가할 필요가 없습니다. 읽기-쓰기 스냅샷 볼륨을 생성할 때 쓰기 액세스를 제공하려면 예약된 용량을 추가해야 합니다.



[1]기본 볼륨;[2]호스트;[3]읽기 전용 스냅샷 볼륨;[4]읽기-쓰기 스냅샷 볼륨;[5] 예약된 용량

스냅샷 롤백

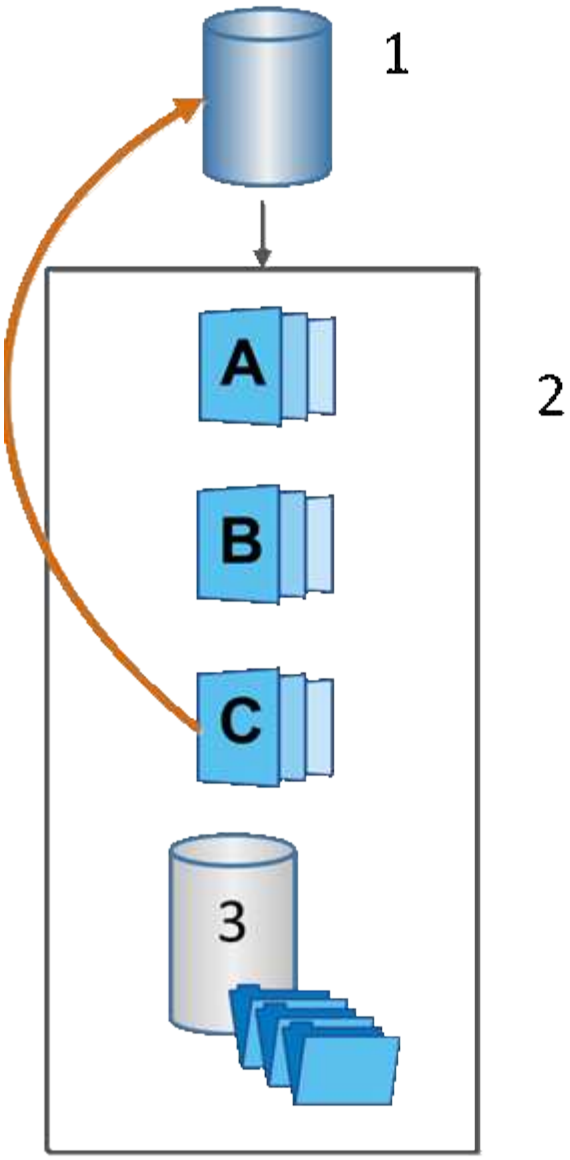
롤백 작업은 기본 볼륨을 선택한 스냅샷에 의해 결정된 이전 상태로 되돌립니다.

롤백의 경우 다음 소스 중 하나에서 스냅샷 이미지를 선택할 수 있습니다.

- * 기본 볼륨의 전체 복원을 위한 스냅샷 이미지 롤백 *.
- * 스냅샷 정합성 보장 그룹 롤백 * - 하나 이상의 볼륨을 롤백하는 데 사용할 수 있습니다.

롤백 중에 스냅샷 기능은 그룹의 모든 스냅샷 이미지를 보존합니다. 또한 I/O 작업이 필요한 경우 이 프로세스 중에 호스트가 기본 볼륨에 액세스할 수 있습니다.

롤백이 시작되면 백그라운드 프로세스가 기본 볼륨의 LBA(논리 블록 주소)를 스윕한 다음, 롤백 스냅샷 이미지에서 복구할 copy-on-write 데이터를 찾습니다. 기본 볼륨은 읽기 및 쓰기에 대해 호스트에서 액세스할 수 있으며 이전에 기록된 모든 데이터를 즉시 사용할 수 있기 때문에 롤백이 진행되는 동안 모든 변경 사항을 포함할 수 있을 만큼 예약된 용량 볼륨이 커야 합니다. 롤백이 완료될 때까지 데이터 전송은 백그라운드 작업으로 계속됩니다.



[1]기본 볼륨;[2]그룹의 스냅샷 개체;[3]스냅샷 그룹의 예약된 용량입니다

스냅샷 및 스냅샷 객체를 생성합니다

스냅샷 이미지를 생성합니다

기본 볼륨 또는 스냅샷 정합성 보장 그룹에서 스냅샷 이미지를 수동으로 생성할 수 있습니다. 이를 _instant snapshot_or_instant image_라고도 합니다.

시작하기 전에

- 기본 볼륨이 최적화되어야 합니다.
- 드라이브가 최적이어야 합니다.
- 스냅샷 그룹은 "재제공"으로 지정할 수 없습니다.
- 예약된 용량 볼륨의 경우 스냅샷 그룹에 대해 연결된 기본 볼륨과 동일한 DA(Data Assurance) 설정을 사용해야

합니다.

단계

1. 다음 작업 중 하나를 수행하여 스냅샷 이미지를 생성합니다.
   - Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다. 개체(기본 볼륨 또는 스냅샷 정합성 보장 그룹)를 선택한 다음 메뉴, 복제 서비스 [인스턴트 스냅샷 생성]을 선택합니다.
   - 스토리지 [스냅샷] 메뉴를 선택합니다. 스냅샷 이미지 * 탭을 선택한 다음 메뉴 생성 [즉시 스냅샷] 을 선택합니다.

     스냅샷 이미지 생성 대화 상자가 나타납니다. 객체(기본 볼륨 또는 스냅샷 정합성 보장 그룹)를 선택하고 * Next * 를 클릭합니다. 볼륨 또는 스냅샷 정합성 보장 그룹에 대해 이전 스냅샷 이미지가 생성된 경우 시스템에서 즉시 인스턴트 스냅샷을 생성합니다. 그렇지 않으면 볼륨 또는 스냅샷 정합성 보장 그룹에 대해 스냅샷 이미지를 처음 생성하는 경우 스냅샷 이미지 생성 확인 대화 상자가 나타납니다.

2. 예약된 용량이 필요하다는 알림을 수락하고 Reserve Capacity 단계로 진행하려면 * Create * 를 클릭합니다.

   용량 예약 대화 상자가 나타납니다.

3. 스피너 상자를 사용하여 용량 비율을 조정한 후 * 다음 * 을 클릭하여 표에 강조 표시된 대상 볼륨을 적용합니다.

   설정 편집 대화 상자가 나타납니다.

4. 스냅샷 이미지에 대한 설정을 적절하게 선택하고 작업을 수행할지 확인합니다.

필드 상세정보

설정	설명
• 스냅샷 이미지 설정 *	스냅샷 이미지 제한
스냅샷 이미지를 지정된 제한 이후 자동으로 삭제하려면 확인란을 선택하고, 제한을 변경하려면 스피너 상자를 사용합니다. 이 확인란의 선택을 취소하면 32개 이미지 후에 스냅샷 이미지 생성이 중지됩니다.	• 예약된 용량 설정 *
다음 경우에 알림:	spinner 상자를 사용하여 스냅샷 그룹의 예약된 용량이 거의 가득 찰 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스냅샷 그룹의 예약된 용량이 지정된 임계값을 초과하는 경우 사전 알림을 사용하여 예약된 용량을 늘리거나 남은 공간이 부족해지기 전에 불필요한 객체를 삭제하십시오.
전체 예약 용량에 대한 정책입니다	다음 정책 중 하나를 선택합니다. • * Purge Oldest snapshot image * — 시스템이 스냅샷 그룹에서 가장 오래된 스냅샷 이미지를 자동으로 제거합니다. 그러면 그룹 내에서 재사용하기 위해 스냅샷 이미지 예약 용량이 해제됩니다. • * 기본 볼륨에 대한 쓰기 거부 * — 예약된 용량이 최대 정의 비율에 도달하면 시스템은 예약된 용량 액세스를 트리거한 기본 볼륨에 대한 모든 I/O 쓰기 요청을 거부합니다.

결과

- System Manager는 스냅샷 이미지 테이블에 새 스냅샷 이미지를 표시합니다. 이 표에는 타임 스탬프와 관련 기본 볼륨 또는 스냅샷 정합성 보장 그룹을 기준으로 새 이미지가 나열됩니다.
- 다음 조건 때문에 스냅샷 생성이 보류 상태로 유지될 수 있습니다.
  - 이 스냅샷 이미지가 포함된 기본 볼륨은 비동기식 미러 그룹의 구성원입니다.
  - 기본 볼륨이 현재 동기화 작업 중입니다. 동기화 작업이 완료되는 즉시 스냅샷 이미지 생성이 완료됩니다.

스냅샷 이미지를 예약합니다

기본 볼륨에 문제가 있는 경우 복구를 설정하고 예약된 백업을 수행하는 스냅샷 스케줄을 생성합니다. 기본 볼륨 또는 스냅샷 정합성 보장 그룹의 스냅샷은 매일, 매주 또는 매월 언제든지 생성할 수 있습니다.

시작하기 전에

기본 볼륨이 최적화되어야 합니다.

이 작업에 대해

이 작업에서는 기존 스냅샷 정합성 보장 그룹 또는 기본 볼륨에 대한 스냅샷 스케줄을 생성하는 방법에 대해 설명합니다.

기본 볼륨 또는 스냅샷 정합성 보장 그룹의 스냅샷 이미지를 생성하는 동시에 스냅샷 스케줄을 생성할 수도 있습니다.

단계

1. 다음 작업 중 하나를 수행하여 스냅샷 스케줄을 생성합니다.
   - Storage [Volumes](저장소 [볼륨]) 메뉴를 선택합니다.

     이 스냅샷 스케줄에 대한 객체(볼륨 또는 스냅샷 정합성 보장 그룹)를 선택한 다음 메뉴: 복제 서비스 [스냅샷 스케줄 생성]을 선택합니다.

   - 스토리지 [스냅샷] 메뉴를 선택합니다.

     Schedules * 탭을 선택한 다음 * Create * 를 클릭합니다.

2. 이 스냅샷 스케줄의 객체(볼륨 또는 스냅샷 정합성 보장 그룹)를 선택하고 * 다음 * 을 클릭합니다.

   스냅샷 일정 생성 대화 상자가 나타납니다.

3. 다음 작업 중 하나를 수행합니다.
   - * 다른 스냅샷 개체에서 이전에 정의한 스케줄을 사용합니다 *.

     고급 옵션이 표시되는지 확인합니다. 추가 옵션 표시 * 를 클릭합니다. 일정 가져오기 * 를 클릭하고 가져올 일정이 있는 개체를 선택한 다음 * 가져오기 * 를 클릭합니다.

   - * 기본 또는 고급 옵션을 수정합니다 *.

     대화 상자의 오른쪽 위에서 * 더 많은 옵션 표시 * 를 클릭하여 모든 옵션을 표시한 후 다음 표를 참조하십시오.

필드 상세정보

필드에 입력합니다	설명
• 기본 설정 *	일 을 선택합니다
스냅샷 이미지에 대한 요일을 개별적으로 선택합니다.	시작 시간
드롭다운 목록에서 일별 스냅샷의 새 시작 시간을 선택합니다(선택 항목은 30분 단위로 제공됨). 시작 시간은 현재 시간보다 30분 먼저 설정됩니다.	시간대
드롭다운 목록에서 스토리지의 시간대를 선택합니다.	• 고급 설정 *
일/월	다음 옵션 중 하나를 선택합니다. • * Daily/Weekly * — 동기화 스냅샷을 위한 개별 요일을 선택합니다. 또한 일일 일정을 원하는 경우 오른쪽 상단에서 * Select All Days * (모든 날짜 선택 *) 확인란을 선택할 수도 있습니다. • * Monthly/Yearly * — 동기화 스냅샷을 위한 개별 월을 선택합니다. On day(s) * 필드에 동기화가 발생하는 날짜를 입력합니다. 유효한 항목은 * 1 * ~ * 31 * 및 * Last * 입니다. 여러 날짜를 쉼표 또는 세미콜론으로 구분할 수 있습니다. 포함 날짜에 하이픈을 사용합니다. 예: 1,3, 4,10-15, Last. 월 단위 일정을 원하는 경우 오른쪽 상단에서 * 모든 월 선택 * 확인란을 선택할 수도 있습니다.
시작 시간	드롭다운 목록에서 일별 스냅샷의 새 시작 시간을 선택합니다(선택 항목은 30분 단위로 제공됨). 시작 시간은 현재 시간보다 30분 먼저 설정됩니다.
시간대	드롭다운 목록에서 스토리지의 시간대를 선택합니다.
스냅샷 간의 일별/시간 스냅샷	하루에 생성할 스냅샷 이미지 수를 선택합니다. 둘 이상의 를 선택한 경우 스냅샷 이미지 사이의 시간도 선택합니다. 여러 스냅샷 이미지의 경우 충분한 예약 용량이 있어야 합니다.
지금 스냅샷 이미지를 생성하시겠습니까?	예약 중인 자동 이미지 외에 인스턴트 이미지를 만들려면 이 확인란을 선택합니다.
시작/종료 날짜 또는 종료 날짜 없음	동기화를 시작할 시작 날짜를 입력합니다. 종료 날짜를 입력하거나 * 종료 날짜 없음 * 을 선택합니다.

4. 다음 작업 중 하나를 수행합니다.
   - 객체가 스냅샷 정합성 보장 그룹인 경우 * 생성 * 을 클릭하여 설정을 적용하고 스케줄을 생성합니다.
   - 객체가 볼륨인 경우 * Next * 를 클릭하여 스냅샷 이미지에 예약된 용량을 할당합니다.

     지정된 예약 용량을 지원하는 후보만 볼륨 후보 테이블에 표시됩니다. 예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

5. 스피너 상자를 사용하여 스냅샷 이미지에 예약된 용량을 할당합니다. 다음 작업 중 하나를 수행합니다.
   - * 기본 설정을 적용합니다. *

     이 권장 옵션을 사용하여 스냅샷 이미지에 예약된 용량을 기본 설정으로 할당합니다.

   - * 데이터 스토리지 요구 사항에 맞게 예약된 용량 설정을 할당합니다. *

     기본 예약된 용량 설정을 변경하는 경우 * 후보 새로 고침 * 을 클릭하여 지정한 예약된 용량에 대한 후보 목록을 새로 고칩니다.

     다음 지침에 따라 예약된 용량을 할당합니다.

     - 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%입니다. 일반적으로 이 용량이면 충분합니다.
     - 필요한 용량은 볼륨에 대한 입출력 쓰기 빈도 및 크기와 스냅샷 이미지 컬렉션의 양과 기간에 따라 달라집니다.

6. 다음 * 을 클릭합니다.

   설정 편집 대화 상자가 나타납니다.

7. 필요에 따라 스냅샷 스케줄의 설정을 편집한 다음 * 마침 * 을 클릭합니다.

필드 상세정보

설정	설명
• 스냅샷 이미지 제한 *	다음과 같은 경우 스냅샷 이미지 자동 삭제 활성화
스냅샷 이미지를 지정된 제한 이후 자동으로 삭제하려면 확인란을 선택하고, 제한을 변경하려면 스피너 상자를 사용합니다. 이 확인란의 선택을 취소하면 32개 이미지 후에 스냅샷 이미지 생성이 중지됩니다.	• 예약된 용량 설정 *
다음 경우에 알림:	스피너 상자를 사용하여 스케줄의 예약된 용량이 거의 가득 찰 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스케줄에 예약된 용량이 지정된 임계값을 초과하는 경우 사전 알림을 사용하여 예약된 용량을 늘리거나 남은 공간이 부족해지기 전에 불필요한 객체를 삭제하십시오.
전체 예약 용량에 대한 정책입니다	다음 정책 중 하나를 선택합니다. • * Purge Oldest snapshot image * — 시스템이 가장 오래된 스냅샷 이미지를 자동으로 지퍼하여 스냅샷 그룹 내에서 재사용할 수 있도록 스냅샷 이미지 예약 용량을 해제합니다. • * 기본 볼륨에 대한 쓰기 거부 * — 예약된 용량이 최대 정의 비율에 도달하면 시스템은 예약된 용량 액세스를 트리거한 기본 볼륨에 대한 모든 I/O 쓰기 요청을 거부합니다.

스냅샷 정합성 보장 그룹을 생성합니다

정합성이 보장된 복제본을 유지하려면 _ 스냅샷 정합성 보장 그룹 _ 이라는 여러 볼륨 세트를 생성할 수 있습니다.

이 그룹을 사용하면 일관성을 위해 모든 볼륨의 스냅샷 이미지를 동시에 만들 수 있습니다. 스냅샷 정합성 보장 그룹에 속한 각 볼륨을 _member volume_이라고 합니다. 스냅샷 정합성 보장 그룹에 볼륨을 추가하면 시스템에서 이 구성원 볼륨에 해당하는 새 스냅샷 그룹을 자동으로 생성합니다.

이 작업에 대해

스냅샷 정합성 보장 그룹 생성 시퀀스를 사용하여 그룹의 구성원 볼륨을 선택하고 구성원 볼륨에 용량을 할당할 수 있습니다.

스냅샷 정합성 보장 그룹을 생성하는 프로세스는 여러 단계로 이루어집니다.

1단계**:** 스냅샷 정합성 보장 그룹에 구성원 추가

구성원을 선택하여 스냅샷 정합성 보장 그룹을 구성하는 볼륨의 컬렉션을 지정합니다. 스냅샷 정합성 보장 그룹에서 수행하는 모든 작업은 선택한 구성원 볼륨으로 균일하게 확장됩니다.

시작하기 전에

구성원 볼륨이 최적화되어야 합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 정합성 보장 그룹 * 탭을 클릭합니다.
3. [스냅샷 일관성 그룹] 생성 메뉴를 선택합니다.

   스냅샷 정합성 보장 그룹 생성 대화 상자가 나타납니다.

4. 구성원 볼륨으로 추가할 볼륨을 스냅샷 정합성 보장 그룹에 선택합니다.
5. 다음 * 을 클릭하고 로 이동합니다2단계: 스냅샷 정합성 보장 그룹의 용량 예약.

2단계**:** 스냅샷 정합성 보장 그룹의 용량 예약

예약된 용량을 스냅샷 정합성 보장 그룹에 연결합니다. System Manager에서는 스냅샷 정합성 보장 그룹의 속성을 기준으로 볼륨 및 용량을 제안합니다. 권장 예약 용량 구성을 수락하거나 할당된 스토리지를 사용자 지정할 수 있습니다.

이 작업에 대해

용량 예약 대화 상자의 볼륨 대상 테이블에는 지정된 예약 용량을 지원하는 후보만 표시됩니다. 예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

단계

1. 스피너 상자를 사용하여 스냅샷 정합성 보장 그룹에 예약된 용량을 할당합니다. 다음 작업 중 하나를 수행합니다.
   - * 기본 설정을 적용합니다 *.

     이 권장 옵션을 사용하여 각 구성원 볼륨에 예약된 용량을 기본 설정으로 할당합니다.

   - * 데이터 스토리지 요구 사항에 맞게 예약된 용량 설정을 할당합니다. *

     다음 지침에 따라 예약된 용량을 할당합니다.

     - 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%입니다. 일반적으로 이 용량이면 충분합니다.
     - 필요한 용량은 볼륨에 대한 입출력 쓰기 빈도 및 크기와 스냅샷 이미지 컬렉션의 양과 기간에 따라 달라집니다.
2. * 선택 사항: * 기본 예약된 용량 설정을 변경하는 경우 * 후보 새로 고침 * 을 클릭하여 지정한 예약된 용량에 대한 후보 목록을 새로 고칩니다.
3. 다음 * 을 클릭하고 로 이동합니다3단계: 스냅샷 정합성 보장 그룹에 대한 설정을 편집합니다.

3단계**:** 스냅샷 정합성 보장 그룹에 대한 설정을 편집합니다

스냅샷 정합성 보장 그룹에 대한 자동 삭제 설정 및 예약된 용량 알림 임계값을 적용하거나 선택합니다.

이 작업에 대해

스냅샷 정합성 보장 그룹 생성 시퀀스를 사용하여 그룹의 구성원 볼륨을 선택하고 구성원 볼륨에 용량을 할당할 수 있습니다.

단계

1. 필요에 따라 스냅샷 정합성 보장 그룹의 기본 설정을 적용하거나 변경합니다.

   필드 상세정보

설정	설명
• 스냅샷 정합성 보장 그룹 설정 *	이름
스냅샷 정합성 보장 그룹의 이름을 지정합니다.	다음과 같은 경우 스냅샷 이미지 자동 삭제 활성화
스냅샷 이미지를 지정된 제한 이후 자동으로 삭제하려면 확인란을 선택하고, 제한을 변경하려면 스피너 상자를 사용합니다. 이 확인란의 선택을 취소하면 32개 이미지 후에 스냅샷 이미지 생성이 중지됩니다.	• 예약된 용량 설정 *
다음 경우에 알림:	spinner 상자를 사용하여 스냅샷 정합성 보장 그룹의 예약된 용량이 거의 꽉 찼을 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스냅샷 정합성 보장 그룹에 예약된 용량이 지정된 임계값을 초과할 경우 사전 알림을 사용하여 예약된 용량을 늘리거나 남은 공간이 부족해지기 전에 불필요한 객체를 삭제하십시오.
전체 예약 용량에 대한 정책입니다	다음 정책 중 하나를 선택합니다. • * Purge Oldest snapshot image * — 시스템이 스냅샷 정합성 보장 그룹에서 가장 오래된 스냅샷 이미지를 자동으로 제거합니다. 이 경우 그룹 내에서 재사용할 수 있도록 스냅샷 이미지 예약 용량이 해제됩니다. • * 기본 볼륨에 대한 쓰기 거부 * — 예약된 용량이 최대 정의 비율에 도달하면 시스템은 예약된 용량 액세스를 트리거한 기본 볼륨에 대한 모든 I/O 쓰기 요청을 거부합니다.

2. 스냅샷 정합성 보장 그룹 구성이 만족스러우면 * 마침 * 을 클릭합니다.

스냅샷 볼륨을 생성하여 볼륨 또는 스냅샷 정합성 보장 그룹의 스냅샷 이미지에 대한 호스트 액세스를 제공합니다. 스냅샷 볼륨을 읽기 전용 또는 읽기-쓰기로 지정할 수 있습니다.

이 작업에 대해

스냅샷 볼륨 생성 시퀀스를 사용하여 스냅샷 이미지에서 스냅샷 볼륨을 생성하고 볼륨이 읽기/쓰기일 경우 예약된 용량을 할당하는 옵션을 제공합니다. 스냅샷 볼륨은 다음 중 하나로 지정할 수 있습니다.

- 읽기 전용 스냅샷 볼륨은 호스트 애플리케이션에 스냅샷 이미지에 포함된 데이터 복제본에 대한 읽기 액세스 권한을 제공하지만 스냅샷 이미지를 수정할 수는 없습니다. 읽기 전용 스냅샷 볼륨에는 연결된 예약 용량이 없습니다.
- 읽기-쓰기 스냅샷 볼륨은 호스트 애플리케이션에 스냅샷 이미지에 포함된 데이터 복제본에 대한 쓰기 액세스 권한을 제공합니다. 호스트 애플리케이션이 수정한 후속 사항을 참조 스냅샷 이미지에 영향을 주지 않고 기본 볼륨에 저장하는 데 사용되는 고유한 예약 용량을 가지고 있습니다.

스냅샷 볼륨을 생성하는 프로세스는 여러 단계로 이루어집니다.

1단계**:** 스냅샷 볼륨의 구성원을 검토합니다

기본 볼륨의 스냅샷 이미지 또는 스냅샷 정합성 보장 그룹을 선택합니다. 스냅샷 정합성 보장 그룹 스냅샷 이미지를 선택하면 스냅샷 정합성 보장 그룹의 구성원 볼륨이 검토를 위해 표시됩니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.
3. Create * 를 선택합니다.

   스냅샷 볼륨 생성 대화 상자가 나타납니다.

4. 스냅샷 볼륨으로 변환할 스냅샷 이미지(볼륨 또는 스냅샷 정합성 보장 그룹)를 선택하고 * 다음 * 을 클릭합니다. 필터 * 필드의 텍스트 항목을 사용하여 목록 범위를 좁힙니다.

   스냅샷 정합성 보장 그룹 스냅샷 이미지를 선택한 경우 구성원 검토 대화 상자가 나타납니다.

   Review Members(구성원 검토) 대화 상자에서 스냅샷 볼륨으로 변환하기 위해 선택한 볼륨 목록을 검토한 후 * Next * (다음 *)를 클릭합니다.

5. 로 이동합니다. 2단계: 호스트에 스냅샷 볼륨을 할당합니다

2단계**:** 호스트에 스냅샷 볼륨을 할당합니다

특정 호스트 또는 호스트 클러스터를 선택하여 스냅샷 볼륨에 할당합니다. 이 할당은 호스트 또는 호스트 클러스터에 스냅샷 볼륨에 대한 액세스 권한을 부여합니다. 필요한 경우 나중에 호스트를 할당할 수 있습니다.

시작하기 전에

- 호스트 페이지에 유효한 호스트 또는 호스트 클러스터가 있습니다.
- 호스트에 대해 호스트 포트 식별자를 정의해야 합니다.
- DA 지원 볼륨을 생성하기 전에 계획된 호스트 연결이 DA(Data Assurance) 기능을 지원하는지 확인하십시오. 스토리지 시스템의 컨트롤러에 있는 호스트 접속 중 하나라도 DA를 지원하지 않으면 연결된 호스트가 DA 지원

볼륨의 데이터에 액세스할 수 없습니다.

이 작업에 대해

볼륨을 할당할 때 다음 지침을 염두에 두십시오.

- 호스트의 운영 체제에는 호스트가 액세스할 수 있는 볼륨 수에 대한 특정 제한이 있을 수 있습니다.
- 스토리지 배열의 각 스냅샷 볼륨에 대해 하나의 호스트 할당을 정의할 수 있습니다.
- 할당된 볼륨은 스토리지 배열의 컨트롤러 간에 공유됩니다.
- 동일한 LUN(Logical Unit Number)은 호스트 또는 호스트 클러스터에서 스냅샷 볼륨을 액세스하는 데 두 번 사용할 수 없습니다. 고유한 LUN을 사용해야 합니다.

호스트 클러스터의 호스트에 대해 설정된 할당과 충돌하는 호스트 클러스터에 볼륨을 할당하려고 하면 호스트에 볼륨을 할당할 수 없습니다.

단계

1. 호스트에 할당 * 대화 상자에서 새 볼륨에 할당할 호스트 또는 호스트 클러스터를 선택합니다. 호스트를 할당하지 않고 볼륨을 생성하려면 드롭다운 목록에서 * 나중에 할당 * 을 선택합니다.
2. 액세스 모드를 선택합니다. 다음 중 하나를 선택합니다.
   - * 읽기/쓰기 * — 이 옵션은 스냅샷 볼륨에 대한 읽기/쓰기 액세스를 호스트에 제공하며 예약된 용량이 필요합니다.
   - * 읽기 전용 * — 이 옵션은 스냅샷 볼륨에 대한 읽기 전용 액세스를 호스트에 제공하며 예약된 용량이 필요하지 않습니다.
3. 다음 * 을 클릭하고 다음 중 하나를 수행합니다.
   - 스냅샷 볼륨이 읽기/쓰기 상태인 경우 용량 검토 대화 상자가 나타납니다. 로 이동합니다. 3단계: 스냅샷 볼륨의 예비 용량을 설정합니다
   - 스냅샷 볼륨이 읽기 전용인 경우 우선 순위 편집 대화 상자가 나타납니다. 로 이동합니다. 4단계: 스냅샷 볼륨에 대한 설정을 편집합니다

3단계**:** 스냅샷 볼륨의 예비 용량을 설정합니다

예약된 용량을 읽기/쓰기 스냅샷 볼륨에 연결합니다. System Manager에서는 기본 볼륨 또는 스냅샷 정합성 보장 그룹의 속성을 기준으로 볼륨 및 용량을 제안합니다. 권장 예약 용량 구성을 수락하거나 할당된 스토리지를 사용자 지정할 수 있습니다.

이 작업에 대해

필요에 따라 스냅샷 볼륨의 예약된 용량을 늘리거나 줄일 수 있습니다. 스냅샷 예약 용량이 필요한 용량보다 큰 경우 크기를 줄여 다른 논리적 볼륨에서 필요한 공간을 확보할 수 있습니다.

단계

1. 스피너 상자를 사용하여 스냅샷 볼륨에 예약된 용량을 할당합니다.

   볼륨 후보 테이블에는 지정된 예약 용량을 지원하는 후보만 표시됩니다.

   다음 작업 중 하나를 수행합니다.

   - * 기본 설정을 적용합니다 *.

이 권장 옵션을 사용하여 스냅샷 볼륨에 예약된 용량을 기본 설정으로 할당합니다.

◦ * 데이터 스토리지 요구 사항을 충족하기 위해 자체 예약된 용량 설정을 할당합니다. *.

기본 예약된 용량 설정을 변경하는 경우 * 후보 새로 고침 * 을 클릭하여 지정한 예약된 용량에 대한 후보 목록을 새로 고칩니다.

다음 지침에 따라 예약된 용량을 할당합니다.

- 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%이며 일반적으로 이 용량이면 충분합니다.
- 필요한 용량은 볼륨에 대한 입출력 쓰기 빈도 및 크기와 스냅샷 이미지 컬렉션의 양과 기간에 따라 달라집니다.

2. * 선택 사항: * 스냅샷 정합성 보장 그룹에 대한 스냅샷 볼륨을 생성하는 경우 예약된 용량 후보 테이블에 "후보 변경" 옵션이 나타납니다. 후보 변경 * 을 클릭하여 예약된 대체 용량을 선택합니다.
3. 다음 * 을 클릭하고 로 이동합니다4단계: 스냅샷 볼륨에 대한 설정을 편집합니다.

4단계**:** 스냅샷 볼륨에 대한 설정을 편집합니다

이름, 캐싱, 예약된 용량 알림 임계값 등과 같은 스냅샷 볼륨의 설정을 변경합니다.

이 작업에 대해

읽기 전용 성능을 개선하기 위해 SSD(Solid State Disk) 캐시에 볼륨을 추가할 수 있습니다. SSD 캐시는 스토리지 어레이에서 논리적으로 그룹화하는 SSD 드라이브 세트로 구성됩니다.

단계

1. 스냅샷 볼륨에 대한 설정을 적절히 적용하거나 변경합니다.

필드 상세정보

설정	설명
• 스냅샷 볼륨 설정 *	이름
스냅샷 볼륨의 이름을 지정합니다.	SSD Cache를 활성화합니다
SSD에서 읽기 전용 캐싱을 설정하려면 이 옵션을 선택합니다.	• 예약된 용량 설정 *
다음 경우에 알림:	• 는 읽기/쓰기 스냅샷 볼륨에 대해서만 표시됩니다 *. spinner 상자를 사용하여 스냅샷 그룹의 예약된 용량이 거의 가득 찰 때 시스템에서 경고 알림을 보내는 백분율 지점을 조정합니다. 스냅샷 그룹의 예약된 용량이 지정된 임계값을 초과하는 경우 사전 알림을 사용하여 예약된 용량을 늘리거나 남은 공간이 부족해지기 전에 불필요한 객체를 삭제하십시오.

2. 스냅샷 볼륨 구성을 검토합니다. 변경하려면 * 뒤로 * 를 클릭합니다.
3. 스냅샷 볼륨 구성이 만족스러우면 * 마침 * 을 클릭합니다.

스냅샷 스케줄을 관리합니다

스냅샷 스케줄의 설정을 변경합니다

스냅샷 스케줄의 경우 자동 수집 시간 또는 수집 빈도를 변경할 수 있습니다.

이 작업에 대해

기존 스냅샷 스케줄에서 설정을 가져오거나 필요에 따라 설정을 수정할 수 있습니다.

스냅샷 스케줄은 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹에 연결되기 때문에 예약된 용량은 스케줄 설정 변경의 영향을 받을 수 있습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Schedules * 탭을 클릭합니다.
3. 변경할 스냅샷 스케줄을 선택한 다음 * 편집 * 을 클릭합니다.

   스냅샷 일정 편집 대화 상자가 나타납니다.

4. 다음 중 하나를 수행합니다.
   - * 다른 스냅샷 개체에서 이전에 정의한 일정 사용 * — * 일정 가져오기 * 를 클릭하고 가져올 일정이 있는 개체를

선택한 다음 * 가져오기 * 를 클릭합니다.

◦ * 스케줄 설정 편집 * — 아래의 필드 세부 정보를 참조하십시오.

필드 상세정보

설정	설명
일/월	다음 옵션 중 하나를 선택합니다. • * Daily/Weekly * — 동기화 스냅샷을 위한 개별 요일을 선택합니다. 또한 일일 일정을 원하는 경우 오른쪽 상단에서 * Select All Days * (모든 날짜 선택 *) 확인란을 선택할 수도 있습니다. • * Monthly/Yearly * — 동기화 스냅샷을 위한 개별 월을 선택합니다. On day(s) * 필드에 동기화가 발생하는 날짜를 입력합니다. 유효한 항목은 * 1 * ~ * 31 * 및 * Last * 입니다. 여러 날짜를 쉼표 또는 세미콜론으로 구분할 수 있습니다. 포함 날짜에 하이픈을 사용합니다. 예: 1,3, 4,10-15, Last. 월 단위 일정을 원하는 경우 오른쪽 상단에서 * 모든 월 선택 * 확인란을 선택할 수도 있습니다.
시작 시간	드롭다운 목록에서 일별 스냅샷의 새 시작 시간을 선택합니다. 선택사항은 30분 단위로 제공됩니다. 시작 시간은 현재 시간보다 30분 먼저 설정됩니다.
시간대	드롭다운 목록에서 스토리지 어레이의 시간대를 선택합니다.
매일 스냅샷 수 스냅샷 사이의 시간입니다	하루에 생성할 스냅샷 이미지 수를 선택합니다. 둘 이상의 을 선택한 경우 복원 지점 사이의 시간도 선택합니다. 여러 복원 지점의 경우 충분한 예약 용량이 있어야 합니다.
시작 날짜 종료 날짜 종료 날짜가 없습니다	동기화를 시작할 시작 날짜를 입력합니다. 종료 날짜를 입력하거나 * 종료 날짜 없음 * 을 선택합니다.

5. 저장 * 을 클릭합니다.

스냅샷 스케줄을 활성화하고 일시 중지합니다

저장 공간을 절약해야 할 경우 스냅숏 이미지의 예약된 컬렉션을 일시적으로 일시 중지할 수 있습니다. 이 방법은 스냅샷 스케줄을 삭제하고 나중에 다시 생성하는 것보다 더 효율적입니다.

이 작업에 대해

예약된 스냅샷 작업을 재개하려면 * Activate * 옵션을 사용할 때까지 스냅샷 스케줄의 상태가 일시 중지된 상태로 유지됩니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 아직 표시되지 않은 경우 * Schedules * (일정 *) 탭을 클릭합니다.

   일정은 페이지에 나와 있습니다.

3. 일시 중지할 활성 스냅샷 스케줄을 선택한 다음 * 활성화/일시 중단 * 을 클릭합니다.

   상태 열 상태가 * Suspended * 로 변경되고 스냅샷 스케줄은 모든 스냅샷 이미지의 수집을 중지합니다.

4. 스냅샷 이미지 수집을 다시 시작하려면 재개할 일시 중지된 스냅샷 스케줄을 선택한 다음 * 활성화/일시 중단 * 을 클릭합니다.

   상태 열 상태가 * 활성 * 으로 변경됩니다.

스냅샷 스케줄을 삭제합니다

스냅샷 이미지를 더 이상 수집하지 않으려는 경우 기존 스냅샷 일정을 삭제할 수 있습니다.

이 작업에 대해

스냅샷 스케줄을 삭제하면 연결된 스냅샷 이미지가 함께 삭제되지 않습니다. 스냅샷 이미지 모음이 특정 시점에 재개될 수 있다고 생각되면 스냅샷 일정을 삭제하는 대신 일시 중지해야 합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Schedules * 탭을 클릭합니다.
3. 삭제할 스냅샷 스케줄을 선택하고 작업을 확인합니다.

결과

기본 볼륨 또는 스냅샷 정합성 보장 그룹에서 모든 스케줄 속성이 제거됩니다.

스냅샷 이미지를 관리합니다

스냅샷 이미지 설정을 봅니다

각 스냅샷 이미지에 할당된 속성, 상태, 예약된 용량 및 관련 객체를 볼 수 있습니다.

이 작업에 대해

스냅샷 이미지와 관련된 객체에는 이 스냅샷 이미지가 복원 지점인 기본 볼륨 또는 스냅샷 정합성 보장 그룹, 연결된 스냅샷 그룹 및 스냅샷 이미지에서 생성된 모든 스냅샷 볼륨이 포함됩니다. 스냅샷 설정을 사용하여 스냅샷 이미지를 복제할지 또는 변환할지를 결정합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 클릭합니다.
3. 보려는 스냅샷 이미지를 선택한 다음 * 설정 보기 * 를 클릭합니다.

   스냅샷 이미지 설정 대화 상자가 나타납니다.

4. 스냅샷 이미지에 대한 설정을 봅니다.

기본 볼륨에 대한 스냅샷 이미지 롤백을 시작합니다

롤백 작업을 수행하여 스냅샷 이미지에 저장된 컨텐츠와 일치하도록 기본 볼륨의 콘텐츠를 변경할 수 있습니다.

롤백 작업은 기본 볼륨과 연결된 스냅샷 이미지의 콘텐츠를 변경하지 않습니다.

시작하기 전에

- 롤백 작업을 시작할 수 있는 충분한 예약 용량을 사용할 수 있습니다.
- 선택한 스냅샷 이미지가 최적이고 선택한 볼륨이 최적입니다.
- 선택한 볼륨에 이미 진행 중인 롤백 작업이 없습니다.

이 작업에 대해

롤백 시작 시퀀스를 사용하면 스토리지 용량을 추가하는 옵션을 제공하면서 기본 볼륨의 스냅샷 이미지에서 롤백을 시작할 수 있습니다. 기본 볼륨에 대해 한 번에 두 개 이상의 롤백 작업을 시작할 수 없습니다.

> 호스트는 새로 롤백된 기본 볼륨에 즉시 액세스할 수 있지만, 롤백이 시작된 후 기존 기본 볼륨에서 호스트 읽기-쓰기 액세스를 허용하지 않습니다. 롤백을 시작하기 직전에 기본 볼륨의 스냅샷을 생성하여 복구를 위해 롤백 전 기본 볼륨을 보존할 수 있습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 선택합니다.
3. 스냅샷 영상을 선택한 다음 Rollback [Start](롤백[시작]) 메뉴를 선택합니다.

   롤백 시작 확인 대화 상자가 나타납니다.

4. * 선택 사항: * 필요한 경우 * 용량 증가 * 옵션을 선택합니다.

   예약된 용량 증가 대화 상자가 나타납니다.

   a. 스피너 상자를 사용하여 용량 비율을 조정합니다.

      선택한 스토리지 객체가 포함된 풀 또는 볼륨 그룹에 사용 가능한 용량이 없고 스토리지 배열에 할당되지 않은 용량이 있는 경우 용량을 추가할 수 있습니다. 새 풀 또는 볼륨 그룹을 생성한 다음 해당 풀 또는 볼륨 그룹의 새 가용 용량을 사용하여 이 작업을 다시 시도할 수 있습니다.

   b. 증가 * 를 클릭합니다.
5. 이 작업을 수행할지 확인한 다음 * Rollback * 을 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 선택한 스냅샷 이미지에 저장된 컨텐츠로 볼륨을 복원합니다.
- 롤백된 볼륨을 호스트 액세스에 즉시 사용할 수 있도록 합니다. 롤백 작업이 완료될 때까지 기다릴 필요가 없습니다.

작업을 마친 후

롤백 작업의 진행률을 보려면 홈 [View Operations in Progress] 메뉴를 선택합니다.

롤백 작업이 성공하지 못하면 작업이 일시 중지됩니다. 일시 중지된 작업을 다시 시작하고 여전히 실패하면 Recovery Guru 절차에 따라 문제를 해결하거나 기술 지원 부서에 문의하십시오.

스냅샷 정합성 보장 그룹 구성원 볼륨에 대한 스냅샷 이미지 롤백을 시작합니다

롤백 작업을 수행하여 스냅샷 정합성 보장 그룹 구성원 볼륨의 콘텐츠를 스냅샷 이미지에 저장된 컨텐츠와 일치하도록 변경할 수 있습니다.

롤백 작업은 스냅샷 정합성 보장 그룹에 연결된 스냅샷 이미지의 컨텐츠를 변경하지 않습니다.

시작하기 전에

- 롤백 작업을 시작할 수 있는 충분한 예약 용량을 사용할 수 있습니다.
- 선택한 스냅샷 이미지가 최적이고 선택한 볼륨이 최적입니다.
- 선택한 볼륨에 이미 진행 중인 롤백 작업이 없습니다.

이 작업에 대해

롤백 시작 시퀀스를 사용하면 스토리지 용량을 추가하는 옵션을 제공하면서 스냅샷 정합성 보장 그룹의 스냅샷 이미지에 대한 롤백을 시작할 수 있습니다. 스냅샷 정합성 보장 그룹에 대해 한 번에 두 개 이상의 롤백 작업을 시작할 수 없습니다.

> 호스트는 새로 롤백된 볼륨에 즉시 액세스할 수 있지만 롤백이 시작된 후에는 기존 구성원 볼륨에서 더 이상 호스트 읽기-쓰기 액세스를 허용하지 않습니다. 복구를 위해 롤백 전 기본 볼륨을 보존하기 위해 롤백을 시작하기 직전에 구성원 볼륨의 스냅샷 이미지를 생성할 수 있습니다.

스냅샷 정합성 보장 그룹의 스냅샷 이미지 롤백을 시작하는 프로세스는 여러 단계로 이루어집니다.

1단계**:** 구성원을 선택합니다

롤백할 구성원 볼륨을 선택해야 합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 선택합니다.
3. 스냅샷 정합성 보장 그룹 스냅샷 이미지를 선택한 다음 Rollback [Start](롤백 [시작]) 메뉴를 선택합니다.

   롤백 시작 대화 상자가 나타납니다.

4. 구성원 볼륨 또는 볼륨을 선택합니다.
5. 다음 * 을 클릭하고 다음 중 하나를 수행합니다.
   - 선택한 구성원 볼륨 중 하나가 스냅샷 이미지를 저장하는 둘 이상의 예약된 용량 객체와 연결된 경우 용량 검토 대화 상자가 나타납니다. 로 이동합니다. 2단계: 용량 검토
   - 선택한 구성원 볼륨 중 스냅샷 이미지를 저장하는 예약된 용량 객체가 두 개 이상 연결되어 있지 않으면 Edit Priority(우선 순위 편집) 대화 상자가 나타납니다. 로 이동합니다. 3단계: 우선 순위 편집

2단계**:** 용량 검토

스냅샷 그룹 및 예약된 용량 볼륨과 같이 둘 이상의 예약된 용량 객체와 연결된 구성원 볼륨을 선택한 경우 롤백 볼륨에 대한 예약된 용량을 검토하고 늘릴 수 있습니다.

단계

1. 예약된 용량이 매우 낮거나 0인 구성원 볼륨 옆에 있는 * Edit * 열에서 * 파일 용량 증가 * 링크를 클릭합니다.

   예약된 용량 증가 대화 상자가 나타납니다.

2. 스피너 상자를 사용하여 용량 비율을 조정한 다음 * 증가 * 를 클릭합니다.

   선택한 스토리지 객체가 포함된 풀 또는 볼륨 그룹에 사용 가능한 용량이 없고 스토리지 배열에 할당되지 않은 용량이 있는 경우 용량을 추가할 수 있습니다. 새 풀 또는 볼륨 그룹을 생성하고 해당 풀 또는 볼륨 그룹의 새 가용 용량을 사용하여 이 작업을 다시 시도할 수 있습니다.

3. 다음 * 을 클릭하고 로 이동합니다3단계: 우선 순위 편집.

   우선 순위 편집 대화 상자가 나타납니다.

3단계**:** 우선 순위 편집

필요한 경우 롤백 작업의 우선 순위를 편집할 수 있습니다.

이 작업에 대해

롤백 우선 순위는 시스템 성능을 희생하여 롤백 작업 전용 시스템 리소스 수를 결정합니다.

단계

1. 슬라이더를 사용하여 필요에 따라 롤백 우선순위를 조정합니다.
2. 이 작업을 수행할지 확인한 다음 * 마침 * 을 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 선택한 스냅샷 이미지에 저장된 컨텐츠로 스냅샷 정합성 보장 그룹 구성원 볼륨을 복원합니다.
- 롤백된 볼륨을 호스트 액세스에 즉시 사용할 수 있도록 합니다. 롤백 작업이 완료될 때까지 기다릴 필요가 없습니다.

작업을 마친 후

롤백 작업의 진행률을 보려면 홈 [View Operations in Progress] 메뉴를 선택합니다.

롤백 작업이 성공하지 못하면 작업이 일시 중지됩니다. 일시 중지된 작업을 다시 시작하고 여전히 실패하면 Recovery Guru 절차에 따라 문제를 해결하거나 기술 지원 부서에 문의하십시오.

스냅샷 이미지 롤백을 재개합니다

스냅샷 이미지 롤백 작업 중에 오류가 발생하면 작업이 자동으로 일시 중지됩니다. 일시 중지 상태인 롤백 작업을 다시 시작할 수 있습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 클릭합니다.
3. 일시 중지된 롤백을 강조 표시한 다음 Rollback [Resume](롤백[재개]) 메뉴를 선택합니다.

   작업이 재개됩니다.

결과

System Manager는 다음 작업을 수행합니다.

- 롤백 작업이 성공적으로 재개되면 작업 진행 중 창에서 롤백 작업의 진행률을 볼 수 있습니다.
- 롤백 작업이 성공하지 못하면 작업이 다시 일시 중지됩니다. Recovery Guru 절차에 따라 문제를 해결하거나 기술 지원 부서에 문의할 수 있습니다.

스냅샷 이미지 롤백을 취소합니다

진행 중인 활성 롤백(활성 데이터 복사), 보류 중인 롤백(리소스 시작을 기다리는 대기 중인 대기 중인 대기열) 또는 오류로 인해 일시 중지된 롤백을 취소할 수 있습니다.

이 작업에 대해

진행 중인 롤백 작업을 취소하면 기본 볼륨이 사용할 수 없는 상태로 돌아가고 실패한 것으로 표시됩니다. 따라서 기본 볼륨의 콘텐츠를 복원하기 위한 복구 옵션이 있는 경우에만 롤백 작업을 취소하는 것이 좋습니다.

> 스냅샷 이미지가 있는 스냅샷 그룹에 자동으로 제거된 스냅샷 이미지가 하나 이상 있는 경우 롤백 작업에 사용된 스냅샷 이미지를 나중에 롤백할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 클릭합니다.
3. 활성 또는 일시 중지된 롤백을 선택한 다음 메뉴 롤백[취소]을 선택합니다.

   롤백 취소 확인 대화 상자가 나타납니다.

4. 예 * 를 클릭하여 확인합니다.

결과

System Manager는 롤백 작업을 중지합니다. 기본 볼륨을 사용할 수 있지만 일관되지 않거나 손상되지 않은 데이터가 있을 수 있습니다.

작업을 마친 후

롤백 작업을 취소한 후에는 다음 작업 중 하나를 수행해야 합니다.

- 기본 볼륨의 내용을 다시 초기화합니다.
- 롤백 취소 작업에 사용된 것과 동일한 스냅샷 이미지 또는 다른 스냅샷 이미지를 사용하여 기본 볼륨을 복원하려면 새 롤백 작업을 수행합니다.

스냅샷 이미지를 삭제합니다

스냅샷 이미지를 삭제하여 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹에서 가장 오래된 스냅샷 이미지를 정리합니다.

이 작업에 대해

단일 스냅샷 이미지를 삭제하거나 생성 타임스탬프가 동일한 스냅샷 정합성 보장 그룹에서 스냅샷 이미지를 삭제할 수 있습니다. 스냅샷 그룹에서 스냅샷 이미지를 삭제할 수도 있습니다.

스냅샷 이미지가 연결된 기본 볼륨 또는 스냅샷 정합성 보장 그룹의 가장 오래된 스냅샷 이미지가 아닌 경우 삭제할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 이미지 * 탭을 클릭합니다.
3. 삭제할 스냅샷 이미지를 선택하고 작업을 수행할지 확인합니다.

   스냅샷 정합성 보장 그룹의 스냅샷 이미지를 선택한 경우 삭제할 각 구성원 볼륨을 선택하고 작업을 수행할지 확인합니다.

4. 삭제 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스토리지 시스템에서 스냅샷 이미지를 삭제합니다.
- 스냅샷 그룹 또는 스냅샷 정합성 보장 그룹 내에서 재사용하기 위해 예약된 용량을 해제합니다.
- 삭제된 스냅샷 이미지에 대해 존재하는 연결된 모든 스냅샷 볼륨을 비활성화합니다.
- 스냅샷 정합성 보장 그룹을 삭제하면 삭제된 스냅샷 이미지와 연결된 구성원 볼륨이 중지됨 상태로 이동합니다.

스냅샷 정합성 보장 그룹을 관리합니다

스냅샷 정합성 보장 그룹에 구성원 볼륨을 추가합니다

기존 스냅샷 정합성 보장 그룹에 새 구성원 볼륨을 추가할 수 있습니다. 새 구성원 볼륨을 추가할 때 구성원 볼륨에 대한 용량도 예약해야 합니다.

시작하기 전에

- 구성원 볼륨이 최적화되어야 합니다.
- 스냅샷 정합성 보장 그룹은 최대 허용 볼륨 수보다 작아야 합니다(구성에 정의된 대로).
- 예약된 각 용량 볼륨은 연결된 구성원 볼륨과 동일한 DA(Data Assurance) 및 보안 설정을 가져야 합니다.

이 작업에 대해

표준 볼륨 또는 씬 볼륨을 스냅샷 정합성 보장 그룹에 추가할 수 있습니다. 기본 볼륨은 풀 또는 볼륨 그룹에 상주할 수 있습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 정합성 보장 그룹 * 탭을 선택합니다.

   테이블이 나타나고 스토리지 시스템과 연결된 모든 스냅샷 정합성 보장 그룹이 표시됩니다.

3. 수정할 스냅샷 정합성 보장 그룹을 선택한 다음 * 구성원 추가 * 를 클릭합니다.

   구성원 추가 대화 상자가 나타납니다.

4. 추가할 구성원 볼륨을 선택한 후 * 다음 * 을 클릭합니다.

   용량 예약 단계가 나타납니다. 볼륨 후보 테이블에는 지정된 예약 용량을 지원하는 후보만 표시됩니다.

5. 스피너 상자를 사용하여 구성원 볼륨에 예약된 용량을 할당합니다. 다음 작업 중 하나를 수행합니다.
   - * 기본 설정을 적용합니다. *

     이 권장 옵션을 사용하여 구성원 볼륨에 예약된 용량을 기본 설정으로 할당합니다.

   - * 데이터 스토리지 요구 사항에 맞게 예약된 용량 설정을 할당합니다. *

     기본 예약된 용량 설정을 변경하는 경우 * 후보 새로 고침 * 을 클릭하여 지정한 예약된 용량에 대한 후보 목록을 새로 고칩니다.

     다음 지침에 따라 예약된 용량을 할당합니다.

     - 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%이며 일반적으로 이 용량이면 충분합니다.
     - 필요한 용량은 볼륨에 대한 입출력 쓰기 빈도 및 크기와 스냅샷 이미지 컬렉션의 양과 기간에 따라 달라집니다.
6. 구성원 볼륨을 추가하려면 * 마침 * 을 클릭합니다.

스냅샷 정합성 보장 그룹에서 구성원 볼륨을 제거합니다

기존 스냅샷 정합성 보장 그룹에서 구성원 볼륨을 제거할 수 있습니다.

이 작업에 대해

스냅샷 정합성 보장 그룹에서 구성원 볼륨을 제거하면 System Manager는 해당 구성원 볼륨과 연결된 스냅샷 개체를 자동으로 삭제합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 정합성 보장 그룹 * 탭을 클릭합니다.
3. 수정할 스냅샷 정합성 보장 그룹 옆에 있는 더하기 기호(+)를 선택하여 확장합니다.
4. 제거할 구성원 볼륨을 선택한 다음 * 제거 * 를 클릭합니다.
5. 작업을 수행할지 확인한 다음 * 제거 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 구성원 볼륨과 연결된 모든 스냅샷 이미지와 스냅샷 볼륨을 삭제합니다.
- 구성원 볼륨과 연결된 스냅샷 그룹을 삭제합니다.
- 구성원 볼륨은 변경 또는 삭제되지 않습니다.

스냅샷 정합성 보장 그룹의 설정을 변경합니다

스냅샷 정합성 보장 그룹의 이름, 자동 삭제 설정 또는 허용되는 최대 스냅샷 이미지 수를 변경하려면 스냅샷 정합성 보장 그룹의 설정을 변경합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. 스냅샷 정합성 보장 그룹 * 탭을 클릭합니다.
3. 편집할 스냅샷 정합성 보장 그룹을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   스냅샷 정합성 보장 그룹 설정 대화 상자가 나타납니다.

4. 필요에 따라 스냅샷 정합성 보장 그룹의 설정을 변경합니다.

필드 상세정보

설정	설명
• 스냅샷 정합성 보장 그룹 설정 *	이름
스냅샷 정합성 보장 그룹의 이름을 변경할 수 있습니다.	자동 삭제
스냅샷 이미지를 지정된 제한 이후 자동으로 삭제하려면 확인란을 선택하고, 제한을 변경하려면 스피너 상자를 사용합니다. 이 확인란의 선택을 취소하면 32개 이미지 후에 스냅샷 이미지 생성이 중지됩니다.	스냅샷 이미지 제한
스냅샷 그룹에 허용되는 최대 스냅샷 이미지 수를 변경할 수 있습니다.	스냅샷 스케줄입니다
이 필드는 스케줄이 스냅샷 정합성 보장 그룹에 연결되어 있는지 여부를 나타냅니다.	• 관련 개체 *
구성원 볼륨	스냅샷 정합성 보장 그룹에 연결된 구성원 볼륨의 수량을 확인할 수 있습니다.

5. 저장 * 을 클릭합니다.

스냅샷 정합성 보장 그룹을 삭제합니다

더 이상 필요하지 않은 스냅샷 정합성 보장 그룹을 삭제할 수 있습니다.

시작하기 전에

모든 구성원 볼륨의 이미지가 더 이상 백업 또는 테스트 용도로 필요하지 않은지 확인합니다.

이 작업에 대해

이 작업은 스냅샷 정합성 보장 그룹과 연결된 모든 스냅샷 이미지 또는 스케줄을 삭제합니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.

2. 스냅샷 정합성 보장 그룹 * 탭을 선택합니다.
3. 삭제할 스냅샷 정합성 보장 그룹을 선택한 다음, 메뉴(Uncommon Tasks[Delete])를 선택합니다.

   스냅샷 정합성 보장 그룹 삭제 확인 대화 상자가 나타납니다.

4. 이 작업을 수행할지 확인한 다음 * 삭제 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스냅샷 정합성 보장 그룹에서 기존 스냅샷 이미지와 스냅샷 볼륨을 모두 삭제합니다.
- 스냅샷 정합성 보장 그룹의 각 구성원 볼륨에 대해 존재하는 모든 연결된 스냅샷 이미지를 삭제합니다.
- 스냅샷 정합성 보장 그룹의 각 구성원 볼륨에 대해 존재하는 연결된 스냅샷 볼륨을 모두 삭제합니다.
- 스냅샷 정합성 보장 그룹의 각 구성원 볼륨에 대해 연결된 모든 예약된 용량을 삭제합니다(선택된 경우).

스냅샷 볼륨 관리

스냅샷 볼륨을 읽기-쓰기 모드로 변환합니다

필요한 경우 읽기 전용 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 읽기-쓰기 모드로 변환할 수 있습니다.

읽기-쓰기 액세스가 가능하도록 변환된 스냅샷 볼륨에는 고유한 예약 용량이 포함되어 있습니다. 이 용량은 참조된 스냅샷 이미지에 영향을 주지 않고 호스트 애플리케이션이 수정한 후속 사항을 기본 볼륨에 저장하는 데 사용됩니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.

   Snapshot Volumes 테이블이 나타나고 스토리지 어레이와 연결된 모든 스냅샷 볼륨이 표시됩니다.

3. 변환할 읽기 전용 스냅샷 볼륨을 선택한 다음 * 읽기/쓰기로 변환 * 을 클릭합니다.

   읽기/쓰기로 변환 대화 상자에 * 용량 예약 * 단계가 활성화된 상태로 나타납니다. 볼륨 후보 테이블에는 지정된 예약 용량을 지원하는 후보만 표시됩니다.

4. 읽기-쓰기 스냅샷 볼륨에 예약된 용량을 할당하려면 다음 작업 중 하나를 수행합니다.
   - * 기본 설정 수락 * — 이 권장 옵션을 사용하여 스냅샷 볼륨에 예약된 용량을 기본 설정으로 할당합니다.
   - * 데이터 스토리지 요구 사항에 맞게 예약된 용량 설정 할당 * — 다음 지침에 따라 예약된 용량을 할당합니다.
     - 예약된 용량의 기본 설정은 기본 볼륨 용량의 40%이며 일반적으로 이 용량이면 충분합니다.
     - 필요한 용량은 볼륨에 대한 I/O 쓰기의 빈도 및 크기에 따라 달라집니다.
5. 설정을 검토하거나 편집하려면 * 다음 * 을 선택하십시오.

   설정 편집 대화 상자가 나타납니다.

6. 스냅샷 볼륨에 대한 설정을 적절히 수락하거나 지정한 다음 * 마침 * 을 선택하여 스냅샷 볼륨을 변환합니다.

필드 상세정보

설정	설명
• 예약된 용량 설정 *	다음 경우에 알림:

스냅샷 볼륨의 볼륨 설정을 변경합니다

스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨에 대한 설정을 변경하여 스냅샷 볼륨 이름을 바꾸거나, SSD 캐싱을 활성화 또는 비활성화하거나, 호스트, 호스트 클러스터 또는 LUN(Logical Unit Number) 할당을 변경할 수 있습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 클릭합니다.
3. 변경할 스냅샷 볼륨을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   Snapshot Volume Settings(스냅샷 볼륨 설정) 대화 상자가 나타납니다.

4. 스냅샷 볼륨에 대한 설정을 적절히 보거나 편집합니다.

필드 상세정보

설정	설명
• 스냅샷 볼륨 *	이름
스냅샷 볼륨의 이름을 변경할 수 있습니다.	할당 대상
스냅샷 볼륨에 대한 호스트 또는 호스트 클러스터 할당을 변경할 수 있습니다.	LUN입니다
스냅샷 볼륨에 대한 LUN 할당을 변경할 수 있습니다.	SSD 캐시
SSD(Solid State Disk)에서 읽기 전용 캐싱을 설정/해제할 수 있습니다.	• 관련 개체 *
스냅샷 이미지	스냅샷 볼륨과 연결된 스냅샷 이미지를 볼 수 있습니다. 스냅샷 이미지는 특정 시점에 캡처된 볼륨 데이터의 논리적 복사본입니다. 복원 지점과 마찬가지로 스냅샷 이미지를 통해 알려진 양호한 데이터 집합으로 롤백할 수 있습니다. 호스트가 스냅샷 이미지를 액세스할 수는 있지만 해당 이미지를 직접 읽거나 쓸 수는 없습니다.
기본 볼륨	스냅샷 볼륨과 연결된 기본 볼륨을 볼 수 있습니다. 기본 볼륨은 스냅샷 이미지가 생성되는 원본입니다. 일반 볼륨이거나 씬 볼륨일 수 있으며 일반적으로 호스트에 할당됩니다. 기본 볼륨은 볼륨 그룹 또는 디스크 풀에 상주할 수 있습니다.
스냅샷 그룹	스냅샷 볼륨과 연결된 스냅샷 그룹을 볼 수 있습니다. 스냅샷 그룹은 단일 기본 볼륨의 스냅샷 이미지 모음입니다.

스냅샷 볼륨을 복사합니다

스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨에서 볼륨 복제 프로세스를 수행할 수 있습니다.

이 작업에 대해

일반 볼륨 복사 작업에서 수행하는 것처럼 스냅샷 볼륨을 타겟 볼륨에 복사할 수 있습니다. 그러나 복제 볼륨 프로세스 중에는 스냅샷 볼륨을 온라인 상태로 유지할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.

   Snapshot Volumes 테이블이 나타나고 스토리지 어레이와 연결된 모든 스냅샷 볼륨이 표시됩니다.

3. 복사할 스냅샷 볼륨을 선택한 다음 * 볼륨 복사 * 를 선택합니다.

   Copy Volume(볼륨 복사) 대화 상자가 나타나고 대상을 선택하라는 메시지가 나타납니다.

4. 복사 대상으로 사용할 타겟 볼륨을 선택한 다음 * 마침 * 을 클릭합니다.

스냅샷 볼륨을 다시 생성합니다

이전에 해제한 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 다시 생성할 수 있습니다. 스냅샷 볼륨을 다시 생성하는 데 새 볼륨을 생성하는 것보다 시간이 적게 소요됩니다.

시작하기 전에

- 스냅샷 볼륨은 Optimal(최적) 또는 Disabled(비활성화) 상태여야 합니다.
- 모든 구성원 스냅샷 볼륨은 사용 안 함 상태여야 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 다시 생성할 수 있습니다.

이 작업에 대해

개별 구성원 스냅샷 볼륨을 다시 생성할 수 없습니다. 전체 스냅샷 정합성 보장 그룹 스냅샷 볼륨만 다시 생성할 수 있습니다.

> 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨이 온라인 복제 관계의 일부인 경우 볼륨에 대해 다시 생성 옵션을 수행할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.

   Snapshot Volumes 테이블이 나타나고 스토리지 어레이와 연결된 모든 스냅샷 볼륨이 표시됩니다.

3. 다시 생성할 스냅샷 볼륨을 선택한 다음 메뉴(Uncommon Tasks[recreate])를 선택합니다.

   스냅샷 볼륨 다시 생성 대화 상자가 나타납니다.

4. 다음 옵션 중 하나를 선택합니다.
   - * 볼륨 <name> * 에서 생성된 기존 스냅샷 이미지입니다

     스냅샷 볼륨을 다시 생성할 기존 스냅샷 이미지를 나타내려면 이 옵션을 선택합니다.

   - * 볼륨 <name> * 의 새(즉시) 스냅샷 이미지

     스냅샷 볼륨을 다시 생성할 새 스냅샷 이미지를 생성하려면 이 옵션을 선택합니다.

5. 재생성 * 을 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 연결된 스냅샷 저장소 볼륨의 모든 `write` 데이터를 삭제합니다.
- 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨 매개 변수는 이전에 비활성화된 볼륨 매개 변수와 동일하게 유지됩니다.
- 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨의 원래 이름을 유지합니다.

스냅샷 볼륨을 비활성화합니다

스냅샷 정합성 보장 그룹이 더 이상 필요하지 않거나 일시적으로 사용을 중지하려는 경우 스냅샷 볼륨 또는 스냅샷 볼륨을 비활성화할 수 있습니다.

이 작업에 대해

다음 조건 중 하나가 적용되는 경우 비활성화 옵션을 사용합니다.

- 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨 사용을 마쳤습니다.
- 나중에 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨(읽기-쓰기로 지정됨)을 다시 생성하려고 하며 다시 생성할 필요가 없도록 관련 예약 용량을 유지하려는 경우
- 읽기-쓰기 스냅샷 볼륨에 대한 쓰기 작업을 중지하여 스토리지 시스템 성능을 높이려는 경우

스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨이 읽기/쓰기로 지정된 경우 이 옵션을 사용하여 연결된 예약된 용량 볼륨에 대한 추가 쓰기 작업을 중지할 수도 있습니다. 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 다시 생성하려는 경우 동일한 기본 볼륨에서 스냅샷 이미지를 선택해야 합니다.

스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨이 온라인 복제 관계의 일부인 경우 볼륨에 대해 Disable 옵션을 수행할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.

   System Manager는 스토리지 배열에 연결된 모든 스냅샷 볼륨을 표시합니다.
3. 비활성화할 스냅샷 볼륨을 선택한 다음 메뉴(Uncommon Tasks[Disable])를 선택합니다.
4. 작업을 수행할지 확인한 다음 * Disable * 을 클릭합니다.

결과

- 스냅샷 볼륨은 기본 볼륨과 연결되어 있습니다.
- 스냅샷 볼륨은 WWN(World Wide Name)을 유지합니다.
- 읽기-쓰기일 경우 스냅샷 볼륨은 연결된 예약 용량을 유지합니다.
- 스냅샷 볼륨은 호스트 할당 및 액세스를 유지합니다. 그러나 읽기-쓰기 요청은 실패합니다.
- 스냅샷 볼륨과 스냅샷 이미지의 연결이 끊어집니다.

스냅샷 볼륨을 삭제합니다

백업 또는 소프트웨어 애플리케이션 테스트를 위해 더 이상 필요하지 않은 스냅샷 볼륨 또는 스냅샷 정합성 보장 그룹 스냅샷 볼륨을 삭제할 수 있습니다.

또한 스냅샷 볼륨과 연결된 스냅샷 예약 용량 볼륨을 삭제하거나 스냅샷 예약 용량 볼륨을 할당되지 않은 볼륨으로 유지할지 여부를 지정할 수 `read-write` 있습니다.

이 작업에 대해

기본 볼륨을 삭제하면 연결된 스냅샷 볼륨 또는 정합성 보장 그룹 스냅샷 볼륨이 자동으로 삭제됩니다. 볼륨 복사본의 스냅샷 볼륨은 * In Progress *(진행 중 *) 상태인 경우 삭제할 수 없습니다.

단계

1. 스토리지 [스냅샷] 메뉴를 선택합니다.
2. Snapshot Volumes * 탭을 선택합니다.

   System Manager는 스토리지 배열에 연결된 모든 스냅샷 볼륨을 표시합니다.
3. 삭제할 스냅샷 볼륨을 선택한 다음 메뉴(Uncommon Tasks[Delete])를 선택합니다.
4. 작업을 수행할지 확인한 다음 * 삭제 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 모든 구성원 스냅샷 볼륨을 삭제합니다(스냅샷 정합성 보장 그룹 스냅샷 볼륨용).
- 연결된 모든 호스트 할당을 제거합니다.

FAQ 를 참조하십시오

내 볼륨, 호스트 또는 호스트 클러스터가 모두 표시되지 않는 이유는 무엇입니까?

DA 지원 기본 볼륨이 있는 스냅샷 볼륨은 DA(Data Assurance) 기능이 지원되지 않는 호스트에 할당할 수 없습니다. DA를 사용할 수 없는 호스트에 스냅샷 볼륨을 할당하기 전에 기본 볼륨에서 DA를 비활성화해야 합니다.

스냅샷 볼륨을 할당할 호스트에 대한 다음 지침을 고려하십시오.

- DA를 사용할 수 없는 입출력 인터페이스를 통해 스토리지 시스템에 접속된 호스트의 경우 DA를 사용할 수 없습니다.
- DA를 사용할 수 없는 호스트 구성원이 하나 이상 있는 경우 호스트 클러스터를 DA를 사용할 수 없습니다.

> ⓘ 스냅샷과 연결된 볼륨(정합성 보장 그룹, 스냅샷 그룹, 스냅샷 이미지 및 스냅샷 볼륨), 볼륨 복제본에서는 DA를 비활성화할 수 없습니다. 있습니다. 기본 볼륨에서 DA를 비활성화하기 전에 관련된 모든 예약 용량 및 스냅샷 객체를 삭제해야 합니다.

스냅샷 이미지란 무엇입니까?

스냅샷 이미지는 특정 시점에 캡처된 볼륨 콘텐츠의 논리적 복사본입니다. 스냅샷 이미지는 최소한의 저장 공간을 사용합니다.

스냅샷 이미지 데이터는 다음과 같이 저장됩니다.

- 스냅샷 이미지가 생성되면 기본 볼륨과 정확히 일치합니다. 스냅샷이 생성된 후 기본 볼륨의 블록 또는 블록 세트에 대해 첫 번째 쓰기 요청이 발생하면 새 데이터가 기본 볼륨에 쓰기되기 전에 원래 데이터가 스냅샷 예약 용량에 복사됩니다.
- 후속 스냅샷에는 첫 번째 스냅샷 이미지가 생성된 이후 변경된 데이터 블록만 포함됩니다. 이후의 각 COW(Copy-On-Write) 작업은 새 데이터를 기본 볼륨에 쓰기 전에 기본 볼륨에서 덮어쓰려고 하는 원본 데이터를 스냅샷 예약 용량에 저장합니다.

스냅샷 이미지를 사용하는 이유

스냅샷을 사용하여 실수로 또는 악의적으로 데이터가 손실되거나 손상되지 않도록 보호하고 복구할 수 있습니다.

스냅샷 정합성 보장 그룹이라고 하는 기본 볼륨 또는 기본 볼륨 그룹을 선택한 후 다음 방법 중 하나 이상으로 스냅샷 이미지를 캡처합니다.

- 단일 기본 볼륨의 스냅샷 이미지 또는 여러 기본 볼륨으로 구성된 스냅샷 정합성 보장 그룹을 생성할 수 있습니다.
- 스냅샷을 수동으로 생성하거나 기본 볼륨 또는 스냅샷 정합성 보장 그룹에 대한 스케줄을 생성하여 주기적 스냅샷 이미지를 자동으로 캡처할 수 있습니다.
- 스냅샷 이미지의 호스트 액세스 가능 스냅샷 볼륨을 생성할 수 있습니다.
- 롤백 작업을 수행하여 스냅샷 이미지를 복구할 수 있습니다.

시스템은 여러 스냅샷 이미지를 복원 지점으로 유지하며, 특정 시점에 알려진 양호한 데이터 세트로 롤백하는 데 사용할 수 있습니다. 롤백 기능을 사용하면 실수로 인한 데이터 삭제 및 데이터 손상을 방지할 수 있습니다.

스냅숏에 사용할 수 있는 볼륨의 종류는 무엇입니까?

표준 볼륨과 씬 볼륨은 스냅샷 이미지를 저장하는 데 사용할 수 있는 유일한 볼륨 유형입니다. 비표준 볼륨은 사용할 수 없습니다. 기본 볼륨은 풀 또는 볼륨 그룹에 상주할 수 있습니다.

스냅샷 정합성 보장 그룹을 생성하는 이유는 무엇입니까?

스냅샷 정합성 보장 그룹은 여러 볼륨에서 동시에 스냅샷 이미지를 생성하려는 경우에 생성됩니다.

예를 들어, 복구를 위해 일관성을 유지해야 하는 여러 볼륨으로 구성된 데이터베이스의 경우 모든 볼륨의 조정된 스냅샷을 수집하여 전체 데이터베이스를 복원하는 데 사용하려면 스냅샷 정합성 보장 그룹이 필요합니다.

스냅샷 정합성 보장 그룹에 포함된 볼륨을 _member volumes_라고 합니다.

스냅샷 정합성 보장 그룹에 대해 다음 스냅샷 작업을 수행할 수 있습니다.

- 구성원 볼륨의 동시 이미지를 가져올 스냅샷 정합성 보장 그룹의 스냅샷 이미지를 생성합니다.

- 구성원 볼륨의 주기적인 동시 이미지를 자동으로 캡처할 스냅샷 정합성 보장 그룹의 스케줄을 생성합니다.
- 스냅샷 정합성 보장 그룹 이미지의 호스트 액세스 가능 스냅샷 볼륨을 생성합니다.
- 스냅샷 정합성 보장 그룹에 대해 롤백 작업을 수행합니다.

스냅샷 볼륨이란 무엇이며 예약 용량은 언제 필요합니까?

스냅샷 볼륨을 사용하면 호스트가 스냅샷 이미지의 데이터에 액세스할 수 있습니다. 스냅샷 볼륨에는 원래 스냅샷 이미지에 영향을 주지 않고 기본 볼륨에 대한 수정 사항을 저장하는 자체 예약 용량이 포함되어 있습니다. 스냅샷 이미지는 호스트에서 읽기 또는 쓰기 액세스가 지원되지 않습니다. 스냅샷 데이터를 읽거나 쓰려면 스냅샷 볼륨을 생성하여 호스트에 할당합니다.

두 가지 유형의 스냅샷 볼륨을 생성할 수 있습니다. 스냅샷 볼륨의 유형에 따라 예약된 용량을 사용할지 여부가 결정됩니다.

- * 읽기 전용 * — 읽기 전용으로 생성된 스냅샷 볼륨은 호스트 응용 프로그램에 스냅샷 이미지에 포함된 데이터 복제본에 대한 읽기 액세스 권한을 제공합니다. 읽기 전용 스냅샷 볼륨은 예약된 용량을 사용하지 않습니다.
- * 읽기-쓰기 * — 읽기-쓰기로 생성된 스냅샷 볼륨을 사용하면 참조된 스냅샷 이미지에 영향을 주지 않고 스냅샷 볼륨을 변경할 수 있습니다. 읽기-쓰기 스냅샷 볼륨은 예약된 용량을 사용하여 이러한 변경 사항을 저장합니다. 언제든지 읽기 전용 스냅샷 볼륨을 읽기-쓰기로 변환할 수 있습니다.

스냅샷 그룹이란 무엇입니까?

스냅샷 그룹은 연결된 단일 기본 볼륨의 시점 스냅샷 이미지 모음입니다.

System Manager는 스냅샷 이미지를 _ 스냅샷 그룹 _ 으로 구성합니다. 스냅샷 그룹은 사용자 작업이 필요하지 않지만 언제든지 스냅샷 그룹의 예약된 용량을 조정할 수 있습니다. 또한 다음 조건이 충족되면 예약된 용량을 생성하라는 메시지가 표시될 수 있습니다.

- 아직 스냅샷 그룹이 없는 기본 볼륨의 스냅샷을 생성할 때마다 System Manager는 자동으로 스냅샷 그룹을 생성합니다. 이렇게 하면 후속 스냅샷 이미지를 저장하는 데 사용되는 기본 볼륨에 예약된 용량이 생성됩니다.
- 기본 볼륨에 대한 스냅샷 스케줄을 생성할 때마다 System Manager가 자동으로 스냅샷 그룹을 생성합니다.

스냅샷 볼륨을 사용하지 않도록 설정하는 이유는 무엇입니까?

스냅샷 이미지에 다른 스냅샷 볼륨을 할당하려는 경우 스냅샷 볼륨을 사용하지 않도록 설정합니다. 비활성화된 스냅샷 볼륨을 나중에 사용할 수 있도록 예약할 수 있습니다.

스냅샷 볼륨이나 정합성 보장 그룹 스냅샷 볼륨이 더 이상 필요하지 않고 나중에 다시 생성하지 않으려는 경우 볼륨을 사용하지 않도록 설정하는 대신 삭제해야 합니다.

사용 안 함 상태란 무엇입니까?

사용 안 함 상태의 스냅샷 볼륨은 현재 스냅샷 이미지에 할당되어 있지 않습니다. 스냅샷 볼륨을 활성화하려면 다시 생성 작업을 사용하여 비활성화된 스냅샷 볼륨에 새 스냅샷 이미지를 할당해야 합니다.

스냅샷 볼륨 특성은 할당된 스냅샷 이미지에 의해 정의됩니다. 읽기-쓰기 작업은 비활성화 상태의 스냅샷 볼륨에서 일시 중단됩니다.

스냅샷 스케줄을 일시 중지하는 이유는 무엇입니까**?**

스케줄이 일시 중지되면 예약된 스냅샷 이미지 생성이 수행되지 않습니다. 스토리지 공간을 절약하기 위해 스냅샷 스케줄을 일시 중지한 다음 나중에 예약된 스냅샷을 다시 시작할 수 있습니다.

스냅샷 스케줄이 필요하지 않은 경우 스케줄을 일시 중지하는 대신 삭제해야 합니다.

미러링

개요

비동기식 미러링 개요

비동기 미러링 기능은 로컬 스토리지 어레이와 원격 스토리지 시스템 간의 데이터 복제를 위한 컨트롤러 수준의 펌웨어 기반 메커니즘을 제공합니다.

비동기식 미러링이란 무엇입니까**?**

Asynchronous Mirroring 는 특정 시점에 기본 볼륨의 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사합니다. 운영 사이트를 즉시 업데이트할 수 있으며 대역폭이 허용할 경우 보조 사이트를 업데이트할 수 있습니다. 네트워크 리소스를 사용할 수 있게 되면 정보가 캐시되어 나중에 전송됩니다.

비동기 미러링은 볼륨별로 생성되지만 그룹 수준에서 관리되므로 특정 스토리지 배열의 운영 볼륨과 별도의 원격 미러링된 볼륨을 연결할 수 있습니다. 이러한 유형의 미러링은 무중단 운영에 대한 요구를 충족하는 데 이상적이며 일반적으로 정기적인 프로세스에 대해 훨씬 더 네트워크 효율적입니다.

자세한 내용:

- "비동기식 미러링의 작동 방식"
- "비동기식 미러링 용어"
- "비동기식 미러 상태입니다"
- "볼륨 소유권"
- "미러 정합성 보장 그룹의 역할 변경"

비동기식 미러링을 구성하려면 어떻게 합니까**?**

Unified Manager 인터페이스를 사용하여 어레이 간 초기 미러링 구성을 수행해야 합니다. 구성이 완료되면 System Manager에서 미러링된 쌍과 일관성 그룹을 관리할 수 있습니다.

자세한 내용:

- "비동기 미러링 사용에 대한 요구 사항"
- "볼륨을 비동기적으로 미러링하는 워크플로"
- "Unified Manager에서 비동기 미러링된 쌍 생성"

관련 정보

비동기 미러링과 관련된 개념에 대해 자세히 알아보십시오.

- "미러 정합성 보장 그룹을 생성하기 전에 알아야 할 사항"
- "대칭 복사 쌍을 만들기 전에 알아야 할 사항"
- "비동기식 미러링과 동기식 미러링의 차이점"

동기 미러링 개요

동기 미러링 기능은 원격 사이트 간에 스토리지 어레이 간에 온라인, 실시간 데이터 복제를 제공합니다.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

동기식 미러링이란 무엇입니까?

Synchronous 미러링 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다. 스토리지 어레이 컨트롤러는 미러링 작업을 관리하는데, 이 작업은 호스트 시스템과 소프트웨어 애플리케이션에 영향을 미치지 않습니다.

이러한 유형의 미러링은 재해 복구와 같은 비즈니스 연속성 목적으로 이상적입니다.

자세한 내용:

- "동기 미러링의 작동 방식"
- "동기 미러링 용어"
- "동기 미러링 상태"
- "볼륨 소유권"
- "미러링된 쌍의 볼륨 간 역할 변경"

동기식 미러링은 어떻게 구성합니까?

Unified Manager 인터페이스를 사용하여 어레이 간 초기 미러링 구성을 수행해야 합니다. 구성이 완료되면 System Manager에서 미러링된 쌍을 관리할 수 있습니다.

자세한 내용:

- "동기 미러링 사용에 대한 요구 사항"
- "볼륨을 동기식으로 미러링하기 위한 워크플로우"
- "동기식 미러링 쌍 생성(Unified Manager에서)"

관련 정보

동기식 미러링과 관련된 개념에 대해 자세히 알아보십시오.

- "대칭 복사 쌍을 만들기 전에 알아야 할 사항"
- "비동기식 미러링과 동기식 미러링의 차이점"

비동기 개념

비동기식 미러링의 작동 방식

비동기식 미러링은 데이터 볼륨을 필요 시 또는 일정에 따라 복제하여 데이터 손상 또는 손실로 인한 다운타임을 최소화 또는 방지합니다.

비동기식 미러링은 특정 시점에 기본 볼륨의 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사합니다. 운영 사이트를 즉시 업데이트할 수 있으며 대역폭이 허용할 경우 보조 사이트를 업데이트할 수 있습니다. 네트워크 리소스를 사용할 수 있게 되면 정보가 캐시되어 나중에 전송됩니다.

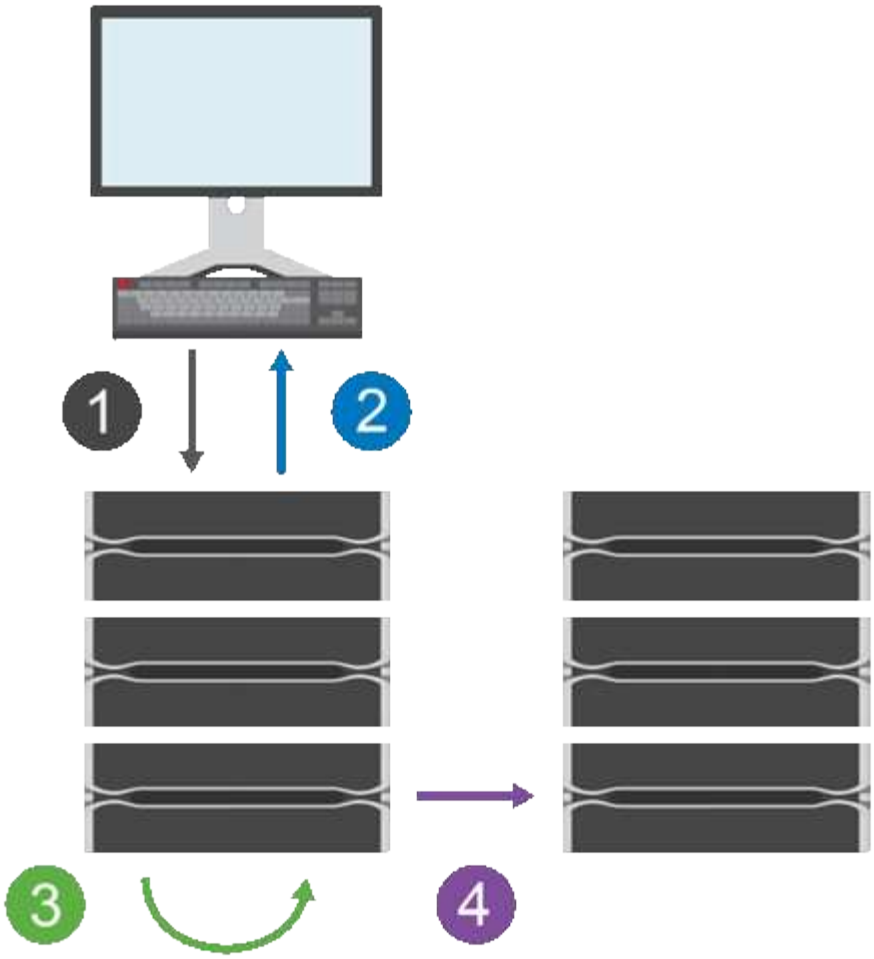
이러한 유형의 미러링은 무중단 운영에 대한 요구를 충족하는 데 이상적이며, 일반적으로 백업 및 아카이브 같은 주기적인 프로세스에 대해 훨씬 더 네트워크 효율적입니다. 비동기식 미러링을 사용하는 이유는 다음과 같습니다.

- 원격 백업 통합.
- 로컬 또는 광역 재해로부터 보호
- 라이브 데이터의 특정 시점 이미지에서 애플리케이션 개발 및 테스트

비동기식 미러링 세션

비동기식 미러링은 특정 시점에 기본 볼륨의 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사합니다. 비동기식 미러링을 통해 운영 사이트를 즉시 업데이트하고 대역폭이 허용할 경우 2차 사이트를 업데이트할 수 있습니다. 네트워크 리소스를 사용할 수 있게 되면 정보가 캐시되어 나중에 전송됩니다.

액티브 비동기식 미러링 세션에는 4가지 기본 단계가 있습니다.



1. 쓰기 작업은 먼저 운영 볼륨의 스토리지 시스템에서 수행됩니다.
2. 작업 상태가 호스트로 반환됩니다.
3. 운영 볼륨의 모든 변경 사항이 기록되고 추적됩니다.
4. 모든 변경 사항은 백그라운드 프로세스로 보조 볼륨의 스토리지 어레이에 전송됩니다.

이러한 단계는 정의된 동기화 간격에 따라 반복되거나 간격이 정의되지 않은 경우 수동으로 반복할 수 있습니다.

비동기식 미러링은 설정된 간격으로만 데이터를 원격 사이트로 전송하므로, 로컬 I/O는 느린 네트워크 연결의 영향을 거의 받지 않습니다. 이 전송은 로컬 I/O에 연결되지 않으므로 애플리케이션 성능에 영향을 주지 않습니다. 따라서 비동기식 미러링은 iSCSI와 같은 느린 연결을 사용하고 로컬 스토리지 시스템과 원격 스토리지 시스템 간의 장거리 연결을 통해 실행될 수 있습니다.

스토리지 어레이의 펌웨어 버전은 최소한 7.84여야 합니다. (각 OS 버전은 서로 다를 수 있음)

정합성 보장 그룹 및 미러링된 페어 미러링

미러 정합성 보장 그룹을 생성하여 로컬 스토리지와 원격 스토리지 시스템 간의 미러링 관계를 설정합니다. 비동기식 미러링 관계는 미러링된 쌍으로 구성되며, 한 스토리지 어레이의 운영 볼륨과 다른 스토리지 어레이의 보조 볼륨으로 구성됩니다.

운영 볼륨이 포함된 스토리지 배열은 대개 운영 사이트에 있으며 활성 호스트를 제공합니다. 보조 볼륨이 포함된 스토리지 배열은 일반적으로 보조 사이트에 있으며 데이터 복제본을 보관합니다. 일반적으로 보조 볼륨에는 데이터의 백업 복사본이 포함되어 있으며 재해 복구에 사용됩니다.

동기화 설정

미러링된 페어를 생성할 때 통신 중단 후 미러링된 페어가 재동기화 작업을 완료하는 데 사용하는 동기화 우선 순위 및 재동기화 정책도 정의합니다.

미러 정합성 보장 그룹을 생성할 때 그룹 내의 모든 미러링된 페어에 대한 동기화 우선 순위 및 재동기화 정책도 정의합니다. 미러링된 페어는 동기화 우선 순위 및 재동기화 정책을 사용하여 통신이 중단된 후 재동기화 작업을 완료합니다.

운영 볼륨의 스토리지 배열이 보조 볼륨에 데이터를 쓸 수 없을 경우 미러링된 쌍의 운영 볼륨과 보조 볼륨의 동기화가 해제됩니다. 이 문제는 다음과 같은 문제로 인해 발생할 수 있습니다.

- 로컬 스토리지와 원격 스토리지 시스템 간의 네트워크 문제입니다.
- 장애가 발생한 보조 볼륨입니다.
- 동기화가 미러링된 쌍에서 수동으로 일시 중단됩니다.
- 미러 그룹 역할 충돌

원격 스토리지 배열의 데이터를 수동 또는 자동으로 동기화할 수 있습니다.

예약된 용량 및 비동기식 미러링

예약된 용량은 동기화가 발생하지 않을 때 운영 볼륨과 보조 볼륨 간의 차이를 추적하는 데 사용됩니다. 또한 각 미러링된 쌍에 대한 동기화 통계를 추적합니다.

미러링된 쌍의 각 볼륨은 고유한 예약 용량을 필요로 합니다.

구성 및 관리

두 어레이 간에 미러링을 설정하고 구성하려면 Unified Manager 인터페이스를 사용해야 합니다. 미러링이 활성화되면 System Manager에서 미러링된 쌍과 동기화 설정을 관리할 수 있습니다.

비동기식 미러링 용어

비동기 미러링 조건이 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
로컬 스토리지 시스템입니다	로컬 스토리지 배열은 사용자가 수행하는 스토리지 배열입니다. Local Role 열에 * Primary * 가 표시되면 스토리지 배열에 미러 관계에서 1차 역할을 가진 볼륨이 포함되어 있음을 나타냅니다. Local Role 열에 * Secondary * 가 표시되면 스토리지 배열에 미러 관계에서 보조 역할을 가진 볼륨이 포함되어 있음을 나타냅니다.
미러 정합성 보장 그룹	미러 정합성 보장 그룹은 하나 이상의 미러링된 쌍에 대한 컨테이너입니다. 비동기식 미러링 작업의 경우 미러 정합성 보장 그룹을 생성해야 합니다.

기간	설명
미러링 쌍	미러링된 쌍은 기본 볼륨 및 보조 볼륨이라는 두 개의 볼륨으로 구성됩니다. 비동기식 미러링에서는 미러링된 쌍이 항상 미러 정합성 보장 그룹에 속합니다. 쓰기 작업은 먼저 운영 볼륨에 대해 수행된 다음 보조 볼륨에 복제됩니다. 미러 정합성 보장 그룹의 미러링된 각 쌍은 동일한 동기화 설정을 공유합니다.
운영 볼륨	미러링된 쌍의 기본 볼륨은 미러링될 소스 볼륨입니다.
원격 스토리지 시스템	원격 스토리지 시스템은 일반적으로 미러링 구성의 데이터 복제본을 보관하는 보조 사이트로 지정됩니다.
예약된 용량입니다	예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.
역할 변경	역할 변경 시 보조 볼륨에 기본 역할이 할당되며, 그 반대의 경우도 마찬가지입니다.
2차 볼륨	미러링된 쌍의 보조 볼륨은 일반적으로 보조 사이트에 위치하며 데이터 복제본을 보관합니다.
동기화	동기화는 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화에서 수행됩니다. 동기화는 통신 중단 후 운영 볼륨과 2차 볼륨의 동기화가 중단된 경우에도 발생합니다. 통신 링크가 다시 작동되면 복제되지 않은 모든 데이터가 보조 볼륨의 스토리지 시스템에 동기화됩니다.

볼륨을 비동기적으로 미러링하는 워크플로

다음 워크플로우를 사용하여 비동기식 미러링을 구성합니다.

1. Unified Manager에서 초기 구성을 수행합니다.
   a. 로컬 스토리지 배열을 데이터 전송 소스로 선택합니다.
   b. 로컬 스토리지의 운영 볼륨과 원격 스토리지의 보조 볼륨을 위한 컨테이너인 기존 미러 정합성 보장 그룹을 생성하거나 선택합니다. 운영 볼륨과 보조 볼륨을 "미러링된 페어"라고 합니다. 미러 정합성 보장 그룹을 처음으로 생성하는 경우 수동 동기화 또는 예약된 동기화를 수행할지 여부를 지정합니다.
   c. 로컬 스토리지 어레이에서 운영 볼륨을 선택한 다음 예약된 용량을 확인합니다. 예약된 용량은 복제 작업에 사용할 물리적 할당 용량입니다.
   d. 원격 스토리지 시스템을 전송 대상, 보조 볼륨으로 선택한 다음 예약된 용량을 결정합니다.
   e. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기 전송에 몇 시간이 걸릴 수 있습니다.
2. 초기 동기화 진행률을 확인합니다.
   a. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
   b. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다.

3. * 선택 사항: * System Manager에서 후속 데이터 전송을 다시 예약하거나 수동으로 수행할 수 있습니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.

> 비동기식 복제는 정기적으로 수행되므로 시스템에서 변경된 블록을 통합하고 네트워크 대역폭을 보존할 수 있습니다. 쓰기 처리량과 쓰기 지연 시간에 미치는 영향은 미미합니다.

비동기 미러링 사용에 대한 요구 사항

비동기식 미러링을 사용하려는 경우 다음 요구사항을 염두에 두십시오.

Unified Manager를 참조하십시오

두 어레이 간에 미러링을 설정하고 구성하려면 Unified Manager 인터페이스를 사용해야 합니다. Unified Manager는 웹 서비스 프록시와 함께 호스트 시스템에 설치됩니다.

- 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
- Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
- Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

지원합니다

- 두 개의 스토리지 어레이가 있어야 합니다.
- 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
- Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
- 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
- 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
- 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
- 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
- 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.

지원되는 연결입니다

비동기 미러링은 FC 또는 iSCSI 연결을 사용하거나 둘 다 로컬 및 원격 스토리지 시스템 간의 통신에 사용할 수 있습니다. 미러 정합성 보장 그룹을 생성할 때 관리자는 둘 다 원격 스토리지 시스템에 접속된 경우 해당 그룹에 대해 FC 또는 iSCSI를 선택할 수 있습니다. 한 채널 유형에서 다른 채널 유형으로 대체 작동이 없습니다.

비동기식 미러링은 스토리지 시스템의 호스트 측 I/O 포트를 사용하여 미러링된 데이터를 운영 측에서 2차 측으로 전달합니다.

- * 파이버 채널(FC) 인터페이스를 통한 미러링 *

  스토리지 어레이의 각 컨트롤러는 가장 높은 번호가 지정된 FC 호스트 포트를 미러링 작업에 사용합니다.

컨트롤러에 기본 FC 포트와 HIC(호스트 인터페이스 카드) FC 포트가 모두 있는 경우 가장 높은 번호가 지정된 포트가 HIC에 있습니다. 전용 포트에 로그온한 호스트는 로그아웃되며 호스트 로그인 요청은 허용되지 않습니다. 이 포트의 I/O 요청은 미러링 작업에 사용되는 컨트롤러에서만 허용됩니다.

전용 미러링 포트는 디렉토리 서비스 및 네임 서비스 인터페이스를 지원하는 FC 패브릭 환경에 연결해야 합니다. 특히 FC-AL 및 지점 간 연결 옵션은 미러 관계에 참여하는 컨트롤러 간의 연결 옵션으로 지원되지 않습니다.

- * iSCSI 인터페이스를 통한 미러링 *

  FC와 달리 iSCSI에는 전용 포트가 필요하지 않습니다. iSCSI 환경에서 비동기 미러링을 사용하는 경우 비동기 미러링에 사용하기 위해 스토리지 어레이의 프런트 엔드 iSCSI 포트 중 하나를 전용으로 지정할 필요가 없습니다. 이러한 포트는 비동기 미러 트래픽과 호스트-스토리지 I/O 연결을 위해 모두 공유됩니다.

  컨트롤러는 iSCSI 이니시에이터가 세션을 설정하려고 시도하는 원격 스토리지 시스템의 목록을 유지합니다. iSCSI 연결을 성공적으로 설정하는 첫 번째 포트는 해당 원격 스토리지 시스템과의 이후의 모든 통신에 사용됩니다. 통신이 실패하면 사용 가능한 모든 포트를 사용하여 새 세션이 시도됩니다.

  iSCSI 포트는 포트별로 어레이 레벨에서 구성됩니다. 구성 메시징 및 데이터 전송을 위한 컨트롤러 간 통신은 다음 설정을 포함한 글로벌 설정을 사용합니다.

  - VLAN: 로컬 시스템과 원격 시스템 모두 동일한 VLAN 설정을 사용하여 통신해야 합니다
  - iSCSI 수신 포트입니다
  - 점보 프레임
  - 이더넷 우선 순위

  > ⓘ iSCSI 인터컨트롤러 통신은 관리 이더넷 포트가 아닌 호스트 연결 포트를 사용해야 합니다.

  비동기식 미러링은 스토리지 시스템의 호스트 측 I/O 포트를 사용하여 미러링된 데이터를 운영 측에서 2차 측으로 전달합니다. 비동기 미러링은 대기 시간이 더 짧고 비용이 저렴한 네트워크에 사용하기 때문에 iSCSI(TCP/IP 기반) 연결이 적합합니다. iSCSI 환경에서 비동기 미러링을 사용하는 경우 비동기 미러링에 사용하기 위해 어레이의 프런트 엔드 iSCSI 포트 중 하나를 전용으로 지정할 필요가 없습니다. 이러한 포트는 비동기 미러 트래픽과 호스트-스토리지 I/O 연결을 위해 모두 공유됩니다

미러링 볼륨 후보

- RAID 레벨, 캐싱 매개 변수 및 세그먼트 크기는 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨에서 서로 다를 수 있습니다.

  > ⓘ EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

- 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.
- 볼륨은 하나의 미러 관계에만 참여할 수 있습니다.
- 볼륨 후보는 동일한 데이터 보안 기능을 공유해야 합니다.
  - 기본 볼륨이 FIPS를 지원할 수 있는 경우 보조 볼륨은 FIPS를 지원할 수 있어야 합니다.
  - 기본 볼륨이 FDE를 지원할 수 있는 경우 보조 볼륨은 FDE를 지원할 수 있어야 합니다.

◦ 주 볼륨이 드라이브 보안을 사용하지 않는 경우 보조 볼륨이 드라이브 보안을 사용하지 않아야 합니다.

- 운영 볼륨과 2차 볼륨은 동일한 드라이브 유형을 공유해야 합니다. 운영 볼륨과 2차 볼륨 간에 NVMe 및 SAS 드라이브를 혼합할 수 없습니다.

예약된 용량입니다

- 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 미러링된 쌍의 보조 볼륨과 운영 볼륨에 예약된 용량 볼륨이 필요합니다.
- 미러링 쌍의 운영 볼륨과 2차 볼륨 모두에 추가 예약 용량이 필요하므로 미러 관계의 두 스토리지 어레이에서 사용 가능한 용량이 있는지 확인해야 합니다.
- 예약된 용량 볼륨은 연결된 미러 볼륨과 동일한 드라이브 유형을 공유해야 합니다.
  - 예약 용량 볼륨이 NVMe 드라이브에 생성된 경우 미러 볼륨도 NVMe 드라이브에 생성해야 합니다.
  - 예약된 용량 볼륨이 SAS 드라이브에 생성된 경우 미러 볼륨도 SAS 드라이브에 생성해야 합니다.

드라이브 보안 기능

- 보안 가능 드라이브를 사용하는 경우 기본 볼륨 및 보조 볼륨에 호환되는 보안 설정이 있어야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
- 보안 가능 드라이브를 사용하는 경우 기본 볼륨과 보조 볼륨은 동일한 드라이브 유형을 사용해야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
- DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.

비동기식 미러 상태입니다

미러 상태는 미러 정합성 보장 그룹 및 미러링된 볼륨 쌍의 상태를 정의합니다.

미러 정합성 보장 그룹의 상태입니다

상태	설명
동기화 중(초기 동기화)	미러링된 볼륨 쌍 간에 완료된 초기 데이터 동기화 진행률 초기 동기화 중에 볼륨이 Degraded/Failed/Optimal/Unknown 상태로 전환될 수 있습니다.
동기화 중(간격 동기화)	미러링된 볼륨 쌍 간에 완료된 주기적 데이터 동기화 진행률
시스템이 일시 중단되었습니다	스토리지 시스템 - 미러 정합성 보장 그룹 레벨에서 미러링된 모든 쌍의 데이터에 대한 일시 중지된 동기화 미러 정합성 보장 그룹에 있는 하나 이상의 미러링된 페어가 중지됨 또는 실패 상태입니다.

상태	설명
사용자가 일시 중단되었습니다	미러 정합성 보장 그룹 레벨에서 미러링된 모든 쌍의 데이터에 대한 사용자 일시 중단 동기화 이 상태는 로컬 스토리지 배열의 변경된 데이터가 원격 스토리지 배열에 복사되는 동안 발생할 수 있는 호스트 응용 프로그램에 대한 성능 영향을 줄이는 데 도움이 됩니다.
일시 중지되었습니다	원격 스토리지 배열에 액세스하는 동안 오류가 발생하여 데이터 동기화 프로세스가 일시적으로 중지되었습니다.
Orphan.(	분리된 미러링된 쌍 볼륨은 정합성 보장 미러 그룹의 구성원 볼륨이 정합성 보장 미러 그룹(운영 측 또는 2차 측)의 한쪽에서 제거되었지만 다른 측에서는 제거되지 않은 경우에 존재합니다. 스토리지 간 통신이 복구되고 미러 구성의 양측이 미러 매개 변수를 조정할 때 분리된 미러링된 쌍 볼륨이 감지됩니다. 미러링된 쌍을 제거하여 분리된 미러 쌍 상태를 수정할 수 있습니다.
역할 변경 보류/진행 중	미러 정합성 보장 그룹 간의 역할 변경이 보류 중이거나 진행 중입니다. 역할 전환 변경(기본 역할 또는 보조 역할)은 선택한 미러 정합성 보장 그룹 내의 모든 비동기식 미러링 쌍에 영향을 줍니다. 보류 중인 역할 변경은 취소할 수 있지만 진행 중인 역할 변경은 취소할 수 없습니다.
역할 충돌	역할 변경 작업 중에 로컬 스토리지와 원격 스토리지 시스템 간의 통신 문제로 인해 미러 정합성 보장 그룹 간에 역할 충돌이 발생했습니다. 통신 문제가 해결되면 역할 충돌이 발생합니다. Recovery Guru를 사용하여 이 오류를 복구합니다. 역할 충돌을 해결할 때는 강제 승격이 허용되지 않습니다.

미러링된 쌍의 상태입니다

미러링된 쌍의 상태는 운영 볼륨과 2차 볼륨의 데이터가 동기화되었는지 여부를 나타냅니다.

상태	설명
동기화 중입니다	미러링된 쌍 간에 완료된 초기 또는 주기적 데이터 동기화의 진행 상태 동기화에는 초기 동기화와 주기적 동기화의 두 가지 유형이 있습니다. 초기 동기화 진행률은 장기 실행 작업 대화 상자에도 표시됩니다.
최적	미러링된 쌍의 볼륨은 동기화되며, 이는 스토리지 어레이 간의 접속이 작동하고 각 볼륨이 원하는 작업 조건에 있음을 나타냅니다.

상태	설명
완료되지 않았습니다	미러링된 쌍 생성 시퀀스가 System Manager에서 지원되지 않고 미러링된 쌍이 보조 스토리지에서 완료되지 않았기 때문에 원격 스토리지 시스템에서 비동기식 미러링 쌍이 불완전합니다. 원격 스토리지 시스템의 미러 정합성 보장 그룹에 볼륨을 추가하면 미러링된 페어 생성 프로세스가 완료됩니다. 이 볼륨은 비동기식 미러링 쌍의 2차 볼륨이 됩니다. 원격 스토리지 배열이 System Manager에 의해 관리되는 경우 미러링된 쌍은 자동으로 완료됩니다.
실패했습니다	운영 볼륨, 보조 볼륨 또는 미러 예약 용량에 장애가 발생하여 비동기식 미러링 작업이 정상적으로 작동하지 않습니다.
Orphan.(	분리된 미러링된 쌍 볼륨은 정합성 보장 미러 그룹의 구성원 볼륨이 정합성 보장 미러 그룹(운영 측 또는 2차 측)의 한쪽에서 제거되었지만 다른 측에서는 제거되지 않은 경우에 존재합니다. 분리된 미러링된 쌍 볼륨은 두 스토리지 어레이와 미러 구성의 두 측면 간에 통신이 복구되면 감지되며 미러 매개 변수가 조정됩니다. 미러링된 쌍을 제거하여 분리된 미러 쌍 상태를 수정할 수 있습니다.
중지되었습니다	미러 정합성 보장 그룹이 시스템 일시 중단 상태이므로 미러링된 페어가 중지 상태입니다.

볼륨 소유권

미러링된 쌍의 기본 컨트롤러 소유자를 변경할 수 있습니다.

미러링된 쌍의 운영 볼륨이 컨트롤러 A에 의해 소유되는 경우, 보조 볼륨은 원격 스토리지 어레이의 컨트롤러 A에 의해 소유됩니다. 운영 볼륨의 소유자를 변경하면 보조 볼륨의 소유자가 자동으로 변경되어 두 볼륨이 동일한 컨트롤러에 의해 소유되도록 합니다. 기본 면의 현재 소유권 변경 사항은 보조 면의 해당 현재 소유권 변경 사항에 자동으로 적용됩니다.

예를 들어, 기본 볼륨은 컨트롤러 A의 소유이며 컨트롤러 B로 변경하면 컨트롤러 소유자가 컨트롤러 B로 변경됩니다. 이 경우 다음 원격 쓰기는 보조 볼륨의 컨트롤러 소유자를 컨트롤러 A에서 B로 변경합니다. 보조 볼륨의 컨트롤러 소유권 변경은 기본 측에서 제어되기 때문에 스토리지 관리자의 특별한 개입이 필요하지 않습니다.

컨트롤러가 재설정됩니다

컨트롤러를 재설정하면 기본 컨트롤러의 기본 측에서 스토리지 어레이의 대체 컨트롤러로 볼륨 소유권이 변경됩니다.

경우에 따라 원격 쓰기가 보조 볼륨에 기록되기 전에 컨트롤러 재설정 또는 스토리지 어레이 전원 사이클에 의해 중단될 수 있습니다. 이 경우 컨트롤러는 미러링된 쌍의 전체 동기화를 수행할 필요가 없습니다.

컨트롤러 재설정 중에 원격 쓰기가 중단되면 기본 측의 새 컨트롤러 소유자는 기본 컨트롤러 소유자의 예약된 용량 볼륨에 있는 로그 파일에 저장된 정보를 읽습니다. 그런 다음 새 컨트롤러 소유자가 영향 받은 데이터 블록을 기본 볼륨에서 보조 볼륨으로 복사하여 미러링된 볼륨을 완전히 동기화할 필요가 없습니다.

미러 정합성 보장 그룹에서 미러링된 페어 간에 역할을 변경할 수 있습니다. 이 작업은 운영 미러 정합성 보장 그룹을 보조 역할로 하향 이동하거나 보조 미러 정합성 보장 그룹을 운영 역할로 상향 이동하여 수행할 수 있습니다.

역할 변경 작업에 대한 다음 정보를 검토합니다.

- 역할 변경은 선택한 미러 정합성 보장 그룹 내의 모든 미러링된 쌍에 영향을 줍니다.
- 미러 정합성 보장 그룹이 보조 역할로 하향 이동되면 해당 미러 정합성 보장 그룹 내의 미러링된 모든 쌍도 보조 역할로 하향 이동되고 그 반대의 경우도 마찬가지입니다.
- 운영 미러 정합성 보장 그룹이 보조 역할로 하향 이동되면 해당 그룹 내의 구성원 볼륨에 할당된 호스트는 더 이상 해당 볼륨에 대한 쓰기 액세스 권한을 갖게 되지 않습니다.
- 미러 정합성 보장 그룹이 운영 역할로 상향 이동되면 해당 그룹 내의 구성원 볼륨을 액세스하는 모든 호스트가 해당 그룹에 쓸 수 있습니다.
- 로컬 스토리지 배열이 원격 스토리지 배열과 통신할 수 없는 경우 로컬 스토리지 배열에서 역할 변경을 강제 실행할 수 있습니다.

역할 변경 강제 적용

로컬 스토리지와 원격 스토리지 시스템 간의 통신 문제로 인해 2차 미러 정합성 보장 그룹 내의 구성원 볼륨이 상향 이동하거나 1차 미러 정합성 보장 내의 구성원 볼륨이 하향 이동하는 것을 방지할 경우 미러 정합성 보장 그룹 간에 역할을 강제로 변경할 수 있습니다 그룹.

보조 측의 미러 정합성 보장 그룹을 운영 역할로 강제 전환할 수 있습니다. 그런 다음 복구 호스트가 해당 미러 정합성 보장 그룹 내에서 새로 상향 이동된 구성원 볼륨에 액세스할 수 있으며 비즈니스 작업을 계속할 수 있습니다.

강제 승급이 허용되고 허용되지 않는 경우는 언제입니까?

미러 정합성 보장 그룹의 모든 구성원 볼륨이 동기화되어 정합성 보장 복구 지점이 있는 경우에만 미러 정합성 보장 그룹의 강제 상향 이동이 허용됩니다.

다음 조건에서는 미러 정합성 보장 그룹의 강제 상향 이동이 허용되지 않습니다.

- 미러 정합성 보장 그룹의 구성원 볼륨 중 하나라도 초기 동기화 중입니다.
- 미러 정합성 보장 그룹의 구성원 볼륨에는 복구 지점의 시점 이미지가 없습니다(예: 예약된 전체 용량 오류).
- 미러 정합성 보장 그룹에 구성원 볼륨이 포함되어 있지 않습니다.
- 미러 정합성 보장 그룹이 Failed, Role-Change-Pending 또는 Role-Change-In-Progress 상태에 있거나 연결된 구성원 볼륨 또는 예약된 용량 볼륨 중 하나라도 장애가 발생한 경우

미러 그룹 역할 충돌

로컬 스토리지와 원격 스토리지 시스템 간의 통신 문제가 해결되면 미러 그룹 역할 충돌 조건이 발생합니다. Recovery Guru를 사용하여 이 오류를 복구합니다. 이중 역할 충돌을 해결할 때는 강제 승격이 허용되지 않습니다.

미러 그룹 역할 충돌 조건 및 후속 복구 단계를 방지하려면 스토리지 시스템 간의 접속이 작동할 때까지 기다린 후 역할을 변경해야 합니다.

역할 변경 진행 중 상태

미러링 구성의 두 스토리지 시스템이 분리되고 미러 정합성 보장 그룹의 운영 측이 강제로 2차 역할로 하향 이동되고 미러 정합성 보장 그룹의 2차 사이트가 1차 역할로 강제 프로모션되는 경우 그런 다음 통신이 복구되면 두 스토리지 시스템의 미러 정합성 보장 그룹이 Role-Change-In-Progress 상태로 전환됩니다.

시스템은 변경 로그를 전송하고, 다시 동기화하고, 미러 정합성 보장 그룹 상태를 정상 작동 상태로 다시 설정하고, 정기적인 동기화를 수행하여 역할 변경 프로세스를 완료합니다.

동기화 개념

동기 미러링의 작동 방식

동기식 미러링은 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다.

동기식 미러링은 EF600 또는 EF300 스토리지 어레이에서 사용할 수 없습니다.

동기식 미러링은 두 스토리지 어레이 중 하나에서 재해가 발생할 경우 중요한 데이터의 복사본을 사용할 수 있으므로 손실된 데이터가 없는 복구 지점 목표(RPO)를 실현합니다. 복제본은 운영 볼륨에 쓸 때마다 보조 볼륨에 쓰기가 수행되므로 항상 운영 데이터와 동일합니다. 보조 볼륨이 운영 볼륨에서 수행된 변경 사항으로 성공적으로 업데이트될 때까지 호스트는 쓰기가 성공했다는 확인 메시지를 받지 않습니다.

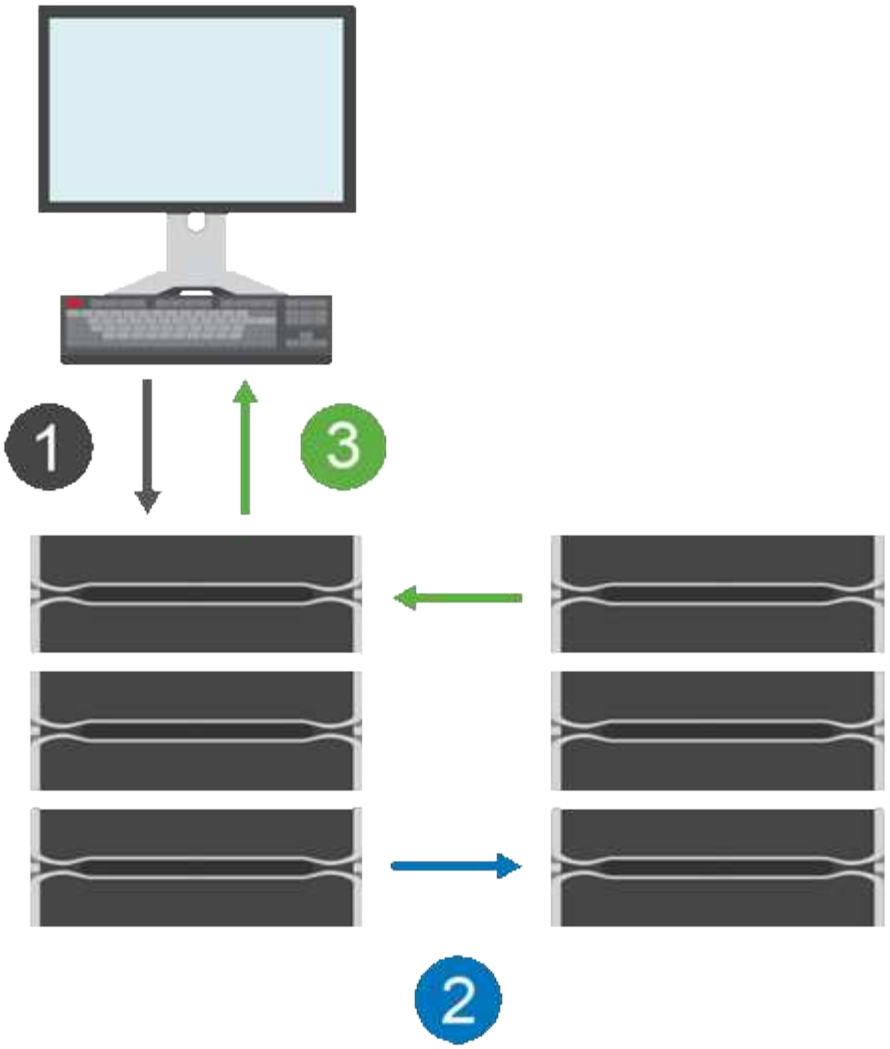
이러한 유형의 미러링은 재해 복구와 같은 비즈니스 연속성 목적으로 이상적입니다.

동기 미러링 관계

동기식 미러링 관계는 운영 볼륨과 별도의 스토리지 어레이의 보조 볼륨으로 구성됩니다. 운영 볼륨이 포함된 스토리지 배열은 대개 운영 사이트에 있으며 활성 호스트를 제공합니다. 보조 볼륨이 포함된 스토리지 배열은 일반적으로 보조 사이트에 있으며 데이터 복제본을 보관합니다. 보조 볼륨은 완전한 정전, 화재 또는 운영 사이트의 하드웨어 장애 등으로 인해 운영 볼륨의 스토리지 어레이를 사용할 수 없는 경우에 사용됩니다.

동기 미러링 세션

동기 미러링 구성 프로세스에는 볼륨을 쌍으로 구성하는 작업이 포함됩니다. 한 스토리지 어레이의 운영 볼륨과 다른 스토리지 어레이의 보조 볼륨으로 구성된 미러링된 쌍을 생성한 후 동기식 미러링을 시작할 수 있습니다. 다음은 동기 미러링의 단계입니다.



1. 쓰기가 호스트에서 제공됩니다.
2. 쓰기가 운영 볼륨에 커밋되고 원격 시스템으로 전파된 다음 보조 볼륨으로 커밋됩니다.
3. 운영 볼륨의 스토리지 배열은 두 쓰기 작업이 성공적으로 완료된 후 호스트 시스템 _after_에 입출력 완료 메시지를 보냅니다.

예약된 용량은 호스트에서 들어오는 쓰기 요청에 대한 정보를 기록하는 데 사용됩니다.

운영 볼륨의 현재 컨트롤러 소유자가 호스트로부터 쓰기 요청을 받으면 컨트롤러는 먼저 운영 볼륨의 예약 용량에 대한 쓰기 정보를 기록합니다. 그런 다음 데이터를 운영 볼륨에 씁니다. 그런 다음 컨트롤러는 원격 쓰기 작업을 시작하여 영향을 받는 데이터 블록을 원격 스토리지 배열의 보조 볼륨으로 복사합니다.

호스트 애플리케이션은 로컬 스토리지 어레이와 원격 스토리지 어레이의 네트워크에서 쓰기가 수행되기를 기다려야 하므로 로컬 입출력 성능을 지나치게 낮추지 않고 미러 관계를 유지하려면 로컬 스토리지 시스템과 원격 스토리지 시스템 간에 매우 빠른 연결이 필요합니다.

재해 복구

동기식 미러링은 데이터가 상주하는 사이트와 물리적으로 멀리 있는 데이터의 복사본을 유지 관리합니다. 운영 사이트에서 정전 또는 홍수 같은 재해가 발생할 경우 보조 사이트에서 데이터에 빠르게 액세스할 수 있습니다.

동기식 미러링 작업이 진행 중인 동안에는 보조 볼륨을 호스트 애플리케이션에 사용할 수 없으므로 로컬 스토리지

어레이에 재해가 발생할 경우 원격 스토리지 시스템으로 페일오버할 수 있습니다. 페일오버하려면 보조 볼륨을 운영 역할로 상향 이동합니다. 그런 다음 복구 호스트가 새로 상향 이동된 볼륨에 액세스할 수 있고 비즈니스 작업을 계속할 수 있습니다.

동기화 설정

미러링된 페어를 생성할 때 통신 중단 후 미러링된 페어가 재동기화 작업을 완료하는 데 사용하는 동기화 우선 순위 및 재동기화 정책도 정의합니다.

두 스토리지 시스템 간의 통신 링크가 작동하지 않는 경우 호스트는 로컬 스토리지 어레이로부터 승인을 계속 받아 액세스 손실을 방지합니다. 통신 링크가 다시 작동 중일 때 복제되지 않은 모든 데이터는 원격 스토리지 시스템에 자동으로 또는 수동으로 다시 동기화될 수 있습니다.

데이터가 자동으로 재동기화되는지 여부는 미러링된 페어의 재동기화 정책에 따라 달라집니다. 자동 재동기화 정책을 사용하면 링크가 다시 작동할 때 미러링된 쌍이 자동으로 재동기화됩니다. 수동 재동기화 정책을 사용하려면 통신 문제가 발생한 후 수동으로 동기화를 다시 시작해야 합니다. 수동 재동기화는 권장 정책입니다.

운영 볼륨이 포함된 스토리지 어레이에서만 미러링된 쌍의 동기화 설정을 편집할 수 있습니다.

동기화되지 않은 데이터

운영 볼륨의 스토리지 시스템이 보조 볼륨에 데이터를 쓸 수 없을 경우 운영 볼륨과 2차 볼륨의 동기화가 해제됩니다. 이 문제는 다음과 같은 문제로 인해 발생할 수 있습니다.

- 로컬 스토리지와 원격 스토리지 시스템 간의 네트워크 문제입니다
- 장애가 발생한 보조 볼륨입니다
- 동기화가 미러링된 쌍에서 수동으로 일시 중단됩니다

분리된 미러링 쌍

구성원 볼륨이 한 쪽(기본 측 또는 보조 측)에서 제거되었지만 다른 쪽에는 제거되지 않은 경우 분리된 미러링된 쌍 볼륨이 존재합니다.

스토리지 간 통신이 복구되고 미러 구성의 양측이 미러 매개 변수를 조정할 때 분리된 미러링된 쌍 볼륨이 감지됩니다.

미러링된 쌍을 제거하여 분리된 미러 쌍 상태를 수정할 수 있습니다.

구성 및 관리

두 어레이 간에 미러링을 설정하고 구성하려면 Unified Manager 인터페이스를 사용해야 합니다. 미러링이 활성화되면 System Manager에서 미러링된 쌍과 동기화 설정을 관리할 수 있습니다.

동기 미러링 용어

동기식 미러링 조건이 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
로컬 스토리지 시스템입니다	로컬 스토리지 배열은 사용자가 수행하는 스토리지 배열입니다. Local Role 열에 * Primary * 가 표시되면 스토리지 배열에 미러 관계에서 1차 역할을 가진 볼륨이 포함되어 있음을 나타냅니다. Local Role 열에 * Secondary * 가 표시되면 스토리지 배열에 미러 관계에서 보조 역할을 가진 볼륨이 포함되어 있음을 나타냅니다.
미러링 쌍	미러링된 쌍은 기본 볼륨 및 보조 볼륨이라는 두 개의 볼륨으로 구성됩니다.
운영 볼륨	미러링된 쌍의 기본 볼륨은 미러링될 소스 볼륨입니다.
복구 지점 목표(RPO)	복구 지점 목표(RPO)는 미러링된 쌍의 운영 볼륨과 2차 볼륨 간에 허용되는 것으로 간주되는 차이를 나타내는 목표를 나타냅니다. 0의 RPO는 운영 볼륨과 2차 볼륨 간의 차이가 허용되지 않음을 나타냅니다. RPO가 0보다 크면 보조 볼륨이 운영 볼륨 뒤에 있거나 지연 시간이 있음을 나타냅니다.
원격 스토리지 시스템	원격 스토리지 시스템은 일반적으로 미러링 구성의 데이터 복제본을 보관하는 보조 사이트로 지정됩니다.
예약된 용량입니다	예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.
역할 변경	역할 변경 시 보조 볼륨에 기본 역할이 할당되며, 그 반대의 경우도 마찬가지입니다.
2차 볼륨	미러링된 쌍의 보조 볼륨은 일반적으로 보조 사이트에 위치하며 데이터 복제본을 보관합니다.
동기화	동기화는 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화에서 수행됩니다. 동기화는 통신 중단 후 운영 볼륨과 2차 볼륨의 동기화가 중단된 경우에도 발생합니다. 통신 링크가 다시 작동되면 복제되지 않은 모든 데이터가 보조 볼륨의 스토리지 시스템에 동기화됩니다.

볼륨을 동기식으로 미러링하기 위한 워크플로우

다음 워크플로우를 사용하여 동기식 미러링을 구성합니다.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

1. Unified Manager에서 초기 구성을 수행합니다.
   a. 데이터 전송을 위한 소스로 로컬 스토리지 배열을 선택합니다.
   b. 로컬 스토리지 어레이에서 운영 볼륨을 선택합니다.
   c. 데이터 전송 대상으로 원격 스토리지 시스템을 선택한 다음 보조 볼륨을 선택합니다.
   d. 동기화 및 재동기화 우선 순위를 선택합니다.
   e. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기 전송에 몇 시간이 걸릴

수 있습니다.

2. 초기 동기화 진행률을 확인합니다.
   a. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
   b. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다. 두 배열은 정상적인 작업을 통해 동기화 상태를 유지하려고 합니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.
3. * 선택 사항: * System Manager에서 동기화 설정을 변경할 수 있습니다.

> 동기식 복제는 지속적이기 때문에 두 사이트 간의 복제 링크는 충분한 대역폭 기능을 제공해야 합니다.

동기 미러링 사용에 대한 요구 사항

동기식 미러링을 사용하려는 경우 다음 요구사항을 염두에 두십시오.

Unified Manager를 참조하십시오

두 어레이 간에 미러링을 설정하고 구성하려면 Unified Manager 인터페이스를 사용해야 합니다. Unified Manager는 웹 서비스 프록시와 함께 호스트 시스템에 설치됩니다.

- 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
- Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
- Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

지원합니다

> 동기식 미러링은 EF300 또는 EF600 스토리지 어레이에서 사용할 수 없습니다.

- 두 개의 스토리지 어레이가 있어야 합니다.
- 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
- Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
- 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
- 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
- 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
- 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
- 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭을 통해 연결됩니다.

지원되는 연결입니다

동기식 미러링을 위한 통신은 FC(Fibre Channel) 호스트 포트가 있는 컨트롤러에서만 지원됩니다.

동기 미러링은 로컬 스토리지 배열과 원격 스토리지 배열의 각 컨트롤러에서 가장 높은 번호의 호스트 포트를 사용합니다. 컨트롤러 HBA(호스트 버스 어댑터) 호스트 포트 4는 일반적으로 미러 데이터 전송용으로 예약되어 있습니다.

미러링 볼륨 후보

- 동기식 미러링 쌍의 운영 볼륨과 2차 볼륨에서는 RAID 레벨, 캐싱 매개 변수, 세그먼트 크기가 다를 수 있습니다.
- 동기식 미러링 쌍의 운영 볼륨과 2차 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨 또는 스냅샷 볼륨일 수 없습니다.
- 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.
- 운영 볼륨에만 연결된 스냅샷이 있거나 볼륨 복제 작업의 소스 또는 타겟 볼륨일 수 있습니다.
- 볼륨은 하나의 미러 관계에만 참여할 수 있습니다.
- 지정된 스토리지 어레이에서 지원되는 볼륨 수는 제한됩니다. 스토리지 배열에 구성된 볼륨 수가 지원되는 제한보다 적었는지 확인합니다. 동기식 미러링이 활성 상태인 경우 생성된 2개의 예약된 용량 볼륨이 볼륨 제한에 대해 계산됩니다.

예약된 용량입니다

- 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 운영 볼륨과 보조 볼륨에 예약된 용량이 필요합니다.
- 예약된 용량 볼륨은 동기식 미러링이 활성화될 때 자동으로 생성됩니다. 미러링된 쌍의 운영 볼륨과 2차 볼륨 모두에 예약된 용량이 필요하므로 동기 미러 관계에 참여하는 두 스토리지 시스템에서 사용 가능한 용량이 충분한지 확인해야 합니다.

드라이브 보안 기능

- 보안 가능 드라이브를 사용하는 경우 기본 볼륨 및 보조 볼륨에 호환되는 보안 설정이 있어야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
- 보안 가능 드라이브를 사용하는 경우 기본 볼륨과 보조 볼륨은 동일한 드라이브 유형을 사용해야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
  - 기본 볼륨에서 FDE(전체 디스크 암호화) 드라이브를 사용하는 경우 보조 볼륨에서 FDE 드라이브를 사용해야 합니다.
  - 운영 볼륨이 FIPS(Federal Information Processing Standards 140-2) 검증 드라이브를 사용하는 경우 2차 볼륨은 FIPS 140-2 검증을 거친 드라이브를 사용해야 합니다.
- DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.

동기 미러링 상태

동기식 미러링 쌍의 상태는 운영 볼륨과 2차 볼륨의 데이터가 동기화되었는지 여부를 나타냅니다. 미러 상태는 미러링된 쌍에 있는 볼륨의 구성 요소 상태와 무관합니다.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

동기식 미러링 쌍은 다음 상태 중 하나일 수 있습니다.

- * 최적 *

미러링된 쌍의 볼륨이 동기화되었음을 나타냅니다. 즉, 스토리지 어레이 간의 패브릭 연결이 작동 중이고 각 볼륨이 원하는 작업 상태에 있음을 나타냅니다.

- * 동기화 중 *

  미러링된 쌍 간의 데이터 동기화 진행률을 보여 줍니다. 이 상태는 초기 동기화 중에도 표시됩니다.

  통신 링크가 중단된 후에는 링크가 중단된 동안 운영 볼륨에서 변경된 데이터 블록만 보조 볼륨으로 복사됩니다.

- * 동기화되지 않음 *

  운영 볼륨의 스토리지 배열이 원격 배열에 들어오는 데이터를 쓸 수 없음을 나타냅니다. 로컬 호스트는 계속 운영 볼륨에 쓸 수 있지만 원격 쓰기는 적용되지 않습니다. 운영 볼륨의 스토리지 배열이 들어오는 데이터를 보조 볼륨에 쓰는 것을 방지할 수 있는 조건이 다를 수 있습니다. 예를 들면 다음과 같습니다.

  ◦ 보조 볼륨에 액세스할 수 없습니다.

  ◦ 원격 스토리지 배열에 액세스할 수 없습니다.

  ◦ 스토리지 시스템 간의 Fabric 접속에 액세스할 수 없습니다.

  ◦ 2차 볼륨은 새로운 WWID(World Wide Identifier)로 업데이트할 수 없습니다.

- * 일시 중단됨 *

  사용자가 동기 미러링 작업을 일시 중단했음을 나타냅니다. 미러링된 쌍이 일시 중지되면 보조 볼륨에 연결을 시도하지 않습니다. 운영 볼륨에 대한 모든 쓰기는 미러 예약 용량 볼륨에 영구적으로 기록됩니다.

- * 실패 *

  운영 볼륨, 보조 볼륨 또는 미러 예약 용량에 장애가 발생하여 동기식 미러링 작업이 정상적으로 작동하지 않음을 나타냅니다.

볼륨 소유권

미러링된 쌍의 기본 컨트롤러 소유자를 변경할 수 있습니다.

EF600 또는 EF300 스토리지 시스템의 동기식 미러링에는 이 기능을 사용할 수 없습니다.

미러링된 쌍의 운영 볼륨이 컨트롤러 A에 의해 소유되는 경우, 보조 볼륨은 원격 스토리지 어레이의 컨트롤러 A에 의해 소유됩니다. 운영 볼륨의 소유자를 변경하면 보조 볼륨의 소유자가 자동으로 변경되어 두 볼륨이 동일한 컨트롤러에 의해 소유되도록 합니다. 기본 면의 현재 소유권 변경 사항은 보조 면의 해당 현재 소유권 변경 사항에 자동으로 적용됩니다.

예를 들어, 기본 볼륨은 컨트롤러 A의 소유이며 컨트롤러 B로 변경하면 컨트롤러 소유자가 컨트롤러 B로 변경됩니다. 이 경우 다음 원격 쓰기는 보조 볼륨의 컨트롤러 소유자를 컨트롤러 A에서 B로 변경합니다. 보조 볼륨의 컨트롤러 소유권 변경은 기본 측에서 제어되기 때문에 스토리지 관리자의 특별한 개입이 필요하지 않습니다.

컨트롤러가 재설정됩니다

컨트롤러를 재설정하면 기본 컨트롤러의 기본 측에서 스토리지 어레이의 대체 컨트롤러로 볼륨 소유권이 변경됩니다.

경우에 따라 원격 쓰기가 보조 볼륨에 기록되기 전에 컨트롤러 재설정 또는 스토리지 어레이 전원 사이클에 의해 중단될 수 있습니다. 이 경우 컨트롤러는 미러링된 쌍의 전체 동기화를 수행할 필요가 없습니다.

컨트롤러 재설정 중에 원격 쓰기가 중단되면 기본 측의 새 컨트롤러 소유자는 기본 컨트롤러 소유자의 예약된 용량 볼륨에 있는 로그 파일에 저장된 정보를 읽습니다. 그런 다음 새 컨트롤러 소유자가 영향 받은 데이터 블록을 기본 볼륨에서 보조 볼륨으로 복사하여 미러링된 볼륨을 완전히 동기화할 필요가 없습니다.

미러링된 쌍의 볼륨 간 역할 변경

미러링된 쌍의 볼륨 간에 역할을 변경할 수 있습니다. 이 작업은 운영 볼륨을 보조 역할로 하향 이동하거나 보조 볼륨을 기본 역할로 상향 이동하여 수행할 수 있습니다.

EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

역할 변경 작업에 대한 다음 정보를 검토합니다.

- 운영 볼륨이 2차 역할로 하향 이동되면 해당 미러링된 쌍의 2차 볼륨이 1차 역할로 상향 이동되거나 그 반대로 상향 이동됩니다.
- 운영 볼륨이 보조 역할로 하향 이동되면 해당 볼륨에 할당된 호스트는 더 이상 해당 볼륨에 대한 쓰기 액세스 권한을 가질 수 없습니다.
- 보조 볼륨이 운영 역할로 프로모션되면 해당 볼륨에 액세스하는 모든 호스트에서 볼륨에 쓸 수 있습니다.
- 로컬 스토리지 배열이 원격 스토리지 배열과 통신할 수 없는 경우 로컬 스토리지 배열에서 역할 변경을 강제 실행할 수 있습니다.

역할 변경 강제 적용

로컬 스토리지 어레이와 원격 스토리지 시스템 간의 통신 문제로 인해 보조 볼륨의 상향 이동 또는 운영 볼륨의 하향 이동이 차단되는 경우 미러링된 쌍의 볼륨 간에 역할 변경을 강제 실행할 수 있습니다.

보조 측의 볼륨을 운영 역할로 강제 전환할 수 있습니다. 그런 다음 복구 호스트가 새로 상향 이동된 볼륨에 액세스할 수 있으며 비즈니스 작업을 계속할 수 있습니다.

원격 스토리지 배열이 복구되고 통신 문제가 해결되면 동기 미러링 - 1차 볼륨 충돌 조건이 발생합니다. 복구 단계에는 볼륨 재동기화가 포함됩니다. Recovery Guru를 사용하여 이 오류를 복구합니다.

강제 승급이 허용되고 허용되지 않는 경우는 언제입니까?

다음 조건에서는 미러링된 쌍의 볼륨을 강제로 승격할 수 없습니다.

- 미러링된 쌍의 볼륨은 초기 동기화 중에 있습니다.
- 미러링된 페어는 실패, 역할 - 변경 - 보류 또는 역할 - 변경 - 진행 중 상태에 있거나 연결된 예약된 용량 볼륨 중 하나라도 실패하면

역할 변경 진행 중 상태

미러링 구성의 두 스토리지 시스템이 분리되고 미러링된 쌍의 기본 볼륨이 보조 역할로 강제 퇴등되고 미러링된 쌍의 보조 볼륨이 기본 역할로 강제 상향 이동된 경우, 그런 다음 통신이 복구되면 두 스토리지 시스템의 볼륨이 Role-Change-In-Progress 상태가 됩니다.

시스템은 변경 로그를 전송하고, 다시 동기화하고, 미러링된 페어 상태를 정상 작동 상태로 다시 설정하고, 동기화를 계속 수행하여 역할 변경 프로세스를 완료합니다.

비동기식 미러 정합성 보장 그룹을 관리합니다

미러 정합성 보장 그룹에 대한 통신을 테스트합니다

통신 링크를 테스트하여 로컬 스토리지 시스템과 미러 정합성 보장 그룹에 연결된 원격 스토리지 시스템 간의 통신 문제를 진단할 수 있습니다.

시작하기 전에

테스트할 미러 정합성 보장 그룹이 로컬 및 원격 스토리지 시스템에 있어야 합니다.

이 작업에 대해

다음 네 가지 테스트를 실행할 수 있습니다.

- * 연결 * — 두 컨트롤러가 통신 경로를 가지고 있는지 확인합니다. 연결 테스트에서는 스토리지 시스템 간에 스토리지 간 메시지를 보낸 다음 원격 스토리지 시스템에 있는 해당 미러 정합성 보장 그룹이 있는지 확인합니다. 또한 원격 스토리지 시스템에 있는 미러 정합성 보장 그룹의 구성원 볼륨이 로컬 스토리지 시스템에 있는 미러 정합성 보장 그룹의 구성원 볼륨과 일치하는지 확인합니다.
- * 지연 시간 * — 미러 정합성 보장 그룹에 연결된 원격 스토리지 시스템의 각 미러링된 볼륨에 SCSI 테스트 유닛 명령을 전송하여 최소, 평균 및 최대 지연 시간을 테스트합니다.
- * 대역폭 * — 검사를 수행하는 어레이에 있는 포트의 협상된 링크 속도뿐만 아니라 최소, 평균 및 최대 대역폭을 테스트하기 위해 원격 스토리지 배열에 두 개의 배열 간 메시지를 보냅니다.
- * 포트 연결 * — 로컬 스토리지 배열의 미러링에 사용되는 포트와 원격 스토리지 배열의 미러링된 데이터를 수신하는 포트를 표시합니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택한 다음 테스트할 미러 정합성 보장 그룹을 선택합니다.
3. 통신 테스트 * 를 선택합니다.

   통신 테스트 대화 상자가 나타납니다.
4. 선택한 미러 정합성 보장 그룹에 연결된 로컬 및 원격 스토리지 시스템 간에 수행할 통신 테스트를 하나 이상 선택한 다음 * 테스트 * 를 클릭합니다.
5. 결과 창에 표시된 정보를 검토합니다.

통신 테스트 상태	설명
정상, 오류 없음	미러 정합성 보장 그룹이 올바르게 통신하고 있습니다.
통과 상태(정상은 아님)	가능한 네트워크 또는 연결 문제를 확인하고 테스트를 다시 시도하십시오.
실패 상태입니다	실패 이유가 표시됩니다. 문제를 해결하려면 Recovery Guru를 참조하십시오.

통신 테스트 상태	설명
포트 연결 오류입니다	로컬 스토리지 배열이 연결되어 있지 않거나 원격 스토리지 배열에 연결할 수 없기 때문일 수 있습니다. 문제를 해결하려면 Recovery Guru를 참조하십시오.

결과

통신 테스트가 완료되면 이 대화 상자에 정상 상태, 통과 상태 또는 실패 상태가 표시됩니다.

통신 테스트가 실패 상태를 반환하는 경우 미러 정합성 보장 그룹 간의 통신이 복구될 때까지 이 대화 상자를 닫은 후에도 테스트가 계속 실행됩니다.

미러 정합성 보장 그룹에 대한 동기화를 일시 중지하거나 다시 시작합니다

미러 정합성 보장 그룹 내의 모든 미러링된 쌍에서 데이터 동기화를 일시 중지하거나 다시 시작할 수 있으므로 개별 미러링된 쌍에서 동기화를 일시 중지하거나 다시 시작하는 것보다 효율적입니다.

이 작업에 대해

그룹에서 동기화를 일시 중단하고 다시 시작하면 호스트 응용 프로그램에 대한 성능 영향을 줄일 수 있습니다. 이 문제는 로컬 스토리지 배열의 변경된 데이터가 원격 스토리지 배열에 복사되는 동안 발생할 수 있습니다.

동기화 작업을 재개하기 위해 Resume 옵션을 사용할 때까지 미러 정합성 보장 그룹 및 미러 페어의 상태가 일시 중지된 상태로 유지됩니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러링된 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 일시 중단 또는 재개하려는 미러 정합성 보장 그룹을 선택한 다음 More[Suspend] 또는 **More › Resume** 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

4. 예 * 를 선택하여 확인합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 미러 관계를 제거하지 않고 미러 정합성 보장 그룹의 미러링된 모든 쌍 간에 데이터 전송을 일시 중단하거나 재개합니다.
- 미러 그룹이 일시 중지된 동안 미러 정합성 보장 그룹의 운영 측에 기록된 모든 데이터를 기록하고 미러 그룹이 재개될 때 미러 정합성 보장 그룹의 보조 측에 데이터를 자동으로 씁니다. 전체 동기화가 필요하지 않습니다.
- suspended_mirror 정합성 보장 그룹의 경우 미러 정합성 보장 그룹 테이블에 * user-suspended * 가 표시됩니다.

- refused_mirror 정합성 보장 그룹의 경우 미러 정합성 보장 그룹이 일시 중지된 동안 운영 볼륨에 기록된 데이터가 보조 볼륨에 즉시 기록됩니다. 자동 동기화 간격이 설정된 경우 주기적 동기화가 다시 시작됩니다.

미러 정합성 보장 그룹의 동기화 설정을 변경합니다

데이터가 처음 동기화될 때 또는 비동기식 미러링 작업 중에 데이터가 다시 동기화될 때 로컬 스토리지 시스템의 미러 정합성 보장 그룹이 사용하는 동기화 설정 및 경고 임계값을 변경할 수 있습니다.

이 작업에 대해

동기화 설정을 변경하면 미러 정합성 보장 그룹 내의 모든 미러링된 쌍의 동기화 작업에 영향을 줍니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러링된 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 편집하려는 미러 정합성 보장 그룹을 선택한 다음 MENU: More [Edit Settings] 를 선택합니다.

   설정 편집 대화 상자가 표시됩니다.

4. 동기화 및 알림 설정을 적절히 편집한 다음 * 저장 * 을 클릭합니다.

필드 상세정보

필드에 입력합니다	설명
미러링된 쌍 동기화…	원격 스토리지 배열의 미러링된 쌍을 수동 또는 자동으로 동기화할지 여부를 지정합니다. • 수동 – 원격 스토리지 배열의 미러링된 쌍을 수동으로 동기화하려면 이 옵션을 선택합니다. • 자동, 매** – 이전 업데이트 시작에서 다음 업데이트 시작까지의 시간 간격을 지정하여 원격 스토리지 배열의 미러링된 쌍을 자동으로 동기화하려면 이 옵션을 선택합니다. 기본 간격은 10분입니다.
알림…	동기화 방법을 자동으로 발생하도록 설정한 경우 다음 경고를 설정합니다. • 동기화 – System Manager가 동기화가 완료되지 않은 알림을 보낸 후 시간을 설정합니다. • 원격 복구 지점 – System Manager가 원격 스토리지 배열의 복구 지점 데이터가 정의된 시간 제한보다 오래되었음을 나타내는 경고를 보낸 후 시간 제한을 설정합니다. 이전 업데이트 종료에서 시간 제한을 정의합니다. • 예약된 용량 임계값 – 예약된 용량 임계값에 근접한 알림을 System Manager에서 보내는 예약 용량 양을 정의합니다. 남은 용량 대비 임계값을 정의합니다.

결과

System Manager는 미러 정합성 보장 그룹의 모든 미러링된 쌍에 대한 동기화 설정을 변경합니다.

미러 정합성 보장 그룹을 수동으로 다시 동기화하십시오

미러 정합성 보장 그룹 내의 모든 미러링된 쌍에 대해 수동으로 재동기화를 시작할 수 있습니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 다시 동기화하려는 미러 정합성 보장 그룹을 선택한 다음 More [Manually resynize] 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

4. 예 * 를 선택하여 확인합니다.

결과

시스템은 다음 작업을 수행합니다.

- 선택한 미러 정합성 보장 그룹 내의 모든 미러링된 쌍에서 데이터의 재동기화를 시작합니다.
- 로컬 스토리지 시스템에서 원격 스토리지 시스템으로 수정된 데이터를 업데이트합니다.

미러 정합성 보장 그룹 간에 동기화되지 않은 데이터 양을 봅니다

로컬 스토리지 시스템의 미러 정합성 보장 그룹과 원격 스토리지 시스템 간에 동기화되지 않은 데이터의 양을 볼 수 있습니다. 미러 정합성 보장 그룹이 동기화되지 않은 상태이면 미러링 작업이 발생하지 않습니다.

이 작업에 대해

선택한 미러 정합성 보장 그룹에 미러링 쌍이 포함되어 있고 동기화가 현재 진행 중이 아닌 경우 이 작업을 수행할 수 있습니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. More(추가) [View unsynchronized data amount(동기화되지 않은 데이터 양 보기)]를 클릭합니다.

   동기화되지 않은 데이터가 있으면 테이블 값에 이 값이 반영됩니다. Data Amount 열에는 동기화되지 않은 데이터 양이 MiB 단위로 표시됩니다.

원격 **IP** 주소를 업데이트합니다

원격 스토리지 배열의 iSCSI IP 주소를 업데이트하여 로컬 스토리지 배열과의 연결을 다시 설정할 수 있습니다.

시작하기 전에

로컬 스토리지 어레이와 원격 스토리지 시스템 모두 iSCSI 접속을 사용하여 비동기식 미러링에 대해 구성되어야 합니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러 정합성 보장 그룹 테이블에는 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 업데이트할 미러 정합성 보장 그룹을 선택한 다음 추가 [원격 IP 주소 업데이트] 메뉴를 선택합니다.

   원격 IP 주소 업데이트 대화 상자가 표시됩니다.

4. 원격 스토리지 배열의 iSCSI IP 주소를 업데이트하려면 * Update * 를 선택합니다.

결과

시스템은 로컬 스토리지 시스템과의 연결을 다시 설정하기 위해 원격 스토리지 배열의 IP 주소를 재설정합니다.

미러 정합성 보장 그룹 역할을 운영 또는 **2**차 역할로 변경합니다

관리를 위해 또는 로컬 스토리지 시스템에 재해가 발생한 경우 미러 정합성 보장 그룹 간에 역할을 변경할 수 있습니다.

이 작업에 대해

로컬 스토리지 시스템에 생성된 미러 정합성 보장 그룹은 운영 역할을 담당합니다. 원격 스토리지 시스템에 생성된 미러 정합성 보장 그룹은 2차 역할을 수행합니다. 로컬 미러 정합성 보장 그룹을 보조 역할로 하향 이동하거나 원격 미러 정합성 보장 그룹을 운영 역할로 상향 이동할 수 있습니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

   미러 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 역할을 변경할 미러 정합성 보장 그룹을 선택한 다음 More [Change role to <Primary|Secondary>] *> * 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

4. 미러 정합성 보장 그룹의 역할을 변경할 것인지 확인한 다음 * 역할 변경 * 을 클릭합니다.

> ⓘ 역할 변경이 요청되었지만 원격 스토리지 어레이에 연결할 수 없는 경우 스토리지 시스템에 연결할 수 없음 대화 상자가 표시됩니다. 예 * 를 클릭하여 역할 변경을 강제 적용합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 미러 정합성 보장 그룹 테이블에는 역할 변경을 진행 중인 미러 정합성 보장 그룹 옆에 "보류 중" 또는 "진행 중" 상태가 표시됩니다. 테이블 셀에 있는 * Cancel * 링크를 클릭하여 보류 중인 역할 변경 작업을 취소할 수 있습니다.
- 연결된 미러 정합성 보장 그룹에 접속할 수 있으면 미러 정합성 보장 그룹 간의 역할이 변경됩니다. System Manager는 보조 미러 정합성 보장 그룹을 기본 역할로 상향 이동하거나 선택 항목에 따라 기본 미러 정합성 보장 그룹을 보조 역할로 하향 이동합니다. 역할 변경은 선택한 미러 정합성 보장 그룹 내의 모든 미러링된 쌍에 영향을 줍니다.

미러 정합성 보장 그룹을 삭제합니다

로컬 스토리지 시스템과 원격 스토리지 시스템에서 더 이상 필요하지 않은 미러 정합성 보장 그룹을 삭제할 수 있습니다.

시작하기 전에

미러 정합성 보장 그룹에서 미러링된 모든 쌍을 제거해야 합니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. 미러 정합성 보장 그룹 * 탭을 선택합니다.

미러 정합성 보장 그룹 테이블이 나타나고 스토리지 시스템과 연결된 모든 미러 정합성 보장 그룹이 표시됩니다.

3. 삭제할 미러 일관성 그룹을 선택한 다음 메뉴, 일반적이지 않은 작업 [삭제] 를 선택합니다.

   확인 메시지가 표시됩니다.

4. 미러 정합성 보장 그룹을 삭제하려면 * Yes * 를 선택합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 먼저 로컬 스토리지의 미러 정합성 보장 그룹을 삭제한 다음 원격 스토리지의 미러 정합성 보장 그룹을 삭제합니다.
- 미러 정합성 보장 그룹 테이블에서 미러 정합성 보장 그룹을 제거합니다.

작업을 마친 후

경우에 따라 미러 정합성 보장 그룹이 로컬 스토리지 시스템에서 성공적으로 삭제되었지만 통신 오류로 인해 미러 정합성 보장 그룹이 원격 스토리지 시스템에서 삭제되지 않는 경우가 있습니다. 이 경우 원격 스토리지 시스템에 액세스하여 해당 미러 정합성 보장 그룹을 삭제해야 합니다.

비동기 미러링 쌍을 관리합니다

비동기식 미러 관계를 제거합니다

미러 쌍을 제거하여 로컬 스토리지 배열의 운영 볼륨과 원격 스토리지 배열의 보조 볼륨에서 미러 관계를 제거합니다.

이 작업에 대해

분리된 미러 쌍에 대한 다음 정보를 검토합니다.

- 분리된 미러링된 쌍은 정합성 보장 미러 그룹의 구성원 볼륨이 한 쪽(로컬 스토리지 어레이 측 또는 원격 스토리지 어레이 측)에서 제거되었지만 다른 쪽에는 제거되지 않은 경우에 존재합니다.
- 분리된 미러 쌍은 스토리지 간 통신이 복구되고 미러 구성의 두 측이 미러 매개 변수를 조정할 때 감지됩니다.
- 미러링된 쌍을 제거하여 분리된 미러 쌍 상태를 수정할 수 있습니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. Mirrored Pair * 탭을 선택합니다.

   미러링된 페어 테이블이 나타나고 스토리지 배열과 연결된 모든 미러링된 쌍이 표시됩니다.

3. 제거하려는 대칭 복사된 쌍을 선택한 다음 * 제거 * 를 클릭합니다.
4. 미러링된 쌍을 제거할지 확인한 다음 * 제거 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 로컬 스토리지 시스템 및 원격 스토리지 시스템의 미러 정합성 보장 그룹에서 미러 관계를 제거하고 예약된 용량을 삭제합니다.

- 운영 볼륨 및 보조 볼륨을 호스트에서 액세스할 수 있고 미러링되지 않은 볼륨으로 반환합니다.
- 비동기 미러링 쌍을 제거하여 비동기 미러링 타일을 업데이트합니다.

예약된 용량을 늘립니다

스토리지 오브젝트의 모든 복제 서비스 작업에 사용되는 물리적으로 할당된 용량인 예약 용량을 늘릴 수 있습니다.

스냅샷 작업의 경우 일반적으로 기본 볼륨의 40%이며, 비동기식 미러링 작업의 경우 일반적으로 기본 볼륨의 20%입니다. 일반적으로 스토리지 객체의 예약된 용량이 가득 차고 있다는 경고가 표시되면 예약 용량을 늘립니다.

시작하기 전에

- 풀 또는 볼륨 그룹의 볼륨은 최적 상태여야 하며 수정 상태가 아니어야 합니다.
- 용량을 늘리기 위해 사용할 풀 또는 볼륨 그룹에 사용 가능한 용량이 있어야 합니다.

  풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우, 할당되지 않은 용량을 미사용 드라이브 형식으로 풀 또는 볼륨 그룹에 추가할 수 있습니다.

이 작업에 대해

다음과 같은 스토리지 객체에 대해 예약 용량을 8GiB씩 늘릴 수 있습니다.

- 스냅샷 그룹
- 스냅샷 볼륨
- 정합성 보장 그룹 구성원 볼륨입니다
- 미러링 쌍 볼륨

운영 볼륨에 많은 변경이 있을 것으로 생각되거나 특정 복사 서비스 작업의 수명이 매우 길 경우 높은 비율을 사용하십시오.

읽기 전용인 스냅샷 볼륨에 대해 예약된 용량을 늘릴 수 없습니다. 읽기-쓰기의 스냅샷 볼륨에만 예약된 용량이 필요합니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. Reserved Capacity * 탭을 선택합니다.
3. 예약된 용량을 늘릴 스토리지 객체를 선택한 다음 * 용량 증가 * 를 클릭합니다.

   예약된 용량 증가 대화 상자가 나타납니다.

4. 스피너 상자를 사용하여 용량 비율을 조정합니다.

   선택한 스토리지 객체가 포함된 풀 또는 볼륨 그룹에 사용 가능한 용량이 없고 스토리지 배열에 할당되지 않은 용량이 있는 경우 새 풀 또는 볼륨 그룹을 생성할 수 있습니다. 그런 다음 해당 풀 또는 볼륨 그룹의 새 가용 용량을 사용하여 이 작업을 다시 시도할 수 있습니다.

5. 증가 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 스토리지 객체에 대한 예약 용량을 늘립니다.
- 새로 추가된 예약된 용량을 표시합니다.

미러링된 페어 볼륨에 대한 예약된 용량 설정을 변경합니다

미러링된 페어 볼륨의 설정을 변경하여 미러링된 페어 볼륨의 예약된 용량이 거의 꽉 찼을 때 SANtricity 시스템 관리자가 알림 메시지를 보내는 백분율 지점을 조정할 수 있습니다.

단계

1. 스토리지 [풀 및 볼륨 그룹] 메뉴를 선택합니다.
2. Reserved Capacity * 탭을 선택합니다.
3. 편집할 미러링된 쌍 볼륨을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   Mirrored Pair Volume Reserved Capacity Settings(미러링된 볼륨 예비 용량 설정) 대화 상자가 나타납니다.

4. 미러링된 페어 볼륨에 대한 예약된 용량 설정을 적절하게 변경합니다.

   필드 상세정보

설정	설명
다음 경우에 알림:	미러링 쌍의 예약된 용량이 거의 꽉 찼을 때 System Manager에서 경고 알림을 보내는 백분율 지점을 Spinner 상자를 사용하여 조정합니다. 미러링된 쌍의 예약된 용량이 지정된 임계값을 초과하면 System Manager에서 경고를 보내, 예약된 용량을 늘릴 수 있도록 합니다. 미러링된 한 쌍의 경고 설정을 변경하면 동일한 미러 정합성 보장 그룹에 속한 모든 미러링된 쌍에 대한 경고 설정이 변경됩니다.

5. 변경 사항을 적용하려면 * 저장 * 을 클릭합니다.

기존 시스템에서 생성된 운영 볼륨에 대해 완전한 미러링 쌍을 제공합니다

SANtricity System Manager로 관리할 수 없는 기존 스토리지 어레이에서 운영 볼륨을 생성한 경우 SANtricity System Manager로 이 어레이에 2차 볼륨을 생성할 수 있습니다.

이 작업에 대해

다른 인터페이스를 사용하는 기존 어레이와 System Manager에서 관리할 수 있는 최신 어레이 간에 비동기식 미러링을 수행할 수 있습니다.

- System Manager를 사용하는 두 스토리지 어레이 간에 미러링할 경우 미러링된 쌍의 생성 순서에 따라 이미 완료된 것이므로 이 작업을 건너뛸 수 있습니다.

- 원격 스토리지 시스템에서 이 작업을 수행합니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. Mirrored Pair * 탭을 선택합니다.

   미러링된 페어 테이블이 나타나고 스토리지 배열과 연결된 모든 미러링된 쌍이 표시됩니다.

3. Incomplete(미완료) 상태의 미러링된 쌍 볼륨을 찾은 다음 미러링된 쌍 열에 표시된 * Complete Mirrored pair(완전 미러링 쌍) * 링크를 클릭합니다.
4. 다음 라디오 버튼 중 하나를 선택하여 미러링된 쌍 생성 시퀀스를 자동으로 완료할지 아니면 수동으로 완료할지를 선택합니다.
   - * 자동 * — 새 보조 볼륨을 생성합니다.

     2차 볼륨을 생성할 기존 풀 또는 볼륨 그룹을 선택하여 미러링된 쌍의 원격 측에 대한 기본 설정을 적용합니다. 이 권장 옵션을 사용하여 보조 볼륨에 예약된 용량을 기본 설정으로 할당합니다.

   - * 수동 * — 기존 볼륨을 선택합니다.

     2차 볼륨에 대한 매개 변수를 정의합니다.

     i. 다음 * 을 클릭하여 보조 볼륨을 선택합니다.

     ii. 보조 볼륨으로 사용할 기존 볼륨을 선택한 후 * Next * 를 클릭하여 예약된 용량을 할당합니다.

     iii. 예약된 용량을 할당합니다. 다음 중 하나를 수행합니다.

     - 기본 설정을 적용합니다.

       예약된 용량의 기본 설정은 기본 볼륨 용량의 20%이며 일반적으로 이 용량이면 충분합니다.

     - 비동기식 미러링과 관련된 데이터 스토리지 요구 사항을 충족하기 위해 예약 용량 설정을 직접 할당합니다.

       필요한 용량은 운영 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 용량을 유지하는 데 필요한 기간에 따라 달라집니다. 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.

       - 미러링 쌍을 장기간 유지하려고 합니다.
       - 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

5. 완료 * 를 선택합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 원격 스토리지 시스템에 보조 볼륨을 생성하고 미러링된 쌍의 원격 측에 예약된 용량을 할당합니다.
- 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화를 시작합니다.
- 미러링되는 볼륨이 씬 볼륨인 경우 초기 동기화 중에 할당된 블록만 보조 볼륨으로 전송됩니다. 이 전송으로 초기

동기화를 완료하기 위해 전송해야 하는 데이터의 양이 줄어듭니다.

- 로컬 스토리지 시스템 및 원격 스토리지 시스템에서 미러링된 쌍에 대한 예약된 용량을 생성합니다.

동기화 미러링 페어를 관리합니다

동기식 미러링에 대한 통신을 테스트합니다

로컬 스토리지 어레이와 원격 스토리지 시스템 간의 통신을 테스트하여 동기 미러링에 참여하는 미러링된 쌍의 통신 문제를 진단할 수 있습니다.

이 작업에 대해

두 가지 테스트가 실행됩니다.

- * 통신 * — 두 스토리지 어레이에 통신 경로가 있는지 확인합니다. 통신 테스트에서는 로컬 스토리지 시스템이 원격 스토리지 시스템과 통신할 수 있고 미러링된 페어와 연결된 보조 볼륨이 원격 스토리지 시스템에 있는지 확인합니다.
- * 지연 시간 * — SCSI 테스트 유닛 명령을 미러링된 페어와 연결된 원격 스토리지 배열의 보조 볼륨으로 전송하여 최소, 평균 및 최대 지연 시간을 테스트합니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.
2. 테스트할 미러링 쌍을 선택한 다음 * 통신 테스트 * 를 선택합니다.
3. Results(결과) 창에 표시된 정보를 검토하고 필요한 경우 표시된 수정 조치를 따릅니다.

> 통신 테스트가 실패하면 미러링된 쌍 간의 통신이 복원될 때까지 이 대화 상자를 닫은 후에도 테스트가 계속 실행됩니다.

미러링된 쌍의 동기화를 일시 중지하고 다시 시작합니다

일시 중지 옵션과 재개 옵션을 사용하여 운영 볼륨의 데이터와 미러링된 쌍의 보조 볼륨의 데이터를 동기화할 시기를 제어할 수 있습니다.

이 작업에 대해

미러링된 쌍이 수동으로 일시 중지된 경우 미러링된 쌍이 수동으로 재개될 때까지 동기화되지 않습니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.
2. 일시 중단 또는 재개할 미러링된 쌍을 선택한 다음 More [Suspend](자세히) 또는 menu: More [Resume](자세히 [재개]) 중 하나를 선택합니다.

   확인 메시지가 표시됩니다.

3. 예 * 를 선택하여 확인합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 미러 관계를 제거하지 않고 미러링된 쌍 간에 데이터 전송을 일시 중단하거나 재개합니다.
- Suspended_Mirrored 쌍의 경우:
  - 미러링된 쌍 테이블에 * Suspended * 를 표시합니다.
  - 동기화가 일시 중단된 동안 미러링된 쌍의 기본 볼륨에 기록된 모든 데이터를 기록합니다.
- _refned_mirrored 쌍의 경우, 동기화가 재개될 때 미러링된 쌍의 보조 볼륨에 데이터를 자동으로 씁니다. 전체 동기화가 필요하지 않습니다.

미러링된 쌍의 볼륨 간에 역할을 변경합니다

동기식 미러링에 사용되는 미러링된 쌍의 두 볼륨 간에 역할 반전을 수행할 수 있습니다. 이 작업은 관리상의 목적이나 로컬 스토리지 어레이에 재해가 발생하는 경우에 필요할 수 있습니다.

이 작업에 대해

운영 볼륨을 보조 역할로 하향 이동하거나 보조 볼륨을 운영 역할로 상향 이동할 수 있습니다. 운영 볼륨에 액세스하는 모든 호스트에는 볼륨에 대한 읽기/쓰기 액세스 권한이 있습니다. 운영 볼륨이 보조 볼륨이 되면 운영 컨트롤러에서 시작한 원격 쓰기만 볼륨에 기록됩니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.
2. 역할을 변경할 볼륨이 포함된 미러링된 쌍을 선택하고 More [Change Role](추가 [역할 변경]) 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

3. 볼륨의 역할을 변경할지 확인한 다음 * 역할 변경 * 을 선택합니다.

   로컬 스토리지 배열이 원격 스토리지 배열과 통신할 수 없는 경우 역할 변경이 요청될 때 시스템에 스토리지 배열에 연결할 수 없음 대화 상자가 표시되지만 원격 스토리지 배열에 연결할 수 없습니다. 예 * 를 클릭하여 역할 변경을 강제 적용합니다.

결과

System Manager에서 다음 작업을 수행합니다.

- 미러링된 쌍의 연결된 볼륨에 연결할 수 있으면 볼륨 간의 역할이 변경됩니다. System Manager는 미러링된 쌍의 보조 볼륨을 기본 역할로 상향 이동하거나 미러링 쌍의 기본 볼륨을 보조 역할로 하향 이동합니다(선택에 따라 다름).

미러링된 쌍의 동기화 설정을 변경합니다

통신 중단 후 미러링된 페어가 재동기화 작업을 완료하는 데 사용하는 동기화 우선 순위 및 재동기화 정책을 변경할 수 있습니다.

이 작업에 대해

운영 볼륨이 포함된 스토리지 어레이에서만 미러링된 쌍의 동기화 설정을 편집할 수 있습니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.

2. 편집하려는 미러링된 쌍을 선택한 다음, MENU: More [Edit settings](추가 [설정 편집])를 선택합니다.

   설정 보기/편집 대화 상자가 표시됩니다.

3. 슬라이더 막대를 사용하여 동기화 우선 순위를 편집합니다.

   동기화 우선 순위는 서비스 입출력 요청과 비교하여 통신 중단 후 재동기화 작업을 완료하는 데 사용되는 시스템 리소스의 양을 결정합니다.

   동기화 속도에 대해 자세히 알아보십시오

   동기화 우선 순위는 5가지입니다.

   - 최저
   - 낮음
   - 중간
   - 높음
   - 최고

   동기화 우선 순위가 가장 낮은 속도로 설정된 경우 입출력 작업의 우선 순위가 지정되고 재동기화 작업이 더 오래 걸립니다. 동기화 우선 순위가 가장 높은 속도로 설정된 경우 재동기화 작업의 우선 순위가 지정되지만 스토리지 시스템의 입출력 작업이 영향을 받을 수 있습니다.

4. 필요에 따라 재동기화 정책을 편집합니다.

   원격 스토리지 시스템에서 미러링된 쌍을 수동 또는 자동으로 재동기화할 수 있습니다.

   - * 수동 * (권장 옵션) — 미러링된 쌍으로 통신이 복구된 후 수동으로 동기화를 재개하려면 이 옵션을 선택합니다. 이 옵션은 데이터를 복구할 수 있는 최적의 기회를 제공합니다.
   - * 자동 * — 통신이 미러링된 쌍으로 복구된 후 재동기화를 자동으로 시작하려면 이 옵션을 선택합니다.

5. 저장 * 을 선택합니다.

동기식 미러 관계를 제거합니다

미러 쌍을 제거하여 로컬 스토리지 배열의 운영 볼륨과 원격 스토리지 배열의 보조 볼륨에서 미러 관계를 제거합니다.

이 작업에 대해

또한 미러링된 쌍을 제거하여 분리된 미러링된 쌍 상태를 수정할 수도 있습니다. 분리된 미러 쌍에 대한 다음 정보를 검토합니다.

- 구성원 볼륨이 한 쪽(로컬/원격)에서 제거되었지만 다른 쪽에는 제거되지 않은 경우 분리된 미러링된 쌍이 존재합니다.
- 어레이 간 통신이 복원되면 분리된 미러링된 쌍이 감지됩니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.

2. 제거하려는 미러링된 쌍을 선택한 다음 Uncommon Tasks[Remove](보기 드문 작업[제거]) 메뉴를 선택합니다.

   미러 관계 제거 대화 상자가 나타납니다.

3. 미러링된 쌍을 제거할지 확인한 다음 * 제거 * 를 클릭합니다.

결과

System Manager는 다음 작업을 수행합니다.

- 로컬 스토리지 시스템 및 원격 스토리지 시스템의 미러링된 페어에서 미러 관계를 제거합니다.
- 운영 볼륨 및 보조 볼륨을 호스트에서 액세스할 수 있고 미러링되지 않은 볼륨으로 반환합니다.
- 동기 미러링 쌍을 제거하여 동기 미러링 타일을 업데이트합니다.

미러링을 비활성화합니다

비동기식 미러링을 비활성화합니다

로컬 및 원격 스토리지 시스템에서 비동기식 미러링을 비활성화하여 스토리지 시스템에서 전용 포트를 정상적으로 사용하도록 다시 설정할 수 있습니다.

시작하기 전에

- 모든 미러 관계를 삭제해야 합니다. 모든 미러 정합성 보장 그룹 및 미러링된 쌍이 로컬 및 원격 스토리지 시스템에서 삭제되었는지 확인합니다.
- 로컬 스토리지 어레이와 원격 스토리지 시스템은 Fibre Channel 패브릭 또는 iSCSI 인터페이스를 통해 접속되어야 합니다.

이 작업에 대해

비동기식 미러링을 비활성화하면 로컬 및 원격 스토리지 시스템에서 미러 작업이 수행되지 않습니다.

단계

1. 메뉴: 스토리지 [비동기 미러링]을 선택합니다.
2. Uncommon Tasks[Deactivate] 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

3. 예 * 를 선택하여 확인합니다.

결과

- 이제 비동기 미러링 통신 전용으로 사용되는 컨트롤러의 HBA 호스트 채널이 호스트 읽기 및 쓰기 요청을 수락할 수 있습니다.
- 이 스토리지 배열의 어느 볼륨도 운영 볼륨 또는 보조 볼륨으로 미러 관계에 참여할 수 없습니다.

동기 미러링을 비활성화합니다

스토리지 어레이에서 동기 미러링 기능을 비활성화하여 미러 데이터 전송용으로 예약된 HBA(호스트 버스 어댑터) 호스트 포트 4의 정상적인 사용을 다시 설정할 수 있습니다.

시작하기 전에

모든 동기식 미러 관계를 삭제해야 합니다. 미러링된 모든 쌍이 스토리지 배열에서 삭제되었는지 확인합니다.

단계

1. 스토리지 [동기식 미러링] 메뉴를 선택합니다.
2. Uncommon Tasks[Deactivate] 메뉴를 선택합니다.

   확인 메시지가 표시됩니다.

3. 예 * 를 선택하여 확인합니다.

결과

- 이제 동기식 미러링 통신 전용의 컨트롤러의 HBA 호스트 포트 4에서 호스트 읽기 및 쓰기 요청을 수락할 수 있습니다.
- 스토리지 배열의 예약된 용량 볼륨이 삭제됩니다.

Async FAQ를 참조하십시오

비동기식 미러링은 동기식 미러링과 어떻게 다릅니까?

비동기 미러링 기능은 동기 미러링 기능과 다릅니다. 한 가지 중요한 방법은 특정 시점의 소스 볼륨 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사하는 것입니다.

동기식 미러링을 사용하면 기본 볼륨의 상태가 특정 시점에 캡처되지 않고 기본 볼륨에서 2차 볼륨으로 이루어진 모든 변경 사항을 반영합니다. 이 유형의 미러에서는 주 볼륨에 쓸 때마다 보조 볼륨에 쓰기가 수행되므로 2차 볼륨은 매 순간마다 1차 볼륨과 동일합니다. 보조 볼륨이 운영 볼륨에서 수행된 변경 사항으로 성공적으로 업데이트될 때까지 호스트는 쓰기가 성공했다는 확인 메시지를 받지 않습니다.

비동기식 미러링을 사용하면 원격 스토리지 시스템이 로컬 스토리지 어레이와 완전히 동기화되지 않으므로 로컬 스토리지 어레이의 손실로 인해 애플리케이션을 원격 스토리지 어레이로 전환해야 하는 경우 일부 트랜잭션이 손실될 수 있습니다.

대칭 복사 피처 비교:

비동기 미러링	동기 미러링
• 복제 방법 *	• * 시점 * 미러링은 사용자 정의 일정에 따라 필요 시 또는 자동으로 수행됩니다. 일정은 분 단위로 정의할 수 있습니다. 동기화 사이의 최소 시간은 10분입니다.
• * 연속 * 미러링은 모든 호스트 쓰기에서 데이터를 복사하여 지속적으로 자동 실행됩니다.	• 예약된 용량 *

비동기 미러링	동기 미러링
• * 다중 * 각 미러링된 쌍에 대해 예약된 용량 볼륨이 필요합니다.	• * 단일 * 미러링된 모든 볼륨에 단일 예약 용량 볼륨이 필요합니다.
• 커뮤니케이션 *	• * iSCSI 및 파이버 채널 * 스토리지 시스템 간의 iSCSI 및 Fibre Channel 인터페이스를 지원합니다.
• 파이버 채널 * 스토리지 시스템 간 Fibre Channel 인터페이스만 지원합니다.	• 거리 *
• * 무제한 * 로컬 스토리지 어레이와 원격 스토리지 시스템 간의 거리 제한이 거의 없으며, 일반적으로 네트워크 기능과 채널 확장 기술에 의해서만 거리가 제한됩니다.	• * 제한 * 일반적으로 지연 시간 및 애플리케이션 성능 요구 사항을 충족하려면 로컬 스토리지 어레이에서 약 10km(6.2마일) 이내에 있어야 합니다.

선택한 미러링 기능에 액세스할 수 없는 이유는 무엇입니까**?**

미러링은 SANtricity Unified Manager 인터페이스에서 구성됩니다.

동기식 미러링은 EF600 또는 EF300 스토리지 어레이에서 사용할 수 없습니다.

두 어레이 간에 미러링을 설정하고 구성하려면 다음을 확인하십시오.

- 웹 서비스 프록시 서비스가 실행되고 있어야 합니다. (Unified Manager는 웹 서비스 프록시와 함께 호스트 시스템에 설치됩니다.)
- Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
- 미러링에 사용할 두 스토리지 어레이가 Unified Manager에서 검색되어야 합니다.
- Unified Manager에는 스토리지 어레이에 대한 유효한 SSL 인증서가 있어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager에서 CA 서명 인증서를 설치할 수 있습니다.

구성 지침은 다음을 참조하십시오.

- "Unified Manager에서 비동기 미러링된 쌍 생성"
- "동기식 미러링 쌍 생성(Unified Manager에서)"

미러 정합성 보장 그룹을 생성하기 전에 알아야 할 내용은 무엇입니까**?**

미러 일관성 그룹을 생성하기 전에 다음 지침을 따르십시오.

EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

Unified Manager의 미러링된 쌍 생성 마법사에서 일관성 그룹을 생성합니다.

Unified Manager에 대한 다음 요구사항을 충족합니다.

- 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
- Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
- Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이에 대한 다음 요구 사항도 충족해야 합니다.

- Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
- 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
- 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
- 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
- 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
- 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.

비동기 미러링 **-** 미러링된 쌍을 만들기 전에 알아야 할 것은 무엇입니까**?**

SANtricity Unified Manager 인터페이스에서 미러링된 쌍을 구성한 다음, SANtricity System Manager에서 쌍을 관리합니다.

대칭 복사된 쌍을 만들기 전에 다음 지침을 따릅니다.

- 두 개의 스토리지 어레이가 있어야 합니다.
- 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
- 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
- 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.
- 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
- 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
- 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
- 웹 서비스 프록시 및 Unified Manager를 설치했습니다. 미러링된 쌍은 Unified Manager 인터페이스에 구성됩니다.

- 두 스토리지 어레이가 Unified Manager에서 검색됩니다.
- 스토리지 시스템에 하나 이상의 미러 정합성 보장 그룹이 있어야 합니다. Unified Manager의 미러링된 쌍 생성 마법사에서 일관성 그룹을 생성합니다.

미러링된 쌍 볼륨에서 예약된 용량을 증가시키기 전에 무엇을 알아야 합니까**?**

일반적으로 미러링된 쌍에 대한 예약된 용량이 가득 차고 있다는 경고가 나타나면 예약된 용량을 늘려야 합니다. 예약 용량은 8GiB의 증분으로 늘릴 수 있습니다.

비동기식 미러링 작업의 경우 예약 용량은 일반적으로 기본 볼륨의 20%입니다. 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.

- 미러링 쌍을 장기간 유지하려고 합니다.
- 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

다음 작업 중 하나를 수행하여 미러링된 쌍에 대해 예약된 용량을 늘릴 수 있습니다.

- Storage[Pools and Volumes Groups](스토리지[풀 및 볼륨 그룹]) 메뉴를 선택한 다음 * Reserved Capacity *(예약된 용량) 탭을 클릭하여 미러링된 쌍 볼륨의 용량 비율을 조정합니다.
- 풀 또는 볼륨 그룹에서 사용 가능한 용량을 사용하여 새 볼륨을 생성합니다.

  풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우 구성되지 않은 용량을 미사용 드라이브 형태로 풀 또는 볼륨 그룹에 추가할 수 있습니다.

요청한 용량으로 예약된 용량을 늘릴 수 없는 이유는 무엇입니까**?**

예약 용량은 4GiB의 증분으로 늘릴 수 있습니다.

다음 지침을 검토하십시오.

- 필요한 경우 확장할 수 있도록 풀 또는 볼륨 그룹에 충분한 가용 용량이 있어야 합니다.

  풀 또는 볼륨 그룹에 사용 가능한 용량이 없는 경우, 할당되지 않은 용량을 미사용 드라이브 형식으로 풀 또는 볼륨 그룹에 추가할 수 있습니다.

- 풀 또는 볼륨 그룹의 볼륨은 최적 상태여야 하며 수정 상태가 아니어야 합니다.
- 용량을 늘리기 위해 사용할 풀 또는 볼륨 그룹에 사용 가능한 용량이 있어야 합니다.

비동기식 미러링 작업의 경우 예약된 용량은 일반적으로 기본 볼륨의 20%입니다. 기본 볼륨에 많은 변경이 있을 것으로 예상되거나 스토리지 오브젝트의 복사 서비스 작업 예상 수명이 매우 길 경우 더 높은 비율을 사용하십시오.

이 비율을 변경하는 이유는 무엇입니까**?**

예약된 용량은 일반적으로 스냅샷 작업을 위한 기본 볼륨의 40%와 비동기식 미러링 작업을 위한 기본 볼륨의 20%입니다.

일반적으로 이 용량이면 충분합니다. 필요한 용량은 기본 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 스토리지 오브젝트의 복사 서비스 작업을 사용할 기간에 따라 달라집니다.

일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 비율을 선택합니다.

- 특정 스토리지 오브젝트의 복사 서비스 작업 수명이 매우 긴 경우
- 입출력 작업이 많은 경우 기본 볼륨에서 데이터 블록의 비율이 크게 변경될 수 있습니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

예약된 용량이 두 개 이상 표시되는 이유는 무엇입니까**?**

풀 또는 볼륨 그룹에 스토리지 객체에 대해 선택한 용량 비율을 충족하는 볼륨이 두 개 이상 있는 경우 여러 후보가 표시됩니다.

복사 서비스 작업을 위해 기본 볼륨에 예약할 물리적 드라이브 공간의 비율을 변경하여 권장되는 후보 목록을 새로 고칠 수 있습니다. 선택한 내용에 따라 가장 적합한 후보가 표시됩니다.

테이블에 사용할 수 없는 값이 표시되는 이유는 무엇입니까**?**

원격 스토리지 배열에 있는 데이터를 표시할 수 없는 경우 테이블에는 사용할 수 없는 값이 나열됩니다.

원격 스토리지 시스템 데이터를 표시하려면 Unified Manager에서 System Manager를 실행합니다.

내 풀 및 볼륨 그룹이 모두 표시되지 않는 이유는 무엇입니까**?**

비동기식 미러링 쌍의 보조 볼륨을 생성하면 비동기식 미러링 쌍의 적합한 풀 및 볼륨 그룹 목록이 표시됩니다. 사용할 수 없는 풀 또는 볼륨 그룹은 해당 목록에 표시되지 않습니다.

풀 또는 볼륨 그룹은 다음과 같은 이유로 적합하지 않을 수 있습니다.

- 풀 또는 볼륨 그룹의 보안 기능이 일치하지 않습니다.
- 풀 또는 볼륨 그룹이 최적화되지 않은 상태입니다.
- 풀 또는 볼륨 그룹의 용량이 너무 작습니다.

비동기식 미러링 **-** 모든 볼륨이 표시되지 않는 이유는 무엇입니까**?**

미러링된 쌍의 기본 볼륨을 선택하면 목록에 모든 적격 볼륨이 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

- 볼륨이 최적이 아닙니다.
- 볼륨이 이미 미러링 관계에 있습니다.
- 씬 볼륨의 경우 자동 확장이 활성화되어야 합니다.

> EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

비동기 미러링 **-** 원격 스토리지 배열의 모든 볼륨을 볼 수 없는 이유는 무엇입니까**?**

원격 스토리지 어레이에서 보조 볼륨을 선택할 경우 목록에 해당 미러링된 쌍에 대해 적합한 볼륨이 모두 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

- 볼륨이 최적이 아닙니다.
- 볼륨이 이미 미러링 관계에 있습니다.
- 운영 볼륨과 2차 볼륨 사이의 씬 볼륨 속성이 일치하지 않습니다.
- DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.
  - 운영 볼륨이 DA를 사용하는 경우 보조 볼륨은 DA를 활성화해야 합니다.
  - 운영 볼륨이 DA를 사용하지 않는 경우 보조 볼륨을 DA로 설정하지 않아야 합니다.

원격 스토리지 어레이의 **IP** 주소를 업데이트하는 이유는 무엇입니까**?**

iSCSI 포트의 IP 주소가 변경되고 로컬 스토리지 배열이 원격 스토리지 배열과 통신할 수 없을 때 원격 스토리지 배열의 IP 주소를 업데이트합니다.

iSCSI 접속과 비동기 미러링 관계를 설정할 때 로컬 및 원격 스토리지 배열은 비동기 미러링 구성에서 원격 스토리지 배열의 IP 주소에 대한 레코드를 저장합니다. iSCSI 포트의 IP 주소가 변경되면 해당 포트를 사용하려는 원격 스토리지 어레이에 통신 오류가 발생합니다.

IP 주소가 변경된 스토리지 배열은 iSCSI 연결을 통해 미러링하도록 구성된 미러 정합성 보장 그룹과 연결된 각 원격 스토리지 배열에 메시지를 보냅니다. 이 메시지를 수신하는 스토리지 어레이는 원격 대상 IP 주소를 자동으로 업데이트합니다.

변경된 IP 주소를 가진 스토리지 배열이 원격 스토리지 배열에 배열 간 메시지를 보낼 수 없는 경우, 시스템은 연결 문제에 대한 경고를 보냅니다. 원격 IP 주소 업데이트 옵션을 사용하여 로컬 스토리지 어레이와의 연결을 다시 설정합니다.

동기화 **FAQ**

비동기식 미러링은 동기식 미러링과 어떻게 다릅니까**?**

비동기 미러링 기능은 동기 미러링 기능과 다릅니다. 한 가지 중요한 방법은 특정 시점의 소스 볼륨 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사하는 것입니다.

동기식 미러링을 사용하면 기본 볼륨의 상태가 특정 시점에 캡처되지 않고 기본 볼륨에서 2차 볼륨으로 이루어진 모든 변경 사항을 반영합니다. 이 유형의 미러에서는 주 볼륨에 쓸 때마다 보조 볼륨에 쓰기가 수행되므로 2차 볼륨은 매 순간마다 1차 볼륨과 동일합니다. 보조 볼륨이 운영 볼륨에서 수행된 변경 사항으로 성공적으로 업데이트될 때까지 호스트는 쓰기가 성공했다는 확인 메시지를 받지 않습니다.

비동기식 미러링을 사용하면 원격 스토리지 시스템이 로컬 스토리지 어레이와 완전히 동기화되지 않으므로 로컬 스토리지 어레이의 손실로 인해 애플리케이션을 원격 스토리지 어레이로 전환해야 하는 경우 일부 트랜잭션이 손실될 수 있습니다.

대칭 복사 피처 비교:

비동기 미러링	동기 미러링
• 복제 방법 *	• * 시점 * 미러링은 사용자 정의 일정에 따라 필요 시 또는 자동으로 수행됩니다. 일정은 분 단위로 정의할 수 있습니다. 동기화 사이의 최소 시간은 10분입니다.
• * 연속 * 미러링은 모든 호스트 쓰기에서 데이터를 복사하여 지속적으로 자동 실행됩니다.	• 예약된 용량 *
• * 다중 * 각 미러링된 쌍에 대해 예약된 용량 볼륨이 필요합니다.	• * 단일 * 미러링된 모든 볼륨에 단일 예약 용량 볼륨이 필요합니다.
• 커뮤니케이션 *	• * iSCSI 및 파이버 채널 * 스토리지 시스템 간의 iSCSI 및 Fibre Channel 인터페이스를 지원합니다.
• 파이버 채널 * 스토리지 시스템 간 Fibre Channel 인터페이스만 지원합니다.	• 거리 *
• * 무제한 * 로컬 스토리지 어레이와 원격 스토리지 시스템 간의 거리 제한이 거의 없으며, 일반적으로 네트워크 기능과 채널 확장 기술에 의해서만 거리가 제한됩니다.	• * 제한 * 일반적으로 지연 시간 및 애플리케이션 성능 요구 사항을 충족하려면 로컬 스토리지 어레이에서 약 10km(6.2마일) 이내에 있어야 합니다.

동기 미러링 **-** 내 볼륨을 모두 볼 수 없는 이유는 무엇입니까**?**

미러링된 쌍의 기본 볼륨을 선택하면 목록에 모든 적격 볼륨이 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

- 볼륨은 스냅샷 볼륨 또는 씬 볼륨과 같은 비표준 볼륨입니다.
- 볼륨이 최적이 아닙니다.
- 볼륨이 이미 미러링 관계에 있습니다.

동기 미러링 **-** 원격 스토리지 어레이의 모든 볼륨이 표시되지 않는 이유는 무엇입니까**?**

원격 스토리지 어레이에서 보조 볼륨을 선택할 경우 목록에 해당 미러링된 쌍에 대해 적합한 볼륨이 모두 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

- 볼륨은 스냅샷 볼륨 또는 씬 볼륨과 같은 비표준 볼륨입니다.
- 볼륨이 최적이 아닙니다.
- 볼륨이 이미 미러링 관계에 있습니다.
- DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.
  - 운영 볼륨이 DA를 사용하는 경우 보조 볼륨은 DA를 활성화해야 합니다.
  - 운영 볼륨이 DA를 사용하지 않는 경우 보조 볼륨을 DA로 설정하지 않아야 합니다.

동기식 미러링 **-** 미러링된 쌍을 만들기 전에 알아야 할 것은 무엇입니까**?**

SANtricity Unified Manager 인터페이스에서 미러링된 쌍을 구성한 다음, SANtricity System Manager에서 쌍을 관리합니다.

대칭 복사 쌍을 만들기 전에 다음 지침을 따릅니다.

- 두 개의 스토리지 어레이가 있어야 합니다.
- 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
- 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
- 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭을 통해 연결됩니다.
- 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
- 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
- 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
- 웹 서비스 프록시 및 Unified Manager를 설치했습니다. 미러링된 쌍은 Unified Manager 인터페이스에 구성됩니다.
- 두 스토리지 어레이가 Unified Manager에서 검색됩니다.

동기화 우선 순위가 동기화 속도에 어떤 영향을 미칩니까**?**

동기화 우선 순위는 시스템 성능과 관련하여 동기화 작업에 할당되는 처리 시간을 정의합니다.

운영 볼륨의 컨트롤러 소유자가 이 작업을 백그라운드에서 수행합니다. 동시에 컨트롤러 소유자가 운영 볼륨에 대한 로컬 I/O 쓰기 및 보조 볼륨에 대한 관련 원격 쓰기를 처리합니다. 재동기화는 컨트롤러 처리 리소스를 입출력 작업에서 전환하므로 재동기화는 호스트 애플리케이션의 성능에 영향을 미칠 수 있습니다.

동기화 우선 순위가 얼마나 오래 걸릴 수 있고 동기화 우선 순위가 시스템 성능에 어떤 영향을 미칠 수 있는지 결정할 수 있도록 이 지침을 염두에 두십시오.

동기화 우선 순위 속도 정보

다음과 같은 우선 순위가 있습니다.

- 최저
- 낮음
- 중간
- 높음
- 최고

우선 순위가 가장 낮은 속도는 시스템 성능을 지원하지만 재동기화에 더 많은 시간이 걸립니다. 우선 순위가 가장 높은 속도가 재동기화를 지원하지만 시스템 성능이 저하될 수 있습니다.

이 지침은 우선 순위 간의 차이를 대략적으로 나타냅니다.

전체 동기화의 우선 순위 속도	최고 동기화 속도에 비해 경과된 시간입니다
최저	최고 우선 순위인 경우 약 8배
낮음	최고 우선 순위인 경우 약 6배
중간	가장 높은 우선 순위에서 약 3배 반 정도 소요됩니다.
높음	최고 우선 순위보다 약 2배 긴 시간.

볼륨 크기 및 호스트 I/O 속도 로드는 동기화 시간 비교에 영향을 줍니다.

수동 동기화 정책을 사용하는 것이 권장되는 이유는 무엇입니까**?**

수동 재동기화는 재동기화 프로세스를 관리하여 데이터를 복구할 수 있는 최적의 기회를 제공하기 때문에 권장됩니다.

자동 재동기화 정책을 사용하고 재동기화 중에 간헐적인 통신 문제가 발생하는 경우 보조 볼륨의 데이터가 일시적으로 손상될 수 있습니다. 재동기화가 완료되면 데이터가 수정됩니다.

원격 스토리지

원격 스토리지 기능 개요

원격 스토리지 기능이 있는 경우 원격 스토리지 시스템에서 스토리지 시스템으로 데이터를 가져올 수 있습니다.

원격 스토리지 기능이란 무엇입니까?

원격 스토리지 _ 기능을 사용하면 원격 스토리지 시스템에서 로컬 E-Series 스토리지 시스템으로 데이터를 가져올 수 있습니다. 원격 시스템은 다른 E-Series 시스템일 수도 있고 다른 공급업체의 시스템일 수도 있습니다. 이 기능은 장비를 업그레이드하는 동안 다운타임을 최소화하면서 데이터 마이그레이션을 간소화하려는 경우에 유용합니다.

원격 저장소를 사용하려면 하위 모델 ID(SMID)에서 이 기능을 활성화해야 합니다.

자세한 내용:

- "원격 스토리지의 작동 방식"
- "원격 스토리지 용어"
- "원격 스토리지 요구 사항"
- "원격 스토리지 볼륨 요구 사항"

이 기능을 사용하여 데이터를 가져오려면 어떻게 해야 합니까?

원격 스토리지 마법사를 사용하여 원격 스토리지 장치(데이터 가져오기 소스)를 E-Series 시스템의 타겟 볼륨에 매핑합니다. 이 마법사는 스토리지 [원격 스토리지] 메뉴에서 사용할 수 있습니다.

자세한 내용:

- "원격 저장소 가져오기"
- "데이터 가져오기의 진행률을 관리합니다"

개념

원격 스토리지의 작동 방식

원격 스토리지 기능을 사용하면 원격 스토리지 시스템에서 로컬 E-Series 스토리지 시스템으로 데이터를 가져올 수 있습니다. 이 기능은 장비를 업그레이드하는 동안 다운타임을 최소화하면서 데이터 마이그레이션을 간소화하려는 경우에 유용합니다.

원격 스토리지 기능을 구성하려면 하드웨어를 설정한 다음 System Manager를 사용하여 원격 스토리지 객체를 생성해야 합니다. 이 구성이 완료되면 가져오기 프로세스가 시작됩니다.

하드웨어 설정

다음 워크플로를 사용하여 하드웨어 연결을 준비합니다.

이러한 단계는 E-Series 및 SANtricity 설명서 센터, 및 에서 "원격 스토리지 기술 보고서" 사용할 수 있는 원격 스토리지 기능에 대한 사용자 가이드에 자세히 설명되어 있습니다. "원격 스토리지 볼륨 개요"

로컬 E-Series 스토리지 시스템:

1. 각 컨트롤러에 원격 스토리지 시스템에 대한 iSCSI 연결이 있는지 확인합니다. 이 연결을 통해 로컬 E-Series 시스템은 원격 시스템에서 호스트로 설정할 수 있는 iSCSI 이니시에이터 역할을 합니다.
2. 가져오기 작업을 위한 대상 볼륨을 생성합니다. 볼륨에 원격 스토리지 시스템의 소스 볼륨과 같거나 큰 용량이 있고 블록 크기가 일치하며 매핑되지 않았는지 확인합니다. 을 "볼륨 생성"참조하십시오.

3. System Manager 인터페이스에서 로컬 E-Series 시스템에 대한 IQN(iSCSI Qualified Name)을 수집합니다. IQN은 나중에 로컬 E-Series 시스템을 원격 스토리지 시스템의 호스트로 설정하는 데 사용됩니다. System Manager에서 메뉴: 설정 [시스템 > iSCSI 설정 > 대상 IQN] 으로 이동합니다.

원격 스토리지 시스템에서 다음을 수행합니다.

1. IQN을 사용하여 원격 시스템에서 로컬 E-Series 시스템을 호스트로 설정합니다. 다음과 같이 적절한 호스트 유형을 설정해야 합니다.
   - 원격 시스템이 E-Series 모델인 경우 을 참조하십시오."호스트 및 호스트 클러스터 개요" "공장 출하 시 기본값 "의 호스트 유형을 사용합니다.
   - 원격 시스템이 다른 공급업체의 시스템인 경우 사용 가능한 옵션에 따라 적절한 호스트 유형을 선택합니다.
2. 모든 I/O를 중지하고, 파일 시스템을 마운트 해제하고, 소스 볼륨의 호스트 또는 애플리케이션에 대한 할당을 제거합니다.
3. 새로 생성한 로컬 E-Series 스토리지 시스템 호스트에 볼륨을 할당합니다.
4. 선택한 소스 볼륨에 대해 원격 스토리지 시스템에서 다음 정보를 수집하여 가져오기를 생성할 수 있도록 합니다.
   - IQN(iSCSI Qualified Name)
   - iSCSI IP 주소입니다
   - 소스 볼륨의 LUN 번호입니다

System Manager 설정

다음 워크플로우를 사용하여 가져올 원격 스토리지 객체를 생성합니다.

1. System Manager 인터페이스의 원격 스토리지 마법사를 사용하여 원격 스토리지 장치(데이터 가져오기 소스)를 E-Series 시스템의 타겟 볼륨에 매핑합니다. 마침 * 을 선택하면 가져오기 프로세스가 시작됩니다.
2. View Operations(작업 보기) 대화 상자 또는 Operations in Progress(작업 진행 중) 패널에서 가져오기를 모니터링합니다. 필요한 경우 프로세스를 일시 중지하고 다시 시작할 수도 있습니다.
3. 필요한 경우 가져오기가 완료되면 소스 볼륨과 타겟 볼륨 간의 연결을 끊거나 향후 가져오기를 위해 연결을 유지합니다.

원격 스토리지 용어

스토리지 어레이에 원격 스토리지 조건이 적용되는 방법에 대해 알아보십시오.

기간	설명
IQN을 선택합니다	iSCSI 이니시에이터 또는 타겟의 고유한 이름인 IQN(iSCSI Qualified Name) 식별자입니다.
LUN입니다	액세스를 위해 호스트에 제공할 수 있는 논리 유닛을 식별하는 데 사용되는 논리 유닛 번호입니다.
원격 스토리지 시스템	데이터가 처음 상주하는 스토리지 시스템입니다. 원격 스토리지 시스템은 E-Series 모델이거나 다른 공급업체의 시스템일 수 있습니다.

기간	설명
원격 저장 장치	데이터가 원격 시스템에 처음 저장되는 물리적 또는 논리적 디바이스입니다. E-Series 스토리지 시스템에서 이를 "볼륨"이라고 합니다.
원격 스토리지 객체	E-Series 시스템이 원격 스토리지 시스템을 식별 및 연결할 수 있는 정보가 포함된 객체입니다. 이 정보에는 원격 스토리지 시스템의 IQN 및 IP 주소가 포함됩니다. 원격 스토리지 개체는 원격 스토리지 시스템과 E-Series 시스템 간의 통신을 나타냅니다.
원격 스토리지 볼륨	E-Series 시스템의 표준 볼륨으로 원격 스토리지 장치에 데이터를 액세스할 수 있습니다.
볼륨	데이터가 저장된 컨테이너입니다. 호스트가 데이터를 액세스할 수 있도록 생성되는 논리적 구성 요소입니다.

원격 스토리지 기능 요구 사항

원격 스토리지 기능을 사용하기 전에 다음 요구 사항 및 제한 사항을 검토하십시오.

지원되는 프로토콜

지원되는 프로토콜은 다음과 같습니다.

- iSCSI
- IPv4를 참조하십시오

최신 E-Series 지원 및 구성 정보는 를 참조하십시오. "NetApp 상호 운용성 매트릭스 툴"

하드웨어 요구 사항

E-Series 스토리지 시스템에는 다음이 포함되어야 합니다.

- 컨트롤러 2개(이중 모드)
- 하나 이상의 iSCSI 연결을 통해 두 E-Series 컨트롤러가 원격 스토리지 시스템과 통신할 수 있도록 지원합니다
- SANtricity OS 11.71 이상
- 하위 모델 ID(SMID)에서 활성화된 원격 스토리지 기능

원격 시스템은 E-Series 스토리지 시스템이거나 다른 공급업체의 시스템일 수 있습니다. 여기에는 다음이 포함되어야 합니다.

- iSCSI 지원 인터페이스

제한 사항

원격 스토리지 기능에는 다음과 같은 제한 사항이 있습니다.

- 미러링이 비활성화되어야 합니다.
- E-Series 시스템의 타겟 볼륨에 스냅샷이 없어야 합니다.

- 가져오기를 시작하기 전에 E-Series 시스템의 타겟 볼륨을 호스트에 매핑해서는 안 됩니다.
- E-Series 시스템의 타겟 볼륨에 리소스 프로비저닝이 비활성화되어 있어야 합니다.
- 원격 스토리지 볼륨을 호스트나 여러 호스트에 직접 매핑하지 않습니다.
- 웹 서비스 프록시는 지원되지 않습니다.
- iSCSI CHAP 암호는 지원되지 않습니다.
- SMcli는 지원되지 않습니다.
- VMware 데이터 저장소는 지원되지 않습니다.
- 가져오기 페어가 있는 경우 관계/가져오기 페어에 있는 스토리지 시스템 하나만 한 번에 업그레이드할 수 있습니다.

원격 스토리지 볼륨 요구 사항

가져오기에 사용되는 볼륨은 크기, 상태 및 기타 조건에 대한 요구 사항을 충족해야 합니다.

원격 스토리지 볼륨

가져오기의 소스 볼륨을 "원격 저장소 볼륨"이라고 합니다. 이 볼륨은 다음 기준을 충족해야 합니다.

- 다른 불러오기의 일부가 될 수 없습니다
- 온라인 상태여야 합니다

가져오기가 시작되면 컨트롤러 펌웨어가 백그라운드에서 원격 저장소 볼륨을 생성합니다. 이러한 백그라운드 프로세스로 인해 원격 스토리지 볼륨은 System Manager에서 관리할 수 없으며 가져오기 작업에만 사용할 수 있습니다.

생성된 원격 스토리지 볼륨은 E-Series 시스템에서 다른 표준 볼륨과 마찬가지로 취급되며, 다음과 같은 예외가 있습니다.

- 원격 스토리지 디바이스의 프록시로 사용할 수 있습니다.
- 다른 볼륨 복사본 또는 스냅샷의 대상으로 사용할 수 없습니다.
- 가져오기가 진행 중인 동안에는 Data Assurance 설정을 변경할 수 없습니다.
- 가져오기 작업을 위해 엄격하게 예약되었으므로 어떤 호스트에도 매핑할 수 없습니다.

각 원격 스토리지 볼륨은 하나의 원격 스토리지 오브젝트에만 연결되지만 하나의 원격 스토리지 객체는 여러 원격 스토리지 볼륨과 연결될 수 있습니다. 원격 스토리지 볼륨은 다음 조합을 사용하여 고유하게 식별됩니다.

- 원격 스토리지 객체 식별자입니다
- 원격 스토리지 디바이스 LUN 번호입니다

타겟 볼륨 후보

타겟 볼륨은 로컬 E-Series 시스템의 타겟 볼륨입니다. 대상 볼륨은 다음 기준을 충족해야 합니다.

- RAID/DDP 볼륨이어야 합니다.
- 원격 스토리지 볼륨과 같거나 큰 용량이 있어야 합니다.
- 원격 스토리지 볼륨과 동일한 블록 크기가 있어야 합니다.

- 유효한 상태(최적)가 있어야 합니다.
- 볼륨 복사본, 스냅샷 복사본, 비동기식 또는 동기식 미러링과 같은 관계는 가질 수 없습니다.
- DDP, 동적 볼륨 확장, 동적 용량 확장, 동적 세그먼트 크기, 동적 RAID 마이그레이션, 동적 용량 감소 등의 재구성 작업을 수행할 수 없습니다. 또는 조각 모음.
- 가져오기를 시작하기 전에 호스트에 매핑할 수 없습니다. 그러나 가져오기가 완료된 후에 매핑할 수 있습니다.
- FRC(Flash Read Cached)를 활성화할 수 없습니다.

System Manager는 원격 스토리지 가져오기 마법사의 일부로 이러한 요구 사항을 자동으로 확인합니다. 대상 볼륨 선택을 위해 모든 요구 사항을 충족하는 볼륨만 표시됩니다.

원격 스토리지 관리

원격 저장소 가져오기

원격 시스템에서 로컬 E-Series 스토리지 시스템으로 스토리지 가져오기를 시작하려면 원격 스토리지 가져오기 마법사를 사용합니다.

시작하기 전에

- E-Series 스토리지 시스템은 원격 스토리지 시스템과 통신하도록 구성해야 합니다.

> 하드웨어 구성에 대한 자세한 내용은 E-Series 및 SANtricity 설명서 센터 의 및 에 나와 있는 원격 스토리지 기능의 사용자 가이드에 나와 있습니다 "원격 스토리지 기술 보고서". "하드웨어를 구성합니다"

- 원격 스토리지 시스템의 경우 다음 정보를 수집합니다.
  - iSCSI IQN입니다
  - iSCSI IP 주소입니다
  - 원격 스토리지 디바이스의 LUN 번호(소스 볼륨)
- 로컬 E-Series 스토리지 시스템의 경우 데이터 가져오기에 사용할 볼륨을 생성하거나 선택합니다. 을 "볼륨 생성 "참조하십시오. 타겟 볼륨은 다음 요구 사항을 충족해야 합니다.
  - 원격 스토리지 디바이스(소스 볼륨)의 블록 크기와 일치합니다.
  - 원격 스토리지 디바이스보다 크거나 같은 용량을 가지고 있습니다.
  - 은(는) 최적 상태이며 사용 가능합니다.

전체 요구 사항 목록은 을 "원격 스토리지 볼륨 요구 사항"참조하십시오.

- * 권장: * 가져오기 프로세스를 시작하기 전에 원격 스토리지 시스템의 볼륨을 백업합니다.

이 작업에 대해

이 작업에서는 원격 스토리지 장치와 로컬 E-Series 스토리지 시스템의 볼륨 간에 매핑을 생성합니다. 구성을 마치면 불러오기가 시작됩니다.

많은 변수가 가져오기 작업과 완료 시간에 영향을 줄 수 있으므로 먼저 더 작은 ""테스트"" 가져오기를 수행하는 것이 좋습니다. 이 테스트를 사용하여 모든 연결이 예상대로 작동하는지, 가져오기 작업이 적절한 시간 내에 완료되는지 확인합니다.

단계

1. Storage[Remote storage](저장[원격 저장]) 메뉴를 선택합니다.
2. 원격 저장소 가져오기 * 를 클릭합니다.

   원격 스토리지 가져오기 마법사가 표시됩니다.

3. 소스 구성 패널의 * 단계 1a * 에서 연결 정보를 입력합니다. 다른 iSCSI 연결을 추가하려면 * 다른 IP 주소 추가 * 를 클릭하여 원격 스토리지에 대한 추가 IP 주소를 포함합니다. 완료되면 * 다음 * 을 클릭합니다.

   필드 상세정보

설정	설명
이름	System Manager 인터페이스에서 식별할 원격 스토리지 디바이스의 이름을 입력합니다. 이름에는 최대 30자를 사용할 수 있으며 문자, 숫자 및 밑줄(_), 대시(-) 및 해시 기호(#)와 같은 특수 문자만 포함할 수 있습니다. 이름에는 공백이 포함될 수 없습니다.
iSCSI 연결 속성	원격 스토리지 디바이스의 접속 속성을 입력합니다. • * IQN(iSCSI Qualified Name) *: iSCSI IQN을 입력합니다. • * IP 주소 *: IPv4 주소를 입력합니다. • * 포트 *: 소스 디바이스와 타겟 디바이스 간의 통신에 사용할 포트 번호를 입력합니다. 기본적으로 포트 번호는 3260입니다.

   Next*를 클릭하면 Configure Source 패널의 * Step 1b*가 표시됩니다.

4. LUN * 필드에서 소스로 사용할 원격 스토리지 디바이스의 LUN 번호를 선택한 후 * Next * 를 클릭합니다.

   Configure Target(대상 구성) 패널이 열리고 가져오기의 대상으로 사용할 볼륨 후보를 표시합니다. 일부 볼륨은 블록 크기, 용량 또는 볼륨 가용성 때문에 후보 목록에 표시되지 않습니다.

5. 이 표에서 E-Series 스토리지 시스템의 타겟 볼륨을 선택합니다. 필요한 경우 슬라이더를 사용하여 가져오기 우선 순위를 변경합니다. 다음 * 을 클릭합니다. 다음 대화 상자에서 를 입력한 다음 * 계속 * 을 클릭하여 작업을 `continue` 확인합니다.

   타겟 볼륨의 용량이 소스 볼륨보다 큰 경우 E-Series 시스템에 연결된 호스트에 추가 용량이 보고되지 않습니다. 새 용량을 사용하려면 가져오기 작업이 완료되고 연결이 끊긴 후에 호스트에서 파일 시스템 확장 작업을 수행해야 합니다.

   대화 상자에서 구성을 확인하면 Review(검토) 패널이 표시됩니다.

6. Review(검토) 패널에서 설정이 정확한지 확인한 다음 * Finish(마침) * 를 클릭하여 가져오기를 시작합니다.

   다른 가져오기를 시작할지 묻는 다른 대화 상자가 열립니다.

7. 필요한 경우 * 예 * 를 클릭하여 다른 원격 스토리지 가져오기를 생성합니다. 예 * 를 클릭하면 소스 구성 패널의 * 단계 1a * 로 돌아갑니다. 여기서 기존 구성을 선택하거나 새 구성을 추가할 수 있습니다. 다른 불러오기를 생성하지 않으려면 * No * 를 클릭하여 대화 상자를 종료합니다.

   가져오기 프로세스가 시작되면 전체 타겟 볼륨을 복사된 데이터로 덮어씁니다. 이 프로세스 중에 호스트가 타겟 볼륨에 새 데이터를 쓰는 경우 새 데이터가 원격 디바이스(소스 볼륨)로 다시 전파됩니다.

8. 원격 스토리지 패널 아래의 작업 보기 대화 상자에서 작업 진행률을 확인합니다.

결과

가져오기 작업을 완료하는 데 필요한 시간은 원격 스토리지 시스템의 크기, 가져오기에 대한 우선 순위 설정 및 스토리지 시스템과 관련 볼륨 모두의 입출력 로드 양에 따라 달라집니다.

가져오기가 완료되면 로컬 볼륨은 원격 저장소 장치의 중복입니다.

작업을 마친 후

두 볼륨 간의 관계를 끊을 준비가 되면 Operations in Progress(작업 진행 중) 보기에서 가져오기 개체의 * Disconnect *(연결 해제 *)를 선택합니다. 관계가 끊기면 로컬 볼륨의 성능이 정상으로 돌아오며 더 이상 원격 연결의 영향을 받지 않습니다.

원격 스토리지 가져오기 진행률을 관리합니다

가져오기 프로세스가 시작된 후 진행 상황을 확인하고 조치를 취할 수 있습니다.

이 작업에 대해

각 가져오기 작업에 대해 작업 진행 중 대화 상자에 완료율과 남은 예상 시간이 표시됩니다. 작업에는 가져오기 우선 순위 변경, 작업 중지 및 다시 시작, 작업 연결 해제 등이 있습니다.

홈 페이지(메뉴: 홈 [진행 중인 작업 표시])에서 진행 중인 작업을 볼 수도 있습니다.

단계

1. 원격 저장소 페이지에서 * 작업 보기 * 를 선택합니다.

   작업 진행 중 대화 상자가 표시됩니다.

2. 필요한 경우 * Actions * 열의 링크를 사용하여 작업을 중지 및 재개하거나, 우선 순위를 변경하거나, 작업 연결을 끊습니다.
   - * 우선 순위 변경 * — 진행 중이거나 보류 중인 작업의 처리 우선 순위를 변경하려면 * 우선 순위 변경 * 을 선택합니다. 작업에 우선 순위를 적용하고 * OK * 를 클릭합니다.
   - * 중지 * — 원격 저장 장치에서 데이터 복사를 일시 중지하려면 * 중지 * 를 선택합니다. 가져오기 쌍 간의 관계는 그대로 유지되며 가져오기 작업을 계속할 준비가 되면 * Resume * 을 선택할 수 있습니다.
   - * 재개 * — 중지된 위치에서 중지되거나 실패한 프로세스를 시작하려면 * 재시작 * 을 선택합니다. 그런 다음 Resume 작업에 우선 순위를 적용하고 * OK * 를 클릭합니다. 이 작업은 처음부터 가져오기를 _not_다시 시작합니다. 처음부터 프로세스를 다시 시작하려면 * Disconnect * 를 선택한 다음 원격 저장소 가져오기 마법사를 통해 가져오기를 다시 만들어야 합니다.

◦ * Disconnect * — 중지, 완료 또는 실패한 가져오기 작업을 위해 소스 볼륨과 대상 볼륨 간의 관계를 끊으려면 * Disconnect * 를 선택합니다.

원격 스토리지에 대한 접속 설정을 수정합니다

설정 보기/편집 옵션을 통해 원격 저장소 구성에 대한 연결 설정을 편집, 추가 또는 삭제할 수 있습니다.

이 작업에 대해

연결 속성을 변경하면 진행 중인 가져오기에 영향을 줍니다. 중단을 방지하려면 가져오기가 실행되지 않을 때만 연결 속성을 변경합니다.

단계

1. Storage[Remote storage](저장[원격 저장]) 메뉴를 선택합니다.
2. 목록에서 수정할 원격 스토리지 객체를 선택합니다.
3. 설정 보기/편집 * 을 클릭합니다.

   원격 저장소 설정 대화 상자가 표시됩니다.

4. 연결 속성 * 탭을 클릭합니다.

   원격 스토리지 가져오기에 대해 구성된 IP 주소 및 포트 설정이 표시됩니다.

5. 다음 작업 중 하나를 수행합니다.
   ◦ * 편집 * — 원격 스토리지 객체의 해당 라인 항목 옆에 있는 * 편집 * 을 클릭합니다. 필드에 수정된 IP 주소 및 /또는 포트 정보를 입력합니다.
   ◦ * 추가 * — * 추가 * 를 클릭한 다음 제공된 필드에 새 IP 주소와 포트 정보를 입력합니다. Add * 를 클릭하여 확인하면 원격 스토리지 객체 목록에 새 접속이 나타납니다.
   ◦ * 삭제 * — 목록에서 원하는 연결을 선택한 다음 * 삭제 * 를 클릭합니다. 제공된 필드에 입력한 다음 * Delete * 를 클릭하여 작업을 `delete` 확인합니다. 원격 스토리지 객체 목록에서 연결이 제거됩니다.
6. 저장 * 을 클릭합니다.

   수정된 접속 설정이 원격 스토리지 객체에 적용됩니다.

원격 스토리지 객체를 제거합니다

가져오기가 완료된 후 로컬 디바이스와 원격 디바이스 간에 더 이상 데이터를 복사하지 않으려면 원격 스토리지 객체를 제거할 수 있습니다.

시작하기 전에

제거하려는 원격 스토리지 객체와 연결된 가져오기가 없는지 확인합니다.

이 작업에 대해

원격 스토리지 객체를 제거하면 로컬 디바이스와 원격 디바이스 간의 접속이 제거됩니다.

단계

1. Storage[Remote storage](저장[원격 저장]) 메뉴를 선택합니다.
2. 목록에서 제거할 원격 스토리지 객체를 선택합니다.
3. 제거 * 를 클릭합니다.

   원격 스토리지 연결 제거 확인 대화 상자가 표시됩니다.

4. 를 입력한 다음 * 제거 * 를 클릭하여 작업을 `remove` 확인합니다.

   선택한 원격 스토리지 객체가 제거됩니다.

FAQ 를 참조하십시오

원격 스토리지 접속을 생성하기 전에 알아야 할 사항은 무엇입니까?

원격 스토리지 기능을 구성하려면 iSCSI를 통해 원격 디바이스 및 타겟 스토리지 시스템을 직접 연결해야 합니다.

iSCSI 시스템 연결을 설정하려면 다음을 참조하십시오.

- "iSCSI 포트를 구성합니다"
- "원격 스토리지 기술 보고서"

원격 볼륨을 제거하라는 메시지가 표시되는 이유는 무엇입니까?

최대 원격 볼륨 수에 도달하면 스토리지 시스템이 사용되지 않는 원격 볼륨을 자동으로 감지하여 제거하라는 메시지를 표시합니다.

생성 프로세스 중에 사용되지 않는 원격 볼륨이 정리되지 않는 경우가 있습니다. 추가 가져오기 작업을 시작하기 전에 시스템이 최적이고 네트워크 연결이 안정적인지 확인하십시오.

대상 어레이에 내 볼륨이 모두 표시되지 않는 이유는 무엇입니까?

원격 스토리지 기능에 대한 가져오기를 구성할 때 블록 크기, 용량 또는 볼륨 가용성 때문에 일부 볼륨이 대상 후보 목록에 나타나지 않을 수 있습니다.

목록에 표시하려면 볼륨 후보:

- 원격 볼륨과 같거나 큰 용량입니다.
- 원격 볼륨과 동일한 블록 크기
- 현재 최적 상태입니다.

다음과 같은 경우 목록에서 볼륨 후보가 제외됩니다.

- 볼륨 복사본, 스냅샷 또는 미러링과 같은 모든 관계
- 재구성 작업이 진행 중입니다.
- 다른 디바이스(호스트 또는 호스트 클러스터)에 매핑

- 읽기 플래시 캐시가 설정되었습니다.

가져오기 시 원격 볼륨에 대해 알아야 할 사항은 무엇입니까**?**

원격 스토리지 기능을 사용할 때는 원격 볼륨이 데이터를 가져온 소스라는 점에 유의해야 합니다.

가져오기가 진행 중이면 데이터가 원격 볼륨에서 대상 스토리지 시스템의 타겟 볼륨으로 전송됩니다. 이러한 두 볼륨의 블록 크기가 일치해야 합니다.

원격 스토리지 가져오기를 시작하기 전에 알아야 할 내용은 무엇입니까**?**

원격 스토리지 기능을 사용하면 원격 스토리지 시스템의 데이터를 로컬 E-Series 스토리지 시스템의 볼륨으로 복사할 수 있습니다. 이 기능을 사용하기 전에 다음 지침을 검토하십시오.

구성

원격 스토리지 가져오기를 생성하기 전에 다음 작업을 완료하고 다음 조건을 확인해야 합니다.

- 로컬 E-Series 스토리지 시스템의 각 컨트롤러에 원격 스토리지 시스템에 대한 iSCSI 연결이 있는지 확인합니다.
- 로컬 E-Series 스토리지 시스템에서 가져오기 작업을 위한 타겟 볼륨을 생성합니다. 볼륨에 소스 볼륨과 같거나 큰 용량이 있고, 소스 볼륨과 일치하는 블록 크기가 있으며, 매핑되지 않았는지 확인합니다. 을 "볼륨 생성 "참조하십시오.
- IQN(iSCSI Qualified Name)을 사용하여 원격 시스템에서 로컬 E-Series 스토리지 시스템을 호스트로 설정합니다. 설정 [시스템 > iSCSI 설정 > 대상 IQN] 메뉴에서 IQN을 볼 수 있습니다. 또한 사용 중인 시스템에 따라 적절한 호스트 유형을 설정해야 합니다.
- 모든 입출력을 중지하고, 파일 시스템을 마운트 해제하고, 원격 스토리지 시스템에서 선택한 볼륨에 대한 호스트 또는 애플리케이션에 대한 할당을 제거합니다.
- 원격 스토리지 시스템에 볼륨을 새로 생성한 로컬 E-Series 스토리지 시스템 호스트에 할당합니다.
- 가져오기를 생성할 수 있도록 원격 스토리지 시스템에서 다음 정보를 수집합니다.
  - IQN(iSCSI Qualified Name)
  - iSCSI IP 주소입니다
  - 소스 데이터가 생성되는 원격 스토리지 디바이스의 LUN 번호입니다
- 가져오기 프로세스가 시작되면 전체 로컬 대상 볼륨을 복사된 데이터로 덮어씁니다. 로컬 대상 볼륨에 기록된 새 데이터는 가져오기가 생성된 후 원격 스토리지 장치의 볼륨에 전파됩니다. 따라서 가져오기 프로세스를 시작하기 전에 원격 스토리지 시스템의 볼륨을 백업하는 것이 좋습니다.

가져오기 프로세스

다음 단계에서는 가져오기 프로세스를 간략하게 설명합니다.

1. System Manager 인터페이스에 액세스한 다음 * 원격 스토리지 * 페이지로 이동합니다. 가져오기 * 를 선택하여 새 가져오기 생성을 시작합니다. 자세한 지침은 을 참조하십시오"원격 저장소 가져오기".

   오프라인 가져오기를 수행하려면 가져오기가 완료될 때까지 대상 볼륨을 매핑하지 마십시오.

2. 가져오기 진행률을 모니터링합니다.

가져오기가 시작되면 타겟 볼륨을 매핑할 수 있습니다. 가져오기 작업을 완료하는 데 필요한 시간은 원격 스토리지 디바이스(소스 볼륨) 크기, 가져오기의 우선 순위 설정, 스토리지 시스템과 관련 볼륨 모두의 입출력 로드 양에 따라 달라집니다.

가져오기 완료 후 타겟 볼륨은 소스의 중복입니다.

3. 매핑 관계를 끊을 준비가 되면 * Operations in Progress * 패널에서 가져오기 개체에 대해 * Disconnect * 를 수행합니다.

가져오기의 연결이 끊기면 로컬 대상의 성능이 정상으로 되돌아가고 원격 연결의 영향을 더 이상 받지 않습니다.

제한 사항

원격 스토리지 기능에는 다음과 같은 제한 사항이 있습니다.

- 미러링이 비활성화되어야 합니다.
- E-Series 시스템의 타겟 볼륨에 스냅샷이 없어야 합니다.
- 가져오기를 시작하기 전에 E-Series 시스템의 타겟 볼륨을 호스트에 매핑해서는 안 됩니다.
- E-Series 시스템의 타겟 볼륨에 리소스 프로비저닝이 비활성화되어 있어야 합니다.
- 원격 스토리지 볼륨을 호스트나 여러 호스트에 직접 매핑하지 않습니다.
- 웹 서비스 프록시는 지원되지 않습니다.
- iSCSI CHAP 암호는 지원되지 않습니다.
- SMcli는 지원되지 않습니다.
- VMware 데이터 저장소는 지원되지 않습니다.
- 가져오기 페어가 있는 경우 관계/가져오기 페어에 있는 스토리지 시스템 하나만 한 번에 업그레이드할 수 있습니다.

추가 정보

원격 스토리지 기능에 대한 자세한 내용은 에서 "원격 스토리지 기술 보고서" 확인할 수 있습니다.

하드웨어 구성 요소

하드웨어 구성 요소 개요

하드웨어 페이지에서 구성 요소 상태를 확인하고 이러한 구성 요소와 관련된 일부 기능을 수행할 수 있습니다.

관리할 수 있는 구성 요소는 무엇입니까**?**

구성 요소 상태를 확인하고 이러한 구성 요소와 관련된 일부 기능을 수행할 수 있습니다.

- 쉘프 — A_shelf_는 스토리지 어레이(컨트롤러, 전원/팬 캐니스터 및 드라이브)용 하드웨어가 포함된 구성 요소입니다. 쉘프는 최대 12, 24 또는 60개의 드라이브를 수용할 수 있도록 3가지 크기로 제공됩니다.
- 컨트롤러 — A_controller_는 스토리지 배열 및 관리 기능을 구현하는 결합된 하드웨어 및 펌웨어입니다. 여기에는 캐시 메모리, 드라이브 지원 및 호스트 연결용 포트가 포함됩니다.

- 드라이브 — A_drive_는 하드 디스크 드라이브(HDD) 또는 솔리드 스테이트 드라이브(SSD)일 수 있습니다. 쉘프 크기에 따라 최대 12, 24 또는 60개의 드라이브를 쉘프에 설치할 수 있습니다.

자세한 내용:

- "하드웨어 페이지"
- "하드웨어 용어"

하드웨어 구성 요소는 어떻게 볼 수 있습니까**?**

스토리지 시스템의 물리적 구성 요소를 그래픽으로 보여 주는 하드웨어 페이지로 이동합니다. 쉘프 보기의 오른쪽 상단에서 * Drives * 또는 * Controllers * 탭을 선택하여 어레이 쉘프의 전면 및 후면 보기 사이를 전환할 수 있습니다.

자세한 내용:

- "쉘프 구성요소 상태 및 설정을 확인합니다"
- "컨트롤러 설정을 봅니다"
- "드라이브 상태 및 설정을 봅니다"

관련 정보

하드웨어와 관련된 개념에 대해 자세히 알아보기:

- "컨트롤러 상태"
- "드라이브 상태"
- "선반 손실 방지 및 서랍 손실 방지"

개념

하드웨어 페이지 및 구성 요소

하드웨어 페이지에서는 스토리지 시스템의 물리적 구성 요소를 그래픽으로 보여 줍니다. 여기에서 구성 요소 상태를 확인하고 이러한 구성 요소와 관련된 일부 기능을 수행할 수 있습니다.

쉘프

쉘프는 스토리지 어레이(컨트롤러, 전원/팬 캐니스터 및 드라이브)용 하드웨어를 포함하는 구성 요소입니다. 쉘프는 다음과 같은 두 가지 유형이 있습니다.

- * 컨트롤러 쉘프 * — 드라이브, 전원/팬 캐니스터 및 컨트롤러를 포함합니다.
- * 드라이브 쉘프 * (또는 * 확장 쉘프 *) — 드라이브, 전원/팬 캐니스터, 2개의 I/O 모듈(IOM)이 포함됩니다. ESM(환경 서비스 모듈(ESM)에는 드라이브 쉘프를 컨트롤러 쉘프에 연결하는 SAS 포트가 포함되어 있습니다.

쉘프는 최대 12, 24 또는 60개의 드라이브를 수용할 수 있도록 3가지 크기로 제공됩니다. 각 쉘프는 컨트롤러 펌웨어에 의해 할당된 ID 번호를 포함합니다. 쉘프 보기의 좌측 상단에 ID가 나타납니다.

하드웨어 페이지의 쉘프 보기에는 앞면 또는 뒷면 구성 요소가 표시됩니다. 쉘프 보기의 오른쪽 상단에서 * Drives * 또는

* Controller * 탭을 선택하여 두 보기 사이를 전환할 수 있습니다. 페이지 하단에서 * Show all front * 또는 * Show all back * 을 선택할 수도 있습니다. 전면 및 후면 뷰는 다음을 나타냅니다.

- * 전면 구성요소 * — 드라이브 및 빈 드라이브 베이.
- * 후면 구성요소 * — 컨트롤러, 전원/팬 캐니스터(컨트롤러 쉘프용) 또는 IOM 및 전원/팬 캐니스터(드라이브 쉘프용)

쉘프와 관련하여 다음 기능을 수행할 수 있습니다.

- 선반 위치 표시등을 켜서 캐비닛이나 랙에서 선반의 물리적 위치를 찾을 수 있도록 합니다.
- 쉘프 보기의 좌측 상단에 표시된 ID 번호를 변경합니다.
- 설치된 드라이브 유형 및 일련 번호와 같은 쉘프 설정을 확인합니다.
- 스토리지 배열의 물리적 레이아웃과 일치하도록 쉘프 보기를 위 또는 아래로 이동합니다.

컨트롤러

컨트롤러는 스토리지 배열 및 관리 기능을 구현하는 결합된 하드웨어 및 펌웨어입니다. 여기에는 캐시 메모리, 드라이브 지원 및 호스트 인터페이스 지원이 포함됩니다.

컨트롤러와 관련된 다음 기능을 수행할 수 있습니다.

- IP 주소 및 속도에 대한 관리 포트를 구성합니다.
- iSCSI 호스트 접속을 구성합니다(iSCSI 호스트가 있는 경우).
- NTP(Network Time Protocol) 서버 및 DNS(Domain Name System) 서버를 구성합니다.
- 컨트롤러 상태 및 설정을 봅니다.
- 로컬 영역 네트워크 외부의 사용자가 SSH 세션을 시작하고 컨트롤러의 설정을 변경할 수 있도록 합니다.
- 컨트롤러를 오프라인, 온라인 또는 서비스 모드로 전환합니다.

드라이브

스토리지 어레이에는 HDD(하드 디스크 드라이브) 또는 SSD(Solid State Drive)가 포함될 수 있습니다. 쉘프 크기에 따라 최대 12, 24 또는 60개의 드라이브를 쉘프에 설치할 수 있습니다.

드라이브와 관련된 다음 기능을 수행할 수 있습니다.

- 드라이브 로케이터 표시등을 켜서 쉘프에 있는 드라이브의 물리적 위치를 찾을 수 있습니다.
- 드라이브 상태 및 설정을 봅니다.
- 드라이브를 다시 할당하고(장애가 발생한 드라이브를 할당되지 않은 드라이브로 논리적으로 교체) 필요한 경우 드라이브를 수동으로 재구성합니다.
- 드라이브를 수동으로 실패하여 교체할 수 있습니다. (드라이브에 결함이 있으면 드라이브를 교체하기 전에 드라이브의 내용을 복사할 수 있습니다.)
- 핫 스페어 할당 또는 할당 취소
- 드라이브를 지웁니다.

다음 하드웨어 용어가 스토리지 어레이에 적용됩니다.

일반 하드웨어 용어**:**

구성 요소	설명
베이	베이는 드라이브 또는 다른 구성 요소가 설치된 쉘프의 슬롯입니다.
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
컨트롤러 쉘프	컨트롤러 쉘프는 드라이브 세트 및 하나 이상의 컨트롤러 캐니스터를 포함합니다. 컨트롤러 캐니스터에는 컨트롤러, 호스트 인터페이스 카드(HIC) 및 배터리가 들어 있습니다.
드라이브	드라이브는 물리적 데이터 저장 매체를 제공하는 전자기 기계 장치 또는 솔리드 스테이트 메모리 장치입니다.
드라이브 쉘프	확장 쉘프라고도 하는 드라이브 쉘프에는 드라이브 세트 및 IOXM(입출력 모듈) 2개가 포함됩니다. IOM에는 드라이브 쉘프를 컨트롤러 쉘프 또는 다른 드라이브 쉘프에 연결하는 SAS 포트가 포함되어 있습니다.
IOM(ESM)	IOM은 드라이브 쉘프를 컨트롤러 쉘프에 연결하기 위한 SAS 포트가 포함된 입력/출력 모듈입니다. 이전 컨트롤러 모델에서 IOM은 환경 서비스 모듈(ESM)이라고 했습니다.
전원/팬 캐니스터	전원/팬 캐니스터는 선반으로 미끄러지는 어셈블리입니다. 여기에는 전원 공급 장치 및 내장형 팬이 포함됩니다.
SFP	SFP는 SFP(Small Form-factor Pluggable) 트랜시버입니다.
쉘프	쉘프는 캐비닛 또는 랙에 설치된 엔클로저입니다. 여기에는 스토리지 어레이의 하드웨어 구성 요소가 포함됩니다. 쉘프는 컨트롤러 쉘프와 드라이브 쉘프의 두 가지 유형이 있습니다. 컨트롤러 쉘프는 컨트롤러와 드라이브를 포함합니다. 드라이브 쉘프는 입/출력 모듈(IOM) 및 드라이브를 포함합니다.
스토리지 시스템	스토리지 어레이에는 쉘프, 컨트롤러, 드라이브, 소프트웨어 및 펌웨어가 포함되어 있습니다.

컨트롤러 용어:

구성 요소	설명
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
컨트롤러 쉘프	컨트롤러 쉘프는 드라이브 세트 및 하나 이상의 컨트롤러 캐니스터를 포함합니다. 컨트롤러 캐니스터에는 컨트롤러, 호스트 인터페이스 카드(HIC) 및 배터리가 들어 있습니다.
DHCP를 선택합니다	DHCP(Dynamic Host Configuration Protocol)는 IP 주소와 같은 네트워크 구성 매개 변수를 동적으로 배포하기 위해 IP(인터넷 프로토콜) 네트워크에서 사용되는 프로토콜입니다.
DNS	DNS(Domain Name System)는 인터넷 또는 개인 네트워크에 연결된 장치의 명명 시스템입니다. DNS 서버는 도메인 이름의 디렉터리를 유지 관리하고 이를 IP(인터넷 프로토콜) 주소로 변환합니다.
이중 구성	Duplex는 스토리지 배열 내의 이중 컨트롤러 모듈 구성입니다. 이중 시스템은 컨트롤러, 논리적 볼륨 경로 및 디스크 경로와 관련하여 완전히 이중화됩니다. 한 컨트롤러에 장애가 발생하면 다른 컨트롤러가 I/O를 인수하여 가용성을 유지합니다. 이중 시스템에는 이중 팬 및 전원 공급 장치가 있습니다.
전이중/반이중 연결	전이중 및 반이중 모드는 연결 모드를 참조하십시오. 전이중 모드에서는 두 장치가 양방향으로 동시에 통신할 수 있습니다. 반이중 모드에서는 장치가 한 번에 한 방향씩 통신할 수 있습니다(한 장치는 메시지를 보내고 다른 장치는 메시지를 받습니다).
HIC	HIC(호스트 인터페이스 카드)는 컨트롤러 캐니스터 내에 선택적으로 설치할 수 있습니다. 컨트롤러에 내장된 호스트 포트를 베이스보드 호스트 포트라고 합니다. HIC에 내장된 호스트 포트를 HIC 포트라고 합니다.
ICMP ping 응답	ICMP(Internet Control Message Protocol)는 네트워크 컴퓨터의 운영 체제에서 메시지를 보내는 데 사용되는 프로토콜입니다. ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.
MAC 주소입니다	MAC 주소(Media Access Control Identifier)는 동일한 물리적 전송 네트워크 인터페이스의 두 포트를 연결하는 별도의 논리 채널을 구분하기 위해 이더넷에서 사용됩니다.
관리 클라이언트	관리 클라이언트는 System Manager 액세스를 위해 브라우저가 설치된 컴퓨터입니다.
MTU	MTU(Maximum Transmission Unit)는 네트워크에서 전송할 수 있는 가장 큰 크기의 패킷 또는 프레임입니다.

구성 요소	설명
NTP	NTP(Network Time Protocol)는 데이터 네트워크의 컴퓨터 시스템 간 클록 동기화를 위한 네트워킹 프로토콜입니다.
단일 구성	Simplex는 스토리지 어레이 내에서 단일 컨트롤러 모듈 구성입니다. 단일 시스템은 컨트롤러 또는 디스크 경로 이중화를 제공하지 않지만 이중 팬 및 전원 공급 장치가 있습니다.
VLAN	VLAN(Virtual Local Area Network)은 동일한 디바이스(스위치, 라우터 등)에서 지원하는 다른 네트워크와 물리적으로 분리된 것처럼 작동하는 논리적 네트워크입니다.

드라이브 용어:

구성 요소	설명
DA	DA(Data Assurance)는 데이터를 컨트롤러를 통해 드라이브로 전송할 때 발생할 수 있는 오류를 확인하고 수정하는 기능입니다. Fibre Channel과 같은 DA 지원 입출력 인터페이스를 사용하는 호스트에서 풀 또는 볼륨 그룹 레벨에서 Data Assurance를 설정할 수 있습니다.
드라이브 보안 기능	드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.
드라이브 쉘프	확장 쉘프라고도 하는 드라이브 쉘프에는 드라이브 세트 및 IOXM(입출력 모듈) 2개가 포함됩니다. IOM에는 드라이브 쉘프를 컨트롤러 쉘프 또는 다른 드라이브 쉘프에 연결하는 SAS 포트가 포함되어 있습니다.
DULBE	DULBE(Deallocated or UnWritten Logical Block Error)는 EF300 또는 EF600 스토리지 어레이가 리소스 프로비저닝된 볼륨을 지원할 수 있도록 하는 NVMe 드라이브의 옵션입니다.
FDE 드라이브	FDE(전체 디스크 암호화) 드라이브는 하드웨어 레벨의 디스크 드라이브에서 암호화를 수행합니다. 하드 드라이브에는 쓰기 중에 데이터를 암호화한 다음 읽기 중에 데이터를 해독하는 ASIC 칩이 포함되어 있습니다.
FIPS 드라이브	FIPS 드라이브는 FIPS(Federal Information Processing Standards) 140-2 레벨 2를 사용합니다. 이러한 드라이브는 강력한 암호화 알고리즘 및 방법을 보장하는 미국 정부 표준을 준수하는 FDE 드라이브입니다. FIPS 드라이브는 FDE 드라이브보다 보안 표준이 더 높습니다.
HDD	하드 디스크 드라이브(HDD)는 자기 코팅으로 회전하는 금속 플래터를 사용하는 데이터 저장 장치입니다.
핫 스페어 드라이브	핫 스페어는 RAID 1, RAID 5 또는 RAID 6 볼륨 그룹의 대기 드라이브 역할을 합니다. 데이터가 없는 완전한 기능을 갖춘 드라이브입니다. 볼륨 그룹에서 드라이브에 장애가 발생하면 컨트롤러는 장애가 발생한 드라이브에서 핫 스페어로 데이터를 자동으로 재구성합니다.
NVMe를 참조하십시오	NVMe(비휘발성 메모리 익스프레스)는 SSD 드라이브와 같은 플래시 기반 스토리지 장치를 위해 설계된 인터페이스입니다. NVMe는 이전 논리 장치 인터페이스와 비교하여 I/O 오버헤드를 줄이고 성능 개선을 포함합니다.
SAS를 참조하십시오	SAS(Serial Attached SCSI)는 컨트롤러를 디스크 드라이브에 직접 연결하는 지점 간 직렬 프로토콜입니다.

구성 요소	설명
보안 지원 드라이브	보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있으며, 이 드라이브는 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이러한 드라이브는 드라이브 보안 기능을 사용하여 추가 보안을 위해 사용할 수 있으므로 보안 -_가능_으로 간주됩니다. 드라이브 보안 기능이 이러한 드라이브에 사용된 볼륨 그룹 및 풀에 대해 활성화된 경우 드라이브는 secure-_enabled_가 됩니다.
보안 지원 드라이브	보안 지원 드라이브는 드라이브 보안 기능과 함께 사용됩니다. 드라이브 보안 기능을 활성화한 다음 보안 -가능 드라이브의 풀 또는 볼륨 그룹에 드라이브 보안을 적용하면 드라이브는 보안- 사용 상태가 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.
SSD를 지원합니다	SSD(Solid-State Disk)는 데이터를 영구적으로 저장하기 위해 솔리드 스테이트 메모리(플래시)를 사용하는 데이터 스토리지 장치입니다. SSD는 기존의 하드 드라이브를 에뮬레이트하며 하드 드라이브에서 사용하는 것과 동일한 인터페이스로 사용할 수 있습니다.

iSCSI 용어**:**

기간	설명
CHAP	CHAP(Challenge Handshake Authentication Protocol) 메서드는 초기 링크 중에 대상 및 이니시에이터의 ID를 확인합니다. 인증은 CHAP*secret*이라는 공유 보안 키를 기반으로 합니다.
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
DHCP를 선택합니다	DHCP(Dynamic Host Configuration Protocol)는 IP 주소와 같은 네트워크 구성 매개 변수를 동적으로 배포하기 위해 IP(인터넷 프로토콜) 네트워크에서 사용되는 프로토콜입니다.
IB	IB(InfiniBand)는 고성능 서버와 스토리지 시스템 간의 데이터 전송을 위한 통신 표준입니다.
ICMP ping 응답	ICMP(Internet Control Message Protocol)는 네트워크 컴퓨터의 운영 체제에서 메시지를 보내는 데 사용되는 프로토콜입니다. ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.
IQN을 선택합니다	IQN(iSCSI Qualified Name) 식별자는 iSCSI 이니시에이터 또는 iSCSI 타겟의 고유한 이름입니다.
iSER	iSER(iSCSI Extensions for RDMA)은 InfiniBand 또는 이더넷과 같은 RDMA 전송을 통해 작동하는 iSCSI 프로토콜을 확장하는 프로토콜입니다.
iSNS를 선택합니다	iSNS(Internet Storage Name Service)는 TCP/IP 네트워크에서 iSCSI 및 Fibre Channel 디바이스를 자동으로 검색, 관리 및 구성할 수 있는 프로토콜입니다.
MAC 주소입니다	MAC 주소(Media Access Control Identifier)는 동일한 물리적 전송 네트워크 인터페이스의 두 포트를 연결하는 별도의 논리 채널을 구분하기 위해 이더넷에서 사용됩니다.
관리 클라이언트	관리 클라이언트는 System Manager 액세스를 위해 브라우저가 설치된 컴퓨터입니다.
MTU	MTU(Maximum Transmission Unit)는 네트워크에서 전송할 수 있는 가장 큰 크기의 패킷 또는 프레임입니다.
RDMA 를 참조하십시오	RDMA(Remote Direct Memory Access)는 네트워크 컴퓨터가 두 컴퓨터의 운영 체제와 관계없이 주 메모리에서 데이터를 교환할 수 있도록 하는 기술입니다.
명명되지 않은 검색 세션	명명되지 않은 검색 세션 옵션이 활성화된 경우 iSCSI 초기자는 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정할 필요가 없습니다.

NVMe 용어:

기간	설명
InfiniBand	IB(InfiniBand)는 고성능 서버와 스토리지 시스템 간의 데이터 전송을 위한 통신 표준입니다.
네임스페이스	네임스페이스는 블록 액세스를 위해 포맷된 NVM 스토리지입니다. 스토리지 배열의 볼륨과 관련된 SCSI의 논리 유닛과 유사합니다.
네임스페이스 ID입니다	네임스페이스 ID는 네임스페이스에 대한 NVMe 컨트롤러의 고유 식별자이며 1에서 255 사이의 값으로 설정할 수 있습니다. SCSI의 LUN(Logical Unit Number)과 유사합니다.
NQN	NVMe 정규화된 이름(NQN)은 원격 스토리지 대상(스토리지 어레이)을 식별하는 데 사용됩니다.
NVM	NVM(비휘발성 메모리)은 다양한 유형의 스토리지 장치에서 사용되는 영구 메모리입니다.
NVMe를 참조하십시오	NVMe(비휘발성 메모리 익스프레스)는 SSD 드라이브와 같은 플래시 기반 스토리지 장치를 위해 설계된 인터페이스입니다. NVMe는 이전 논리 장치 인터페이스와 비교하여 I/O 오버헤드를 줄이고 성능 개선을 포함합니다.
NVMe - oF	NVMe-oF(Non-Volatile Memory Express over Fabrics)는 NVMe 명령 및 데이터가 호스트와 스토리지 간의 네트워크를 통해 전송되도록 하는 사양입니다.
NVMe 컨트롤러	호스트 연결 프로세스 중에 NVMe 컨트롤러가 생성됩니다. 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다.
NVMe 전담팀	큐는 NVMe 인터페이스를 통해 명령 및 메시지를 전달하는 데 사용됩니다.
NVMe 하위 시스템	NVMe 호스트 연결이 있는 스토리지 어레이
RDMA 를 참조하십시오	RDMA(Remote Direct Memory Access)를 사용하면 네트워크 인터페이스 카드(NIC) 하드웨어에 전송 프로토콜을 구현하여 서버 내외부로 데이터를 더욱 직접 이동할 수 있습니다.
RoCE	RoCE(RDMA over Converged Ethernet)는 이더넷 네트워크를 통한 RDMA(Remote Direct Memory Access)를 지원하는 네트워크 프로토콜입니다.
SSD를 지원합니다	SSD(Solid-State Disk)는 데이터를 영구적으로 저장하기 위해 솔리드 스테이트 메모리(플래시)를 사용하는 데이터 스토리지 장치입니다. SSD는 기존의 하드 드라이브를 에뮬레이트하며 하드 드라이브에서 사용하는 것과 동일한 인터페이스로 사용할 수 있습니다.

쉘프 구성요소 관리

하드웨어 구성 요소 보기

하드웨어 페이지에서는 부품을 쉽게 찾을 수 있는 정렬 및 필터링 기능을 제공합니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 다음 표에 설명된 기능을 사용하여 하드웨어 구성 요소를 봅니다.

기능	설명
드라이브, 컨트롤러 및 구성 요소 보기	전면 및 후면 쉘프 보기 사이를 전환하려면 맨 오른쪽에서 * 드라이브 * 또는 * 컨트롤러 및 구성 요소 * 를 선택합니다(현재 보기에 따라 표시되는 링크). Drives* 보기에는 드라이브 및 비어 있는 드라이브 베이가 표시됩니다. 컨트롤러 및 구성요소 * 보기에는 컨트롤러 및 모든 IOM(ESM) 모듈, 전원/팬 캐니스터 또는 빈 컨트롤러 베이가 표시됩니다. 페이지 하단에서 * Show all drives * 를 선택할 수도 있습니다.
드라이브 보기 필터	스토리지 배열에 다른 유형의 물리적 및 논리적 속성이 있는 드라이브가 포함된 경우 * Hardware * 페이지에는 드라이브 보기 필터가 포함됩니다. 이러한 필터 필드를 사용하면 페이지에 표시되는 드라이브 유형을 제한하여 특정 드라이브를 빠르게 찾을 수 있습니다. Show drives that are… * 에서 왼쪽에 있는 필터 필드(기본적으로 * any drive type * 표시)를 클릭하여 물리적 속성(예: 용량 및 속도)의 드롭다운 목록을 표시합니다. 오른쪽에 있는 필터 필드를 클릭하면(기본적으로 스토리지 배열의 * 아무 곳이나 표시) 논리적 속성(예: 볼륨 그룹 할당)의 드롭다운 목록이 표시됩니다. 이러한 필터를 함께 또는 별도로 사용할 수 있습니다. 스토리지 배열에 동일한 물리적 속성을 공유하는 드라이브가 포함되어 있으면 왼쪽에 있는 * Any drive type * 필드가 나타나지 않습니다. 드라이브가 모두 동일한 논리 위치에 있는 경우 오른쪽에 있는 스토리지 배열 * 필드의 * 아무 곳이나 나타나지 않습니다.
범례	구성 요소는 특정 색상으로 표시되어 해당 역할 상태를 나타냅니다. 이러한 상태에 대한 설명을 확장하고 축소하려면 * 범례 * 를 클릭합니다.
상태 아이콘 세부 정보를 표시합니다	상태 표시기에는 가용성 상태에 대한 텍스트 설명이 포함될 수 있습니다. 이 상태 텍스트를 표시하거나 숨기려면 * 상태 아이콘 세부 정보 표시 * 를 클릭합니다.
쉘프/쉘프 아이콘	각 쉘프 뷰에는 속성 및 상태와 함께 관련 명령 목록이 제공됩니다. 명령 드롭다운 목록을 보려면 * Shelf * 를 클릭합니다. 상단에 있는 아이콘 중 하나를 선택하여 컨트롤러, IOM(ESM), 전원 공급 장치, 팬, 온도, 배터리 및 SFP.
쉘프 주문	하드웨어 페이지에서 쉘프를 재정렬할 수 있습니다. 각 쉘프 보기의 오른쪽 위에 있는 위/아래 화살표를 사용하여 쉘프의 위/아래 순서를 변경합니다.

부품 상태를 표시하거나 숨깁니다

드라이브, 컨트롤러, 팬 및 전원 공급 장치의 상태 설명을 표시할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 후면 또는 전면 구성요소 보기:
   - 컨트롤러 및 전원/팬 캐니스터 구성 요소를 보려면 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
   - 드라이브를 보려면 컨트롤러 및 전원/팬 캐니스터 구성 요소가 표시되면 * Drives * 탭을 클릭하십시오.
3. 팝업 상태 설명을 보거나 숨기려면:
   - 상태 아이콘에 대한 팝업 설명을 보려면 쉘프 보기의 오른쪽 위에 있는 * 상태 아이콘 세부 정보 표시 * 를 클릭합니다(확인란을 선택).
   - 팝업 설명을 숨기려면 * 상태 아이콘 세부 정보 표시 * 를 다시 클릭합니다(확인란 선택 취소).
4. 전체 상태 세부 정보를 보려면 쉘프 보기에서 구성 요소를 선택한 다음 * 설정 보기 * 를 선택합니다.
5. 색상이 지정된 구성 요소에 대한 설명을 보려면 * 범례 * 를 선택합니다.

전면과 후면 보기 사이를 전환합니다

하드웨어 페이지에는 쉘프의 앞면 또는 뒷면 보기가 표시될 수 있습니다.

이 작업에 대해

후면 뷰에는 컨트롤러/IOM 및 전원 팬 캐니스터가 표시됩니다. 전면 보기에는 드라이브가 표시됩니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.

   그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

4. 선택적으로 페이지 하단에 있는 * Show all front * 또는 * Show all back * 을 선택할 수 있습니다.

쉘프의 보기 순서를 변경합니다

캐비닛에 있는 쉘프의 물리적 순서에 맞게 하드웨어 페이지에 표시되는 쉘프 순서를 변경할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 쉘프 보기의 오른쪽 위에서 위쪽 또는 아래쪽 화살표를 선택하여 하드웨어 페이지에 표시된 쉘프의 순서를 재정렬합니다.

선반 로케이터 조명을 켭니다

하드웨어 페이지에 표시된 쉘프의 물리적 위치를 찾으려면 쉘프 로케이터 표시등을 켜면 됩니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 컨트롤러 쉘프 또는 드라이브 쉘프의 드롭다운 목록을 선택한 다음 * 로케이터 표시등 켜기 * 를 선택합니다.

   선반의 로케이터 표시등이 켜집니다.

3. 쉘프를 물리적으로 찾았으면 대화 상자로 돌아가서 * Turn off * 를 선택합니다.

쉘프 **ID**를 변경합니다

쉘프 ID는 스토리지 어레이의 쉘프를 고유하게 식별하는 번호입니다. 각 쉘프 보기의 왼쪽 상단에서 00 또는 01로 시작하여 연속 번호가 지정됩니다.

이 작업에 대해

컨트롤러 펌웨어가 쉘프 ID를 자동으로 할당하지만, 다른 주문 스키마를 만들려면 해당 번호를 변경할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 컨트롤러 쉘프 또는 드라이브 쉘프의 드롭다운 목록을 선택한 다음 * ID 변경 * 을 선택합니다.
3. 쉘프 ID 변경 대화 상자에서 드롭다운 목록을 선택하여 사용 가능한 번호를 표시합니다.

   이 대화 상자에는 현재 활성 쉘프에 할당된 ID가 표시되지 않습니다.

4. 사용 가능한 번호를 선택한 다음 * 저장 * 을 클릭합니다.

   선택한 번호에 따라 하드웨어 페이지에서 쉘프 주문을 재정렬할 수 있습니다. 필요한 경우 각 쉘프 오른쪽 상단의 위쪽/아래쪽 화살표를 사용하여 순서를 재조정할 수 있습니다.

쉘프 구성요소 상태 및 설정을 확인합니다

하드웨어 페이지에서는 전원 공급 장치, 팬 및 배터리를 포함한 쉘프 구성 요소의 상태와 설정을 제공합니다.

이 작업에 대해

사용 가능한 구성 요소는 쉘프 유형에 따라 다릅니다.

- * 드라이브 쉘프 * — 단일 쉘프에 드라이브 세트, 전원/팬 캐니스터, I/O 모듈(IOM) 및 기타 지원 구성 요소가 포함되어 있습니다.
- * 컨트롤러 쉘프 * — 단일 쉘프에 드라이브 세트, 하나 또는 두 개의 컨트롤러 캐니스터, 전원/팬 캐니스터 및 기타 지원 구성 요소가 포함됩니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 컨트롤러 쉘프 또는 드라이브 쉘프의 드롭다운 목록을 선택한 다음 * 설정 보기 * 를 선택합니다.

   쉘프 구성요소 설정 대화 상자가 열리고 쉘프 구성요소와 관련된 상태와 설정을 보여주는 탭이 표시됩니다. 선택한 쉘프의 유형에 따라 테이블에 설명된 일부 탭이 나타나지 않을 수 있습니다.

탭을 클릭합니다	설명
쉘프	Shelf * 탭에는 다음 속성이 표시됩니다. • * Shelf ID * — 스토리지 배열의 셸프를 고유하게 식별합니다. 컨트롤러 펌웨어가 이 번호를 할당하지만 Shelf [Change ID] 메뉴를 선택하여 변경할 수 있습니다. • * 쉘프 경로 이중화 * — 쉘프와 컨트롤러 간 연결에 대체 방법이 있는지(예) 여부를 지정합니다(아니요). • * 현재 드라이브 유형 * — 드라이브에 내장된 기술 유형(예: 보안 기능이 있는 SAS 드라이브)을 표시합니다. 드라이브 유형이 두 개 이상인 경우 두 기술이 모두 표시됩니다. • * 일련 번호 * — 쉘프의 일련 번호를 표시합니다.
IOM(ESM)	ESM(ESM) * 탭에는 환경 서비스 모듈(ESM)이라고도 하는 입력/출력 모듈(IOM)의 상태가 표시됩니다. 드라이브 쉘프에 있는 구성 요소의 상태를 모니터링하고 드라이브 트레이와 컨트롤러 사이의 연결 지점 역할을 합니다. 상태는 Optimal(최적), Failed(실패), Optimal(최적)(미스와이어) 또는 Uncertified(미인증)일 수 있습니다. 기타 정보에는 펌웨어 버전 및 구성 설정 버전이 포함됩니다. 최대 및 현재 데이터 속도와 카드 통신 상태(예 또는 아니요)를 보려면 * 더 많은 설정 표시 * 를 선택합니다. 쉘프 드롭다운 목록 옆의 IOM 아이콘을 선택하여 이 상태를 확인할 수도 있습니다.
전원 공급 장치	전원 공급 장치* 탭에는 전원 공급 장치 캐니스터 및 전원 공급 장치 자체의 상태가 표시됩니다. 상태는 최적, 실패, 제거 또는 알 수 없음일 수 있습니다. 전원 공급 장치의 부품 번호도 표시됩니다. Shelf(쉘프) 드롭다운 목록 옆에 있는 Power Supply(전원 공급 장치) 아이콘을 선택하여 이 상태를 볼 수도 있습니다.
팬	Fans* 탭은 팬 캐니스터 및 팬 자체의 상태를 표시합니다. 상태는 최적, 실패, 제거 또는 알 수 없음일 수 있습니다. Shelf(쉘프) 드롭다운 목록 옆에 있는 Fan(팬) 아이콘을 선택하여 이 상태를 볼 수도 있습니다.
온도	Temperature * 탭은 센서, 컨트롤러, 전원/팬 캐니스터 등 쉘프 구성요소의 온도 상태를 표시합니다. 상태는 최적, 공칭 온도 초과, 최대 온도 초과 또는 알 수 없음일 수 있습니다. Shelf(선반) 드롭다운 목록 옆에 있는 Temperature(온도) 아이콘을 선택하여 이 상태를 볼 수도 있습니다.

탭을 클릭합니다	설명
배터리	batteries * (배터리 *) 탭은 컨트롤러 배터리의 상태를 표시합니다. 상태는 최적, 실패, 제거 또는 알 수 없음일 수 있습니다. 기타 정보에는 배터리 사용 기간, 교체 시까지 남은 일 수, 학습 주기 및 학습 사이클 사이의 주 등이 포함됩니다. Shelf(쉘프) 드롭다운 목록 옆에 있는 배터리 아이콘을 선택하여 이 상태를 볼 수도 있습니다.
SFP	SFP * 탭은 컨트롤러의 SFP(Small Form-factor Pluggable) 트랜시버 상태를 표시합니다. 상태는 최적, 실패 또는 알 수 없음일 수 있습니다. 부품 번호, 일련 번호 및 SFP 공급업체를 보려면 * 더 많은 설정 표시 * 를 선택합니다. Shelf(쉘프) 드롭다운 목록 옆에 있는 SFP 아이콘을 선택하여 이 상태를 볼 수도 있습니다.

3. 닫기 * 를 클릭합니다.

배터리 학습 주기를 업데이트합니다

학습 사이클은 스마트 배터리 게이지를 보정하기 위한 자동 사이클입니다. 이 주기는 8주 간격(컨트롤러당)으로 같은 요일 및 시간에 자동으로 시작되도록 예약됩니다. 다른 일정을 설정하려면 학습 주기를 조정할 수 있습니다.

이 작업에 대해

학습 사이클을 업데이트하면 두 컨트롤러 배터리가 모두 영향을 받습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 컨트롤러 쉘프의 드롭다운 목록을 선택한 다음 * 설정 보기 * 를 선택합니다.
3. 배터리 * 탭을 선택합니다.
4. 배터리 학습 사이클 업데이트 * 를 선택합니다.

   배터리 학습 주기 업데이트 대화 상자가 열립니다.

5. 드롭다운 목록에서 새 요일 및 시간을 선택합니다.
6. 저장 * 을 클릭합니다.

컨트롤러 관리

컨트롤러 상태

컨트롤러를 온라인, 오프라인 및 서비스 모드의 세 가지 상태로 둘 수 있습니다.

온라인 상태입니다

온라인 상태는 컨트롤러의 정상 작동 상태입니다. 이는 컨트롤러가 정상적으로 작동하고 I/O 작업을 위해 사용할 수 있음을 의미합니다.

컨트롤러를 온라인 상태로 설정하면 해당 상태가 Optimal(최적)으로 설정됩니다.

오프라인 상태입니다

오프라인 상태는 일반적으로 스토리지 어레이에 두 개의 컨트롤러가 있을 때 교체할 컨트롤러를 준비하는 데 사용됩니다. 컨트롤러는 두 가지 방법으로 오프라인 상태를 입력할 수 있습니다. 즉, 명시적 명령을 실행하거나 컨트롤러에 장애가 발생할 수 있습니다. 컨트롤러는 다른 명시적 명령을 실행하거나 오류가 발생한 컨트롤러를 교체하여 오프라인 상태를 종료할 수 있습니다. 스토리지 어레이에 두 개의 컨트롤러가 있는 경우에만 컨트롤러를 오프라인으로 전환할 수 있습니다.

컨트롤러가 오프라인 상태인 경우 다음 조건이 적용됩니다.

- 컨트롤러는 I/O에 사용할 수 없습니다
- 해당 컨트롤러를 통해서는 스토리지 어레이를 관리할 수 없습니다.
- 해당 컨트롤러가 현재 소유한 모든 볼륨은 다른 컨트롤러로 이동됩니다.
- 캐시 미러링이 비활성화되어 있고 모든 볼륨이 캐시 모드를 통해 쓰기로 변경됩니다.

서비스 모드

서비스 모드는 일반적으로 기술 지원 부서에서 다른 컨트롤러를 진단할 수 있도록 모든 스토리지 어레이 볼륨을 하나의 컨트롤러로 이동하는 데 사용됩니다. 컨트롤러는 서비스 모드로 수동으로 배치되어야 하며 서비스 작업이 완료된 후 수동으로 다시 온라인 상태로 전환되어야 합니다.

컨트롤러가 서비스 모드에 있으면 다음 조건이 적용됩니다.

- 컨트롤러는 I/O에 사용할 수 없습니다
- 기술 지원 부서에서는 직렬 포트 또는 네트워크 연결을 통해 컨트롤러에 액세스하여 잠재적인 문제를 분석할 수 있습니다.
- 해당 컨트롤러가 현재 소유한 모든 볼륨은 다른 컨트롤러로 이동됩니다.
- 캐시 미러링이 비활성화되어 있고 모든 볼륨이 캐시 모드를 통해 쓰기로 변경됩니다.

IP 주소 할당 고려 사항

기본적으로 컨트롤러는 두 네트워크 포트에서 DHCP가 활성화된 상태로 제공됩니다. 고정 IP 주소를 할당하거나, 기본 고정 IP 주소를 사용하거나, DHCP 할당 IP 주소를 사용할 수 있습니다. IPv6 상태 비저장 자동 구성을 사용할 수도 있습니다.

IPv6은 새 컨트롤러에서 기본적으로 해제되어 있지만 대체 방법을 사용하여 관리 포트 IP 주소를 구성한 다음 System Manager를 사용하여 관리 포트에서 IPv6을 사용하도록 설정할 수 있습니다.

네트워크 포트가 "링크 다운" 상태, 즉 LAN에서 연결이 끊어진 경우 시스템은 구성을 정적, 0.0.0.0(이전 릴리스) IP 주소 표시 또는 보고된 IP 주소 없이 DHCP 활성화(이후 릴리스)로 보고합니다. 네트워크 포트가 "링크 업" 상태(즉, LAN에 연결됨)에 있으면 DHCP를 통해 IP 주소를 얻으려고 시도합니다.

컨트롤러가 특정 네트워크 포트에서 DHCP 주소를 얻을 수 없는 경우 기본 IP 주소로 복원되며 이 주소는 최대 3분이 걸릴 수 있습니다. 기본 IP 주소는 다음과 같습니다.

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

IP 주소 할당 시:

- 고객 지원을 위해 컨트롤러에 포트 2를 예약합니다. 기본 네트워크 설정(DHCP 사용)을 변경하지 마십시오.
- E2800 및 E5700 컨트롤러의 정적 IP 주소를 설정하려면 SANtricity 시스템 관리자 를 사용합니다. E2700 및 E5600 컨트롤러의 정적 IP 주소를 설정하려면 SANtricity 스토리지 관리자를 사용하십시오. 정적 IP 주소를 구성한 후에는 모든 링크 다운/업 이벤트를 통해 설정된 상태로 유지됩니다.
- DHCP를 사용하여 컨트롤러의 IP 주소를 할당하려면 컨트롤러를 DHCP 요청을 처리할 수 있는 네트워크에 연결합니다. 영구 DHCP 임대를 사용합니다.

> 기본 주소는 링크 다운 이벤트 간에 유지되지 않습니다. 컨트롤러의 네트워크 포트가 DHCP를 사용하도록 설정된 경우 컨트롤러는 케이블 삽입, 재부팅 및 전원 주기를 포함하여 모든 연결 이벤트에서 DHCP 주소를 가져오려고 시도합니다. DHCP 시도가 실패할 때마다 해당 포트의 기본 정적 IP 주소가 사용됩니다.

관리 포트를 구성합니다

컨트롤러에는 시스템 관리에 사용되는 이더넷 포트가 포함되어 있습니다. 필요한 경우 전송 매개 변수와 IP 주소를 변경할 수 있습니다.

이 작업에 대해

이 절차를 수행하는 동안 포트 1을 선택한 다음 속도 및 포트 주소 지정 방법을 결정합니다. 포트 1은 관리 클라이언트가 컨트롤러 및 System Manager에 액세스할 수 있는 네트워크에 연결합니다.

> 두 컨트롤러 중 하나에서 포트 2를 사용하지 마십시오. 포트 2는 기술 지원 부서에서 사용하도록 예약되어 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 구성할 관리 포트가 있는 컨트롤러를 클릭합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. 관리 포트 구성 * 을 선택합니다.

   관리 포트 구성 대화 상자가 열립니다.

5. 포트 1이 표시되는지 확인한 후 * 다음 * 을 클릭합니다.
6. 구성 포트 설정을 선택한 후 * 다음 * 을 클릭합니다.

   필드 상세정보

필드에 입력합니다	설명
속도 및 이중 모드	자동 협상 설정 유지 System Manager가 스토리지 어레이와 네트워크 간의 전송 매개 변수를 결정하도록 하거나, 네트워크의 속도와 모드를 알고 있는 경우 드롭다운 목록에서 매개 변수를 선택합니다. 유효한 속도 및 이중 모드 조합만 목록에 표시됩니다.
IPv4 사용/IPv6 사용	IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오.

   IPv4 사용 * 을 선택하면 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택하면 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택하면 먼저 IPv4 설정 대화 상자가 열리고 * 다음 * 을 클릭하면 IPv6 설정 대화 상자가 열립니다.

7. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다.

필드 상세정보

필드에 입력합니다	설명
DHCP 서버에서 자동으로 구성을 가져옵니다	구성을 자동으로 가져오려면 이 옵션을 선택합니다.
수동으로 정적 설정을 지정합니다	이 옵션을 선택한 다음 컨트롤러의 IP 주소를 입력합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다. IP 주소 구성을 변경하면 스토리지 배열에 대한 관리 경로가 손실됩니다. SANtricity Unified Manager를 사용하여 네트워크의 어레이를 전체적으로 관리하는 경우 사용자 인터페이스를 열고 관리 [Discover] 메뉴로 이동합니다. SANtricity 저장소 관리자를 사용하는 경우 EMW(엔터프라이즈 관리 창)에서 장치를 제거하고 메뉴 편집 [스토리지 배열 추가]를 선택하여 EMW에 다시 추가한 다음 새 IP 주소를 입력해야 합니다.

8. 마침 * 을 클릭합니다.

결과

관리 포트 구성은 컨트롤러 설정, 관리 포트 탭에 표시됩니다.

NTP 서버 주소를 구성합니다

컨트롤러가 NTP 서버를 주기적으로 쿼리하여 내부 시간 시계를 업데이트하도록 NTP(Network Time Protocol) 서버에 대한 연결을 구성할 수 있습니다.

시작하기 전에

- 네트워크에 NTP 서버가 설치 및 구성되어 있어야 합니다.
- 기본 NTP 서버의 주소와 선택적 백업 NTP 서버의 주소를 알아야 합니다. 이러한 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.

NTP 서버에 대해 하나 이상의 도메인 이름을 입력하는 경우 NTP 서버 주소를 확인하기 위해 DNS 서버도 구성해야 합니다. NTP를 구성하고 도메인 이름을 제공한 컨트롤러에서만 DNS 서버를 구성해야 합니다.

이 작업에 대해

NTP를 사용하면 스토리지 어레이가 SNTP(Simple Network Time Protocol)를 사용하여 컨트롤러의 시계를 외부 호스트와 자동으로 동기화할 수 있습니다. 컨트롤러는 구성된 NTP 서버를 주기적으로 쿼리한 다음 결과를 사용하여 내부 시간 클럭을 업데이트합니다. 하나의 컨트롤러에만 NTP가 활성화되어 있는 경우 대체 컨트롤러는 NTP가 활성화된 컨트롤러와 해당 시계를 정기적으로 동기화합니다. 어떤 컨트롤러도 NTP를 활성화하지 않으면 컨트롤러가 주기적으로 시계를 서로 동기화합니다.

두 컨트롤러 모두에서 NTP를 구성할 필요는 없지만, 그렇게 하면 하드웨어 또는 통신 장애 시 스토리지 어레이의 동기화 상태를 유지할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 구성할 컨트롤러를 클릭합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. NTP 서버 구성 * 을 선택합니다.

   NTP(네트워크 시간 프로토콜) 서버 구성 대화 상자가 열립니다.

5. 컨트롤러 * (* A * 또는 * B *)에서 NTP 활성화를 선택합니다.

   대화 상자에 추가 선택 사항이 나타납니다.

6. 다음 옵션 중 하나를 선택합니다.
   - * DHCP 서버에서 NTP 서버 주소 자동으로 가져오기 * — 감지된 NTP 서버 주소가 표시됩니다.

     스토리지 배열이 정적 NTP 주소를 사용하도록 설정된 경우 NTP 서버가 나타나지 않습니다.

   - * NTP 서버 주소 수동 지정 * — 기본 NTP 서버 주소와 백업 NTP 서버 주소를 입력합니다. 백업 서버는 선택 사항입니다. (이 주소 필드는 라디오 버튼을 선택한 후에 나타납니다.) 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
7. * 선택 사항: * 백업 NTP 서버에 대한 서버 정보 및 인증 자격 증명을 입력합니다.
8. 저장 * 을 클릭합니다.

결과

NTP 서버 구성은 컨트롤러 설정, * DNS/NTP * 탭에 표시됩니다.

DNS 서버 주소를 구성합니다

DNS(Domain Name System)는 컨트롤러 및 NTP(Network Time Protocol) 서버의 정규화된 도메인 이름을 확인하는 데 사용됩니다. 스토리지 배열의 관리 포트는 IPv4 또는 IPv6 프로토콜을 동시에 지원할 수 있습니다.

시작하기 전에

- 네트워크에 DNS 서버가 설치 및 구성되어 있어야 합니다.
- 기본 DNS 서버의 주소와 선택적 백업 DNS 서버의 주소를 알고 있습니다. 이러한 주소는 IPv4 주소 또는 IPv6 주소일 수 있습니다.

이 작업에 대해

이 절차에서는 기본 및 백업 DNS 서버 주소를 지정하는 방법에 대해 설명합니다. 운영 DNS 서버에 장애가 발생할 경우 사용하도록 백업 DNS 서버를 선택적으로 구성할 수 있습니다.

DHCP(Dynamic Host Configuration Protocol)를 사용하여 스토리지 배열의 관리 포트를 이미 구성했고 DHCP 설정과 연결된 하나 이상의 DNS 또는 NTP 서버가 있는 경우 DNS 또는 NTP를 수동으로 구성할 필요가 없습니다. 이 경우 스토리지 시스템은 이미 DNS/NTP 서버 주소를 자동으로 가져야만 합니다. 그러나 아래 지침에 따라 대화 상자를 열고 올바른 주소가 감지되는지 확인해야 합니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 구성할 컨트롤러를 선택합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. DNS 서버 구성 * 을 선택합니다.

   DNS(Domain Name System) 서버 구성 대화 상자가 열립니다.

5. 다음 옵션 중 하나를 선택합니다.
   - * DHCP 서버에서 DNS 서버 주소 자동으로 가져오기 * — 감지된 DNS 서버 주소가 표시됩니다.

     스토리지 배열이 정적 DNS 주소를 사용하도록 설정된 경우 DNS 서버가 나타나지 않습니다.

   - * DNS 서버 주소 수동 지정 * — 기본 DNS 서버 주소와 백업 DNS 서버 주소를 입력합니다. 백업 서버는 선택 사항입니다. (이 주소 필드는 라디오 버튼을 선택한 후에 나타납니다.) 이러한 주소는 IPv4 주소 또는 IPv6 주소일 수 있습니다.
6. 저장 * 을 클릭합니다.
7. 다른 컨트롤러에 대해 이 단계를 반복합니다.

결과

DNS 구성은 컨트롤러 설정, * DNS/NTP * 탭에 표시됩니다.

컨트롤러 설정을 봅니다

호스트 인터페이스, 드라이브 인터페이스 및 관리 포트의 상태와 같은 컨트롤러에 대한 정보를 볼 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 다음 작업 중 하나를 수행하여 컨트롤러 설정을 표시합니다.
   - 컨트롤러를 클릭하여 컨텍스트 메뉴를 표시한 다음 * 설정 보기 * 를 선택합니다.
   - 컨트롤러 아이콘(* Shelf* 드롭다운 목록 옆에 있음)을 선택합니다. 이중 구성의 경우, 대화 상자에서 * 컨트롤러 A * 또는 * 컨트롤러 B * 를 선택한 후 * 다음 * 을 클릭합니다.

     컨트롤러 설정 대화 상자가 열립니다.

4. 속성 설정 간에 이동할 탭을 선택합니다.

   일부 탭에는 오른쪽 위에 * 더 많은 설정 표시 * 에 대한 링크가 있습니다.

   필드 상세정보

탭을 클릭합니다	설명
베이스	컨트롤러 상태, 모델 이름, 교체 부품 번호, 현재 펌웨어 버전 및 비휘발성 NVSRAM(Static Random Access Memory) 버전을 표시합니다.
캐시	데이터 캐시, 프로세서 캐시 및 캐시 백업 장치를 포함하는 컨트롤러의 캐시 설정을 표시합니다. 캐시 백업 디바이스는 컨트롤러의 전원이 끊길 경우 캐시의 데이터를 백업하는 데 사용됩니다. 상태는 최적, 실패, 제거, 알 수 없음, 쓰기 보호됨, 또는 호환되지 않습니다.
호스트 인터페이스	에서는 호스트 인터페이스 정보 및 각 포트의 링크 상태를 보여 줍니다. 호스트 인터페이스는 컨트롤러와 호스트(예: 파이버 채널 또는 iSCSI) 간의 연결입니다. HIC(호스트 인터페이스 카드) 위치는 베이스보드 또는 슬롯(베이)에 있습니다. "베이스보드"는 HIC 포트가 컨트롤러에 내장되어 있음을 나타냅니다. "슬롯" 포트는 HIC 옵션 중 입니다.
드라이브 인터페이스	에서는 드라이브 인터페이스 정보 및 각 포트의 링크 상태를 보여 줍니다. 드라이브 인터페이스는 컨트롤러와 드라이브(예: SAS) 간의 연결입니다.
관리 포트	에는 컨트롤러에 액세스하는 데 사용되는 호스트 이름 및 원격 로그인이 활성화되었는지 여부와 같은 관리 포트 세부 정보가 나와 있습니다. 관리 포트는 컨트롤러와 관리 클라이언트를 연결합니다. 관리 클라이언트는 System Manager에 액세스하기 위해 브라우저가 설치되어 있습니다.
DNS/NTP	에서는 DNS 서버와 NTP 서버의 주소 지정 방법 및 IP 주소를 보여 줍니다 (이러한 서버가 System Manager에서 구성된 경우). DNS(Domain Name System)는 인터넷 또는 개인 네트워크에 연결된 장치의 명명 시스템입니다. DNS 서버는 도메인 이름의 디렉터리를 유지 관리하고 이를 IP(인터넷 프로토콜) 주소로 변환합니다. NTP(Network Time Protocol)는 데이터 네트워크의 컴퓨터 시스템 간 클록 동기화를 위한 네트워킹 프로토콜입니다.

5. 닫기 * 를 클릭합니다.

원격 로그인**(SSH)** 구성

원격 로그인을 활성화하면 로컬 영역 네트워크 외부의 사용자가 SSH 세션을 시작하고 컨트롤러의 설정에 액세스할 수 있습니다.

SANtricity 버전 11.74 이상에서는 사용자가 SSH 키 및/또는 SSH 암호를 입력하도록 요구하여 MFA(Multifactor Authorization)를 구성할 수도 있습니다. SANtricity 버전 11.73 및 이전 버전의 경우 이 기능에는 SSH 키 및 암호를 사용한 다단계 인증 옵션이 _NOT_포함됩니다.

보안 위험 * — 보안상의 이유로 기술 지원 담당자만 원격 로그인 기능을 사용할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 원격 로그인을 구성할 컨트롤러를 클릭합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. Configure remote login (SSH) * 를 선택합니다. (SANtricity 버전 11.73 및 이전 버전의 경우 이 메뉴 항목은 * 원격 로그인 변경 * 입니다.)

   원격 로그인을 활성화하기 위한 대화 상자가 열립니다.

5. 원격 로그인 사용 * 확인란을 선택합니다.

   이 설정은 다음과 같은 세 가지 인증 옵션을 사용하여 원격 로그인을 제공합니다.

   - * 암호만 *. 이 옵션을 선택하면 * 저장 * 을 클릭할 수 있습니다. 이중 시스템이 있는 경우 이전 단계를 수행하여 두 번째 컨트롤러에서 원격 로그인을 활성화할 수 있습니다.
   - * SSH 키 또는 암호 *. 이 옵션의 경우 다음 단계를 진행하십시오.
   - * 패스워드와 SSH 키 * 둘 다. 이 옵션의 경우 * 원격 로그인에 대해 승인된 공개 키 및 암호 필요 * 확인란을 선택하고 다음 단계를 진행합니다.

6. [인증 공개 키] * 필드를 채웁니다. 이 필드에는 OpenSSH * authorized_keys * 파일 형식의 인증된 공개 키 목록이 들어 있습니다.

   Authorized public key* 필드를 채울 때 다음 지침을 숙지하십시오.

   - 공인 공개 키 * 필드는 두 컨트롤러에 모두 적용되며 첫 번째 컨트롤러에서만 구성해야 합니다.
   - authorized_keys * 파일은 한 줄에 하나의 키만 포함해야 합니다. # 및 빈 줄로 시작하는 줄은 무시됩니다. 파일 형식에 대한 자세한 내용은 을 참조하십시오"OpenSSH에 대한 인증 키 구성".
   - authorized_keys * 파일은 다음 예제와 유사합니다.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. 작업을 마치면 * 저장 * 을 클릭합니다.
8. 이중 시스템의 경우 위의 단계를 따라 두 번째 컨트롤러에서 원격 로그인을 활성화할 수 있습니다. 암호와 SSH 키 모두에 대한 옵션을 구성하는 경우 원격 로그인을 위해 * 승인된 공개 키 및 암호 필요 * 확인란을 다시 선택해야 합니다.
9. 기술 지원 부서의 문제 해결이 끝나면 원격 로그인 구성 대화 상자로 돌아가서 * 원격 로그인 사용 * 확인란을 선택 취소하여 원격 로그인을 비활성화할 수 있습니다. 두 번째 컨트롤러에서 원격 로그인이 활성화된 경우 확인 대화 상자가 열리고 두 번째 컨트롤러에서도 원격 로그인을 비활성화할 수 있습니다.

   원격 로그인을 비활성화하면 현재 SSH 세션이 종료되고 새 로그인 요청이 거부됩니다.

컨트롤러를 온라인으로 설정합니다

컨트롤러가 오프라인 상태 또는 서비스 모드인 경우 다시 온라인 상태로 전환할 수 있습니다.

단계

1. 하드웨어 * 를 선택합니다.
2. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.

   그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

3. 오프라인 상태 또는 서비스 모드에 있는 컨트롤러를 클릭합니다.

   컨트롤러의 상황에 맞는 메뉴가 나타납니다.

4. 온라인으로 전환 * 을 선택하고 작업을 수행할지 확인합니다.

결과

다중 경로 드라이버로 복원된 기본 경로를 검색하는 데 최대 10분이 걸릴 수 있습니다.

각 볼륨에 대한 I/O 요청이 수신되면 이 컨트롤러가 원래 소유했던 볼륨이 자동으로 컨트롤러로 다시 이동됩니다. 경우에 따라 * redistribute volumes * 명령을 사용하여 볼륨을 수동으로 재배포해야 할 수도 있습니다.

컨트롤러를 오프라인으로 전환합니다

그렇게 하라는 지시가 있으면 컨트롤러를 오프라인으로 설정할 수 있습니다.

시작하기 전에

- 스토리지 어레이에는 2개의 컨트롤러가 필요합니다. 오프라인 상태로 전환하지 않는 컨트롤러는 온라인 상태여야 합니다(최적 상태).
- 사용 중인 볼륨이 없거나 이러한 볼륨을 사용하는 모든 호스트에 다중 경로 드라이버가 설치되어 있는지 확인합니다.

이 작업에 대해

[CAUTION]
====
Recovery Guru 또는 기술 지원 부서의 지시가 없는 한 컨트롤러를 오프라인으로 전환하지 마십시오.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 오프라인으로 설정할 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. 오프라인 상태로 전환 * 을 선택하고 작업을 수행할지 확인합니다.

.결과
System Manager에서 컨트롤러의 상태를 오프라인으로 업데이트하는 데 몇 분 정도 걸릴 수 있습니다. 상태가 업데이트되기 전에는 다른 작업을 시작하지 마십시오.

[[ID1a4fe78e844830c22196d811c5d3330b]]
= 컨트롤러를 서비스 모드로 전환합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
그렇게 하라는 지시가 있으면 컨트롤러를 서비스 모드로 전환할 수 있습니다.

.시작하기 전에
* 스토리지 어레이에는 2개의 컨트롤러가 있어야 합니다. 서비스 모드에 있지 않은 컨트롤러는 온라인 상태여야 합니다(최적 상태).
* 사용 중인 볼륨이 없거나 이러한 볼륨을 사용하는 모든 호스트에 다중 경로 드라이버가 설치되어 있는지 확인합니다.

[NOTE]
====

컨트롤러를 서비스 모드로 전환하면 성능이 크게 저하될 수 있습니다. 기술 지원 부서의 지시가 있는 경우를 제외하고, 컨트롤러를 서비스 모드로 설정하지 마십시오.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 서비스 모드로 전환할 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. 서비스 모드에서 * 위치 * 를 선택하고 작업을 수행할지 확인합니다.

[[IDb9c07bc458f7e18514715997cac158fd]]
= 컨트롤러를 재설정(재부팅)합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
일부 문제는 컨트롤러 재설정(재부팅)이 필요합니다. 컨트롤러에 물리적으로 액세스할 수 없는 경우에도 컨트롤러를 재설정할 수 있습니다.

.시작하기 전에
* 스토리지 어레이에는 2개의 컨트롤러가 있어야 합니다. 재설정하지 않은 컨트롤러는 온라인 상태여야 합니다(최적 상태).
* 사용 중인 볼륨이 없거나 이러한 볼륨을 사용하는 모든 호스트에 다중 경로 드라이버가 설치되어 있는지 확인합니다.

.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 재설정할 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. 재설정 * 을 선택하고 작업을 수행할지 확인합니다.

:leveloffset: -1

= iSCSI 포트를 관리합니다

:leveloffset: +1

[[IDdbebf4a4e80c89451daa2cf98616f6c8]]
= iSCSI 포트를 구성합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
컨트롤러에 iSCSI 호스트 연결이 포함된 경우 하드웨어 페이지에서 iSCSI 포트 설정을 구성할 수 있습니다.

.시작하기 전에
* 컨트롤러에 iSCSI 포트가 포함되어야 합니다. 그렇지 않으면 iSCSI 설정을 사용할 수 없습니다.
* 네트워크 속도(포트와 호스트 간의 데이터 전송 속도)를 알아야 합니다.

[NOTE]
====
iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 나타납니다.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 구성할 iSCSI 포트가 있는 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. iSCSI 포트 구성 * 을 선택합니다.
+
[NOTE]
====
iSCSI 포트 구성 * 옵션은 System Manager가 컨트롤러에서 iSCSI 포트를 감지한 경우에만 나타납니다.

====
+
iSCSI 포트 구성 대화 상자가 열립니다.

. 드롭다운 목록에서 구성할 포트를 선택한 후 * 다음 * 을 클릭합니다.
. 구성 포트 설정을 선택한 후 * 다음 * 을 클릭합니다.
+
모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 포트 설정 표시 * 링크를 클릭합니다.

+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 포트 설정 | 설명

 a|
구성된 이더넷 포트 속도(특정 유형의 호스트 인터페이스 카드에만 나타남)
 a|
포트에서 SFP의 속도 기능과 일치하는 속도를 선택합니다.

 a|
FEC(Forward Error Correction) 모드(특정 유형의 호스트 인터페이스 카드에만 나타남)
 a|
필요한 경우 지정된 호스트 포트에 대한 FEC 모드 중 하나를 선택합니다.

NOTE: Reed Solomon 모드는 25Gbps 포트 속도를 지원하지 않습니다.

 a|
IPv4 사용/IPv6 사용
 a|
IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오.

NOTE: 포트 액세스를 비활성화하려면 두 확인란을 모두 선택 취소합니다.

a|
TCP 수신 대기 포트(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)
a|
필요한 경우 새 포트 번호를 입력합니다.

수신 대기 포트는 컨트롤러가 호스트 iSCSI 초기자의 iSCSI 로그인을 수신 대기하기 위해 사용하는 TCP 포트 번호입니다. 기본 수신 대기 포트는 3260입니다. 3260 또는 49152와 65535 사이의 값을 입력해야 합니다.

a|
MTU 크기(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)
a|
필요한 경우 MTU(Maximum Transmission Unit)에 대한 새 크기를 바이트 단위로 입력합니다.

기본 MTU(Maximum Transmission Unit) 크기는 프레임당 1,500바이트입니다. 1500 ~ 9000 사이의 값을 입력해야 합니다.

a|
ICMP Ping 응답을 활성화합니다
a|
ICMP(Internet Control Message Protocol)를 활성화하려면 이 옵션을 선택합니다. 네트워크로 연결된 컴퓨터의 운영 체제는 이 프로토콜을 사용하여 메시지를 전송합니다. 이러한 ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.

|===
====
+
IPv4 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 * 다음 * 을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다. 모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 설정 표시 * 링크를 클릭합니다.
+
.필드 상세정보
[%collapsible]

====
[cols="25h,~"]
|===
| 포트 설정 | 설명

a|
자동으로 구성을 가져옵니다
a|
구성을 자동으로 가져오려면 이 옵션을 선택합니다.

a|
수동으로 정적 설정을 지정합니다
a|
이 옵션을 선택한 다음 필드에 정적 주소를 입력합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다.

a|
VLAN 지원을 활성화합니다(* 추가 설정 표시 * 를 클릭하여 사용 가능).
a|
VLAN을 활성화하고 해당 ID를 입력하려면 이 옵션을 선택합니다. VLAN은 동일한 스위치, 동일한 라우터 또는 둘 다에서 지원되는 다른 물리적 LAN(가상 LAN)과 물리적으로 분리된 것처럼 동작하는 논리 네트워크입니다.

a|
이더넷 우선 순위 활성화(* 추가 설정 표시 * 를 클릭하여 사용 가능)
a|
네트워크 액세스 우선 순위를 결정하는 매개변수를 활성화하려면 이 옵션을 선택합니다. 슬라이더를 사용하여 1(최저)과 7(최고) 사이의 우선순위를 선택합니다.

이더넷과 같은 공유 LAN(Local Area Network) 환경에서는 많은 스테이션이 네트워크 액세스에 대해 경합할 수 있습니다. 액세스는 선착순으로 제공됩니다. 두 스테이션이 동시에 네트워크에 액세스하려고 시도할 수 있으며, 이로 인해 두 스테이션이 다시 꺼졌다가 다시 시도하기 전에 대기하게 됩니다. 스위치 포트에 하나의 스테이션만 연결되어 있는 스위치 이더넷의 경우 이 프로세스가 최소화됩니다.

|===
====
. 마침 * 을 클릭합니다.

```
[[ID078a48de3e679446076007481ddde700]]
= iSCSI 인증을 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
iSCSI 네트워크의 보안을 강화하기 위해 컨트롤러(타겟)와 호스트(이니시에이터) 간에 인증을
설정할 수 있습니다.

System Manager에서는 CHAP(Challenge Handshake Authentication Protocol) 방법을
사용하여 초기 링크 중에 대상 및 초기자의 ID를 확인합니다. 인증은 _CHAP secret_이라는 공유
보안 키를 기반으로 합니다.

.시작하기 전에
타겟(컨트롤러)에 대한 CHAP 암호를 설정하기 전이나 후에 이니시에이터(iSCSI 호스트)에 대한
CHAP 암호를 설정할 수 있습니다. 이 작업의 지침을 따르기 전에 호스트가 iSCSI 연결을 먼저
수행할 때까지 기다린 다음 개별 호스트에 CHAP 암호를 설정해야 합니다. 연결이 완료되면
호스트의 IQN 이름과 해당 CHAP 암호가 iSCSI 인증 대화 상자(이 작업에 설명되어 있음)에
나열되며, 수동으로 입력할 필요가 없습니다.

.이 작업에 대해
다음 인증 방법 중 하나를 선택할 수 있습니다.

* * 단방향 인증 * -- 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 설정을
사용합니다(단방향 인증).
* * 양방향 인증 * -- 컨트롤러와 iSCSI 호스트가 모두 인증(양방향 인증)을 수행할 수 있도록
하려면 이 설정을 사용합니다. 이 설정은 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록
하고, iSCSI 호스트가 컨트롤러의 ID를 인증할 수 있도록 하여 두 번째 수준의 보안을
제공합니다.


[NOTE]
====
iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 설정에서 * 인증 구성 * 을 클릭합니다.
+
```

현재 설정된 방법을 보여 주는 Configure Authentication 대화 상자가 나타납니다. 또한 호스트에 CHAP 암호가 구성되어 있는지 여부도 표시됩니다.

. 다음 중 하나를 선택합니다.
+
** * 인증 없음 * -- 컨트롤러가 iSCSI 호스트의 ID를 인증하지 않도록 하려면 이 옵션을 선택하고 * 마침 * 을 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
** * 단방향 인증 * -- 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 옵션을 선택하고 * 다음 * 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.
** * 양방향 인증 * -- 컨트롤러와 iSCSI 호스트가 인증을 수행하도록 허용하려면 이 옵션을 선택하고 * 다음 * 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.

. 단방향 또는 양방향 인증의 경우 컨트롤러의 CHAP 암호(타겟)를 입력하거나 확인합니다. CHAP 암호는 12자에서 57자 사이의 인쇄 가능한 ASCII 문자여야 합니다.
+
[NOTE]
====
컨트롤러에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

====
. 다음 중 하나를 수행합니다.
+
** one-way_authentication을 구성하는 경우 * Finish * 를 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
** two-way_authentication을 구성하는 경우 * Next * 를 클릭하여 이니시에이터 CHAP 구성 대화 상자를 표시합니다.

. 양방향 인증의 경우, 12-57자의 인쇄 가능한 ASCII 문자일 수 있는 iSCSI 호스트(이니시에이터)에 대한 CHAP 암호를 입력하거나 확인합니다. 특정 호스트에 대해 양방향 인증을 구성하지 않으려면 이니시에이터 CHAP 암호 필드를 비워 둡니다.
+
[NOTE]
====
호스트에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

====
. 마침 * 을 클릭합니다.

.결과
인증을 지정하지 않은 경우, 컨트롤러와 iSCSI 호스트 간의 iSCSI 로그인 시퀀스 중에 인증이 발생합니다.

[[ID8b72e29d051e016270360af4ec8af7c6]]
= iSCSI 검색 설정을 활성화합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
iSCSI 네트워크에서 스토리지 디바이스 검색과 관련된 설정을 설정할 수 있습니다.

대상 검색 설정을 사용하면 iSNS(Internet Storage Name Service) 프로토콜을 사용하여 스토리지 배열의 iSCSI 정보를 등록하고 명명되지 않은 검색 세션을 허용할지 여부를 결정할 수 있습니다.

.시작하기 전에
iSNS 서버가 정적 IP 주소를 사용하는 경우 iSNS 등록에 해당 주소를 사용할 수 있어야 합니다. IPv4와 IPv6가 모두 지원됩니다.

.이 작업에 대해
iSCSI 검색과 관련된 다음 설정을 활성화할 수 있습니다.

* * iSNS 서버를 사용하여 타겟을 등록합니다. * -- 이 옵션을 설정하면 스토리지 어레이가 iSNS 서버의 iSCSI IQN(Qualified Name) 및 포트 정보를 등록합니다. 이 설정은 iSNS 검색을 허용하므로 이니시에이터는 iSNS 서버에서 IQN 및 포트 정보를 검색할 수 있습니다.
* * 이름 없는 검색 세션 활성화 * -- 이름 없는 검색 세션이 활성화되면 이니시에이터(iSCSI 호스트)가 검색 유형 연결을 위한 로그인 시퀀스 중에 타겟(컨트롤러)의 IQN을 제공할 필요가 없습니다. 비활성화된 경우 호스트는 IQN을 제공하여 컨트롤러에 검색 세션을 설정해야 합니다. 하지만 정상(입출력 베어링) 세션에 대해서는 타겟 IQN이 항상 필요합니다. 이 설정을 비활성화하면 권한이 없는 iSCSI 호스트가 해당 IP 주소만 사용하여 컨트롤러에 연결하는 것을 방지할 수 있습니다.

[NOTE]
====
iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 설정 * 에서 * 대상 검색 설정 보기/편집 * 을 클릭합니다.
+
대상 검색 설정 대화 상자가 나타납니다. iSNS 서버 사용 *... 필드 아래에 컨트롤러가 이미 등록되어 있는지 여부를 나타내는 대화 상자가 나타납니다.

. 컨트롤러를 등록하려면 * iSNS 서버를 사용하여 대상 등록 * 을 선택한 후 다음 중 하나를 선택합니다.
+
** * DHCP 서버에서 자동으로 구성 가져오기 * -- DHCP(Dynamic Host Configuration Protocol) 서버를 사용하여 iSNS 서버를 구성하려면 이 옵션을 선택합니다. 이 옵션을 사용하는 경우 컨트롤러의 모든 iSCSI 포트에서도 DHCP를 사용하도록 구성해야 합니다. 필요한 경우 컨트롤러 iSCSI 포트 설정을 업데이트하여 이 옵션을 활성화합니다.
+
[NOTE]
====
DHCP 서버가 iSNS 서버 주소를 제공하려면 옵션 43--""공급업체 특정 정보"를 사용하도록 DHCP 서버를 구성해야 합니다. 이 옵션은 데이터 바이트 0xa-0xd(10-13)로 iSNS 서버 IPv4 주소를 포함해야 합니다.

====
** * 수동으로 정적 구성 지정 * -- iSNS 서버의 정적 IP 주소를 입력하려면 이 옵션을 선택합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) 필드에 IPv4 주소 또는 IPv6 주소를 입력합니다. 둘 다 구성한 경우 IPv4가 기본값입니다. 또한 TCP 수신 대기 포트를 입력합니다(기본값 3205를 사용하거나 49152와 65535 사이의 값을 입력합니다).

. 스토리지 배열이 명명되지 않은 검색 세션에 참여할 수 있도록 하려면 * 명명되지 않은 검색 세션 활성화 * 를 선택합니다.
+
** 이 옵션을 설정하면 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정하는 데 iSCSI 이니시에이터가 필요하지 않습니다.
** 비활성화된 경우 이니시에이터가 타겟 IQN을 제공하지 않으면 검색 세션이 차단됩니다. 명명되지 않은 검색 세션을 비활성화하면 보안이 강화됩니다.

. 저장 * 을 클릭합니다.

.결과
System Manager에서 iSNS 서버에 컨트롤러를 등록하려고 하면 진행률 표시줄이 나타납니다. 이 프로세스는 최대 5분 정도 걸릴 수 있습니다.

[[IDabc5271fb0bc00bc8ed3d40be2d7f315]]
= iSCSI 통계 패키지를 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열에 대한 iSCSI 연결에 대한 데이터를 볼 수 있습니다.

.이 작업에 대해
System Manager는 이러한 유형의 iSCSI 통계를 표시합니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

NOTE: System Manager에 표시되는 통계 유형은 스토리지 어레이에 사용할 수 있는 통계를 기반으로 합니다.

* * 이더넷 MAC 통계 * -- MAC(Media Access Control)에 대한 통계를 제공합니다. 또한 MAC는 실제 주소 또는 MAC 주소라는 주소 지정 메커니즘을 제공합니다. MAC 주소는 각 네트워크 어댑터에 할당된 고유한 주소입니다. MAC 주소는 하위 네트워크 내의 대상으로 데이터 패킷을 전송하는 데 도움이 됩니다.
* * 이더넷 TCP/IP 통계 * -- TCP(Transmission Control Protocol) 및 IP(Internet Protocol)인 TCP/IP에 대한 통계를 제공합니다. TCP를 사용하면 네트워크로 연결된 호스트의 응용 프로그램이 서로 연결을 만들어 데이터를 패킷으로 교환할 수 있습니다. IP는 패킷 교환 방식의 네트워크를 통해 데이터를 전달하는 데이터 지향 프로토콜입니다. IPv4 통계 및 IPv6 통계는 별도로 표시됩니다.
* * 이더넷 커널 통계 * -- iSCSI 장치의 플랫폼 커널 드라이버에 대한 통계를 제공합니다. 커널 통계는 TCP/IP 통계 옵션과 유사한 네트워크 데이터를 표시합니다. 그러나 커널 통계 데이터는 iSCSI 하드웨어에서 직접 수집되지 않고 플랫폼 커널 드라이버에서 수집됩니다.
* * 로컬 대상/초기자(프로토콜) 통계 * -- iSCSI 대상에 대한 통계를 표시합니다. iSCSI 타겟은 해당 스토리지 미디어에 대한 블록 수준 액세스를 제공하고 비동기 미러링 작업에서 이니시에이터로 사용될 때 스토리지 배열에 대한 iSCSI 통계를 표시합니다.
* * DCBX 작업 상태 통계 * -- 다양한 DCBX(Data Center Bridging Exchange) 기능의 작동 상태를 표시합니다.
* * LLDP TLV statistics * -- LLDP(Link Layer Discovery Protocol) TLV(Type Length Value) 통계를 표시합니다.
* * DCBX TLV 통계 * -- DCB(데이터 센터 브리징) 환경에서 스토리지 배열 호스트 포트를 식별하는 정보를 표시합니다. 이 정보는 식별 및 기능 목적으로 네트워크 피어와 공유됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

.단계
. 지원 [지원 센터 > 진단] 탭을 선택합니다.
. iSCSI 통계 패키지 보기 * 를 선택합니다.
. 탭을 클릭하여 다양한 통계 집합을 봅니다.
. 기준선을 설정하려면 * Set new baseline * 을 클릭합니다.
+
기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. 모든 iSCSI 통계에는 동일한

기준이 사용됩니다.

[[ID38f32c747937fa803dc423b40f0db432]]
= iSCSI 세션을 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열에 대한 iSCSI 연결에 대한 자세한 정보를 볼 수 있습니다. iSCSI 세션은 비동기 미러 관계에서 호스트 또는 원격 스토리지 배열에 대해 발생할 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 세션 보기/종료 * 를 선택합니다.
+
현재 iSCSI 세션 목록이 나타납니다.

. * 선택 사항: * 특정 iSCSI 세션에 대한 추가 정보를 보려면 세션을 선택한 다음 * 세부 정보 보기 * 를 클릭합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 항목 | 설명

a|
세션 식별자(SSID)
a|
iSCSI 이니시에이터와 iSCSI 타겟 간의 세션을 식별하는 16진수 문자열입니다. SSID는 ISID와 TPGT로 구성됩니다.

a|
이니시에이터 세션 ID(ISID)
a|

세션 식별자의 이니시에이터 부분입니다. 초기자는 로그인 중에 ISID를 지정합니다.

a|
대상 포털 그룹
a|
iSCSI 타겟입니다.

a|
대상 포털 그룹 태그(TPGT)
a|
세션 식별자의 대상 부분. iSCSI 대상 포털 그룹의 16비트 숫자 식별자입니다.

a|
이니시에이터 iSCSI 이름입니다
a|
이니시에이터의 전 세계에서 고유한 이름입니다.

a|
이니시에이터 iSCSI 레이블
a|
System Manager에 설정된 사용자 레이블입니다.

a|
이니시에이터 iSCSI 별칭입니다
a|
iSCSI 노드와 연결할 수도 있는 이름입니다. 별칭을 사용하면 조직에서 사용자에게 친숙한 문자열을 iSCSI 이름과 연결할 수 있습니다. 그러나 별칭은 iSCSI 이름을 대체하는 것이 아닙니다. 이니시에이터 iSCSI 별칭은 호스트에서만 설정할 수 있고 System Manager에서는 설정할 수 없습니다

a|
호스트
a|
스토리지 배열에 입력 및 출력을 전송하는 서버입니다.

a|
연결 ID(CID)
a|
이니시에이터와 타겟 간의 세션 내 접속에 대한 고유한 이름입니다. 초기자는 이 ID를 생성하여 로그인 요청 중에 대상에 제공합니다. 연결이 닫히라는 로그아웃 중에도 연결 ID가 표시됩니다.

a|
포트 식별자입니다
a|
연결과 관련된 컨트롤러 포트입니다.

a|
이니시에이터 IP 주소입니다
a|
이니시에이터의 IP 주소입니다.

a|
협상된 로그인 매개 변수
a|
iSCSI 세션 로그인 중에 트랜잭션되는 매개 변수입니다.

a|
인증 방법
a|
iSCSI 네트워크에 액세스할 사용자를 인증하는 기술입니다. 유효한 값은 * CHAP * 및 * 없음 * 입니다.

a|
헤더 다이제스트 방법입니다
a|
iSCSI 세션에 대해 가능한 헤더 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.

a|
데이터 다이제스트 방법입니다
a|
iSCSI 세션에 대해 가능한 데이터 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.

a|
최대 연결 수
a|
iSCSI 세션에 허용되는 최대 연결 수입니다. 최대 연결 수는 1 ~ 4입니다. 기본값은 * 1 * 입니다.

a|
대상 별칭
a|
대상과 연관된 레이블입니다.

a|
이니시에이터 별칭입니다
a|
이니시에이터와 연결된 레이블입니다.

a|
대상 IP 주소입니다
a|
iSCSI 세션의 타겟의 IP 주소입니다. DNS 이름은 지원되지 않습니다.

a|
초기 R2T
a|
초기 전송 준비 상태입니다. 상태는 * 예 * 또는 * 아니요 * 일 수 있습니다.

a|
최대 버스트 길이

a|
이 iSCSI 세션의 최대 SCSI 페이로드(바이트) 최대 버스트 길이는 512에서 262,144(256KB)입니다. 기본값은 * 262,144(256KB) * 입니다.

a|
첫 번째 버스트 길이
a|
이 iSCSI 세션에 대한 요청되지 않은 데이터의 SCSI 페이로드입니다. 첫 번째 버스트 길이는 512에서 131,072(128KB)일 수 있습니다. 기본값은 * 65,536(64KB) * 입니다.

a|
기본 대기 시간입니다
a|
연결 종료 또는 연결 재설정 후 연결을 시도하기 전에 대기하는 최소 시간(초)입니다. 기본 대기 시간은 0에서 3600 사이입니다. 기본값은 * 2 * 입니다.

a|
기본 유지 시간
a|
연결 종료 또는 연결 재설정 후에도 연결이 가능한 최대 시간(초)입니다. 기본 유지 시간은 0에서 3600 사이입니다. 기본값은 * 20 * 입니다.

a|
최대 미결 R2T
a|
이 iSCSI 세션에 대해 최대 "전송 준비 완료" 수입니다. 전송 준비 완료 최대 값은 1에서 16 사이의 값일 수 있습니다. 기본값은 * 1 * 입니다.

a|
복구 수준 오류
a|
이 iSCSI 세션에 대한 오류 복구 수준입니다. 오류 복구 레벨 값은 항상 * 0 * 으로 설정됩니다.

a|

최대 수신 데이터 세그먼트 길이
 a|
이니시에이터 또는 타겟이 iSCSI PDU(페이로드 데이터 유닛)에서 수신할 수 있는 최대 데이터 양입니다.

 a|
대상 이름입니다
 a|
대상의 공식 이름(별칭 아님). 대상 이름(_iqn_format)입니다.

 a|
이니시에이터 이름입니다
 a|
이니시에이터의 공식 이름(별칭 아님) _iqn_ 또는 _eui_format을 사용하는 이니시에이터 이름입니다.

|===
====
. * 선택 사항: * 보고서를 파일에 저장하려면 * 저장 * 을 클릭합니다.
+
파일은 브라우저의 다운로드 폴더에 파일 이름과 함께 `iscsi-session-connections.txt` 저장됩니다.

[[IDca68ae1f92405158e1744f7e47b019bb]]
= iSCSI 세션을 종료합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
더 이상 필요하지 않은 iSCSI 세션을 종료할 수 있습니다. 비동기식 미러 관계의 호스트 또는 원격 스토리지 배열에서 iSCSI 세션이 발생할 수 있습니다.

.이 작업에 대해
다음과 같은 이유로 iSCSI 세션을 종료할 수 있습니다.

* * 무단 액세스 * -- iSCSI 초기자가 로그온되어 있고 액세스 권한이 없는 경우 iSCSI 세션을 종료하여 iSCSI 초기자를 스토리지 배열에서 강제로 끌 수 있습니다. 사용 가능한 인증 방법이 없으므로 iSCSI 초기자가 로그온할 수 있습니다.
* * 시스템 다운타임 * -- 스토리지 배열을 중지시켜야 하고 iSCSI 초기자가 여전히 로그온 상태인 것을 볼 경우 iSCSI 세션을 종료하여 스토리지 배열에서 iSCSI 초기자를 가져올 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 세션 보기/종료 * 를 선택합니다.
+
현재 iSCSI 세션 목록이 나타납니다.

. 종료할 세션을 선택합니다
. 세션 종료 * 를 클릭하고 작업을 수행할지 확인합니다.

[[IDf34d71db0a3a8930314b44521b1f5e74]]
= InfiniBand 포트를 통해 iSER 구성
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트에 대한 네트워크 연결을 구성할 수 있습니다.

.시작하기 전에
* 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함되어야 합니다. 그렇지 않으면 InfiniBand를 통한 iSER 설정을 System Manager에서 사용할 수 없습니다.
* 호스트 연결의 IP 주소를 알아야 합니다.

.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 구성하려는 InfiniBand 포트를 통해 iSER이 있는 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.
+
InfiniBand 포트를 통해 iSER 구성 대화 상자가 열립니다.

. 드롭다운 목록에서 구성할 HIC 포트를 선택한 다음 호스트의 IP 주소를 입력합니다.
. 구성 * 을 클릭합니다.
. 구성을 완료한 다음 * Yes * 를 클릭하여 iSER을 InfiniBand 포트로 재설정합니다.

[[ID77ded2996c57097359f3f86624646cc9]]
= InfiniBand 통계를 통해 iSER 보기
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 어레이의 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트 연결에 대한 데이터를 볼 수 있습니다.

.이 작업에 대해
System Manager는 InfiniBand 통계를 통해 다음과 같은 유형의 iSER을 보여 줍니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

* * 로컬 타겟(프로토콜) 통계 * -- InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이 통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
* InfiniBand 인터페이스 통계 * 를 통한 * iSER -- InfiniBand 인터페이스의 모든 iSER 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된 성능 통계 및 링크 오류 정보가 포함됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. InfiniBand 통계 * 를 통해 iSER 보기 * 를 선택합니다.
. 탭을 클릭하여 다양한 통계 집합을 봅니다.
. * 선택 사항: * 기준선을 설정하려면 * 새 기준선 설정 * 을 클릭합니다.
+
기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. InfiniBand 통계에서 모든 iSER에 동일한 기준선이 사용됩니다.

```
:leveloffset: -1


= NVMe 포트 관리

:leveloffset: +1


[[ID09a373348977dcff193ad7f7d34fbcac]]
= NVMe 개요
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
일부 컨트롤러에는 패브릭을 통해 NVMe(비휘발성 메모리 익스프레스)를 구현하기 위한 포트가 포함되어 있습니다. NVMe를 사용하면 호스트와 스토리지 어레이 간에 고성능 통신이 가능합니다.



== NVMe란 무엇입니까?

_NVM_은 "비휘발성 메모리"를 나타내며 다양한 유형의 저장 장치에 사용되는 영구 메모리입니다. _NVMe_(NVM Express)는 NVM 장치와의 고성능 다중 대기열 통신을 위해 특별히 설계된 표준 인터페이스 또는 프로토콜입니다.



== NVMe over Fabrics란?

_NVMe over Fabrics (NVMe-oF) _ 는 NVMe 메시지 기반 명령 및 데이터가 네트워크를 통해 호스트 컴퓨터와 스토리지 간에 전송되도록 하는 기술 사양입니다. Fabric을 사용하는 호스트에서 NVMe 스토리지 어레이(_subsystem_)에 액세스할 수 있습니다. NVMe 명령은 호스트 측과 하위 시스템 측 모두에서 전송 추상화 계층에서 활성화 및 캡슐화됩니다. 이를 통해 고성능 NVMe 인터페이스 엔드 투 엔드를 호스트에서 스토리지로 확장하고 명령 세트를 표준화하여 단순화합니다.

NVMe-oF 스토리지는 호스트에 로컬 블록 스토리지 디바이스로 표시됩니다. 다른 블록 스토리지 디바이스와 마찬가지로 볼륨(_namespace_)을 파일 시스템에 마운트할 수 있습니다. REST API, SMcli 또는 SANtricity System Manager를 사용하여 필요에 따라 스토리지를 프로비저닝할 수 있습니다.
```

== NVMe 적격 이름(NQN)이란 무엇입니까?

NVMe 정규화된 이름(NQN)은 원격 스토리지 타겟을 식별하는 데 사용됩니다. 스토리지 배열의 NVMe 정규화된 이름은 항상 서브시스템에 의해 할당되며 수정할 수 없습니다. 전체 어레이에 대해 하나의 NVMe 정규화된 이름만 있습니다. NVMe 적격 이름은 223자로 제한됩니다. iSCSI 정규화된 이름과 비교할 수 있습니다.

== 네임스페이스 및 네임스페이스 ID란 무엇입니까?

네임스페이스는 SCSI의 논리 유닛과 동일하며 어레이의 볼륨과 관련이 있습니다. NSCID(Namespace ID)는 SCSI의 LUN(Logical Unit Number)과 동일합니다. 네임스페이스 생성 시 NSID를 만들고 1에서 255 사이의 값으로 설정할 수 있습니다.

== NVMe 컨트롤러란 무엇입니까?

호스트 이니시에이터에서 스토리지 시스템의 타겟으로 연결되는 경로를 나타내는 SCSI I_T Nexus와 마찬가지로, 호스트 연결 프로세스 중에 생성된 NVMe 컨트롤러는 스토리지 어레이의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 호스트의 NQN 및 호스트 포트 식별자는 NVMe 컨트롤러를 고유하게 식별합니다. NVMe 컨트롤러는 단일 호스트에만 연결될 수 있지만 여러 네임스페이스에 액세스할 수 있습니다.

SANtricity System Manager를 사용하여 호스트에 대한 네임스페이스 ID를 설정하고 네임스페이스에 액세스할 수 있는 호스트를 구성할 수 있습니다. 그런 다음 NVMe 컨트롤러가 생성되면 NVMe 컨트롤러에서 액세스할 수 있는 네임스페이스 ID 목록을 생성하여 허용 가능한 연결을 구성하는 데 사용합니다.

[[ID074480ee3fce0e4381e473e1491b565d]]
= InfiniBand 포트를 통해 NVMe를 구성합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
컨트롤러에 InfiniBand 연결을 통한 NVMe가 포함된 경우 하드웨어 페이지에서 NVMe 포트 설정을 구성할 수 있습니다.

.시작하기 전에
* 컨트롤러에서 NVMe over InfiniBand 호스트 포트를 포함해야 합니다. 그렇지 않으면 System Manager에서 NVMe over InfiniBand 설정을 사용할 수 없습니다.
* 호스트 연결의 IP 주소를 알아야 합니다.

[NOTE]
====
NVMe over InfiniBand 설정 및 기능은 스토리지 어레이 컨트롤러에 NVMe over InfiniBand 포트가 포함된 경우에만 표시됩니다.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 구성할 NVMe over InfiniBand 포트가 있는 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. Configure NVMe over InfiniBand ports * 를 선택합니다.
+
Configure NVMe over InfiniBand Ports 대화상자가 열립니다.

. 드롭다운 목록에서 구성할 HIC 포트를 선택한 다음 IP 주소를 입력합니다.
+
200GB 사용 HIC를 포함하는 EF600 스토리지 어레이를 구성하는 경우 이 대화 상자에 물리적 포트(외부)용 IP 주소 필드와 가상 포트(내부)용 IP 주소 필드가 2개 표시됩니다. 두 포트에 대해 고유한 IP 주소를 할당해야 합니다. 이러한 설정을 통해 호스트는 각 포트 간에 경로를 설정하고 HIC는 최대 성능을 달성할 수 있습니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

. 구성 * 을 클릭합니다.
. 구성을 완료한 다음 * Yes * 를 클릭하여 NVMe over InfiniBand 포트를 재설정합니다.

[[ID4e67ab7e353175c538a1d099c83deeab]]
= NVMe over RoCE 포트를 구성합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
컨트롤러에 NVMe over RoCE(RDMA over Converged Ethernet)에 대한 연결이 포함되어 있는 경우 하드웨어 페이지에서 NVMe 포트 설정을 구성할 수 있습니다.

.시작하기 전에
* 컨트롤러에 NVMe over RoCE 호스트 포트가 포함되어야 합니다. 그렇지 않으면 System Manager에서 NVMe over RoCE 설정을 사용할 수 없습니다.
* 호스트 연결의 IP 주소를 알아야 합니다.

.단계
. 하드웨어 * 를 선택합니다.
. 그래픽에 드라이브가 표시되면 * Controllers & Components * 탭을 클릭하십시오.
+
그래픽이 변경되어 드라이브 대신 컨트롤러가 표시됩니다.

. 구성할 NVMe over RoCE 포트가 있는 컨트롤러를 클릭합니다.
+
컨트롤러의 상황에 맞는 메뉴가 나타납니다.

. RoCE 포트를 통한 NVMe 구성 * 을 선택합니다.
+
RoCE 포트를 통한 NVMe 구성 대화 상자가 열립니다.

. 드롭다운 목록에서 구성할 HIC 포트를 선택합니다.
. 다음 * 을 클릭합니다.
+
모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 포트 설정 표시 * 링크를 클릭합니다.

+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 포트 설정 | 설명

a|
이더넷 포트 속도를 구성했습니다
a|
포트에서 SFP의 속도 기능과 일치하는 속도를 선택합니다.

a|

IPv4 사용/IPv6 사용
 a|
IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오.

NOTE: 포트 액세스를 비활성화하려면 두 확인란을 모두 선택 취소합니다.

 a|
MTU 크기(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)
 a|
필요한 경우 MTU(Maximum Transmission Unit)에 대한 새 크기를 바이트 단위로 입력합니다.

기본 MTU(Maximum Transmission Unit) 크기는 프레임당 1,500바이트입니다. 1500 ~ 9000 사이의 값을 입력해야 합니다.

|===
====
+
IPv4 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 * 다음 * 을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 포트 설정 | 설명

 a|
자동으로 구성을 가져옵니다
 a|
구성을 자동으로 가져오려면 이 옵션을 선택합니다.

 a|
수동으로 정적 설정을 지정합니다
 a|
이 옵션을 선택한 다음 필드에 정적 주소를 입력합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다.

IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다. 200GB 사용 HIC를 포함하는 EF600 스토리지 어레이를 구성하는 경우 이 대화 상자에 네트워크 매개 변수에 대한 두 개의 필드 세트가 물리적 포트(외부)에 대해, 가상 포트(내부)에 대해 하나씩 표시됩니다. 두 포트에 대해 고유한 매개 변수를 할당해야 합니다. 이러한 설정을 통해 호스트는 각 포트 간에 경로를 설정하고 HIC는 최대 성능을 달성할 수 있습니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

|===
====
. 마침 * 을 클릭합니다.

[[IDa72bf150247196548c869f522935984e]]
= NVMe over Fabrics 통계 보기
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 어레이에 대한 NVMe over Fabrics 연결에 대한 데이터를 볼 수 있습니다.

.이 작업에 대해
System Manager에는 이러한 유형의 NVMe over Fabrics 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

* * NVMe 하위 시스템 통계 * -- NVMe 컨트롤러 및 해당 대기열에 대한 통계를 표시합니다. NVMe 컨트롤러는 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 연결 실패, 재설정 및 종료 같은 항목에 대한 NVMe 하위 시스템 통계를 검토할 수 있습니다.
* RDMA 인터페이스 통계 * -- RDMA 인터페이스의 모든 NVMe over Fabrics 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트에 연결된 성능 통계 및 링크 오류 정보가 포함됩니다. 이 탭은 NVMe over Fabrics 포트를 사용할 수 있을 때만 나타납니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. View NVMe over Fabrics Statistics * 를 선택합니다.
. * 선택 사항: * 기준선을 설정하려면 * 새 기준선 설정 * 을 클릭합니다.
+
기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. 모든 NVMe 통계에 동일한

기준선이 사용됩니다.

```
:leveloffset: -1

= 드라이브 관리

:leveloffset: +1

[[IDf9549c8ea3e2c03f06dd930f9d9d302b]]
= 드라이브 상태
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity System Manager에서 드라이브의 다양한 상태를 보고합니다.

== 액세스 가능성 상태

[cols="25h,~"]
|===
| 상태 | 정의

 a|
무시됨
 a|
드라이브가 물리적으로 존재하지만 컨트롤러가 어느 포트에서나 드라이브와 통신할 수 없습니다.

 a|
호환되지 않습니다
 a|
다음 조건 중 하나가 존재합니다.

* 드라이브가 스토리지 배열에 사용하도록 인증되지 않았습니다.
```

* 드라이브의 섹터 크기가 다릅니다.
* 이전 또는 최신 펌웨어 버전에서 사용할 수 없는 구성 데이터가 드라이브에 있습니다.

 a|
제거되었습니다
 a|
스토리지 배열에서 드라이브가 부적절하게 제거되었습니다.

 a|
발표
 a|
컨트롤러는 두 포트의 드라이브와 통신할 수 있습니다.

 a|
응답하지 않습니다
 a|
드라이브가 명령에 응답하지 않습니다.

|===

== 역할 상태

[cols="25h,~"]
|===
| 상태 | 정의

 a|
할당됨
 a|
드라이브가 풀 또는 볼륨 그룹의 구성원입니다.

 a|
사용 중인 핫 스페어
 a|
현재 드라이브가 장애가 발생한 드라이브를 대체하는 데 사용되고 있습니다. 핫 스페어는 풀이 아닌 볼륨 그룹에서만 사용됩니다.

```
 a|
대기 핫 스페어
 a|
장애가 발생한 드라이브를 교체할 준비가 되었습니다. 핫 스페어는 풀이 아닌 볼륨 그룹에서만 사용됩니다.


 a|
할당되지 않음
 a|
드라이브가 풀 또는 볼륨 그룹의 구성원이 아닙니다.

|===


== 가용성 상태입니다

[cols="25h,~"]
|===
| 상태 | 정의


 a|
실패했습니다
 a|
드라이브가 작동하지 않습니다. 드라이브의 데이터를 사용할 수 없습니다.


 a|
임박한 장애
 a|
드라이브가 곧 고장날 수 있다는 것이 감지되었습니다. 드라이브의 데이터를 계속 사용할 수 있습니다.


 a|
오프라인
 a|
일반적으로 드라이브를 내보내는 볼륨 그룹의 일부이거나 펌웨어 업그레이드를 진행 중이므로 데이터를 저장할 수 없습니다.
```

```
 a|
최적
 a|
드라이브가 정상적으로 작동합니다.

|===



[[ID6bf7bad1b82ff3447db14a5b43eb0c34]]
= SSD(Solid State Disk)
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SSD(Solid-State Disk)는 데이터를 영구적으로 저장하기 위해 솔리드 스테이트 메모리(플래시)를 사용하는 데이터 스토리지 장치입니다. SSD는 기존의 하드 드라이브를 에뮬레이트하며 하드 드라이브에서 사용하는 것과 동일한 인터페이스로 사용할 수 있습니다.



== SSD의 장점

하드 드라이브에 비해 SSD의 장점은 다음과 같습니다.

* 빠른 시작(스핀업 없음)
* 더 짧은 지연 시간
* 높은 IOPS(초당 I/O 작업)
* 구동 부품 수가 줄어들어 안정성이 높아집니다
* 전력 사용량 감소
* 열이 적게 생성되고 냉각이 적게 필요합니다



== SSD 식별

하드웨어 페이지에서 전면 쉘프 보기에서 SSD를 찾을 수 있습니다. SSD가 설치되었음을 나타내는 번개 모양 아이콘이 표시되는 드라이브 베이를 찾습니다.
```

== 볼륨 그룹

볼륨 그룹의 모든 드라이브는 동일한 미디어 유형(모든 SSD 또는 모든 하드 드라이브)이어야 합니다. 볼륨 그룹은 미디어 유형 또는 인터페이스 유형을 혼합하여 사용할 수 없습니다.

== 캐싱

컨트롤러의 쓰기 캐싱은 항상 SSD에 사용됩니다. 쓰기 캐싱은 성능을 개선하고 SSD의 수명을 연장합니다.

컨트롤러 캐시 외에 SSD 캐시 기능을 구현하여 전체 시스템 성능을 개선할 수 있습니다. SSD Cache에서는 데이터가 볼륨에서 복사되어 두 개의 내부 RAID 볼륨(컨트롤러당 1개)에 저장됩니다.

[[IDc9b4dac39433ef22c355fbbe5eb97c40]]
= 드라이브 보기를 제한합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열에 서로 다른 유형의 물리적 및 논리적 속성이 있는 드라이브가 포함되어 있는 경우 Hardware(하드웨어) 페이지에서는 드라이브 보기를 제한하고 특정 드라이브를 찾는 데 도움이 되는 필터 필드를 제공합니다.

.이 작업에 대해
드라이브 필터는 특정 논리적 위치(예: 볼륨 그룹 1)에서 특정 보안 속성(예: 보안 가능)을 가진 특정 유형의 물리적 드라이브(예: 모든 SAS)로만 보기를 제한할 수 있습니다. 이러한 필터를 함께 또는 별도로 사용할 수 있습니다.

[NOTE]
====
모든 드라이브가 동일한 물리적 속성을 공유하는 경우 * Show drives that are... * filter 필드가 나타나지 않습니다. 모든 드라이브가 동일한 논리 속성을 공유하는 경우 스토리지 배열 * 필터 필드의 * 아무 곳이나 나타나지 않습니다.

====
.단계
. 하드웨어 * 를 선택합니다.
. 첫 번째 필터 필드(* Show drives that are... * 아래)에서 드롭다운 화살표를 클릭하여 사용 가능한 드라이브 유형 및 보안 속성을 표시합니다.

+
드라이브 유형은 다음과 같습니다.

+
** 드라이브 미디어 유형(SSD, HDD)
** 드라이브 인터페이스 유형입니다
** 드라이브 용량(최고 - 최저)
** 드라이브 속도(최고 ~ 최저) 보안 속성에는 다음이 포함될 수 있습니다.
** 보안 가능
** 보안이 설정되었습니다
** DA(Data Assurance) 가능
** FIPS 규격
** FIPS 규격(FIPS 140-2)
** FIPS 규격(FIPS 140-3)
+
이러한 속성이 모든 드라이브에서 동일한 경우 드롭다운 목록에 표시되지 않습니다. 예를 들어, 스토리지 어레이에 SAS 인터페이스 및 15000RPM의 속도가 포함된 모든 SSD 드라이브가 포함되어 있지만 일부 SSD의 용량이 서로 다른 경우, 드롭다운 목록에는 필터링 선택 항목으로서 용량만 표시됩니다.

+
필드에서 옵션을 선택하면 필터 기준과 일치하지 않는 드라이브가 그래픽 보기에서 회색으로 표시됩니다.

. 두 번째 필터 상자에서 드롭다운 화살표를 클릭하여 드라이브의 사용 가능한 논리 위치를 표시합니다.
+
[NOTE]
====
필터 기준을 지우려면 필터 상자 오른쪽 끝에 있는 * Clear * 를 선택합니다.

====
+
논리 위치는 다음과 같습니다.

+
** 풀
** 볼륨 그룹
** 핫 스페어
** SSD 캐시
** 할당되지 않음
+
필드에서 옵션을 선택하면 필터 기준과 일치하지 않는 드라이브가 그래픽 보기에서 회색으로 표시됩니다.

. 선택적으로 필터 필드 맨 오른쪽에 있는 * 로케이터 라이트 켜기 * 를 선택하여 표시된 드라이브의 로케이터 라이트를 켤 수 있습니다.
+
이렇게 하면 스토리지 배열에서 드라이브를 물리적으로 찾을 수 있습니다.

[[ID512563b5c430a3a8167fa78d1d8655d4]]
= 드라이브 로케이터 표시등을 켭니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Hardware 페이지에서 로케이터 표시등을 켜서 스토리지 배열의 드라이브의 물리적 위치를 찾을 수 있습니다.

.이 작업에 대해
하드웨어 페이지에 표시된 단일 드라이브 또는 여러 드라이브를 찾을 수 있습니다.

.단계
. 하드웨어 * 를 선택합니다.
. 하나 이상의 드라이브를 찾으려면 다음 중 하나를 수행합니다.
+
** * 단일 드라이브 * -- 쉘프 그래픽에서 실제로 어레이에서 찾을 드라이브를 찾습니다. (그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.) 드라이브를 클릭하여 컨텍스트 메뉴를 표시한 다음 * 로케이터 표시등 켜기 * 를 선택합니다.
+
드라이브 로케이터 표시등이 켜집니다. 드라이브를 물리적으로 찾았으면 대화 상자로 돌아가서 * 끄기 * 를 선택합니다.

** * 다중 드라이브 * -- 필터 필드의 왼쪽 드롭다운 목록에서 물리적 드라이브 유형을 선택하고 오른쪽 드롭다운 목록에서 논리 드라이브 유형을 선택합니다. 기준과 일치하는 드라이브 수가 필드 맨 오른쪽에 표시됩니다. 그런 다음 * 로케이터 조명 켜기 * 를 클릭하거나 컨텍스트 메뉴에서 * 필터링된 모든 드라이브 찾기 * 를 선택할 수 있습니다. 드라이브를 물리적으로 찾았으면 대화 상자로 돌아가서 * 끄기 * 를 선택합니다.

```
[[ID68f9261dbf3a7671ddde8efb759ab45a]]
= 드라이브 상태 및 설정을 봅니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미디어 유형, 인터페이스 유형, 용량 등 드라이브의 상태와 설정을 볼 수 있습니다.

.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 상태 및 설정을 보려는 드라이브를 선택합니다.
+
드라이브의 컨텍스트 메뉴가 열립니다.

. 설정 보기 * 를 선택합니다.
+
드라이브 설정 대화 상자가 열립니다.

. 모든 설정을 보려면 대화 상자 오른쪽 위에 있는 * 더 많은 설정 표시 * 를 클릭합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명


 a|
상태
 a|
최적, 오프라인, 중요하지 않은 오류 및 실패를 표시합니다. 최적 상태는 원하는 작동 상태를 나타냅니다.



 a|
모드를 선택합니다
 a|
```

Assigned, Unassigned, Hot Spare Standby 또는 Hot Spare 사용 중 을 표시합니다.

a|
위치
a|
에서는 드라이브가 위치한 쉘프 및 베이 번호를 보여 줍니다.

a|
보호 대상/보호 대상/보호 가능
a|
드라이브가 풀, 볼륨 그룹 또는 SSD 캐시에 할당된 경우 이 필드에는 "Assigned To(할당 대상)"가 표시됩니다. 값은 풀 이름, 볼륨 그룹 이름 또는 SSD 캐시 이름일 수 있습니다. 드라이브가 핫 스페어에 할당되고 해당 모드가 대기 모드인 경우 이 필드에 "보호할 수 있음"이 표시됩니다. 핫 스페어가 하나 이상의 볼륨 그룹을 보호할 수 있는 경우 볼륨 그룹 이름이 나타납니다. 볼륨 그룹을 보호할 수 없는 경우 0개의 볼륨 그룹이 표시됩니다.

드라이브가 핫 스페어에 할당되고 해당 모드가 사용 중이면 이 필드에 "보호 중"이 표시됩니다. 값은 영향을 받는 볼륨 그룹의 이름입니다.

드라이브를 지정하지 않으면 이 필드가 나타나지 않습니다.

a|
미디어 유형
a|
하드 디스크 드라이브(HDD) 또는 솔리드 스테이트 디스크(SSD)일 수 있는 드라이브에서 사용하는 레코딩 미디어의 유형을 표시합니다.

a|
사용된 내구성(SSD 드라이브가 있는 경우에만 표시됨)
a|
현재까지 드라이브에 기록된 데이터의 양을 이론적인 총 쓰기 한계로 나눈 값입니다.

a|
인터페이스 유형입니다
a|
SAS와 같이 드라이브에서 사용하는 인터페이스 유형을 표시합니다.

a|
드라이브 경로 이중화
a|
드라이브와 컨트롤러 사이의 연결이 중복되었는지(예) 여부를 표시합니다(아니요).

a|
용량(GiB)
a|
드라이브의 가용 용량(구성된 총 용량)을 표시합니다.

a|
속도(RPM)
a|
RPM으로 속도를 표시합니다(SSD의 경우 표시되지 않음).

a|
현재 데이터 속도입니다
a|
드라이브와 스토리지 어레이 간의 데이터 전송 속도를 표시합니다.

a|
논리 섹터 크기(바이트)
a|
드라이브가 사용하는 논리 섹터 크기를 표시합니다.

a|
물리적 섹터 크기(바이트)
a|
드라이브가 사용하는 물리적 섹터 크기를 표시합니다. 일반적으로 물리적 섹터 크기는 하드 디스크 드라이브의 경우 4096바이트입니다.

a|
드라이브 펌웨어 버전입니다

a|
드라이브 펌웨어의 버전 레벨을 표시합니다.

a|
전 세계 식별자
a|
드라이브의 고유한 16진수 식별자를 표시합니다.

a|
제품 ID
a|
제조업체에서 할당한 제품 ID를 표시합니다.

a|
일련 번호입니다
a|
드라이브의 일련 번호를 표시합니다.

a|
제조업체
a|
드라이브의 공급업체를 표시합니다.

a|
제조 날짜
a|
드라이브가 빌드된 날짜를 표시합니다.

NOTE: NVMe 드라이브에는 사용할 수 없습니다.

a|
보안 가능
a|
드라이브가 안전한지(예) 여부를 표시합니다(아니요). 보안이 가능한 드라이브는 FDE(전체 디스크

암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브(레벨 140-2 또는 140-3)일 수 있으며, 이 드라이브는 쓰기 중 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이러한 드라이브는 드라이브 보안 기능을 사용하여 추가 보안을 위해 사용할 수 있으므로 보안 -_가능_으로 간주됩니다. 드라이브 보안 기능이 이러한 드라이브에 사용된 볼륨 그룹 및 풀에 대해 활성화된 경우 드라이브는 secure-_enabled_가 됩니다.

a|
보안이 설정되었습니다

a|
드라이브가 안전한지(예) 여부를 표시합니다(아니요). 보안 지원 드라이브는 드라이브 보안 기능과 함께 사용됩니다. 드라이브 보안 기능을 활성화한 다음 보안 -_가능_드라이브의 풀 또는 볼륨 그룹에 드라이브 보안을 적용하면 드라이브가 보안 -_활성화됨_이 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.

a|
읽기/쓰기 액세스가 가능합니다

a|
드라이브가 읽기/쓰기 액세스 가능(예) 상태인지 여부(아니요)를 표시합니다.

a|
드라이브 보안 키 식별자입니다

a|
에는 보안 지원 드라이브의 보안 키가 나와 있습니다. 드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.

a|
DA(Data Assurance) 가능

a|
DA(Data Assurance) 기능의 사용 여부(예) 또는 사용 안 함(아니요)을 표시합니다. DA(Data Assurance)는 데이터를 컨트롤러를 통해 드라이브로 전송할 때 발생할 수 있는 오류를 확인하고 수정하는 기능입니다. Fibre Channel과 같은 DA 지원 입출력 인터페이스를 사용하는 호스트에서 풀 또는 볼륨 그룹 레벨에서 Data Assurance를 설정할 수 있습니다.

```
 a|
DULBE 가능
 a|
할당 해제 또는 기록되지 않은 논리 블록 오류(DULBE)의 옵션이 사용(예) 또는 사용 안 함
(아니요)으로 설정되어 있는지 여부를 나타냅니다. DULBE는 EF300 또는 EF600 스토리지
어레이가 리소스 프로비저닝된 볼륨을 지원할 수 있도록 NVMe 드라이브에 대한 옵션입니다.

|===
====
. 닫기 * 를 클릭합니다.




[[ID59c0419230a45d63f746064d2177d93a]]
= 드라이브를 논리적으로 교체합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
드라이브에 장애가 발생하거나 다른 이유로 인해 드라이브를 교체하려는 경우, 장애가 발생한
드라이브를 할당되지 않은 드라이브 또는 완전히 통합된 핫 스페어로 논리적으로 교체할 수
있습니다.

.이 작업에 대해
드라이브를 논리적으로 교체하면 드라이브가 할당되고 연결된 풀 또는 볼륨 그룹의 영구 구성원이
됩니다.

논리 교체 옵션을 사용하여 다음 유형의 드라이브를 교체할 수 있습니다.

* 오류가 발생한 드라이브
* 드라이브가 없습니다
* Recovery Guru에서 SSD 드라이브의 수명이 거의 다 되었음을 알립니다
* Recovery Guru에서 드라이브 오류가 임박한 것으로 통보한 하드 드라이브입니다
* 할당된 드라이브(풀이 아닌 볼륨 그룹의 드라이브에 대해서만 사용 가능)


.시작하기 전에
교체 드라이브의 특징은 다음과 같습니다.

* 최적 상태
* 할당되지 않음 상태
* 교체할 드라이브와 동일한 속성(미디어 유형, 인터페이스 유형 등)
```

* 동일한 FDE 기능(권장, 필수 아님)
* 동일한 DA 기능(권장, 필수 아님)

.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 논리적으로 교체할 드라이브를 클릭합니다.
+
드라이브의 컨텍스트 메뉴가 나타납니다.

. 논리적으로 바꾸기 * 를 클릭합니다.
. * 선택 사항: * 교체 후 * 실패 드라이브 * 확인란을 선택하여 교체 후 원래 드라이브에 장애가 발생합니다.
+
이 확인란은 원래 할당된 드라이브가 실패했거나 누락되지 않은 경우에만 활성화됩니다.

. Select a replacement drive* 표에서 사용할 교체 드라이브를 선택합니다.
+
이 표에는 교체하려는 드라이브와 호환되는 드라이브만 나열되어 있습니다. 가능한 경우 쉘프 손실 방지 및 드로어 손실 방지 기능을 유지하는 드라이브를 선택합니다.

. 바꾸기 * 를 클릭합니다.
+
원래 드라이브에 오류가 발생하거나 누락된 경우 패리티 정보를 사용하여 교체 드라이브에서 데이터가 재구성됩니다. 이 재구성이 자동으로 시작됩니다. 드라이브 장애 표시등이 꺼지고 풀 또는 볼륨 그룹의 드라이브 작동 표시등이 깜박이기 시작합니다.

+
원본 드라이브에 오류가 발생하거나 누락된 경우 해당 데이터가 교체 드라이브로 복사됩니다. 이 복사 작업은 자동으로 시작됩니다. 복사 작업이 완료되면 시스템은 원래 드라이브를 할당되지 않은 상태로 전환하거나 이 확인란을 선택한 경우 실패 상태로 전환합니다.

[[IDed9db20c892d9a911f743c91dcef8876]]
= 드라이브를 수동으로 재구성합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
드라이브 재구성은 일반적으로 드라이브를 교체한 후 자동으로 시작됩니다. 드라이브 재구성이 자동으로 시작되지 않으면 수동으로 재구성을 시작할 수 있습니다.

[NOTE]
====
기술 지원 부서 또는 Recovery Guru에서 지시한 경우에만 이 작업을 수행하십시오.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 수동으로 재구성할 드라이브를 클릭합니다.
+
드라이브의 컨텍스트 메뉴가 나타납니다.

. Reconstruct * 를 선택하고 작업을 수행할지 확인합니다.

[[IDa02f795cac6d6cf9303295b3f1949be8]]
= 드라이브를 초기화(포맷)합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
할당된 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 드라이브를 초기화(포맷)해야 새 스토리지 어레이에서 사용할 수 있습니다.

.이 작업에 대해
초기화하면 드라이브에서 이전 구성 정보가 제거되고 할당되지 않은 상태로 돌아갑니다. 그런 다음 새 스토리지 배열의 새 풀 또는 볼륨 그룹에 드라이브를 추가할 수 있습니다.

단일 드라이브를 이동할 때 드라이브 초기화 작업을 사용합니다. 전체 볼륨 그룹을 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 드라이브를 초기화할 필요가 없습니다.

[CAUTION]
====
* 데이터 손실 가능성 * -- 드라이브를 초기화하면 드라이브의 모든 데이터가 손실됩니다. 기술

지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 초기화하려는 드라이브를 클릭합니다.
+
드라이브의 컨텍스트 메뉴가 나타납니다.

. Initialize * 를 선택하고 작업을 수행할지 확인합니다.

[[ID7fe6c8f50685545df234bf6afa436507]]
= 드라이브 오류
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
그렇게 하라는 지시가 있으면 드라이브를 수동으로 실패할 수 있습니다.

.이 작업에 대해
System Manager는 스토리지 배열의 드라이브를 모니터링합니다. 드라이브에서 많은 오류가 발생하는 것을 감지하면 Recovery Guru에서 드라이브 장애가 임박했음을 알립니다. 이 경우 교체 드라이브를 사용할 수 있는 경우 드라이브가 장애를 갖고 우선 조치를 취할 수 있습니다. 교체 드라이브를 사용할 수 없는 경우 드라이브가 스스로 고장날 때까지 기다릴 수 있습니다.

[CAUTION]
====
* 데이터 액세스 손실 가능성 * -- 이 작업은 데이터 손실이나 데이터 중복성의 손실을 초래할 수 있습니다. 기술 지원 부서 또는 Recovery Guru에서 지시한 경우에만 이 작업을 수행하십시오.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 실패하려는 드라이브를 클릭합니다.
+
드라이브의 컨텍스트 메뉴가 나타납니다.

. 실패 * 를 선택합니다.
. 실패 전에 * 드라이브의 내용 복사 * 확인란을 선택한 상태로 유지합니다.
+
복사 옵션은 할당된 드라이브 및 비 RAID 0 볼륨 그룹에 대해서만 나타납니다.

+
드라이브에 장애가 발생하기 전에 드라이브의 내용을 복사해야 합니다. 구성에 따라 드라이브의 내용을 먼저 복사하지 않으면 연결된 풀 또는 볼륨 그룹의 모든 데이터 또는 데이터 중복성이 손실될 수 있습니다.

+
복사 옵션을 사용하면 재구성 작업보다 더 빠르게 드라이브를 복구할 수 있으며 복사 작업 중에 다른 드라이브에 장애가 발생할 경우 볼륨 장애 가능성이 줄어듭니다.

. 드라이브에 오류가 발생할지 확인합니다.
+
드라이브에 오류가 발생한 후 30초 이상 기다린 후 제거하십시오.

[[ID9dc56e39c5ed7bbe1e49d25618d68a4b]]
= 드라이브를 지웁니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
지우기 옵션을 사용하여 시스템에서 제거할 할당되지 않은 드라이브를 준비할 수 있습니다. 이 절차에서는 데이터를 영구적으로 제거하여 데이터를 다시 읽을 수 없도록 합니다.

.시작하기 전에
드라이브가 할당되지 않은 상태여야 합니다.

.이 작업에 대해
드라이브의 모든 데이터를 영구적으로 제거하려는 경우에만 지우기 옵션을 사용합니다. 드라이브가 안전하게 활성화된 경우 Erase(지우기) 옵션은 암호화 지우기를 수행하고 드라이브의 보안 속성을 다시 보안 기능으로 재설정합니다.

[NOTE]
====
지우기 기능은 일부 이전 드라이브 모델을 지원하지 않습니다. 이러한 이전 모델 중 하나를 지우려고 하면 오류 메시지가 나타납니다.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 선택적으로 필터 필드를 사용하여 쉘프의 할당되지 않은 모든 드라이브를 볼 수 있습니다. Show drives that are... * 드롭다운 목록에서 * Unassigned * 를 선택합니다.
+
쉘프 보기에는 할당되지 않은 드라이브만 표시되며 다른 모든 드라이브는 회색으로 표시됩니다.

. 드라이브의 상황에 맞는 메뉴를 열려면 지울 드라이브를 클릭합니다. (여러 드라이브를 선택하려면 드라이브 지우기 대화 상자에서 선택할 수 있습니다.)
+
[CAUTION]
====
* 데이터 손실 가능성 * -- 지우기 작업을 실행 취소할 수 없습니다. 절차를 진행하는 동안 올바른 드라이브를 선택해야 합니다.

====
. 컨텍스트 메뉴에서 * Erase * 를 선택합니다.
+
Erase Drives(드라이브 지우기) 대화 상자가 열리고 지우기 작업에 사용할 수 있는 모든 드라이브가 표시됩니다.

. 필요한 경우 테이블에서 추가 드라이브를 선택합니다. ALL_DRIVE를 선택할 수 없습니다. 하나의 드라이브가 선택 해제되어 있는지 확인하십시오.
. 을 입력하여 작업을 확인한 `erase` 다음 * Erase * 를 클릭합니다.
+
[CAUTION]
====
이 작업을 계속 진행하십시오. 다음 대화 상자에서 예를 클릭하면 작업을 중단할 수 없습니다.

====
. 예상 완료 시간 대화 상자에서 * 예 * 를 클릭하여 지우기 작업을 계속합니다.

.결과
지우기 작업에는 몇 분 또는 몇 시간이 걸릴 수 있습니다. 홈 [View Operations in Progress] 메뉴에서 상태를 볼 수 있습니다. 지우기 작업이 완료되면 다른 볼륨 그룹 또는

디스크 풀 또는 다른 스토리지 어레이에서 드라이브를 사용할 수 있습니다.

.작업을 마친 후
드라이브를 다시 사용하려면 먼저 초기화해야 합니다. 이렇게 하려면 드라이브의 컨텍스트 메뉴에서 * Initialize * 를 선택합니다.

[[ID658d2bfd6be52524625002a65d3ea640]]
= 잠긴 NVMe 또는 FIPS 드라이브의 잠금을 해제하거나 재설정합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
하나 이상의 잠긴 NVMe 또는 FIPS 드라이브를 스토리지 어레이에 삽입하면 드라이브와 연결된 보안 키 파일을 추가하여 드라이브 데이터의 잠금을 해제할 수 있습니다. 보안 키가 없는 경우 PSID(Physical Security ID)를 입력하여 잠긴 각 드라이브에서 재설정을 수행하여 보안 속성을 재설정하고 드라이브 데이터를 지울 수 있습니다.

.시작하기 전에
* Unlock(잠금 해제) 옵션의 경우 관리 클라이언트(System Manager에 액세스하는 데 사용되는 브라우저가 있는 시스템)에서 보안 키 파일(확장자 포함 `.slk`)을 사용할 수 있는지 확인합니다. 키와 관련된 암호도 알아야 합니다.
* 재설정 옵션의 경우 재설정할 각 드라이브에서 PSID를 찾아야 합니다. PSID를 찾으려면 드라이브를 물리적으로 분리하고 드라이브 레이블에서 PSID 문자열(최대 32자)을 찾은 다음 드라이브를 다시 설치합니다.

.이 작업에 대해
이 작업에서는 보안 키 파일을 스토리지 어레이로 가져와서 NVMe 또는 FIPS 드라이브에서 데이터를 잠금 해제하는 방법을 설명합니다. 보안 키를 사용할 수 없는 경우 이 작업에서는 잠긴 드라이브에서 재설정을 수행하는 방법도 설명합니다.

[NOTE]
====
드라이브가 외부 키 관리 서버를 사용하여 잠긴 경우 System Manager의 메뉴: 설정 [시스템 > 보안 키 관리]을 선택하여 외부 키 관리를 구성하고 드라이브의 잠금을 해제합니다.

====
하드웨어 페이지 또는 메뉴에서 잠금 해제 기능에 액세스할 수 있습니다: 설정 [시스템 > 보안 키 관리]. 아래 작업은 하드웨어 페이지의 지침을 제공합니다.

.단계

. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 잠금 해제 또는 재설정할 NVMe 또는 FIPS 드라이브를 선택합니다.
+
드라이브의 컨텍스트 메뉴가 열립니다.

. 보안 키 파일을 적용하려면 * 잠금 해제 * 를 선택하고, 보안 키 파일이 없으면 * 재설정 * 을 선택합니다.
+
이러한 옵션은 잠긴 NVMe 또는 FIPS 드라이브를 선택한 경우에만 표시됩니다.

+
[CAUTION]
====
재설정 작업 중에는 모든 데이터가 삭제됩니다. 보안 키가 없는 경우에만 재설정을 수행하십시오. 잠긴 드라이브를 재설정하면 드라이브의 모든 데이터가 영구적으로 제거되고 보안 속성이 "보안 가능"으로 재설정되지만 활성화되지는 않습니다. * 이 작업은 되돌릴 수 없습니다. *

====
. 다음 중 하나를 수행합니다.
+
.. * 잠금 해제 *: * 보안 드라이브 잠금 해제 * 대화 상자에서 * 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다. 그런 다음 암호를 입력하고 * Unlock * (잠금 해제 *)을 클릭합니다.
.. * Reset *: * Reset Locked Drive * (잠긴 드라이브 재설정 *) 대화 상자에서 필드에 PSID 문자열을 입력한 다음 `RESET` 확인을 입력합니다. 재설정 * 을 클릭합니다.
+
잠금 해제 작업의 경우 이 작업을 한 번만 수행하면 모든 NVMe 또는 FIPS 드라이브를 잠금 해제할 수 있습니다. 재설정 작업의 경우 재설정할 각 드라이브를 개별적으로 선택해야 합니다.

.결과
이제 드라이브를 다른 볼륨 그룹 또는 디스크 풀 또는 다른 스토리지 어레이에서 사용할 수 있습니다.

:leveloffset: -1

= 핫 스페어 관리

```
:leveloffset: +1


[[IDd78a7ae8327120f240e18a25164568ac]]
= 핫 스페어 드라이브 개요
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
핫 스페어는 SANtricity System Manager용 RAID 1, RAID 5 또는 RAID 6 볼륨 그룹에서
대기 드라이브로 작동합니다.

데이터가 없는 완전한 기능을 갖춘 드라이브입니다. 볼륨 그룹에서 드라이브에 장애가 발생하면
컨트롤러는 장애가 발생한 드라이브에서 핫 스페어로 할당된 드라이브로 데이터를 자동으로
재구성합니다.

핫 스페어는 특정 볼륨 그룹 전용이 아닙니다. 핫 스페어와 드라이브가 다음 속성을 공유하는 한
스토리지 배열의 모든 장애 드라이브에 사용할 수 있습니다.

* 동일한 용량(또는 핫 스페어의 더 큰 용량)
* 동일한 미디어 유형(예: HDD 또는 SSD)
* 동일한 인터페이스 유형(예: SAS)




== 핫 스페어 식별 방법

초기 설치 마법사 또는 하드웨어 페이지에서 핫 스페어를 할당할 수 있습니다. 핫 스페어가
할당되었는지 확인하려면 하드웨어 페이지로 이동하여 분홍색으로 표시된 드라이브 베이를 찾습니다.



== 핫 스페어 적용 범위

핫 스페어 범위는 다음과 같습니다.

* 할당되지 않은 드라이브는 RAID 1, RAID 5 또는 RAID 6 볼륨 그룹의 핫 스페어로
예약됩니다.
+
[NOTE]
====
핫 스페어는 데이터 보호 방법이 다른 풀에 사용할 수 없습니다. 풀은 추가 드라이브를 예약하지
```

않고 풀의 각 드라이브에 예비 용량(_preservation capacity_)을 예약합니다. 풀에서 드라이브에 장애가 발생할 경우 컨트롤러는 해당 여유 용량으로 데이터를 재구성합니다.

====
* RAID 1, RAID 5 또는 RAID 6 볼륨 그룹 내의 드라이브에 장애가 발생하면 컨트롤러는 자동으로 중복 데이터를 사용하여 오류가 발생한 드라이브의 데이터를 재구성합니다. 핫 스페어는 물리적 스왑 없이 장애가 발생한 드라이브를 자동으로 대체합니다.
* 장애가 발생한 드라이브를 물리적으로 교체한 경우, 핫 스페어 드라이브에서 교체한 드라이브로 데이터를 재복사하는 작업이 수행됩니다. 핫 스페어 드라이브를 볼륨 그룹의 영구 구성원으로 지정한 경우에는 카피백 작업이 필요하지 않습니다.
* 볼륨 그룹에 대한 트레이 손실 방지 및 드로어 손실 보호는 볼륨 그룹을 구성하는 드라이브의 위치에 따라 달라집니다. 드라이브 장애 및 핫 스페어 드라이브의 위치 때문에 트레이 손실 방지 및 드로어 손실 보호가 손실될 수 있습니다. 트레이 손실 방지 및 서랍 손실 보호가 영향을 받지 않도록 하려면, 카피백 프로세스를 시작하기 위해 고장난 드라이브를 교체해야 합니다.
* 핫 스페어 드라이브가 장애가 발생한 드라이브로 자동 대체되기 때문에 스토리지 어레이 볼륨은 장애가 발생한 드라이브를 교체하는 동안 온라인 상태로 유지되고 액세스할 수 있습니다.

== 핫 스페어 드라이브 용량에 대한 고려 사항

보호하려는 드라이브의 총 용량과 같거나 더 큰 용량의 드라이브를 선택합니다. 예를 들어, 18GiB 드라이브의 용량이 8GiB인 경우 9GiB 이상의 드라이브를 핫 스페어로 사용할 수 있습니다. 일반적으로 스토리지 어레이에서 가장 큰 드라이브의 용량과 같거나 큰 용량이 아니면 드라이브를 핫 스페어로 할당하지 마십시오.

[NOTE]
====
물리적 용량이 동일한 핫 스페어를 사용할 수 없는 경우 드라이브의 "사용된 용량"이 핫 스페어 드라이브의 용량보다 작거나 같은 경우 용량이 낮은 드라이브를 핫 스페어로 사용할 수 있습니다.

====

== 미디어 및 인터페이스 유형에 대한 고려 사항

핫 스페어로 사용되는 드라이브는 보호할 드라이브와 동일한 미디어 유형 및 인터페이스 유형을 공유해야 합니다. 예를 들어, HDD 드라이브는 SSD 드라이브의 핫 스페어로 사용할 수 없습니다.

== 보안 가능 드라이브에 대한 고려 사항

FDE 또는 FIPS와 같은 보안 지원 드라이브는 보안 기능이 있거나 없는 드라이브의 핫 스페어로 사용할 수 있습니다. 그러나 보안이 가능하지 않은 드라이브는 보안 기능이 있는 드라이브의 핫 스페어로 사용할 수 없습니다.

핫 스페어에 사용할 보안 지원 드라이브를 선택하면 System Manager에서 보안 지우기를 수행하라는 메시지를 표시합니다. Secure Erase는 드라이브의 보안 속성을 보안 가능 상태로 재설정하지만 보안 사용 가능으로 다시 설정합니다.

[NOTE]
====
드라이브 보안 기능을 활성화한 다음 보안 가능 드라이브에서 풀 또는 볼륨 그룹을 생성하면 해당 드라이브는 _secure-enabled_가 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.

====

== 권장되는 핫 스페어 드라이브 수입니다

초기 설정 마법사를 사용하여 핫 스페어를 자동으로 생성한 경우 System Manager에서는 특정 미디어 유형 및 인터페이스 유형의 드라이브 30개마다 핫 스페어 하나를 생성합니다. 그렇지 않으면 스토리지 배열의 볼륨 그룹 간에 핫 스페어 드라이브를 수동으로 생성할 수 있습니다.

[[IDc0c0dcc2dacec108f18dc8abd4f81aee]]
= 핫 스페어를 할당합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
RAID 1, RAID 5 또는 RAID 6 볼륨 그룹의 추가 데이터 보호를 위해 핫 스페어를 대기 드라이브로 할당할 수 있습니다. 이러한 볼륨 그룹 중 하나에서 장애가 발생하면 컨트롤러가 장애가 발생한 드라이브에서 핫 스페어로 데이터를 재구성합니다.

.시작하기 전에
* RAID 1, RAID 5 또는 RAID 6 볼륨 그룹을 만들어야 합니다. (핫 스페어는 풀에 사용할 수 없습니다. 대신 풀에서는 데이터 보호를 위해 각 드라이브 내의 여유 용량을 사용합니다.)
* 다음 기준을 충족하는 드라이브를 사용할 수 있어야 합니다.
+
** 할당되지 않음, 최적 상태
** 볼륨 그룹의 드라이브(예: SSD)와 동일한 미디어 유형입니다.
** 볼륨 그룹의 드라이브와 동일한 인터페이스 유형(예: SAS)
** 볼륨 그룹에 있는 드라이브의 사용된 용량과 같거나 더 큰 용량입니다.

.이 작업에 대해
이 작업에서는 하드웨어 페이지에서 핫 스페어를 수동으로 할당하는 방법에 대해 설명합니다. 권장되는 적용 범위는 드라이브 세트당 2개의 핫 스페어입니다.

[NOTE]
====
핫 스페어는 초기 설정 마법사에서 할당할 수도 있습니다. 하드웨어 페이지에서 분홍색으로 표시된 드라이브 베이를 찾아 핫 스페어가 이미 할당되었는지 확인할 수 있습니다.

====
.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 핫 스페어로 사용할 할당되지 않은 드라이브(회색으로 표시됨)를 선택합니다.
+
드라이브의 컨텍스트 메뉴가 열립니다.

. 핫 스페어 할당 * 을 선택합니다.
+
드라이브가 보안이 설정된 경우 Secure Erase Drive(드라이브 지우기) 대화 상자가 열립니다. 보안 지원 드라이브를 핫 스페어로 사용하려면 먼저 Secure Erase(보안 지우기) 작업을 수행하여 모든 데이터를 제거하고 보안 속성을 재설정해야 합니다.

+
[CAUTION]
====
* 데이터 손실 가능성 * -- 올바른 드라이브를 선택했는지 확인하십시오. 보안 지우기 작업을 완료한 후에는 데이터를 복구할 수 없습니다.

====
+
드라이브가 * 보안 활성화되지 않음 * 인 경우 핫 스페어 드라이브 할당 확인 대화 상자가 열립니다.

. 대화 상자의 텍스트를 검토하고 작업을 확인합니다.
+
이 드라이브는 이제 핫 스페어임을 나타내는 분홍색으로 하드웨어 페이지에 표시됩니다.

.결과
RAID 1, RAID 5 또는 RAID 6 볼륨 그룹 내의 드라이브에 장애가 발생하면 컨트롤러는 자동으로

중복 데이터를 사용하여 오류가 발생한 드라이브에서 핫 스페어로 데이터를 재구성합니다.

[[ID3d2a97782dda5528083788dbf9fb12d2]]
= 핫 스페어 할당을 취소합니다
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
핫 스페어를 할당되지 않은 드라이브로 다시 변경할 수 있습니다.

.시작하기 전에
핫 스페어는 Optimal(최적), Standby(대기) 상태여야 합니다.

.이 작업에 대해
장애가 발생한 드라이브를 현재 페일오버하는 핫 스페어를 할당 해제할 수 없습니다. 핫 스페어가 최적의 상태가 아닌 경우, 드라이브 할당을 취소하기 전에 Recovery Guru 절차에 따라 문제를 해결하십시오.

.단계
. 하드웨어 * 를 선택합니다.
. 그림에 컨트롤러가 표시되면 * Drives * 탭을 클릭합니다.
+
그래픽이 변경되어 컨트롤러 대신 드라이브가 표시됩니다.

. 할당 취소할 핫 스페어 드라이브(분홍색으로 표시됨)를 선택합니다.
+
분홍색 드라이브 베이를 가로지르는 대각선이 있는 경우 핫 스페어가 현재 사용 중이며 할당을 취소할 수 없습니다.

+
드라이브의 컨텍스트 메뉴가 열립니다.

. 드라이브의 드롭다운 목록에서 * 핫 스페어 할당 해제 * 를 선택합니다.
+
이 대화 상자에는 이 핫 스페어를 제거하여 영향을 받는 모든 볼륨 그룹이 표시되며 다른 핫 스페어가 보호 중인 경우 이 그룹이 표시됩니다.

. 지정 해제 작업을 확인합니다.

.결과
드라이브가 할당되지 않음(회색으로 표시됨)으로 돌아갑니다.

```
:leveloffset: -1


= 쉘프 FAQ

:leveloffset: +1


[[ID4ebd53e714d09c171c151fcc5fced19b]]
= 선반 손실 방지 및 서랍 손실 방지란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
쉘프 손실 보호 및 드로어 손실 보호는 단일 쉘프 또는 드로어에 장애가 발생해도 데이터 액세스를 유지할 수 있는 풀 및 볼륨 그룹의 속성입니다.



== 선반 손실 방지

쉘프는 드라이브 또는 드라이브와 컨트롤러를 포함합니다. 쉘프 손실 방지: 단일 드라이브 쉘프로 통신이 두절되는 경우 풀 또는 볼륨 그룹의 볼륨에서 데이터에 액세스할 수 있습니다. 예를 들어, 통신 장애가 발생할 경우 드라이브 쉘프에 대한 전원 공급이 중단되거나 두 I/O 모듈(IOM)이 모두 실패할 수 있습니다.

[NOTE]
====
풀 또는 볼륨 그룹에서 드라이브가 이미 장애가 발생한 경우에는 쉘프 손실 보호가 보장되지 않습니다. 이 경우, 드라이브 쉘프와 풀 또는 볼륨 그룹의 다른 드라이브에 액세스하지 못하면 데이터가 손실됩니다.

====
쉘프 손실 방지 기준은 다음 표에 설명된 보호 방법에 따라 다릅니다.

[cols="1a,1a,1a"]
|===
| 레벨 | 셸프 손실 방지 기준 | 필요한 최소 쉘프 수입니다


 a|
```

수영장
 a|
풀은 5개 이상의 쉘프의 드라이브를 포함해야 하며 각 쉘프에 동일한 수의 드라이브가 있어야 합니다. 셸프 손실 보호는 고용량 셸프에는 적용되지 않습니다. 시스템에 고용량 셸프가 포함되어 있는 경우 문서함 손실 보호 를 참조하십시오.
 a|
5

 a|
RAID 6 를 참조하십시오
 a|
볼륨 그룹은 단일 쉘프에 드라이브를 2개 이상 포함하지 않습니다.
 a|
3

 a|
RAID 3 또는 RAID 5
 a|
볼륨 그룹의 각 드라이브는 별도의 쉘프에 있습니다.
 a|
3

 a|
RAID 1 를 참조하십시오
 a|
RAID 1 쌍의 각 드라이브는 별도의 쉘프에 있어야 합니다.
 a|
2

 a|
RAID 0 를 참조하십시오
 a|
선반 손실 보호를 달성할 수 없습니다.
 a|
해당 없음

|===

== 서랍 손실 방지

드라이브 액세스를 위해 서랍식 용지함은 셸프의 구획 중 하나입니다. 고용량 쉘프에만 서랍이 있습니다. 드로어 손실 보호는 단일 드로어와의 통신이 완전히 손실되는 경우 풀 또는 볼륨 그룹의 볼륨에 있는 데이터에 액세스할 수 있도록 보장합니다. 통신 손실의 예로는 드로어에 대한 전원 손실 또는 드로어 내 내부 구성 요소의 고장이 있습니다.

[NOTE]
====
풀 또는 볼륨 그룹에서 드라이브에 장애가 이미 발생한 경우에는 드로어 손실 보호가 보장되지 않습니다. 이 경우 드로어(풀 또는 볼륨 그룹의 다른 드라이브)에 액세스하지 못하게 되면 데이터가 손실됩니다.

====
드로어 손실 방지 기준은 다음 표에 설명된 보호 방법에 따라 다릅니다.

[cols="1a,1a,1a"]
|===
| 레벨 | 서랍 손실 방지 기준 | 필요한 최소 드로어 수입니다

 a|
수영장
 a|
풀 후보는 모든 드로어의 드라이브를 포함해야 하며 각 드로어에 동일한 수의 드라이브가 있어야 합니다.

풀에는 5개 이상의 서랍에서 나온 드라이브가 포함되어야 하며 각 드로어에 동일한 수의 드라이브가 있어야 합니다.

60-드라이브 쉘프는 15, 20, 25, 30, 35, 40, 45, 50, 55 또는 60개 드라이브. 초기 생성 후 풀에 5의 배수로 증분을 추가할 수 있습니다.
 a|
5

 a|
RAID 6 를 참조하십시오
 a|
볼륨 그룹은 단일 드로어에 2개 이상의 드라이브를 포함하지 않습니다.
 a|
3

 a|

RAID 3 또는 RAID 5
 a|
볼륨 그룹의 각 드라이브는 별도의 드로어에 있습니다.
 a|
3

 a|
RAID 1 를 참조하십시오
 a|
미러링된 쌍의 각 드라이브는 별도의 드로어에 위치해야 합니다.
 a|
2

 a|
RAID 0 를 참조하십시오
 a|
문서함 손실 방지를 달성할 수 없습니다.
 a|
해당 없음

|===

[[ID28a6800489a0d5499edcf9a3c11ea9db]]
= 배터리 학습 사이클이란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
학습 사이클은 스마트 배터리 게이지를 보정하기 위한 자동 사이클입니다.

학습 사이클은 다음과 같은 단계로 구성됩니다.

* 제어된 배터리 방전
* 휴식 기간
* 충전

배터리는 사전 설정된 임계값으로 방전됩니다. 이 단계에서는 배터리 게이지가 보정됩니다.

런 사이클에는 다음 매개변수가 필요합니다.

* 완전히 충전된 배터리
* 과열된 배터리가 없습니다

이중 컨트롤러 시스템에 대한 학습 사이클이 동시에 발생합니다. 두 개 이상의 배터리 또는 배터리 셀 세트에서 백업 전원을 사용하는 컨트롤러의 경우 학습 사이클이 순차적으로 발생합니다.

학습 사이클은 일정한 간격으로, 동시에 같은 요일에 자동으로 시작되도록 예약됩니다. 주기 사이의 간격은 주 단위로 설명됩니다.

[NOTE]
====
학습 사이클을 완료하는 데 몇 시간이 걸릴 수 있습니다.

====

:leveloffset: -1

= 컨트롤러 FAQ

:leveloffset: +1

[[ID30045ac83ae4aa5c77ec136f7cdc7370]]
= 자동 협상이란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
자동 협상은 네트워크 인터페이스가 다른 네트워크 인터페이스와 자체 연결 매개변수(속도 및 이중 모드)를 자동으로 조정하는 기능입니다.

자동 협상은 일반적으로 관리 포트를 구성하는 데 선호되는 설정입니다. 그러나 협상에 실패하면 네트워크 인터페이스 설정이 일치하지 않으면 네트워크 성능에 심각한 영향을 미칠 수 있습니다. 이 상태가 허용되지 않는 경우 네트워크 인터페이스 설정을 올바른 구성으로 수동으로 설정해야 합니다. 자동 협상은 컨트롤러의 이더넷 관리 포트에 의해 수행됩니다. iSCSI 호스트 버스 어댑터가 자동 협상을 수행하지 않습니다.

[NOTE]
====
자동 협상이 실패할 경우 컨트롤러는 최소 공통 분모인 10BASE-T 반이중 모드로 연결을 시도합니다.

====

[[IDfabbdb9fc64920400f505e289d98675e]]
= IPv6 상태 비저장 주소 자동 구성이란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
상태 비저장 자동 구성을 사용하는 경우 호스트는 서버에서 주소 및 기타 구성 정보를 얻지 못합니다.

IPv6의 상태 비저장 자동 구성은 링크 로컬 주소, 멀티캐스팅 및 ND(Neighbor Discovery) 프로토콜을 지원합니다. IPv6는 내부 데이터 링크 계층 주소에서 주소의 인터페이스 ID를 생성할 수 있습니다.

상태 비저장 자동 구성 및 상태 저장 자동 구성은 서로 보완됩니다. 예를 들어, 호스트는 상태 비저장 자동 구성을 사용하여 자체 주소를 구성할 수 있지만 상태 저장 자동 구성을 사용하여 다른 정보를 얻을 수 있습니다. 스테이트풀 자동 구성을 사용하면 호스트가 서버에서 주소 및 기타 구성 정보를 얻을 수 있습니다. 또한 IPv6(인터넷 프로토콜 버전 6)에서는 네트워크의 모든 IP 주소를 한 번에 다시 지정할 수 있는 방법을 정의합니다. IPv6은 서버의 필요 없이 IP 주소 및 기타 매개 변수를 자동으로 구성하는 네트워크 디바이스의 방법을 정의합니다.

상태 비저장 자동 구성을 사용하는 경우 장치는 다음 단계를 수행합니다.

. * 링크 로컬 주소 생성 * -- 장치는 링크 로컬 주소를 생성합니다. 로컬 주소는 10비트이고 그 뒤에 54개의 0이 있으며 그 뒤에 64비트 인터페이스 ID가 붙습니다.
. * 링크-로컬 주소의 고유성 테스트 * -- 노드는 생성하는 링크-로컬 주소가 로컬 네트워크에서 이미 사용되고 있지 않은지 확인하기 위해 테스트합니다. 노드는 ND 프로토콜을 사용하여 인접 요청 메시지를 보냅니다. 이에 따라, 로컬 네트워크는 다른 장치가 이미 링크 로컬 주소를 사용하고 있음을 나타내는 인접 광고 메시지를 수신 대기합니다. 이 경우 새 링크 로컬 주소를 생성하거나 자동 구성에 실패하고 다른 방법을 사용해야 합니다.
. * 링크 로컬 주소 할당 * -- 장치가 고유성 테스트를 통과하면 장치는 해당 IP 인터페이스에 링크 로컬 주소를 할당합니다. 링크 로컬 주소는 인터넷을 통한 통신이 아니라 로컬 네트워크에서의 통신에 사용할 수 있습니다.
. * 라우터 연락처 * -- 노드는 로컬 라우터에 연결을 시도하여 구성을 계속하는 방법에 대한 자세한 정보를 제공합니다. 이 연락처는 공유기가 주기적으로 보내는 라우터 알림 메시지를 듣거나 특정 라우터 요청 메시지를 전송하여 공유기에 수행할 작업에 대한 정보를 요청하는 방식으로

수행됩니다.
. * 노드 방향 제공 * -- 라우터는 자동 구성 진행 방법에 대한 노드의 방향을 제공합니다. 또는 라우터는 호스트에 글로벌 인터넷 주소를 확인하는 방법을 알려줍니다.
. * 글로벌 주소 구성 * -- 호스트는 전역적으로 고유한 인터넷 주소를 사용하여 자체적으로 구성됩니다. 이 주소는 일반적으로 라우터에 의해 호스트에 제공된 네트워크 접두사로 형성됩니다.

[[ID637e270daabda7f950a0c9ef87819d40]]
= DHCP 또는 수동 구성 중 어떤 것을 선택합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
네트워크 구성의 기본 방법은 DHCP(Dynamic Host Configuration Protocol)입니다. 네트워크에 DHCP 서버가 없는 경우 항상 이 옵션을 사용하십시오.

[[ID9988b8bdaa12fb18d74ec3c86deddba4]]
= DHCP 서버란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
DHCP(Dynamic Host Configuration Protocol)는 IP(인터넷 프로토콜) 주소 할당 작업을 자동화하는 프로토콜입니다.

TCP/IP 네트워크에 연결된 각 장치에는 고유한 IP 주소가 할당되어야 합니다. 이러한 장치에는 스토리지 배열의 컨트롤러가 포함됩니다.

DHCP를 사용하지 않으면 네트워크 관리자가 이러한 IP 주소를 수동으로 입력합니다. DHCP를 사용하는 경우 클라이언트가 TCP/IP 작업을 시작해야 할 때 클라이언트는 주소 정보 요청을 브로드캐스트합니다. DHCP 서버는 요청을 받고, 임대 기간이라는 지정된 시간 동안 새 주소를 할당하고, 클라이언트에 주소를 보냅니다. DHCP를 사용하면 장치가 네트워크에 연결될 때마다 다른 IP 주소를 가질 수 있습니다. 일부 시스템에서는 장치가 연결되어 있는 동안에도 장치의 IP 주소가 변경될 수 있습니다.

```
[[IDe62a9436786658fcab6cfc8d947e8667]]
= DHCP 서버를 어떻게 구성합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
스토리지 배열의 컨트롤러에 대해 고정 IP(인터넷 프로토콜) 주소를 사용하려면 DHCP(동적 호스트 구성 프로토콜) 서버를 구성해야 합니다.

DHCP 서버가 할당하는 IP 주소는 일반적으로 동적이며 임대 기간이 만료되므로 변경할 수 있습니다. 서버 및 라우터와 같은 일부 장치는 정적 주소를 사용해야 합니다. 스토리지 어레이의 컨트롤러에도 고정 IP 주소가 필요합니다.

정적 주소를 할당하는 방법에 대한 자세한 내용은 DHCP 서버 설명서를 참조하십시오.



[[ID654813dc7be38161186d0821dae16141]]
= 컨트롤러 네트워크 구성을 변경해야 하는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
대역외 관리를 사용하는 경우 각 컨트롤러의 네트워크 구성(IP(인터넷 프로토콜) 주소, 서브네트워크 마스크(서브넷 마스크) 및 게이트웨이)을 설정해야 합니다.

DHCP(Dynamic Host Configuration Protocol) 서버를 사용하여 네트워크 구성을 설정할 수 있습니다. DHCP 서버를 사용하지 않는 경우 네트워크 구성을 수동으로 입력해야 합니다.



[[IDcb4e6b842c93577c72bdcc84404346c4]]
= 네트워크 구성은 어디에서 얻을 수 있습니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
네트워크 관리자로부터 IP(인터넷 프로토콜) 주소, 서브네트워크 마스크(서브넷 마스크) 및
```

게이트웨이 정보를 얻을 수 있습니다.

컨트롤러에서 포트를 구성할 때 이 정보가 필요합니다.

[[ID1c9124e3292fb63870b99f51aa8dcbc4]]
= ICMP ping 응답이란?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
ICMP(Internet Control Message Protocol)는 TCP/IP 제품군의 프로토콜 중 하나입니다.

`ICMP echo request`및(`ICMP echo reply` 메시지는 일반적으로 메시지라고 `ping` 합니다. `Ping` 는 시스템 관리자가 네트워크 장치 간의 연결을 수동으로 테스트하고 네트워크 지연 및 패킷 손실을 테스트하는 데 사용하는 문제 해결 도구입니다. 이 `ping` 명령은 를 네트워크의 장치로 전송하며 `ICMP echo request`, 장치는 즉시 에 응답합니다(`ICMP echo reply`. 회사의 네트워크 보안 정책을 (`ICMP echo reply`모든 장치에서 비활성화해야 하는 경우도 있습니다. `ping`

[[ID8b5a9bfe324d7bbc0e2f4f1eff95ceeb]]
= DHCP 서버에서 포트 구성 또는 iSNS 서버를 언제 새로 고쳐야 합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
서버를 수정하거나 업그레이드할 때마다 DHCP 서버를 새로 고치고, 현재 스토리지 어레이와 사용할 스토리지 배열에 관련된 DHCP 정보가 변경되었습니다.

특히 DHCP 서버가 다른 주소를 할당할 것이라는 사실을 알고 있을 때 DHCP 서버에서 포트 구성 또는 iSNS 서버를 새로 고칩니다.

[NOTE]
====
포트 구성을 새로 고치면 해당 포트의 모든 iSCSI 연결이 손상될 수 있습니다.

====

[[IDeec3293f4c31b9e43f28548653a4e9f3]]
= 관리 포트를 구성한 후에는 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 어레이의 IP 주소를 변경한 경우 SANtricity Unified Manager에서 글로벌 어레이 보기를 업데이트할 수 있습니다.

Unified Manager에서 글로벌 어레이 보기를 업데이트하려면 인터페이스를 열고 관리 [검색] 메뉴로 이동합니다.

SANtricity 저장소 관리자를 계속 사용하는 경우 EMW(엔터프라이즈 관리 창)로 이동하여 새 IP 주소를 제거하고 다시 추가해야 합니다.

[[ID18983075b513a21ff8df779ec83951a0]]
= 스토리지 시스템이 최적화되지 않은 모드인 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
최적화되지 않은 모드의 스토리지 시스템은 잘못된 시스템 구성 상태로 인해 발생합니다. 이러한 상태에도 불구하고 기존 볼륨에 대한 일반 I/O 액세스는 완벽하게 지원되지만 SANtricity System Manager에서는 일부 작업을 금지합니다.

다음 이유 중 하나로 스토리지 시스템이 잘못된 시스템 구성으로 전환될 수 있습니다.

* 컨트롤러가 규정 준수 범위를 벗어났을 수 있습니다. 이는 잘못된 SMID(Submodel ID) 코드를 가지고 있거나 프리미엄 기능 제한을 초과했기 때문일 수 있습니다.
* 드라이브 펌웨어 다운로드와 같은 내부 서비스 작업이 진행 중입니다.
* 컨트롤러가 패리티 오류 임계값을 초과하고 잠금을 시작했습니다.
* 일반 잠금 조건이 발생했습니다.

```
:leveloffset: -1


= iSCSI FAQ

:leveloffset: +1


[[IDa837f50b994c891cee3af3336b577336]]
= 등록을 위해 iSNS 서버를 사용하면 어떻게 됩니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
iSNS(Internet Storage Name Service) 서버 정보를 사용하는 경우 iSNS 서버를 쿼리하여 타겟(컨트롤러)에서 정보를 검색하도록 호스트(이니시에이터)를 구성할 수 있습니다.

이 등록을 통해 iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하고 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간의 쿼리를 허용합니다.



[[ID758586bd14bd36922595106e10c1f533]]
= iSCSI에 대해 자동으로 지원되는 등록 방법은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
iSCSI 구현에서는 iSNS(Internet Storage Name Service) 검색 방법이나 대상 보내기 명령을 사용할 수 있습니다.

iSNS 방법을 사용하면 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간에 iSNS 검색을 수행할 수 있습니다. iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하기 위해 타겟 컨트롤러를 등록합니다.

iSNS를 구성하지 않으면 iSCSI 호스트가 iSCSI 검색 세션 중에 대상 보내기 명령을 전송할 수 있습니다. 이에 따라 컨트롤러는 포트 정보(예: 대상 IQN, 포트 IP 주소, 수신 포트 및 대상 포트 그룹)를 반환합니다. iSNS를 사용하는 경우 호스트 이니시에이터가 iSNS 서버에서 대상 IP를 검색할 수 있으므로 이 검색 방법은 필요하지 않습니다.
```

```
[[ID406207af0d58af20bd44b5bf94fe304a]]
= InfiniBand 통계를 통해 iSER을 어떻게 해석합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
View iSER over InfiniBand Statistics(InfiniBand를 통한 iSER 통계 보기) 대화
상자에는 로컬 타겟(프로토콜) 통계와 iSER over InfiniBand(IB) 인터페이스 통계가
표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

* * 로컬 타겟(프로토콜) 통계 * -- InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이
통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
* InfiniBand 인터페이스 통계 * 를 통한 * iSER -- InfiniBand 인터페이스의
InfiniBand 포트를 통해 모든 iSER에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된
성능 통계 및 링크 오류 정보가 포함됩니다.


각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후
수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.



[[IDc54299d4d2a27df7294b6938f9c105bd]]
= InfiniBand를 통해 iSER을 구성하거나 진단하려면 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
다음 표에는 InfiniBand 세션을 통해 iSER을 구성 및 관리하는 데 사용할 수 있는
SANtricity 시스템 관리자 기능이 나와 있습니다.

[NOTE]
====
InfiniBand를 통한 iSER 설정은 스토리지 어레이의 컨트롤러에 InfiniBand 호스트 관리
포트를 통한 iSER이 포함된 경우에만 사용할 수 있습니다.

====
[cols="35h,~"]
|===
```

| 조치 | 위치

a|
InfiniBand 포트를 통해 iSER 구성
a|
. 하드웨어 * 를 선택합니다.
. 컨트롤러 및 구성 요소 * 탭을 선택합니다.
. 컨트롤러를 선택합니다.
. InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.

또는

. 설정 [시스템] 메뉴를 선택합니다.
. InfiniBand 설정을 통해 * iSER * 로 스크롤한 다음 * InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.

a|
InfiniBand 통계를 통해 iSER 보기
a|
. 설정 [시스템] 메뉴를 선택합니다.
. InfiniBand 설정 * 을 통해 * iSER로 스크롤한 다음 * InfiniBand 통계 * 를 통해 iSER 보기 * 를 선택합니다.

|===

[[ID48935ce11164f9f17a2a6029bdfc0269]]
= iSCSI를 구성하거나 진단하려면 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
iSCSI 세션은 비동기 미러 관계의 호스트 또는 원격 스토리지 시스템에서 발생할 수 있습니다. 다음 표에는 이러한 iSCSI 세션을 구성하고 관리하는 데 사용할 수 있는 SANtricity 시스템 관리자 기능이 나열되어 있습니다.

[NOTE]
====
iSCSI 설정은 스토리지 배열이 iSCSI를 지원하는 경우에만 사용할 수 있습니다.

====

== iSCSI를 구성합니다

[cols="1a,1a"]
|===
| 조치 | 위치

 a|
iSCSI 설정을 관리합니다
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. 모든 관리 기능을 보려면 * iSCSI 설정 * 으로 스크롤합니다.

 a|
iSCSI 포트를 구성합니다
 a|
. 하드웨어 * 를 선택합니다.
. 컨트롤러 및 구성 요소 * 탭을 선택합니다.
. 컨트롤러를 선택합니다.
. iSCSI 포트 구성 * 을 선택합니다.

 a|
호스트 CHAP 암호를 설정합니다
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 설정 * 으로 스크롤한 다음 * 인증 구성 * 을 선택합니다.

또는

. 스토리지 [호스트] 메뉴를 선택합니다.
. 호스트 구성원을 선택합니다.
. 메뉴: 설정 보기/편집 [호스트 포트] 탭을 클릭합니다.

```
|===


== iSCSI를 진단합니다

[cols="1a,1a"]
|===
| 조치 | 위치


 a|
iSCSI 세션을 보거나 종료합니다
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 설정 * 으로 스크롤한 다음 * iSCSI 세션 보기/종료 * 를 선택합니다.


또는

. 지원 [지원 센터 > 진단] 탭을 선택합니다.
. iSCSI 세션 보기/종료 * 를 선택합니다.




 a|
iSCSI 통계를 봅니다
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. iSCSI 설정 * 으로 스크롤한 다음 * iSCSI 통계 패키지 보기 * 를 선택합니다.


또는

. 지원 [지원 센터 > 진단] 탭을 선택합니다.
. iSCSI 통계 패키지 보기 * 를 선택합니다.


|===



:leveloffset: -1


= NVMe FAQ를 참조하십시오
```

```
:leveloffset: +1


[[ID128636ece7837b4f811c67832af903c8]]
= NVMe over Fabrics 통계를 어떻게 해석합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
NVMe over Fabrics 통계 보기 대화 상자에는 NVMe 하위 시스템과 RDMA 인터페이스에 대한 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

* * NVMe 하위 시스템 통계 * -- NVMe 컨트롤러 및 해당 대기열에 대한 통계를 표시합니다. NVMe 컨트롤러는 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 연결 실패, 재설정 및 종료 같은 항목에 대한 NVMe 하위 시스템 통계를 검토할 수 있습니다. 이러한 통계에 대한 자세한 내용을 보려면 * 표 제목에 대한 범례 보기 * 를 클릭하십시오.
* RDMA 인터페이스 통계 * -- RDMA 인터페이스의 모든 NVMe over Fabrics 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트에 연결된 성능 통계 및 링크 오류 정보가 포함됩니다. 이 탭은 NVMe over Fabrics 포트를 사용할 수 있을 때만 나타납니다. 통계에 대한 자세한 내용을 보려면 * 표 제목에 대한 범례 보기 * 를 클릭합니다.


각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.



[[IDe5b5325104f64205b224f71256b6d14a]]
= InfiniBand를 통해 NVMe를 구성하거나 진단하려면 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
다음 표에는 InfiniBand 세션을 구성하고 관리하는 데 사용할 수 있는 SANtricity System Manager 기능이 나열되어 있습니다.

[NOTE]
====
NVMe over InfiniBand 설정은 스토리지 어레이 컨트롤러에 NVMe over InfiniBand 포트가
```

포함된 경우에만 사용할 수 있습니다.

====
[cols="35h,~"]
|===
| 조치 | 위치

 a|
InfiniBand 포트를 통해 NVMe를 구성합니다
 a|
. 하드웨어 * 를 선택합니다.
. 컨트롤러 및 구성 요소 * 탭을 선택합니다.
. 컨트롤러를 선택합니다.
. Configure NVMe over InfiniBand ports * 를 선택합니다.

또는

. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 스크롤하여 * NVMe over InfiniBand settings * 로 이동한 다음 * Configure NVMe over InfiniBand Ports * 를 선택합니다.

 a|
InfiniBand를 통한 NVMe 통계 보기
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 스크롤하여 * NVMe over InfiniBand settings * 를 선택한 다음 * View NVMe over Fabrics Statistics * 를 선택합니다.

|===

[[ID763154e9287febbe3666286287928f5f]]
= NVMe over RoCE를 구성 또는 진단하려면 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
하드웨어 및 설정 페이지에서 NVMe over RoCE를 구성 및 관리할 수 있습니다.

[NOTE]
====
NVMe over RoCE 설정은 스토리지 어레이의 컨트롤러에 NVMe over RoCE 포트가 포함된 경우에만 사용할 수 있습니다.

====
[cols="35h,~"]
|===
| 조치 | 위치

 a|
NVMe over RoCE 포트를 구성합니다
 a|
. 하드웨어 * 를 선택합니다.
. 컨트롤러 및 구성 요소 * 탭을 선택합니다.
. 컨트롤러를 선택합니다.
. RoCE 포트를 통한 NVMe 구성 * 을 선택합니다.

또는

. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 * NVMe over RoCE 설정 * 으로 스크롤한 다음 * Configure NVMe over RoCE Ports * 를 선택합니다.

 a|
NVMe over Fabrics 통계 보기
 a|
. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 * NVMe over RoCE 설정 * 으로 스크롤한 다음 * NVMe over Fabrics 통계 보기 * 를 선택합니다.

|===

[[ID5d5f07ec8a5de428c9104ce80cbe318c]]
= 하나의 물리적 포트에 대해 두 개의 IP 주소가 있는 이유는 무엇입니까?
:allow-uri-read:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
EF600 스토리지 어레이에는 2개의 HIC, 즉 외부 스토리지와 내부 HIC를 각각 하나씩 포함할 수 있습니다.

이 구성에서는 외부 HIC를 내부 보조 HIC에 연결합니다. 외부 HIC에서 액세스할 수 있는 각 물리적 포트에는 내부 HIC에서 연결된 가상 포트가 있습니다.

최대 200GB 성능을 얻으려면 호스트가 각 포트에 연결을 설정할 수 있도록 물리적 포트와 가상 포트 모두에 대해 고유한 IP 주소를 할당해야 합니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.



[[ID74202d651e1171ef553102b5bcb0b485]]
= 물리적 포트 하나에 대해 두 개의 매개 변수 세트가 있는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
EF600 스토리지 어레이에는 2개의 HIC, 즉 외부 스토리지와 내부 HIC를 각각 하나씩 포함할 수 있습니다.

이 구성에서는 외부 HIC를 내부 보조 HIC에 연결합니다. 외부 HIC에서 액세스할 수 있는 각 물리적 포트에는 내부 HIC에서 연결된 가상 포트가 있습니다.

최대 200GB 성능을 얻으려면 호스트가 각 포트에 대한 연결을 설정할 수 있도록 물리적 포트와 가상 포트 모두에 대해 매개 변수를 할당해야 합니다. 가상 포트에 매개 변수를 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.



:leveloffset: -1


= 드라이브 FAQ

:leveloffset: +1
```

[[ID072bef0f5403acd8b1abfc3cddbfe9a4]]
= 핫 스페어 드라이브란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
핫 스페어는 RAID 1, RAID 5 또는 RAID 6 볼륨 그룹의 대기 드라이브 역할을 합니다. 데이터가 없는 완전한 기능을 갖춘 드라이브입니다. 볼륨 그룹에서 드라이브에 장애가 발생하면 컨트롤러는 장애가 발생한 드라이브에서 핫 스페어로 데이터를 자동으로 재구성합니다.

스토리지 배열의 드라이브에 오류가 발생하면 물리 스왑 없이 핫 스페어 드라이브가 장애가 발생한 드라이브로 자동 대체됩니다. 드라이브에 오류가 발생할 때 핫 스페어 드라이브를 사용할 수 있는 경우 컨트롤러는 중복 데이터를 사용하여 오류가 발생한 드라이브에서 핫 스페어 드라이브로 데이터를 재구성합니다.

핫 스페어 드라이브는 특정 볼륨 그룹 전용이 아닙니다. 대신 용량이 같거나 더 작은 스토리지 배열의 모든 장애 드라이브에 핫 스페어 드라이브를 사용할 수 있습니다. 핫 스페어 드라이브는 보호 드라이브와 동일한 미디어 유형(HDD 또는 SSD)이어야 합니다.

[NOTE]
====
핫 스페어 드라이브는 풀에서 지원되지 않습니다. 풀은 핫 스페어 드라이브 대신 풀을 구성하는 각 드라이브 내의 보존 용량을 사용합니다.

====

[[ID0e3e725b088c643464e2c3cb1137d66b]]
= 보존 용량이란?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Preservation capacity는 잠재적 드라이브 장애를 지원하기 위해 풀에 예약된 용량(드라이브 수)입니다.

풀이 생성되면 시스템은 풀의 드라이브 수에 따라 기본 보존 용량을 자동으로 예약합니다.

풀은 재구성 중에 보존 용량을 사용하지만 볼륨 그룹은 동일한 목적으로 핫 스페어 드라이브를 사용합니다. 보존 용량 방법은 재구성을 더 빠르게 수행할 수 있도록 핫 스페어 드라이브에 비해

향상된 기능입니다. 보존 용량은 핫 스페어 드라이브의 경우 드라이브 하나가 아닌 풀의 여러 드라이브에 분산되므로 드라이브 한 개의 속도나 가용성에 의해 제한되지 않습니다.

[[ID5fee99126b2ea6ea8c78e448bb6d616b]]
= 드라이브를 논리적으로 교체하는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
드라이브에 장애가 발생하거나 다른 이유로 드라이브를 교체하고 스토리지 어레이에 할당되지 않은 드라이브가 있는 경우, 장애가 발생한 드라이브를 할당되지 않은 드라이브로 논리적으로 교체할 수 있습니다. 할당되지 않은 드라이브가 없는 경우 드라이브를 물리적으로 교체할 수 있습니다.

원래 드라이브의 데이터는 교체 드라이브에 복사 또는 재구성됩니다.

[[IDbcf4de8abe3a15f4574079ecd7b90b5d]]
= 재구성 중인 드라이브의 상태는 어디에서 확인할 수 있습니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-hardware/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Operations In Progress 대시보드에서 드라이브 재구성 상태를 볼 수 있습니다.

홈 페이지에서 오른쪽 상단의 * View Operations in Progress * 링크를 클릭합니다.

드라이브에 따라 전체 재구성에 상당한 시간이 걸릴 수 있습니다. 볼륨 소유권이 변경된 경우 신속한 재구성 대신 전체 재구성이 이루어질 수 있습니다.

:leveloffset: -1

:leveloffset: -1

= 경고

```
:leveloffset: +1


[[ID3752650a2d10b12cb5e1b4db5213d660]]
= 경고 개요
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
이메일, SNMP 트랩 및 syslog 메시지를 통해 스토리지 어레이에 대한 경고를 보내도록
SANtricity 시스템 관리자를 구성할 수 있습니다.



== 알림이란 무엇입니까?

_Alerts_ 스토리지 시스템에서 발생하는 중요한 이벤트를 관리자에게 알립니다. 이벤트에는 배터리
장애, 최적화에서 오프라인으로 이동하는 구성 요소 또는 컨트롤러의 중복 오류와 같은 문제가
포함될 수 있습니다. 모든 중요 이벤트는 일부 경고 및 정보 이벤트와 함께 "alertable"으로
간주됩니다.

자세한 내용:

* xref:{relative_path}how-alerts-work.html["알림의 작동 방식"]
* xref:{relative_path}alerts-terminology.html["경고 용어"]




== 알림을 구성하려면 어떻게 합니까?

경고를 하나 이상의 e-메일 주소로 보내거나, SNMP 서버에 대한 SNMP 트랩으로 보내거나,
syslog 서버에 메시지로 보내도록 구성할 수 있습니다. 경고 구성은 설정 [경고] 메뉴에서 사용할
수 있습니다.

자세한 내용:

* xref:{relative_path}configure-mail-server-and-recipients-for-
alerts.html["메일 서버 및 받는 사람이 알림을 받도록 구성합니다"]
* xref:{relative_path}configure-syslog-server-for-alerts.html["경고에 대한
syslog 서버를 구성합니다"]
* xref:{relative_path}configure-snmp-alerts.html["SNMP 경고를 구성합니다"]
```

== 관련 정보

경고와 관련된 개념에 대해 자세히 알아보기:

* xref:{relative_path}../sm-support/overview-event-log.html["이벤트 로그 개요"]
* xref:{relative_path}why-are-timestamps-inconsistent-between-the-array-and-alerts.html["시간 스탬프가 일치하지 않습니다"]

= 개념

:leveloffset: +1

[[IDca1911bca8abc0c0bfeeedb9cc690c3e]]
= 알림의 작동 방식
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
알림은 스토리지 시스템에서 발생하는 중요한 이벤트를 관리자에게 알립니다. 알림은 이메일, SNMP 트랩 및 syslog를 통해 보낼 수 있습니다.

알림 프로세스는 다음과 같이 작동합니다.

. 관리자는 System Manager에서 다음 경고 방법 중 하나 이상을 구성합니다.
+
** * 이메일 * -- 메시지가 이메일 주소로 전송됩니다.
** SNMP * -- SNMP 트랩이 SNMP 서버로 전송됩니다.
** * Syslog * -- 메시지가 syslog 서버로 전송됩니다.

. 스토리지 배열의 이벤트 모니터에서 문제를 감지하면 해당 문제에 대한 정보를 이벤트 로그에 기록합니다(메뉴: 지원 [이벤트 로그]). 예를 들어, 배터리 오류, 최적화에서 오프라인으로 이동하는 구성 요소 또는 컨트롤러의 중복 오류와 같은 이벤트가 문제에 포함될 수 있습니다.
. 이벤트 모니터에서 이벤트가 "alertable"이라고 판단하면 구성된 경고 방법(e-메일, SNMP

및/또는 syslog)을 사용하여 알림을 보냅니다. 모든 중요 이벤트는 일부 경고 및 정보 이벤트와 함께 "alertable"으로 간주됩니다.

== 알림 구성

초기 설정 마법사(e-메일 알림만 해당) 또는 경고 페이지에서 경고를 구성할 수 있습니다. 현재 구성을 확인하려면 설정 [경고] 메뉴로 이동하십시오.

경고 타일에는 다음 중 하나에 해당하는 경고 구성이 표시됩니다.

* 구성되지 않았습니다.
* 구성됨. 하나 이상의 경고 방법이 설정되었습니다. 구성된 경고 방법을 확인하려면 커서를 바둑판식으로 가져갑니다.

== 경고 정보

알림에는 다음과 같은 유형의 정보가 포함될 수 있습니다.

* 스토리지 배열의 이름입니다.
* 이벤트 로그 엔트리와 관련된 이벤트 오류 유형입니다.
* 이벤트가 발생한 날짜 및 시간입니다.
* 이벤트에 대한 간략한 설명입니다.

[NOTE]
====
Syslog 알림은 RFC 5424 메시징 표준을 따릅니다.

====

[[ID3b4603ab891a321080a611ec3f158a5c]]
= 경고 용어
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

알림 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

[cols="25h,~"]
|===
| 구성 요소 | 설명

a|
이벤트 모니터
a|
이벤트 모니터는 스토리지 시스템에 상주하며 백그라운드 작업으로 실행됩니다. 이벤트 모니터에서 스토리지 배열의 이상 징후를 감지하면 해당 문제에 대한 정보를 이벤트 로그에 기록합니다. 배터리 오류, 최적화에서 오프라인으로 이동하는 구성 요소 또는 컨트롤러의 중복 오류와 같은 문제가 포함될 수 있습니다. 이벤트 모니터에서 이벤트가 "alertable"이라고 판단하면 구성된 경고 방법(e-메일, SNMP 및/또는 syslog)을 사용하여 알림을 보냅니다. 모든 중요 이벤트는 일부 경고 및 정보 이벤트와 함께 "alertable"으로 간주됩니다.

a|
메일 서버
a|
메일 서버는 이메일 경고를 보내고 받는 데 사용됩니다. 서버는 SMTP(Simple Mail Transfer Protocol)를 사용합니다.

a|
SNMP를 선택합니다
a|
SNMP(Simple Network Management Protocol)는 IP 네트워크의 장치 간에 정보를 관리 및 공유하는 데 사용되는 인터넷 표준 프로토콜입니다.

a|
SNMP 트랩
a|
SNMP 트랩은 SNMP 서버로 전송되는 알림입니다. 트랩에는 스토리지 배열 관련 주요 문제에 대한 정보가 포함되어 있습니다.

a|
SNMP 트랩 대상입니다
a|
SNMP 트랩 대상은 SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소입니다.

```
 a|
커뮤니티 이름입니다
 a|
커뮤니티 이름은 SNMP 환경에서 네트워크 서버의 암호 역할을 하는 문자열입니다.



 a|
MIB 파일
 a|
MIB(Management Information Base) 파일은 스토리지 어레이에서 모니터링 및 관리되는
데이터를 정의합니다. SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일해야
합니다. 이 MIB 파일은 지원 사이트의 System Manager 소프트웨어와 함께 사용할 수 있습니다.



 a|
MIB 변수
 a|
MIB(Management Information Base) 변수는 스토리지 배열 이름, 배열 위치 및 SNMP
GetRequests에 대한 응답으로 연락 담당자 등의 값을 반환할 수 있습니다.



 a|
Syslog를 클릭합니다
 a|
Syslog는 네트워크 장치가 로깅 서버에 이벤트 메시지를 보내는 데 사용하는 프로토콜입니다.



 a|
UDP입니다
 a|
UDP(User Datagram Protocol)는 패킷 헤더에서 소스 및 대상 포트 번호를 지정하는 전송
계층 프로토콜입니다.

|===



:leveloffset: -1
```

```
= 이메일 알림을 관리합니다

:leveloffset: +1


[[ID54f706f62d9d3043f5723c6eca2676c8]]
= 메일 서버 및 받는 사람이 알림을 받도록 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
전자 메일 알림을 구성하려면 메일 서버 주소와 경고 받는 사람의 전자 메일 주소를 지정해야 합니다. 최대 20개의 이메일 주소가 허용됩니다.

.시작하기 전에
* 메일 서버의 주소를 사용할 수 있어야 합니다. 주소는 IPv4 또는 IPv6 주소이거나 정규화된 도메인 이름일 수 있습니다.
+
[NOTE]
====
정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

====
* 알림 발송자로 사용할 이메일 주소를 사용할 수 있어야 합니다. 경고 메시지의 "보낸 사람" 필드에 나타나는 주소입니다. SMTP 프로토콜에 보낸 사람 주소가 필요합니다. 이 주소가 없으면 오류 결과가 발생합니다.
* 알림 수신자의 이메일 주소를 사용할 수 있어야 합니다. 받는 사람은 일반적으로 네트워크 관리자 또는 스토리지 관리자의 주소입니다. 최대 20개의 이메일 주소를 입력할 수 있습니다.


.이 작업에 대해
이 작업은 메일 서버를 구성하고, 보낸 사람과 받는 사람의 전자 메일 주소를 입력하고, 경고 페이지에서 입력한 모든 전자 메일 주소를 테스트하는 방법을 설명합니다.

[NOTE]
====
초기 설정 마법사에서 이메일 알림을 구성할 수도 있습니다.

====
.단계
. 설정 [알림] 메뉴를 선택합니다.
. 이메일 * 탭을 선택합니다.
```

+
이메일 서버가 아직 구성되지 않은 경우 이메일 탭에 "메일 서버 구성"이 표시됩니다.

. 메일 서버 구성 * 을 선택합니다.
+
메일 서버 구성 대화 상자가 열립니다.

. 메일 서버 정보를 입력한 다음 * 저장 * 을 클릭합니다.
+
** * 메일 서버 주소 * -- 메일 서버의 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
+
[NOTE]
====
정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

====
** * 이메일 발신자 주소 * -- 이메일 발신자로 사용할 유효한 이메일 주소를 입력합니다. 이 주소는 전자 메일 메시지의 "보낸 사람" 필드에 나타납니다.
** * 암호화 * -- 메시지를 암호화하려면 암호화 유형으로 * SMTPS * 또는 * STARTTLS * 를 선택한 다음 암호화된 메시지의 포트 번호를 선택합니다. 그렇지 않으면 * 없음 * 을 선택합니다.
** * 사용자 이름 및 암호 * -- 필요한 경우 보내는 보낸 사람 및 메일 서버와 함께 인증을 위한 사용자 이름과 암호를 입력합니다.
** * 전자 메일에 연락처 정보 포함 * -- 경고 메시지에 보낸 사람의 연락처 정보를 포함하려면 이 옵션을 선택한 다음 이름과 전화 번호를 입력합니다.
+
저장 * 을 클릭하면 이메일 주소가 경고 페이지의 이메일 탭에 나타납니다.

. 이메일 추가 * 를 선택합니다.
+
이메일 추가 대화 상자가 열립니다.

. 경고 수신자에 대한 이메일 주소를 하나 이상 입력한 다음 * 추가 * 를 클릭합니다.
+
이메일 주소는 경고 페이지에 나타납니다.

. 이메일 주소가 유효한지 확인하려면 * Test all email * 을 클릭하여 수신자에게 테스트 메시지를 보냅니다.

.결과
e-메일 알림을 구성한 후 이벤트 모니터는 alertable 이벤트가 발생할 때마다 지정된 수신자에게 e-메일 메시지를 보냅니다.

```
[[ID415ab5e2925dc5b18c1fdd9a07467474]]
= 알림에 대한 이메일 주소를 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
전자 메일 알림을 받는 사람의 전자 메일 주소를 변경할 수 있습니다.

.시작하기 전에
편집하려는 이메일 주소는 경고 페이지의 이메일 탭에서 정의해야 합니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. 이메일 * 탭을 선택합니다.
. [전자 메일 주소] * 테이블에서 변경할 주소를 선택한 다음 맨 오른쪽에 있는 * 편집 * (연필) 아이콘을 클릭합니다.
+
행이 편집 가능한 필드가 됩니다.

. 새 주소를 입력한 다음 * 저장 * (확인 표시) 아이콘을 클릭합니다.
+
[NOTE]
====
변경 사항을 취소하려면 * Cancel * (X) 아이콘을 선택합니다.

====


.결과
경고 페이지의 이메일 탭에는 업데이트된 이메일 주소가 표시됩니다.



[[ID38d86b90dc9e64adaf844e8fe1e5b669]]
= 알림에 대한 이메일 주소를 추가합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
최대 20명의 전자 메일 알림을 받는 사람을 추가할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. 이메일 * 탭을 선택합니다.
. 이메일 추가 * 를 선택합니다.
+
이메일 추가 대화 상자가 열립니다.

. 빈 필드에 새 이메일 주소를 입력합니다. 둘 이상의 주소를 추가하려면 * 다른 이메일 추가 * 를 선택하여 다른 필드를 엽니다.
. 추가 * 를 클릭합니다.

.결과
경고 페이지의 이메일 탭에는 새 이메일 주소가 표시됩니다.

[[ID5aca92c3f9348a6ef3eea36b2cf2bd44]]
= 알림에 대한 메일 서버 또는 이메일 주소를 삭제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 정의한 메일 서버를 제거하여 알림이 더 이상 이메일 주소로 전송되지 않도록 하거나 개별 이메일 주소를 제거할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. 이메일 * 탭을 선택합니다.
. 테이블에서 다음 중 하나를 수행합니다.
+
** 알림이 더 이상 전자 메일 주소로 전송되지 않도록 메일 서버를 제거하려면 메일 서버의 행을 선택합니다.
** 알림이 더 이상 이 주소로 전송되지 않도록 전자 메일 주소를 제거하려면 삭제할 전자 메일 주소의 행을 선택합니다. 테이블 오른쪽 위에 있는 * Delete * (삭제 *) 버튼을 선택할 수 있습니다.

. 삭제 * 를 클릭하고 작업을 확인합니다.

```
[[ID03f57f852eb41fef8ba0931608b7acb3]]
= 알림에 대한 메일 서버를 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
전자 메일 알림에 사용되는 메일 서버 주소 및 전자 메일 보낸 사람 주소를 변경할 수 있습니다.

.시작하기 전에
변경하고 있는 메일 서버의 주소를 사용할 수 있어야 합니다. 주소는 IPv4 또는 IPv6 주소이거나 정규화된 도메인 이름일 수 있습니다.

[NOTE]
====
정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

====
.단계
. 설정 [알림] 메뉴를 선택합니다.
. 이메일 * 탭을 선택합니다.
. 메일 서버 구성 * 을 선택합니다.
+
메일 서버 구성 대화 상자가 열립니다.

. 메일 서버 주소, 보낸 사람 정보 및 연락처 정보를 편집합니다.
+
** * 메일 서버 주소 * -- 메일 서버의 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 편집합니다.
+
[NOTE]
====
정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

====
** e-메일 보낸 사람 주소 * -- e-메일을 보낸 사람으로 사용할 e-메일 주소를 편집합니다. 이 주소는 전자 메일 메시지의 "보낸 사람" 필드에 나타납니다.
** * 전자 메일에 연락처 정보 포함 * -- 보낸 사람의 연락처 정보를 편집하려면 이 옵션을
```

선택한 다음 이름과 전화 번호를 편집합니다.

. 저장 * 을 클릭합니다.

:leveloffset: -1

= SNMP 경고를 관리합니다

:leveloffset: +1

[[ID70c31b2f0f6e488f8b144f6212b7e855]]
= SNMP 경고를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMP(Simple Network Management Protocol) 경고를 구성하려면 스토리지 배열의 이벤트 모니터에서 SNMP 트랩을 보낼 수 있는 서버를 하나 이상 식별해야 합니다. 이 구성에는 커뮤니티 이름 또는 사용자 이름과 서버의 IP 주소가 필요합니다.

.시작하기 전에
* 네트워크 서버는 SNMP 서비스 애플리케이션으로 구성되어야 합니다. 이벤트 모니터가 해당 주소로 트랩 메시지를 보낼 수 있도록 이 서버의 네트워크 주소(IPv4 또는 IPv6 주소)가 필요합니다. 둘 이상의 서버를 사용할 수 있습니다(최대 10대의 서버가 허용됨).
* MIB(Management Information Base) 파일이 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일되었습니다. 이 MIB 파일은 모니터링 및 관리되는 데이터를 정의합니다.
+
MIB 파일이 없는 경우 NetApp Support 사이트에서 얻을 수 있습니다.

+
** 로 이동합니다. https://mysupport.netapp.com/site/global/dashboard["NetApp 지원"^]
** Downloads * 탭을 클릭한 다음 * Downloads * 를 선택합니다.
** E-Series SANtricity OS 컨트롤러 소프트웨어 * 를 클릭합니다.
** 최신 릴리스 다운로드 * 를 선택합니다.
** 로그인합니다.
** 주의 사항 및 라이센스 계약에 동의합니다.

** 컨트롤러 유형에 대한 MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을 다운로드합니다.

.이 작업에 대해
이 작업에서는 트랩 대상에 대한 SNMP 서버를 식별하고 구성을 테스트하는 방법을 설명합니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
처음 설정할 때 SNMP 탭에 "커뮤니티/사용자 구성"이 표시됩니다.

. 커뮤니티/사용자 구성 * 을 선택합니다.
+
SNMP 버전 선택 대화 상자가 열립니다.

. 경고에 대한 SNMP 버전을 선택합니다. * SNMPv2c * 또는 * SNMPv3 *.
+
선택한 항목에 따라 커뮤니티 구성 대화 상자 또는 SNMPv3 사용자 구성 대화 상자가 열립니다.

. SNMPv2c(커뮤니티) 또는 SNMPv3(사용자)에 대한 적절한 지침을 따릅니다.
+
** * SNMPv2c(커뮤니티) * -- 커뮤니티 구성 대화 상자에서 네트워크 서버에 대한 커뮤니티 문자열을 하나 이상 입력합니다. 커뮤니티 이름은 알려진 관리 스테이션 집합을 식별하는 문자열이며 일반적으로 네트워크 관리자가 만듭니다. 인쇄 가능한 ASCII 문자만 포함됩니다. 최대 256개의 커뮤니티를 추가할 수 있습니다. 완료되면 * Save * 를 클릭합니다.
** * SNMPv3(사용자) * -- SNMPv3 사용자 구성 대화 상자에서 * 추가 * 를 클릭한 후 다음 정보를 입력합니다.
+
*** * 사용자 이름 * -- 사용자를 식별할 이름을 입력합니다. 최대 31자까지 입력할 수 있습니다.
*** * 엔진 ID * -- 메시지에 대한 인증 및 암호화 키를 생성하는 데 사용되는 엔진 ID를 선택합니다. 이 ID는 관리 도메인에서 고유해야 합니다. 대부분의 경우 * Local * 을 선택해야 합니다. 비표준 구성이 있는 경우 * 사용자 정의 * 를 선택합니다. 다른 필드는 신뢰할 수 있는 엔진 ID를 10자에서 32자 사이의 짝수 문자로 16진수 문자열로 입력해야 하는 위치에 나타납니다.
*** * 인증 자격 증명 * -- 사용자 ID를 보장하는 인증 프로토콜을 선택합니다. 그런 다음 인증 프로토콜을 설정하거나 변경할 때 필요한 인증 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다.
*** * 개인 정보 보호 자격 증명 * -- 메시지의 내용을 암호화하는 데 사용되는 개인 정보 보호 프로토콜을 선택합니다. 그런 다음 개인 정보 보호 프로토콜을 설정하거나 변경할 때 필요한 개인 정보 보호 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다. 완료되면 * 추가 * 를 클릭한 다음 * 닫기 * 를 클릭합니다.

. SNMP 탭이 선택된 경고 페이지에서 * 트랩 대상 추가 * 를 클릭합니다.
+
트랩 대상 추가 대화 상자가 열립니다.

. 하나 이상의 트랩 대상을 입력하고 관련 커뮤니티 이름 또는 사용자 이름을 선택한 다음 * 추가 * 를 클릭합니다.
+
** * 트랩 대상 * -- SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소를 입력합니다.
** * 커뮤니티 이름 또는 사용자 이름 * -- 드롭다운에서 이 트랩 대상에 대한 커뮤니티 이름(SNMPv2c) 또는 사용자 이름(SNMPv3)을 선택합니다. (하나만 정의한 경우 이 필드에 이름이 이미 나타납니다.)
** * 인증 실패 트랩 전송 * -- 인식되지 않는 커뮤니티 이름 또는 사용자 이름으로 인해 SNMP 요청이 거부될 때마다 트랩 대상에 알리려면 이 옵션(확인란)을 선택합니다. 추가 * 를 클릭하면 * 알림 * 페이지의 * SNMP * 탭에 트랩 대상 및 관련 이름이 나타납니다.

. 트랩이 유효한지 확인하려면 표에서 트랩 대상을 선택한 다음 * Test Trap Destination * 을 클릭하여 구성된 주소로 테스트 트랩을 보냅니다.

.결과
이벤트 모니터는 alertable 이벤트가 발생할 때마다 SNMP 트랩을 서버로 전송합니다.

[[IDafb10767d1e362a92c3e5152fe4d495c]]
= SNMP 경고에 대한 트랩 대상을 추가합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMP 트랩을 보내기 위해 최대 10대의 서버를 추가할 수 있습니다.

.시작하기 전에
* 추가하려는 네트워크 서버는 SNMP 서비스 애플리케이션으로 구성되어야 합니다. 이벤트 모니터가 해당 주소로 트랩 메시지를 보낼 수 있도록 이 서버의 네트워크 주소(IPv4 또는 IPv6 주소)가 필요합니다. 둘 이상의 서버를 사용할 수 있습니다(최대 10대의 서버가 허용됨).
* MIB(Management Information Base) 파일이 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일되었습니다. 이 MIB 파일은 모니터링 및 관리되는 데이터를 정의합니다.
+
MIB 파일이 없는 경우 NetApp Support 사이트에서 얻을 수 있습니다.

+
** 로 이동합니다. https://mysupport.netapp.com/site/global/dashboard["NetApp 지원"^]
** Downloads * 를 클릭한 다음 * Downloads * 를 선택합니다.
** E-Series SANtricity OS 컨트롤러 소프트웨어 * 를 클릭합니다.
** 최신 릴리스 다운로드 * 를 선택합니다.
** 로그인합니다.
** 주의 사항 및 라이센스 계약에 동의합니다.
** 컨트롤러 유형에 대한 MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을 다운로드합니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
현재 정의된 트랩 대상이 테이블에 나타납니다.

. Add Trap Desations * 를 선택합니다.
+
트랩 대상 추가 대화 상자가 열립니다.

. 하나 이상의 트랩 대상을 입력하고 관련 커뮤니티 이름 또는 사용자 이름을 선택한 다음 * 추가 * 를 클릭합니다.
+
** * 트랩 대상 * -- SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소를 입력합니다.
** * 커뮤니티 이름 또는 사용자 이름 * -- 드롭다운에서 이 트랩 대상에 대한 커뮤니티 이름(SNMPv2c) 또는 사용자 이름(SNMPv3)을 선택합니다. (하나만 정의한 경우 이 필드에 이름이 이미 나타납니다.)
** * 인증 실패 트랩 전송 * -- 인식되지 않는 커뮤니티 이름 또는 사용자 이름으로 인해 SNMP 요청이 거부될 때마다 트랩 대상에 알리려면 이 옵션(확인란)을 선택합니다. 추가 * 를 클릭하면 트랩 대상 및 관련 커뮤니티 이름 또는 사용자 이름이 테이블에 나타납니다.

. 트랩이 유효한지 확인하려면 표에서 트랩 대상을 선택한 다음 * Test Trap Destination * 을 클릭하여 구성된 주소로 테스트 트랩을 보냅니다.

.결과
이벤트 모니터는 alertable 이벤트가 발생할 때마다 SNMP 트랩을 서버로 전송합니다.

[[ID3e95cd04bd70380b84c5ea8c2fb1680d]]

```
= SNMP MIB 변수를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SNMP 알림의 경우 SNMP 트랩에 나타나는 MIB(Management Information Base) 변수를
선택적으로 구성할 수 있습니다. 이러한 변수는 스토리지 배열 이름, 배열 위치 및 담당자를
반환할 수 있습니다.

.시작하기 전에
MIB 파일은 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일해야 합니다.

MIB 파일이 없는 경우 다음과 같이 얻을 수 있습니다.

* 로 이동합니다. https://mysupport.netapp.com/site/global/dashboard["NetApp
지원"^]
* Downloads * 를 클릭한 다음 * Downloads * 를 선택합니다.
* E-Series SANtricity OS 컨트롤러 소프트웨어 * 를 클릭합니다.
* 최신 릴리스 다운로드 * 를 선택합니다.
* 로그인합니다.
* 주의 사항 및 라이센스 계약에 동의합니다.
* 컨트롤러 유형에 대한 MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을
다운로드합니다.


.이 작업에 대해
이 작업에서는 SNMP 트랩에 대한 MIB 변수를 정의하는 방법에 대해 설명합니다. 이러한 변수는
SNMP GetRequests에 응답하여 다음 값을 반환할 수 있습니다.

* `sysName` (스토리지 배열 이름)
* `sysLocation` (스토리지 어레이의 위치)
* `sysContact` (관리자 이름)


.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
. SNMP MIB 변수 구성 * 을 선택합니다.
+
Configure SNMP MIB Variables(SNMP MIB 변수 구성) 대화 상자가 열립니다.

. 다음 값 중 하나 이상을 입력한 다음 * 저장 * 을 클릭합니다.
+
```

** * Name * -- MIB 변수의 `sysName`값입니다. 예를 들어 스토리지 배열의 이름을 입력합니다.
** *Location* -- MIB 변수의 `sysLocation`값입니다. 예를 들어 스토리지 배열의 위치를 입력합니다.
** * Contact * -- MIB 변수의 `sysContact`값입니다. 예를 들어 스토리지 시스템을 담당하는 관리자를 입력합니다.

.결과
이러한 값은 스토리지 배열 경고에 대한 SNMP 트랩 메시지에 표시됩니다.

[[ID1c0ac5724be3011053c548f6f06fbfe7]]
= SNMPv2c 트랩에 대한 커뮤니티를 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv2c 트랩에 대한 커뮤니티 이름을 편집할 수 있습니다.

.시작하기 전에
커뮤니티 이름을 만들어야 합니다.

.단계
. 메뉴: [Alerts](경고) 설정 을 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 커뮤니티 이름이 테이블에 나타납니다.

. 커뮤니티 구성 * 을 선택합니다.
. 새 커뮤니티 이름을 입력한 다음 * 저장 * 을 클릭합니다. 커뮤니티 이름은 인쇄 가능한 ASCII 문자만 포함할 수 있습니다.

.결과
Alerts 페이지의 SNMP 탭에 업데이트된 커뮤니티 이름이 표시됩니다.

[[ID32ca4f941b1bf0b5f62a2e724f7b8408]]

```
= SNMPv3 트랩에 대한 사용자 설정을 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SNMPv3 트랩에 대한 사용자 정의를 편집할 수 있습니다.

.시작하기 전에
SNMPv3 트랩에 대한 사용자를 생성해야 합니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 사용자 이름이 테이블에 나타납니다.

. 사용자 정의를 편집하려면 테이블에서 사용자를 선택한 다음 * 사용자 구성 * 을 클릭합니다.
. 대화 상자에서 * 설정 보기/편집 * 을 클릭합니다.
. 다음 정보를 편집합니다.
+
** * 사용자 이름 * -- 사용자를 식별하는 이름을 변경합니다. 이름은 최대 31자까지 가능합니다.
** * 엔진 ID * -- 메시지에 대한 인증 및 암호화 키를 생성하는 데 사용되는 엔진 ID를 선택합니다. 이 ID는 관리 도메인에서 고유해야 합니다. 대부분의 경우 * Local * 을 선택해야 합니다. 비표준 구성이 있는 경우 * 사용자 정의 * 를 선택합니다. 다른 필드는 신뢰할 수 있는 엔진 ID를 10자에서 32자 사이의 짝수 문자로 16진수 문자열로 입력해야 하는 위치에 나타납니다.
** * 인증 자격 증명 * -- 사용자 ID를 보장하는 인증 프로토콜을 선택합니다. 그런 다음 인증 프로토콜을 설정하거나 변경할 때 필요한 인증 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다.
** * 개인 정보 보호 자격 증명 * -- 메시지의 내용을 암호화하는 데 사용되는 개인 정보 보호 프로토콜을 선택합니다. 그런 다음 개인 정보 보호 프로토콜을 설정하거나 변경할 때 필요한 개인 정보 보호 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다.




.결과
Alerts 페이지의 SNMP 탭에 업데이트된 설정이 표시됩니다.



[[ID5fa5e7d3885e0c45b6e23393237fd0cc]]
= SNMPv2c 트랩에 대한 커뮤니티를 추가합니다
```

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SNMPv2c 트랩에 대해 최대 256개의 커뮤니티 이름을 추가할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 커뮤니티 이름이 테이블에 나타납니다.

. 커뮤니티 구성 * 을 선택합니다.
+
커뮤니티 구성 대화 상자가 열립니다.

. 다른 커뮤니티 추가 * 를 선택합니다.
. 새 커뮤니티 이름을 입력한 다음 * 저장 * 을 클릭합니다.


.결과
새 커뮤니티 이름이 Alerts 페이지의 SNMP 탭에 나타납니다.



[[ID97e7c182fb1d761006bef6223c081ef6]]
= SNMPv3 트랩에 사용자를 추가합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SNMPv3 트랩을 위해 최대 256명의 사용자를 추가할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 사용자 이름이 테이블에 나타납니다.
```

. 사용자 구성 * 을 선택합니다.
+
SNMPv3 사용자 구성 대화 상자가 열립니다.

. 추가 * 를 선택합니다.
. 다음 정보를 입력한 다음 * 추가 * 를 클릭합니다.
+
** * 사용자 이름 * -- 사용자를 식별할 이름을 입력합니다. 최대 31자까지 입력할 수 있습니다.
** * 엔진 ID * -- 메시지에 대한 인증 및 암호화 키를 생성하는 데 사용되는 엔진 ID를 선택합니다. 이 ID는 관리 도메인에서 고유해야 합니다. 대부분의 경우 * Local * 을 선택해야 합니다. 비표준 구성이 있는 경우 * 사용자 정의 * 를 선택합니다. 다른 필드는 신뢰할 수 있는 엔진 ID를 10자에서 32자 사이의 짝수 문자로 16진수 문자열로 입력해야 하는 위치에 나타납니다.
** * 인증 자격 증명 * -- 사용자 ID를 보장하는 인증 프로토콜을 선택합니다. 그런 다음 인증 프로토콜을 설정하거나 변경할 때 필요한 인증 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다.
** * 개인 정보 보호 자격 증명 * -- 메시지의 내용을 암호화하는 데 사용되는 개인 정보 보호 프로토콜을 선택합니다. 그런 다음 개인 정보 보호 프로토콜을 설정하거나 변경할 때 필요한 개인 정보 보호 암호를 입력합니다. 암호는 8자에서 128자 사이여야 합니다.

[[ID340e7f68820bae22454941c3df35ccc6]]
= SNMPv2c 트랩에 대한 커뮤니티를 제거합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv2c 트랩에 대한 커뮤니티 이름을 제거할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 커뮤니티 이름이 * Alerts * 페이지에 나타납니다.

. 커뮤니티 구성 * 을 선택합니다.
+
커뮤니티 구성 대화 상자가 열립니다.

. 삭제할 커뮤니티 이름을 선택한 다음 오른쪽 끝에 있는 * 제거 * (X) 아이콘을 클릭합니다.

+
트랩 대상이 이 커뮤니티 이름과 연결된 경우 커뮤니티 제거 확인 대화 상자에 영향을 받는 트랩 대상 주소가 표시됩니다.

. 작업을 확인한 다음 * 제거 * 를 클릭합니다.

.결과
커뮤니티 이름 및 관련 트랩 대상이 경고 페이지에서 제거됩니다.

[[ID13601beec1915640e4fa98f0c1a0afc4]]
= SNMPv3 트랩을 위해 사용자를 제거합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SNMPv3 트랩에 대한 사용자를 제거할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 및 사용자 이름이 경고 페이지에 나타납니다.

. 사용자 구성 * 을 선택합니다.
+
SNMPv3 사용자 구성 대화 상자가 열립니다.

. 삭제할 사용자 이름을 선택한 다음 * 삭제 * 를 클릭합니다.
. 작업을 확인한 다음 * 삭제 * 를 클릭합니다.

.결과
사용자 이름 및 관련 트랩 대상이 경고 페이지에서 제거됩니다.

[[IDfa5411e0ac1f18680d32f0d85c0ab6b6]]
= 트랩 대상을 삭제합니다
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
스토리지 배열의 이벤트 모니터가 더 이상 SNMP 트랩을 해당 주소로 보내지 않도록 트랩 대상
주소를 삭제할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. SNMP * 탭을 선택합니다.
+
트랩 대상 주소가 테이블에 나타납니다.

. 트랩 대상을 선택한 다음 페이지 오른쪽 위에 있는 * Delete * (삭제 *)를 클릭합니다.
. 작업을 확인한 다음 * 삭제 * 를 클릭합니다.
+
대상 주소가 알림 페이지에 더 이상 나타나지 않습니다.



.결과
삭제된 트랩 대상은 더 이상 스토리지 배열의 이벤트 모니터로부터 SNMP 트랩을 수신하지
않습니다.



:leveloffset: -1


= syslog 알림을 관리합니다

:leveloffset: +1


[[IDda553e53f342353baf7a786fe91fbb1e]]
= 경고에 대한 syslog 서버를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
syslog 알림을 구성하려면 syslog 서버 주소와 UDP 포트를 입력해야 합니다. 최대 5개의
```

syslog 서버가 허용됩니다.

.시작하기 전에
* syslog 서버 주소를 사용할 수 있어야 합니다. 이 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
* syslog 서버의 UDP 포트 번호를 사용할 수 있어야 합니다. 이 포트는 일반적으로 514입니다.

.이 작업에 대해
이 작업은 syslog 서버의 주소와 포트를 입력한 다음 입력한 주소를 테스트하는 방법을 설명합니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. Syslog * 탭을 선택합니다.
+
syslog 서버가 아직 정의되지 않은 경우 경고 페이지에 "Syslog 서버 추가"가 표시됩니다.

. Add Syslog Servers * 를 클릭합니다.
+
Add Syslog Server 대화 상자가 열립니다.

. 하나 이상의 syslog 서버에 대한 정보(최대 5개)를 입력한 다음 * 추가 * 를 클릭합니다.
+
** * 서버 주소 * -- 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
** * UDP 포트 * -- 일반적으로 syslog에 대한 UDP 포트는 514입니다. 구성된 syslog 서버가 테이블에 표시됩니다.

. 서버 주소로 테스트 알림을 보내려면 * 모든 Syslog 서버 테스트 * 를 선택합니다.

.결과
이벤트 모니터는 경고 가능 이벤트가 발생할 때마다 syslog 서버에 경고를 보냅니다. 감사 로그에 대한 syslog 설정을 추가로 구성하려면 를 참조하십시오 https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-audit-logs.html["감사 로그를 위해 syslog 서버를 구성합니다"].

NOTE: 여러 syslog 서버가 구성된 경우 구성된 모든 syslog 서버가 감사 로그를 수신합니다.

[[IDebbfc5bd68a68380e82d4fcdd80fee09]]
= 경고를 위해 syslog 서버를 편집합니다
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
syslog 알림을 수신하는 데 사용되는 서버 주소를 편집할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. Syslog * 탭을 선택합니다.
. 테이블에서 syslog 서버 주소를 선택한 다음 오른쪽 끝에 있는 * Edit * (연필) 아이콘을 클릭합니다.
+
행이 편집 가능한 필드가 됩니다.

. 서버 주소와 UDP 포트 번호를 편집한 다음 * 저장 * (확인 표시) 아이콘을 클릭합니다.


.결과
업데이트된 서버 주소가 테이블에 나타납니다.



[[ID4ac77b97ed0cd5d4bbd1fa6979cd3716]]
= 경고에 대한 syslog 서버를 추가합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
syslog 알림에 최대 5개의 서버를 추가할 수 있습니다.

.시작하기 전에
* syslog 서버 주소를 사용할 수 있어야 합니다. 이 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
* syslog 서버의 UDP 포트 번호를 사용할 수 있어야 합니다. 이 포트는 일반적으로 514입니다.


.단계
. 설정 [알림] 메뉴를 선택합니다.
. Syslog * 탭을 선택합니다.
. Add Syslog Servers * 를 선택합니다.
+
```

Add Syslog Server 대화 상자가 열립니다.

. 다른 syslog 서버 추가 * 를 선택합니다.
. syslog 서버에 대한 정보를 입력한 다음 * 추가 * 를 클릭합니다.
+
** * Syslog Server Address * -- 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
** * UDP 포트 * -- 일반적으로 syslog에 대한 UDP 포트는 514입니다.

+

NOTE: 최대 5개의 syslog 서버를 구성할 수 있습니다.

.결과
syslog 서버 주소가 테이블에 나타납니다.

[[IDc8bef38178293bf104bfe58865429c7b]]
= 경고를 위해 syslog 서버를 삭제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
더 이상 경고를 받지 않도록 syslog 서버를 삭제할 수 있습니다.

.단계
. 설정 [알림] 메뉴를 선택합니다.
. Syslog * 탭을 선택합니다.
. syslog 서버 주소를 선택한 다음 오른쪽 위에서 * 제거 * 를 클릭합니다.
+
Confirm Delete Syslog Server(Syslog 서버 삭제 확인) 대화 상자가 열립니다.

. 작업을 확인한 다음 * 삭제 * 를 클릭합니다.

.결과
제거한 서버는 더 이상 이벤트 모니터로부터 경고를 받지 않습니다.

```
:leveloffset: -1


= FAQ 를 참조하십시오

:leveloffset: +1


[[IDed94478d34b087979d53d39fa708e955]]
= 경고가 비활성화되면 어떻게 합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
관리자가 스토리지 어레이에서 발생하는 중요한 이벤트에 대한 알림을 받도록 하려면 경고 방법을 구성해야 합니다.

SANtricity System Manager로 관리되는 스토리지 어레이의 경우 경고 페이지에서 경고를 구성합니다. 경고 알림은 이메일, SNMP 트랩 또는 syslog 메시지를 통해 보낼 수 있습니다. 또한 초기 설정 마법사에서 이메일 경고를 구성할 수도 있습니다.



[[ID96164038af2f8d4f7c7de7f5f50cec28]]
= SNMP 또는 syslog 알림을 구성하려면 어떻게 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
e-메일 알림 외에도 SNMP(Simple Network Management Protocol) 트랩 또는 syslog 메시지를 통해 보낼 알림을 구성할 수 있습니다.

SNMP 또는 syslog 알림을 구성하려면 설정 [경고] 메뉴로 이동합니다.



[[ID2f2b161151115b62ead9abbc68b24f56]]
= 타임스탬프가 스토리지와 알림 간에 일치하지 않는 이유는 무엇입니까?
:allow-uri-read:
```

```
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
스토리지 시스템에서 알림을 보낼 때 알림을 받는 타겟 서버 또는 호스트의 표준 시간대가 올바르지 않습니다. 대신 스토리지 배열은 로컬 시간(GMT)을 사용하여 경고 레코드에 사용되는 타임스탬프를 생성합니다. 따라서 스토리지 어레이의 타임스탬프와 알림을 수신하는 서버 또는 호스트의 일치하지 않는 부분이 표시될 수 있습니다.

스토리지 배열이 경고를 보낼 때 표준 시간대에 대해 올바르지 않기 때문에 경고의 타임스탬프는 GMT-상대 시간이며 시간 영역 오프셋이 0입니다. 현지 시간대에 맞는 타임스탬프를 계산하려면 GMT에서 시간 오프셋을 결정한 다음 타임스탬프에서 해당 값을 더하거나 빼야 합니다.



:leveloffset: -1


:leveloffset: -1


= 배열 설정

:leveloffset: +1


[[IDdabef8a7535a2aa10c8da96d87c20e38]]
= 설정 개요
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
일부 일반적인 어레이 설정 및 추가 기능에 대해 SANtricity 시스템 관리자를 구성할 수 있습니다.



== 구성할 수 있는 설정은 무엇입니까?

배열 설정에는 다음이 포함됩니다.
```

```
* xref:{relative_path}cache-settings-and-performance.html["캐시 설정 및 성능"]
* xref:{relative_path}automatic-load-balancing-overview.html["자동 로드
밸런싱"]
* xref:{relative_path}how-add-on-features-work.html["애드온 기능"]
* xref:{relative_path}overview-drive-security.html["드라이브 보안"]




== 관련 작업

시스템 설정 관련 작업에 대한 자세한 내용:

* xref:{relative_path}download-cli.html["CLI(Command Line Interface)
다운로드"]
* xref:{relative_path}create-internal-security-key.html["내부 보안 키를
생성합니다"]
* xref:{relative_path}create-external-security-key.html["외부 보안 키를
만듭니다"]
* xref:{relative_path}../sm-hardware/configure-iscsi-ports-
hardware.html["iSCSI 포트를 구성합니다"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-infiniband-ports-
hardware.html["IB 포트를 통해 NVMe 구성"]
* xref:{relative_path}../sm-hardware/configure-nvme-over-roce-ports-
hardware.html["NVMe over RoCE 포트를 구성합니다"]




= 개념

:leveloffset: +1


[[ID2a951fe8d58a7c24fb174ef6eee5759d]]
= 캐시 설정 및 성능
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
캐시 메모리는 드라이브 미디어보다 액세스 시간이 빠른 컨트롤러의 임시 휘발성 저장 영역입니다.

캐싱을 사용하면 전반적인 I/O 성능을 다음과 같이 향상시킬 수 있습니다.
```

* 읽기를 위해 호스트에서 요청된 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브 액세스가 필요하지 않습니다.
* 쓰기 데이터는 처음에는 캐시에 기록되기 때문에 데이터가 드라이브에 기록될 때까지 기다리지 않고 애플리케이션을 계속 사용할 수 있습니다.

기본 캐시 설정은 대부분의 환경에 대한 요구 사항을 충족하지만 원하는 경우 변경할 수 있습니다.

== 스토리지 캐시 설정입니다

스토리지 배열의 모든 볼륨에 대해 시스템 페이지에서 다음 값을 지정할 수 있습니다.

* * 플러싱에 대한 시작 값 * -- 캐시 플러시를 트리거하는 캐시에 기록되지 않은 데이터의 비율입니다(디스크에 쓰기). 캐시에 기록되지 않은 데이터의 지정된 시작 백분율이 있으면 플러시가 트리거됩니다. 기본적으로 컨트롤러는 캐시가 80% 찰 때 캐시를 플러시합니다.
* * 캐시 블록 크기 * -- 캐시 관리를 위한 조직 단위인 각 캐시 블록의 최대 크기입니다. 캐시 블록 크기는 기본적으로 8KiB이지만 4, 8, 16 또는 32KiB로 설정할 수 있습니다. 가장 많이 사용되는 애플리케이션의 입출력 크기로 캐시 블록 크기를 설정하는 것이 좋습니다. 파일 시스템 또는 데이터베이스 애플리케이션은 일반적으로 더 작은 크기를 사용하며, 더 큰 크기는 대용량 데이터 전송이나 순차적 I/O가 필요한 애플리케이션에 적합합니다

== 볼륨 캐시 설정입니다

스토리지 배열의 개별 볼륨의 경우 Volumes(볼륨) 페이지(메뉴: Storage(저장소) [Volumes](볼륨))에서 다음 값을 지정할 수 있습니다.

* * 읽기 캐싱 * -- 읽기 캐시는 드라이브에서 읽은 데이터를 저장하는 버퍼입니다. 읽기 작업의 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브에 액세스할 필요가 없습니다. 데이터가 플러시될 때까지 읽기 캐시에 남아 있습니다.
+
** * 동적 읽기 캐시 프리페치 * -- 동적 캐시 읽기 프리페치를 사용하면 컨트롤러에서 드라이브에서 캐시로 데이터 블록을 읽는 동안 순차적 데이터 블록을 추가로 캐시에 복사할 수 있습니다. 이 캐싱은 향후 캐시에서 데이터 요청을 채울 수 있는 기회를 높여줍니다. 동적 캐시 읽기 프리페치는 순차적 I/O를 사용하는 멀티미디어 애플리케이션에 중요합니다 캐시로 프리페치되는 데이터의 속도와 양은 호스트 읽기의 속도 및 요청 크기에 따라 자동으로 조정됩니다. 랜덤 액세스로 인해 데이터를 캐시로 프리페치하지 않습니다. 이 기능은 읽기 캐시를 사용하지 않는 경우 적용되지 않습니다.

* * 쓰기 캐시 * -- 쓰기 캐시는 아직 드라이브에 기록되지 않은 호스트의 데이터를 저장하는 버퍼입니다. 데이터는 드라이브에 기록될 때까지 쓰기 캐시에 유지됩니다. 쓰기 캐싱은 I/O 성능을

높일 수 있습니다.
+
[CAUTION]
====
* 데이터 손실 가능성 * -- 배터리 없이 * 쓰기 캐싱 * 옵션을 활성화하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다.

====
+
** * 배터리 없는 쓰기 캐싱 * -- 배터리 없는 쓰기 캐싱 설정을 사용하면 배터리가 없거나, 고장, 방전되거나, 완전히 충전되지 않았더라도 쓰기 캐싱을 계속할 수 있습니다. 일반적으로 배터리 없이 쓰기 캐시를 선택하는 것은 권장되지 않습니다. 전원이 끊길 경우 데이터가 손실될 수 있기 때문입니다. 일반적으로 쓰기 캐시는 배터리가 충전되거나 장애가 발생한 배터리를 교체할 때까지 컨트롤러에 의해 일시적으로 꺼집니다.
** * 미러링으로 쓰기 캐싱 * -- 한 컨트롤러의 캐시 메모리에 기록된 데이터가 다른 컨트롤러의 캐시 메모리에도 쓰일 때 미러링을 사용하는 쓰기 캐시가 발생합니다. 따라서 한 컨트롤러에 장애가 발생하면 다른 컨트롤러가 처리되지 않은 모든 쓰기 작업을 완료할 수 있습니다. 쓰기 캐시 미러링은 쓰기 캐시가 설정되고 두 개의 컨트롤러가 있는 경우에만 사용할 수 있습니다. 볼륨 생성 시 기본 설정은 미러링을 사용한 쓰기 캐시입니다.

[[IDac20d99f92f34a3898c7cb12e732670d]]
= 자동 로드 밸런싱 개요
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
자동 로드 밸런싱은 시간이 지남에 따라 로드 변화에 동적으로 대응하고 볼륨 컨트롤러 소유권을 자동으로 조정하여 워크로드가 컨트롤러 간에 이동할 때 로드 불균형 문제를 해결함으로써 I/O 리소스 관리를 개선합니다.

각 컨트롤러의 워크로드는 지속적으로 모니터링되며 호스트에 설치된 다중 경로 드라이버의 협력을 통해 필요할 때마다 자동으로 균형을 맞출 수 있습니다. 컨트롤러 간에 워크로드가 자동으로 재조정되면 스토리지 관리자는 스토리지 어레이의 로드 변경을 수용하기 위해 볼륨 컨트롤러 소유권을 수동으로 조정해야 하는 부담을 덜 수 있습니다.

자동 로드 밸런싱이 활성화되면 다음 기능을 수행합니다.

* 컨트롤러 리소스 활용률을 자동으로 모니터링 및 균형 조정

* 필요한 경우 볼륨 컨트롤러 소유권을 자동으로 조정하여 호스트와 스토리지 어레이 간의 I/O 대역폭을 최적화합니다.

== 자동 로드 밸런싱 활성화 및 비활성화

자동 로드 밸런싱은 모든 스토리지 어레이에서 기본적으로 활성화됩니다.

다음과 같은 이유로 스토리지 어레이에서 자동 로드 밸런싱을 사용하지 않도록 설정할 수 있습니다.

* 워크로드의 균형을 맞추기 위해 특정 볼륨의 컨트롤러 소유권을 자동으로 변경하지 않으려는 경우
* 부하 분산이 의도적으로 설정된 고도로 조정된 환경에서 컨트롤러 간에 특정 분포를 이룰 수 있습니다.

== 자동 로드 밸런싱 기능을 지원하는 호스트 유형입니다

스토리지 어레이 레벨에서 자동 로드 밸런싱이 활성화되어 있더라도 호스트 또는 호스트 클러스터에 대해 선택하는 호스트 유형은 이 기능의 작동 방식에 직접적인 영향을 미칩니다.

여러 컨트롤러에 걸쳐 스토리지 어레이의 워크로드를 밸런싱할 때 자동 로드 밸런싱 기능은 두 컨트롤러가 액세스할 수 있고 자동 로드 밸런싱 기능을 지원할 수 있는 호스트 또는 호스트 클러스터에만 매핑된 볼륨을 이동하려고 시도합니다.

이렇게 하면 로드 밸런싱 프로세스로 인해 호스트가 볼륨에 액세스하지 못하게 됩니다. 하지만 자동 로드 밸런싱을 지원하지 않는 호스트에 매핑된 볼륨이 있으면 스토리지 시스템의 워크로드 균형 조정 기능에 영향을 줍니다. 자동 로드 균형 조정을 위해 다중 경로 드라이버는 TPGS를 지원해야 하며 호스트 유형은 다음 표에 포함되어야 합니다.

[NOTE]
====
호스트 클러스터에서 자동 로드 밸런싱을 사용하려면 해당 그룹의 모든 호스트가 자동 로드 밸런싱을 지원할 수 있어야 합니다.

====
[cols="1a,1a"]
|===
| 자동 로드 밸런싱을 지원하는 호스트 유형입니다 | 이 다중 경로 드라이버를 사용합니다

 a|
Windows 또는 Windows 클러스터형
 a|

NetApp E-Series DSM을 사용한 MPIO

a|
Linux DM-MP(커널 3.10 이상)
a|
DM-MP(장치 핸들러 포함) `scsi_dh_alua`

a|
VMware
a|
플러그인을 사용하는 NMP(기본 다중 경로 플러그인) `VMW_SATP_ALUA Storage Array Type`

|===
[NOTE]
====
사소한 예외를 제외하고 자동 로드 밸런싱을 지원하지 않는 호스트 유형은 이 기능이 활성화되어 있는지 여부에 관계없이 계속 정상적으로 작동합니다. 한 가지 예외는 시스템에 페일오버가 있는 경우 데이터 경로가 반환될 때 스토리지 어레이가 매핑되지 않았거나 할당되지 않은 볼륨을 소유 컨트롤러로 다시 이동하는 것입니다. 비 자동 로드 밸런싱 호스트에 매핑되거나 할당된 볼륨은 이동되지 않습니다.

====
특정 다중 경로 드라이버, OS 레벨, 컨트롤러-드라이브 트레이 지원에 대한 호환성 정보는 를 https://mysupport.netapp.com/matrix["상호 운용성 매트릭스 툴"^] 참조하십시오.

== 자동 로드 밸런싱 기능과 OS 호환성을 확인합니다

새(또는 기존) 시스템을 설정하기 전에 자동 로드 밸런싱 기능과 OS 호환성을 확인하십시오.

. 로 https://mysupport.netapp.com/matrix["상호 운용성 매트릭스 툴"^] 이동하여 해결 방법을 찾고 지원을 확인합니다.
+
시스템에서 Red Hat Enterprise Linux 6 또는 SUSE Linux Enterprise Server 11을 실행하는 경우 기술 지원 부서에 문의하십시오.

. 를 업데이트하고 `/etc/multipath.conf file` 구성합니다.
. 해당 공급업체 및 제품에 대해 및 `detect_prio` 가 모두 로 설정되어 `yes` 있는지 `retain_attached_device_handler` 확인하거나 기본 설정을 사용합니다.

```
:leveloffset: -1


= 스토리지 설정을 구성합니다

:leveloffset: +1


[[IDc4515005bba8928e709f6a2a1b653c1b]]
= 스토리지 배열 이름을 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SANtricity 시스템 관리자의 제목 표시줄에 나타나는 스토리지 배열 이름을 변경할 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 일반 * 에서 * 이름: * 필드를 찾습니다.
+
스토리지 배열 이름이 정의되지 않은 경우 이 필드에는 "알 수 없음"이 표시됩니다.

. 스토리지 배열 이름 옆에 있는 * Edit * (연필) 아이콘을 클릭합니다.
+
필드를 편집할 수 있게 됩니다.

. 새 이름을 입력합니다.
+
이름에는 문자, 숫자 및 밑줄(_), 대시(-) 및 해시 기호(#)를 사용할 수 있습니다. 이름에는 공백을 사용할 수 없습니다. 이름의 최대 길이는 30자입니다. 이름은 고유해야 합니다.

. 저장 * (확인 표시) 아이콘을 클릭합니다.
+
[NOTE]
====
변경하지 않고 편집 가능한 필드를 닫으려면 * Cancel * (X) 아이콘을 클릭합니다.

====


.결과
새 이름이 SANtricity 시스템 관리자의 제목 표시줄에 나타납니다.
```

[[ID68fc76ea53f37f57a4dfe0160588319a]]
= 스토리지 배열 로케이터 표시등을 켭니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
캐비닛에서 스토리지 배열의 물리적 위치를 찾으려면 해당 로케이터(LED) 표시등을 켜면 됩니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 일반 * 에서 * 스토리지 배열 로케이터 표시등 켜기 * 를 클릭합니다.
+
스토리지 배열 찾기 표시등 켜기 대화 상자가 열리고 해당 스토리지 배열의 로케이터 표시등이 켜집니다.

. 스토리지 배열을 물리적으로 찾았으면 대화 상자로 돌아가서 * 끄기 * 를 선택합니다.

.결과
로케이터 표시등이 꺼지고 대화 상자가 닫힙니다.

[[IDa83a46627d08def0a4f27fa80217caa4]]
= 스토리지 배열 클록을 동기화합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
NTP(네트워크 시간 프로토콜)가 활성화되지 않은 경우 컨트롤러의 시계를 수동으로 설정하여 관리 클라이언트(SANtricity 시스템 관리자에 액세스하는 브라우저를 실행하는 데 사용되는 시스템)와 동기화할 수 있습니다.

.이 작업에 대해
동기화는 이벤트 로그의 이벤트 타임 스탬프가 호스트 로그 파일에 기록된 타임 스탬프와 일치하도록 합니다. 동기화 프로세스 중에도 컨트롤러는 사용 가능하고 정상적으로 작동합니다.

[NOTE]
====
System Manager에서 NTP가 활성화되어 있는 경우 이 옵션을 사용하여 시계를 동기화하지 마십시오. 대신 NTP는 SNTP(Simple Network Time Protocol)를 사용하여 외부 호스트와 시계를 자동으로 동기화합니다.

====
[NOTE]
====
동기화 후 성능 통계가 손실되거나 비뚤어지거나, 일정(ASUP, 스냅샷 등)이 영향을 받고, 로그 데이터의 타임스탬프가 비뚤어지는 것을 확인할 수 있습니다. NTP를 사용하면 이 문제가 방지됩니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. General * 에서 * Synchronize Storage Array Clocks * 를 클릭합니다.
+
스토리지 배열 시계 동기화 대화 상자가 열립니다. 컨트롤러 및 관리 클라이언트로 사용되는 컴퓨터의 현재 날짜 및 시간을 표시합니다.

+
[NOTE]
====
단일 스토리지 어레이의 경우 하나의 컨트롤러만 표시됩니다.

====
. 대화 상자에 표시된 시간이 일치하지 않으면 * Synchronize * 를 클릭합니다.

.결과
동기화에 성공하면 이벤트 로그 및 호스트 로그에 대해 이벤트 타임 스탬프가 동일합니다.

[[ID27aecf34b087576d1d6b3d10721e4791]]
= 스토리지 배열 구성을 저장합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열의 구성 정보를 스크립트 파일에 저장하여 동일한 구성으로 추가 스토리지 배열을

설정하는 시간을 절약할 수 있습니다.

.시작하기 전에
스토리지 시스템에서 논리적 구성 설정을 변경하는 작업을 수행해서는 안 됩니다. 이러한 작업의 예로는 볼륨 생성 또는 삭제, 컨트롤러 펌웨어 다운로드, 핫 스페어 드라이브 할당 또는 수정, 볼륨 그룹에 용량(드라이브) 추가 등이 있습니다.

.이 작업에 대해
스토리지 배열 구성을 저장하면 스토리지 배열에 대한 스토리지 배열 설정, 볼륨 구성, 호스트 구성 또는 호스트-볼륨 할당을 포함하는 CLI(Command Line Interface) 스크립트가 생성됩니다. 생성된 이 CLI 스크립트를 사용하여 정확히 동일한 하드웨어 구성을 가진 다른 스토리지 어레이로 구성을 복제할 수 있습니다.

그러나 재해 복구에 이 생성된 CLI 스크립트를 사용해서는 안 됩니다. 대신 시스템 복원을 수행하려면 수동으로 생성한 구성 데이터베이스 백업 파일을 사용하거나 기술 지원 부서에 문의하여 최신 자동 지원 데이터에서 이 데이터를 얻으십시오.

이 작업은 _ 이(가) 다음 설정을 저장하지 않습니다.

* 배터리 수명
* 컨트롤러 시간입니다
* NVSRAM(Nonvolatile Static Random Access Memory) 설정입니다
* 모든 프리미엄 기능
* 스토리지 배열 암호입니다
* 하드웨어 구성 요소의 작동 상태 및 상태입니다
* 볼륨 그룹의 작동 상태(최적 상태 제외) 및 상태입니다
* 미러링 및 볼륨 복사본과 같은 복사 서비스를 이용할 수 있습니다

[CAUTION]
====
* 응용 프로그램 오류 위험 * -- 스토리지 배열에 논리 구성 설정을 변경할 작업이 진행 중인 경우에는 이 옵션을 사용하지 마십시오. 이러한 작업의 예로는 볼륨 생성 또는 삭제, 컨트롤러 펌웨어 다운로드, 핫 스페어 드라이브 할당 또는 수정, 볼륨 그룹에 용량(드라이브) 추가 등이 있습니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 스토리지 배열 구성 저장 * 을 선택합니다.
. 저장할 구성 항목을 선택합니다.
+
** 스토리지 배열 설정입니다
** 볼륨 구성
** 호스트 구성
** 호스트-볼륨 할당

+
[NOTE]
====
Host-to-volume Assignments * 항목을 선택하면 * Volume configuration * 항목과 * Host configuration * 항목도 기본적으로 선택됩니다. "볼륨 구성"과 "호스트 구성"을 저장하지 않으면 "호스트 대 볼륨 할당"을 저장할 수 없습니다.

====
. 저장 * 을 클릭합니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `storage-array-configuration.cfg`저장됩니다.

.작업을 마친 후
저장된 스토리지 배열 구성을 다른 스토리지 배열에 로드하려면 SANtricity 명령줄 인터페이스(SMcli)와 함께 `-f` 파일을 적용하는 옵션을 `.cfg` 사용합니다.

[NOTE]
====
Unified Manager 인터페이스를 사용하여 스토리지 어레이 구성을 다른 스토리지 어레이에 로드할 수도 있습니다(메뉴 선택: 관리 [설정 가져오기]).

====

[[ID7e203aef6ffcadaff77fc57a1387e61f]]
= 스토리지 배열 구성을 지웁니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열에서 모든 풀, 볼륨 그룹, 볼륨, 호스트 정의 및 호스트 할당을 삭제하려면 구성 지우기 작업을 사용합니다.

.시작하기 전에
스토리지 배열 구성을 지우기 전에 데이터를 백업합니다.

.이 작업에 대해
스토리지 배열 구성 지우기 옵션에는 두 가지가 있습니다.

* * 볼륨 * -- 일반적으로 볼륨 옵션을 사용하여 테스트 스토리지 어레이를 프로덕션 스토리지 어레이로 재구성할 수 있습니다. 예를 들어, 테스트용으로 스토리지 어레이를 구성한 다음 테스트를 마치면 테스트 구성을 제거하고 운영 환경에 맞게 스토리지 어레이를 설정할 수 있습니다.
* * 스토리지 배열 * -- 일반적으로 스토리지 배열 옵션을 사용하여 스토리지 배열을 다른 부서 또는 그룹으로 이동할 수 있습니다. 예를 들어, 엔지니어링 팀에서 스토리지 어레이를 사용하고 있고 이제 엔지니어링 팀에서 새 스토리지 어레이를 가져오므로 현재 스토리지 어레이를 재구성할 관리 위치로 이동할 수 있습니다.
+
스토리지 배열 옵션은 일부 추가 설정을 삭제합니다.

[cols="1a,1a,1a"]
|===
| | 볼륨 | 스토리지

a|
ARVM을 비활성화합니다
a|
X
a|
X

a|
풀 및 볼륨 그룹을 삭제합니다
a|
X
a|
X

a|
볼륨을 삭제합니다
a|
X
a|
X

a|
호스트 및 호스트 클러스터를 삭제합니다

```
 a|
X
 a|
X



 a|
호스트 할당을 삭제합니다
 a|
X
 a|
X



 a|
스토리지 배열 이름을 삭제합니다
 a|
 a|
X



 a|
스토리지 캐시 설정을 기본값으로 재설정합니다
 a|
 a|
X

|===
[CAUTION]
====
* 데이터 손실 위험 * -- 이 작업은 스토리지 배열의 모든 데이터를 삭제합니다. (보안 지우기는 수행하지 않습니다.) 이 작업을 시작한 후에는 취소할 수 없습니다. 기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 스토리지 배열 구성 지우기 * 를 선택합니다.
. 드롭다운 목록에서 * Volume * 또는 * Storage Array * 를 선택합니다.
. * 선택 사항: * 데이터가 아닌 구성을 저장하려면 대화 상자의 링크를 사용합니다.
. 작업을 수행할지 확인합니다.


.결과
```

* 현재 구성이 삭제되어 스토리지 어레이의 기존 데이터가 모두 제거됩니다.
* 모든 드라이브가 할당되지 않았습니다.

[[ID74a303fd714304f9eb1d7334c0797c17]]
= 스토리지 배열에 대한 캐시 설정을 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열의 모든 볼륨에 대해 캐시 메모리 설정을 조정하여 플러싱과 블록 크기를 조정할 수 있습니다.

.이 작업에 대해
캐시 메모리는 컨트롤러의 임시 휘발성 저장 공간으로, 드라이브 미디어보다 액세스 시간이 더 빠릅니다. 캐시 성능을 조정하려면 다음 설정을 조정할 수 있습니다.

[cols="25h,~"]
|===
| 캐시 설정 | 설명

a|
요청 캐시 플러싱을 시작합니다
a|
Start demand cache flashing은 캐시 플러시(디스크에 쓰기)를 트리거하는 캐시에 기록되지 않은 데이터의 비율을 지정합니다. 기본적으로 캐시 플러싱은 기록되지 않은 데이터가 80% 용량에 도달하면 시작됩니다. 쓰기 작업이 주로 수행되는 환경에서는 더 높은 비율이 적합하므로 새 쓰기 요청은 디스크로 이동할 필요 없이 캐시로 처리될 수 있습니다. 입출력 오류가 발생하는 환경(데이터 버스트 사용)에서 낮은 설정은 더 낫기 때문에 시스템이 데이터 버스트 사이에 캐시를 자주 플러시합니다. 그러나 시작 비율이 80%보다 낮으면 성능이 저하될 수 있습니다.

a|
캐시 블록 크기
a|
캐시 블록 크기는 각 캐시 블록의 최대 크기를 결정합니다. 이 크기는 캐시 관리를 위한 조직 단위입니다. 기본적으로 블록 크기는 32KiB입니다. 시스템은 캐시 블록 크기를 4, 8, 16 또는 32KiB로 설정할 수 있습니다. 애플리케이션은 스토리지 성능에 영향을 미치는 다양한 블록 크기를 사용합니다. 파일 시스템 또는 데이터베이스 애플리케이션에 적합한 크기는 더 작습니다. 더 큰

크기는 멀티미디어와 같이 순차적 I/O를 생성하는 응용 프로그램에 이상적입니다.

|===
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 스크롤하여 * 추가 설정 * 을 찾은 다음 * 캐시 설정 변경 * 을 클릭합니다.
+
캐시 설정 변경 대화 상자가 열립니다.

. 다음 값을 조정합니다.
+
** * 요청 캐시 플러싱 시작 * -- 사용자 환경에서 사용되는 I/O에 적합한 비율을 선택합니다. 80% 미만의 값을 선택하면 성능이 저하될 수 있습니다.
** ** 캐시 블록 크기 --** 응용 프로그램에 적합한 크기를 선택합니다.

. 저장 * 을 클릭합니다.

[[ID50da875355eee27dff69f5ccd0eda183]]
= 자동 로드 밸런싱을 설정합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
자동 로드 밸런싱 기능은 호스트로부터 들어오는 I/O 트래픽이 두 컨트롤러 간에 동적으로 관리 및 균형 조정되도록 합니다. 이 기능은 기본적으로 사용하도록 설정되어 있지만 SANtricity System Manager에서 사용하지 않도록 설정할 수 있습니다.

.이 작업에 대해
자동 로드 밸런싱이 활성화되면 다음 기능을 수행합니다.

* 컨트롤러 리소스 활용률을 자동으로 모니터링 및 균형 조정
* 필요한 경우 볼륨 컨트롤러 소유권을 자동으로 조정하여 호스트와 스토리지 어레이 간의 I/O 대역폭을 최적화합니다.

다음과 같은 이유로 스토리지 어레이에서 자동 로드 밸런싱을 사용하지 않도록 설정할 수 있습니다.

* 워크로드의 균형을 맞추기 위해 특정 볼륨의 컨트롤러 소유권을 자동으로 변경하지 않으려는 경우
* 부하 분산이 의도적으로 설정된 고도로 조정된 환경에서 컨트롤러 간에 특정 분포를 이룰 수

있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 자동 로드 밸런싱 활성화/비활성화 * 를 클릭합니다.
+
이 옵션 아래의 텍스트는 기능이 현재 활성화되어 있는지 여부를 나타냅니다.

+
확인 대화 상자가 열립니다.

. 계속하려면 * 예 * 를 클릭하여 확인하십시오.
+
이 옵션을 선택하면 기능을 활성화/비활성화 상태로 전환할 수 있습니다.

+
[NOTE]
====
이 기능이 비활성화에서 사용으로 이동되면 호스트 연결 보고 기능도 자동으로 활성화됩니다.

====

[[IDfc545c7b84e8e64dbe43cf13dd1f7d97]]
= 레거시 관리 인터페이스를 활성화 또는 비활성화합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열과 관리 클라이언트 간의 통신 방법인 레거시 관리 인터페이스(기호)를 설정하거나 해제할 수 있습니다.

.이 작업에 대해
기본적으로 레거시 관리 인터페이스는 켜져 있습니다. 이 기능을 해제하면 스토리지 어레이와 관리 클라이언트에서 더욱 안전한 통신 방법(https를 통한 REST API)을 사용합니다. 그러나 특정 툴 및 작업이 비활성화된 경우 영향을 받을 수 있습니다.

[NOTE]
====

EF600 스토리지 시스템의 경우 이 기능은 기본적으로 비활성화되어 있습니다.

====
이 설정은 다음과 같은 작업에 영향을 줍니다.

* * On * (기본값) -- CLI 및 OCI 어댑터와 같은 다른 툴을 사용하여 미러링을 구성하는 데 필요한 설정입니다.
* * Off * -- 스토리지 어레이와 관리 클라이언트 간 통신에서 기밀성을 강화하고 외부 도구에 액세스하는 데 필요한 설정입니다. LDAP(Directory Server)를 구성할 때 권장되는 설정입니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 관리 인터페이스 변경 * 을 클릭합니다.
. 대화 상자에서 * 예 * 를 클릭하여 계속합니다.

:leveloffset: -1

= 애드온 기능을 구성합니다

:leveloffset: +1

[[ID58176969da3db00ca61bc27a6e3e572d]]
= 애드온 기능의 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
추가 기능은 SANtricity System Manager의 표준 구성에 포함되지 않는 기능으로, 활성화하려면 키가 필요할 수 있습니다. 애드온 기능은 단일 프리미엄 기능 또는 번들 기능 팩일 수 있습니다.

다음 단계에서는 프리미엄 기능 또는 기능 팩을 사용하는 방법을 개괄적으로 설명합니다.

. 다음 정보를 얻습니다.
+
** 설치할 기능의 스토리지 배열을 식별하는 섀시 일련 번호 및 기능 활성화 식별자. 이러한 항목은 System Manager에서 사용할 수 있습니다.

** 기능 활성화 코드 - 기능 구매 시 지원 사이트에서 사용할 수 있습니다.

. 스토리지 공급업체에 문의하거나 프리미엄 기능 활성화 사이트에 액세스하여 기능 키를 얻습니다. 섀시 일련 번호, 활성화 식별자 및 활성화를 위한 기능 코드를 제공합니다.
. System Manager를 사용하여 기능 키 파일을 사용하여 프리미엄 기능 또는 기능 팩을 활성화합니다.

[[ID3b40ccdea97880378da83cafcdbba6ff]]
= 애드온 기능 용어
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
애드온 기능 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명

a|
기능 활성화 식별자
a|
Feature Enable Identifier는 특정 스토리지 배열을 식별하는 고유한 문자열입니다. 이 식별자는 프리미엄 기능을 사용할 때 특정 스토리지 어레이에만 연결되도록 합니다. 이 문자열은 시스템 페이지의 추가 기능 아래에 표시됩니다.

a|
피처 키 파일
a|
기능 키 파일은 프리미엄 기능 또는 기능 팩의 잠금 해제 및 활성화를 위해 제공되는 파일입니다.

a|
기능 팩
a|
기능 팩은 스토리지 배열 속성을 변경하는 번들(예: 프로토콜을 Fibre Channel에서 iSCSI로

변경)입니다. 기능 팩을 사용하려면 특수 키가 필요합니다.

 a|
프리미엄 기능
 a|
프리미엄 기능은 추가 옵션으로, 이를 활성화하려면 키가 필요합니다. System Manager의 표준 구성에는 포함되어 있지 않습니다.

|===

[[ID860efd21aa3508f8c7ea905b7c10f5e1]]
= 기능 키 파일을 가져옵니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 어레이에서 프리미엄 기능 또는 기능 팩을 활성화하려면 먼저 기능 키 파일을 구해야 합니다. 키는 하나의 스토리지 배열에만 연결됩니다.

.이 작업에 대해
이 작업에서는 기능에 필요한 정보를 수집한 다음 기능 키 파일에 대한 요청을 보내는 방법을 설명합니다. 필수 정보는 다음과 같습니다.

* 섀시 일련 번호입니다
* 기능 활성화 식별자
* 기능 활성화 코드

.단계
. System Manager에서 섀시 일련 번호를 찾아 기록합니다. 지원 센터 타일에 마우스를 올려 놓으면 이 일련 번호를 볼 수 있습니다.
. System Manager에서 Enable Identifier 기능을 찾습니다. 설정 [시스템] 메뉴로 이동한 다음 아래로 스크롤하여 * 추가 기능 * 으로 이동합니다. Feature Enable Identifier * 를 찾습니다. 기능 식별자 활성화 의 번호를 기록합니다.
. 기능 활성화를 위한 코드를 찾아 기록합니다. 기능 팩의 경우 이 코드는 변환을 수행하기 위한 적절한 지침에 나와 있습니다.
+
프리미엄 기능의 경우 지원 사이트에서 다음과 같이 활성화 코드에 액세스할 수 있습니다.

+
.. 에 https://mysupport.netapp.com/site/global/dashboard["NetApp 지원 "^]로그인합니다.
.. 사용 중인 제품의 * 소프트웨어 라이선스 * 로 이동합니다.
.. 스토리지 어레이 섀시의 일련 번호를 입력하고 * Go * 를 클릭합니다.
.. 라이센스 키 * 열에서 기능 활성화 코드를 찾습니다.
.. 원하는 기능에 대한 기능 활성화 코드를 기록합니다.

. 섀시 일련 번호, 활성화 식별자 및 기능 활성화를 위한 코드와 같은 정보를 사용하여 스토리지 공급업체에 이메일 또는 텍스트 문서를 보내 기능 키 파일을 요청합니다.
+
로 이동하여 필요한 정보를 입력하여 기능 또는 기능 팩을 구할 수도 http://partnerspfk.netapp.com["NetApp 라이센스 활성화: 스토리지 어레이 프리미엄 기능 활성화"^] 있습니다. (이 사이트의 지침은 기능 팩이 아닌 프리미엄 기능에 대한 것입니다.)

.작업을 마친 후
기능 키 파일이 있는 경우 프리미엄 기능 또는 기능 팩을 활성화할 수 있습니다.

[[IDd96b977a47e9db895982b4b43bfbb762]]
= 프리미엄 기능 지원
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
프리미엄 기능은 활성화를 위한 키가 필요한 추가 옵션입니다.

.시작하기 전에
* 기능 키를 받았습니다. 필요한 경우 기술 지원 부서에 키를 문의하십시오.
* 키 파일을 관리 클라이언트(System Manager 액세스를 위한 브라우저가 있는 시스템)에 로드했습니다.

.이 작업에 대해
이 작업에서는 System Manager를 사용하여 프리미엄 기능을 활성화하는 방법을 설명합니다.

[NOTE]
====
프리미엄 기능을 비활성화하려면 (`disable storageArray) (featurePack |

feature=featureAttributeList`CLI(명령줄 인터페이스)에서 Disable Storage Array Feature(스토리지 배열 기능 사용 안 함) 명령을 사용해야 합니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 추가 기능 * 에서 * 프리미엄 기능 사용 * 을 선택합니다.
+
Premium 기능 사용 대화 상자가 열립니다.

. 찾아보기 * 를 클릭한 다음 키 파일을 선택합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 사용 * 을 클릭합니다.

[[ID45dcab59be20f5bfa9e798a1720151fb]]
= 기능 팩을 활성화합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
기능 팩은 스토리지 배열 속성을 변경하는 번들(예: 프로토콜을 Fibre Channel에서 iSCSI로 변경)입니다. 기능 팩에는 지원을 위한 특수 키가 필요합니다.

.시작하기 전에
* 새 스토리지 배열 속성의 변환 및 준비를 설명하는 적절한 지침을 따랐습니다. 호스트 프로토콜 변환 지침은 해당 컨트롤러 모델의 하드웨어 유지보수 가이드를 참조하십시오.
* 스토리지 배열이 오프라인이므로 호스트 또는 애플리케이션이 이를 액세스하지 않습니다.
* 모든 데이터가 백업됩니다.
* 기능 팩 파일을 받았습니다.
+
기능 팩 파일이 관리 클라이언트(System Manager 액세스를 위한 브라우저가 있는 시스템)에 로드됩니다.

[NOTE]
====
다운타임 유지 관리 창을 예약하고 호스트와 컨트롤러 사이의 모든 I/O 작업을 중지해야 합니다.

또한 변환을 성공적으로 완료할 때까지 스토리지 배열의 데이터에 액세스할 수 없습니다.

====
.이 작업에 대해
이 작업에서는 System Manager를 사용하여 기능 팩을 설정하는 방법에 대해 설명합니다. 작업을 마치면 스토리지 배열을 다시 시작해야 합니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 추가 기능 * 아래에서 * 기능 팩 변경 * 을 선택합니다.
. 찾아보기 * 를 클릭한 다음 키 파일을 선택합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. `change`필드에 입력합니다.
. 변경 * 을 클릭합니다.
+
기능 팩 마이그레이션이 시작되고 컨트롤러가 재부팅됩니다. 기록되지 않은 캐시 데이터가 삭제되어 입출력 작업이 발생하지 않습니다. 두 컨트롤러가 자동으로 재부팅되므로 새로운 기능 팩이 적용됩니다. 재부팅이 완료되면 스토리지 배열이 응답 상태로 돌아갑니다.

:leveloffset: -1

[[ID5ea7a084775da86cf572c3403baa4281]]
= CLI(Command Line Interface) 다운로드
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity System Manager에서 CLI(Command Line Interface) 패키지를 다운로드할 수 있습니다.

CLI는 스토리지 시스템을 구성하고 모니터링하기 위한 텍스트 기반 방법을 제공합니다. https를 통해 통신하며 외부에서 설치된 관리 소프트웨어 패키지에서 사용할 수 있는 CLI와 동일한 구문을 사용합니다. CLI를 다운로드하는 데 키가 필요하지 않습니다.

.시작하기 전에
CLI 명령을 실행하려는 관리 시스템에서 Java Runtime Environment(JRE) 버전 8 이상을

사용할 수 있어야 합니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 추가 기능 * 에서 * 명령줄 인터페이스 * 를 선택합니다.
+
ZIP 패키지가 브라우저로 다운로드됩니다.

. ZIP 파일을 스토리지 배열에 대한 CLI 명령을 실행할 관리 시스템에 저장한 다음 파일의 압축을 풉니다.
+
이제 DOS C: 프롬프트와 같은 운영 체제 프롬프트에서 CLI 명령을 실행할 수 있습니다. CLI 명령 참조는 System Manager 사용자 인터페이스 오른쪽 위의 도움말 메뉴에서 사용할 수 있습니다.

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDb5746b631544eb68de9a2c777fc0149f]]
= 자동 로드 밸런싱이란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-storage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
자동 로드 밸런싱 기능은 자동화된 I/O 밸런싱을 제공하고 호스트에서 들어오는 I/O 트래픽이 두 컨트롤러 간에 동적으로 관리 및 균형 조정되도록 합니다.

자동 로드 밸런싱 기능은 시간이 지남에 따라 로드 변화에 동적으로 반응하여 볼륨 컨트롤러 소유권을 자동으로 조정하여 컨트롤러 간에 워크로드가 이동할 때 발생하는 로드 불균형 문제를 해결하여 I/O 리소스 관리를 향상시킵니다.

각 컨트롤러의 워크로드는 지속적으로 모니터링되며 호스트에 설치된 다중 경로 드라이버의 협력을 통해 필요할 때마다 자동으로 균형을 맞출 수 있습니다. 컨트롤러 간에 워크로드가 자동으로 재조정되면 스토리지 관리자는 스토리지 어레이의 로드 변경을 수용하기 위해 볼륨 컨트롤러 소유권을 수동으로 조정해야 하는 부담을 덜 수 있습니다.

자동 로드 밸런싱이 활성화되면 다음 기능을 수행합니다.

* 컨트롤러 리소스 활용률을 자동으로 모니터링 및 균형 조정
* 필요한 경우 볼륨 컨트롤러 소유권을 자동으로 조정하여 호스트와 스토리지 어레이 간의 I/O 대역폭을 최적화합니다.

[NOTE]
====
컨트롤러의 SSD Cache를 사용하도록 할당된 볼륨은 자동 로드 밸런싱 전송을 지원하지 않습니다.

====

[[IDbcc6615ea2d5451b02e4b6e7543ae581]]
= 컨트롤러 캐시란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
컨트롤러 캐시는 두 가지 유형의 I/O(I/O) 작업, 즉 컨트롤러 및 호스트 간, 컨트롤러 및 디스크 간 작업을 간소화하는 물리적 메모리 공간입니다.

읽기 및 쓰기 데이터 전송의 경우 호스트와 컨트롤러는 고속 연결을 통해 통신합니다. 그러나 디스크가 상대적으로 느린 장치이기 때문에 컨트롤러의 백엔드에서 디스크와의 통신이 느려집니다.

컨트롤러 캐시가 데이터를 수신하면 컨트롤러는 데이터가 현재 보유 중인 호스트 애플리케이션에 확인합니다. 이렇게 하면 호스트 애플리케이션이 I/O가 디스크에 기록될 때까지 기다릴 필요가 없습니다. 대신 응용 프로그램에서 작업을 계속할 수 있습니다. 또한 서버 애플리케이션에서 캐시된 데이터에 쉽게 액세스할 수 있으므로 데이터에 액세스하기 위해 디스크를 추가로 읽을 필요가 없습니다.

컨트롤러 캐시는 다음과 같은 여러 가지 방법으로 스토리지 어레이의 전반적인 성능에 영향을 줍니다.

* 캐시는 버퍼 역할을 하므로 호스트 및 디스크 데이터 전송을 동기화할 필요가 없습니다.
* 호스트의 읽기 또는 쓰기 작업에 대한 데이터가 이전 작업의 캐시에 있을 수 있으므로 디스크를 액세스할 필요가 없습니다.
* 쓰기 캐시를 사용하는 경우 이전 쓰기 작업의 데이터가 디스크에 기록되기 전에 호스트에서 후속 쓰기 명령을 전송할 수 있습니다.
* 캐시 프리페치가 설정된 경우 순차적 읽기 액세스가 최적화됩니다. 캐시 프리페치를 사용하면 디스크에서 데이터를 읽는 대신 캐시에서 데이터를 더 많이 찾을 수 있습니다.

[CAUTION]

```
====
* 데이터 손실 가능성 * -- 배터리 없이 * 쓰기 캐싱 * 옵션을 활성화하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다.

====



[[ID82b55f6ac4ea401a2e9ffa6b527a70b8]]
= 캐시 플러싱이란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
캐시에 기록되지 않은 데이터의 양이 특정 수준에 도달하면 컨트롤러는 캐시된 데이터를 드라이브에 주기적으로 씁니다. 이 쓰기 프로세스를 "플러시"라고 합니다.

컨트롤러는 캐시 플러싱에 두 가지 알고리즘(요구 기반 및 사용 기간 기반)을 사용합니다. 컨트롤러는 캐시된 데이터의 양이 캐시 플러시 임계값 아래로 떨어질 때까지 수요 기반 알고리즘을 사용합니다. 기본적으로 플러시는 캐시의 80%가 사용 중일 때 시작됩니다.

System Manager에서 "Start demand cache flashing" 임계값을 설정하여 사용자 환경에서 사용되는 입출력 유형을 가장 잘 지원할 수 있습니다. 주로 쓰기 작업을 수행하는 환경에서는 "Start demand cache flashing" 비율을 높게 설정하여 새 쓰기 요청을 디스크로 이동하지 않고 캐시로 처리할 수 있는 확률을 높여야 합니다. 백분율 설정은 더 많은 데이터가 캐시에 남아 있도록 캐시 플러시 수를 제한하여 캐시 적중률이 증가할 수 있습니다.

입출력 오류가 발생하는 환경(데이터 급증)에서는 낮은 캐시 플러시를 사용하여 시스템이 데이터 버스트 사이에 캐시를 자주 플러시할 수 있습니다. 다양한 부하를 처리하는 다양한 I/O 환경에서 또는 로드 유형을 알 수 없는 경우 임계값을 양호한 중간 지면으로 50%로 설정합니다. 시작 비율이 80%보다 낮은 경우 호스트 읽기에 필요한 데이터를 사용할 수 없기 때문에 성능이 저하될 수 있습니다. 낮은 비율을 선택하면 캐시 레벨을 유지하는 데 필요한 디스크 쓰기 수도 증가하여 시스템 오버헤드가 증가합니다.

연령 기반 알고리즘은 쓰기 데이터가 디스크에 플러시되기 전에 캐시에 남아 있을 수 있는 기간을 지정합니다. 컨트롤러는 캐시 플러시 임계값에 도달할 때까지 연령 기반 알고리즘을 사용합니다. 기본값은 10초이지만 이 기간은 비활성 기간 동안에만 계산됩니다. System Manager에서 플러시 타이밍을 수정할 수 없습니다. 대신 CLI(Command-Line Interface)에서 * 스토리지 배열 설정 * 명령을 사용해야 합니다.

[CAUTION]
====
* 데이터 손실 가능성 * -- 배터리 없이 * 쓰기 캐싱 * 옵션을 활성화하고 보호를 위한 범용
```

전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다.

====

[[ID94d83c3d4fc6527f9bb7af7dc0cce0d5]]
= 캐시 블록 크기란 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 시스템의 컨트롤러는 캐시를 "블록"으로 구성합니다. 이는 8, 16, 32KiB 크기의 메모리 청크입니다. 스토리지 시스템의 모든 볼륨이 동일한 캐시 공간을 공유하기 때문에 볼륨에 캐시 블록 크기가 하나만 있을 수 있습니다.

애플리케이션은 스토리지 성능에 영향을 미칠 수 있는 다양한 블록 크기를 사용합니다. 기본적으로 System Manager의 블록 크기는 32KiB이지만 값을 8, 16, 32KiB로 설정할 수 있습니다. 파일 시스템 또는 데이터베이스 애플리케이션에 적합한 크기는 더 작습니다. 크기가 클수록 대용량 데이터 전송, 순차 I/O 또는 멀티미디어와 같은 고대역폭이 필요한 응용 프로그램에 적합합니다.

[[IDd5d94346c0c801231fac6343cae75877]]
= 스토리지 배열 클록은 언제 동기화해야 합니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity 시스템 관리자에 표시된 타임스탬프가 관리 클라이언트(브라우저를 통해 SANtricity System Manager에 액세스하는 컴퓨터)에 표시된 타임스탬프와 일치하지 않는 경우 스토리지 배열의 컨트롤러 시계를 수동으로 동기화해야 합니다. 이 작업은 SANtricity System Manager에서 NTP(네트워크 시간 프로토콜)가 활성화되어 있지 않은 경우에만 필요합니다.

[NOTE]
====
시계를 수동으로 동기화하는 대신 NTP 서버를 사용하는 것이 좋습니다. NTP는 SNTP(Simple Network Time Protocol)를 사용하여 외부 서버와 시계를 자동으로 동기화합니다.

====

시스템 페이지에서 사용할 수 있는 스토리지 배열 시계 동기화 대화 상자에서 동기화 상태를 확인할 수 있습니다. 대화 상자에 표시된 시간이 일치하지 않으면 동기화를 실행합니다. 이 대화 상자를 주기적으로 볼 수 있습니다. 이 대화 상자는 컨트롤러 시계의 시간 디스플레이가 서로 분리되어 더 이상 동기화되지 않았음을 나타냅니다.

```
:leveloffset: -1


:leveloffset: -1


= 드라이브 보안

:leveloffset: +1


[[IDf4783c7eff5b214600f3e14f92f725e0]]
= 드라이브 보안 개요
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
보안 키 관리 페이지에서 드라이브 보안 및 키 관리를 구성할 수 있습니다.



== 드라이브 보안이란 무엇입니까?

_Drive Security_ 는 스토리지 어레이에서 제거할 때 보안이 설정된 드라이브의 데이터에 대한 무단 액세스를 방지하는 기능입니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다. FDE 또는 FIPS 드라이브를 어레이에서 물리적으로 제거할 경우, 해당 드라이브가 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 드라이브는 보안 잠금 상태가 됩니다. a_security key_는 이러한 유형의 드라이브와 스토리지 배열의 컨트롤러 간에 공유되는 문자의 문자열입니다.

자세한 내용:

* xref:{relative_path}how-the-drive-security-feature-works.html["드라이브 보안 기능의 작동 방식"]
* xref:{relative_path}how-security-key-management-works.html["보안 키 관리의
```

작동 방식"]
* xref:{relative_path}drive-security-terminology.html["드라이브 보안 용어"]

== 키 관리는 어떻게 구성합니까?

드라이브 보안을 구현하려면 어레이에 FDE 드라이브 또는 FIPS 드라이브가 설치되어 있어야 합니다. 이러한 드라이브의 키 관리를 구성하려면 메뉴 설정 [시스템 > 보안 키 관리]로 이동하여 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 마지막으로 볼륨 설정에서 "보안 가능"을 선택하여 풀 및 볼륨 그룹에 대해 드라이브 보안을 설정합니다.

자세한 내용:

* xref:{relative_path}create-internal-security-key.html["내부 보안 키를 생성합니다"]
* xref:{relative_path}create-external-security-key.html["외부 보안 키를 만듭니다"]
* xref:{relative_path}../sm-storage/create-pool-manually.html["풀을 수동으로 생성합니다"]
* xref:{relative_path}../sm-storage/create-volume-group.html["볼륨 그룹을 생성합니다"]

== 드라이브의 잠금을 해제하려면 어떻게 해야 합니까?

키 관리를 구성한 다음 나중에 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우, 드라이브의 암호화된 데이터에 액세스하려면 보안 키를 새 스토리지 배열에 다시 할당해야 합니다.

자세한 내용:

* xref:{relative_path}unlock-drives-using-an-internal-security-key.html["내부 키 관리 사용 시 드라이브 잠금을 해제합니다"]
* xref:{relative_path}unlock-drives-using-an-external-security-key.html["외부 키 관리 사용 시 드라이브 잠금을 해제합니다"]

== 관련 정보

키 관리와 관련된 작업에 대해 자세히 알아보십시오.

```
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-key-management-server.html["키 관리 서버에서 인증에 CA 서명 인증서를 사용합니다"]
* xref:{relative_path}back-up-security-key.html["보안 키를 백업합니다"]
```

```
= 개념

:leveloffset: +1


[[ID7e432007a1e3f509018bfaace7e2607e]]
= 드라이브 보안 기능의 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다.

이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.



== 드라이브 보안을 구현하는 방법

드라이브 보안을 구현하려면 다음 단계를 수행하십시오.

. 스토리지 어레이에 FDE 드라이브 또는 FIPS 드라이브와 같은 보안 지원 드라이브를 제공합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
. 컨트롤러 및 드라이브에서 읽기/쓰기 액세스를 위해 공유하는 일련의 문자인 보안 키를 생성합니다. 컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 외부 키 관리의 경우 키 관리 서버를 사용하여 인증을 설정해야 합니다.
. 풀 및 볼륨 그룹에 대해 드라이브 보안 설정:
+
** 풀 또는 볼륨 그룹을 생성합니다(후보 테이블의 * Secure-Capable * 열에서 * Yes * 를 찾습니다).
```

** 새 볼륨을 생성할 때 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 * 보안 가능 * 옆에 * 예 * 가 표시됨).

== 드라이브 보안 작동 방식

FDE 또는 FIPS 중 어떤 보안 가능 드라이브도 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이 암호화 및 암호 해독은 성능 또는 사용자 워크플로에 영향을 주지 않습니다. 각 드라이브에는 드라이브에서 전송할 수 없는 고유한 암호화 키가 있습니다.

드라이브 보안 기능은 보안 기능이 있는 드라이브를 통해 추가 보호 계층을 제공합니다. 드라이브 보안을 위해 이러한 드라이브의 볼륨 그룹 또는 풀을 선택한 경우 드라이브는 데이터에 대한 액세스를 허용하기 전에 보안 키를 찾습니다. 드라이브의 기존 데이터에 영향을 주지 않고 언제든지 풀 및 볼륨 그룹에 대해 드라이브 보안을 설정할 수 있습니다. 그러나 드라이브의 모든 데이터를 지우지 않으면 드라이브 보안을 비활성화할 수 없습니다.

== 스토리지 어레이 레벨에서 드라이브 보안이 작동하는 방식

드라이브 보안 기능을 사용하면 스토리지 배열의 보안 지원 드라이브와 컨트롤러 간에 공유되는 보안 키를 만들 수 있습니다. 드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다.

보안 사용 드라이브가 스토리지 어레이에서 제거되어 다른 스토리지 배열에 다시 설치된 경우 드라이브는 보안 잠금 상태가 됩니다. 재배치된 드라이브는 데이터에 다시 액세스하기 전에 보안 키를 찾습니다. 데이터 잠금을 해제하려면 소스 스토리지 어레이에서 보안 키를 적용합니다. 잠금 해제 프로세스가 완료되면 다시 찾은 드라이브가 대상 스토리지 배열에 이미 저장된 보안 키를 사용하며 가져온 보안 키 파일이 더 이상 필요하지 않습니다.

[NOTE]
====
내부 키 관리의 경우 실제 보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 이 형식은 사람이 읽을 수 있는 형식도 아니며 사용자가 액세스할 수도 없습니다.

====

== 드라이브 보안이 볼륨 수준에서 작동하는 방식

보안 가능 드라이브에서 풀 또는 볼륨 그룹을 생성할 때 해당 풀 또는 볼륨 그룹에 대해 드라이브 보안을 설정할 수도 있습니다. Drive Security 옵션을 사용하면 드라이브 및 관련 볼륨 그룹과 풀의 보안이 __enabled_로 설정됩니다.

보안이 설정된 볼륨 그룹 및 풀을 생성하기 전에 다음 지침을 염두에 두십시오.

* 볼륨 그룹 및 풀은 전적으로 보안이 가능한 드라이브로 구성되어야 합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
* 볼륨 그룹 및 풀이 최적의 상태여야 합니다.

[[ID5bf2b560c65e78776fbcb2b7d849aa89]]
= 보안 키 관리의 작동 방식
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
드라이브 보안 기능을 구현하는 경우 FIPS 또는 FDE(Secure-Enabled Drive)에 데이터 액세스를 위한 보안 키가 필요합니다. 보안 키는 이러한 유형의 드라이브와 스토리지 배열의 컨트롤러 사이에서 공유되는 문자의 문자열입니다.

드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다.

다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

* 컨트롤러의 영구 메모리에서 내부 키 관리.
* 외부 키 관리 서버의 외부 키 관리.

== 내부 키 관리

내부 키는 컨트롤러의 영구 메모리에 액세스할 수 없는 위치에 유지되고 "숨김"됩니다. 내부 키 관리를 구현하려면 다음 단계를 수행하십시오.

. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.

. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
. 식별자 및 암호 구문을 정의하는 내부 보안 키를 만듭니다. 식별자는 보안 키와 연결된 문자열이며, 컨트롤러와 키에 연결된 모든 드라이브에 저장됩니다. 암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 내부 키를 만들려면 설정 [시스템 > 보안 키 관리 > 내부 키 만들기] 메뉴로 이동합니다.

보안 키는 컨트롤러에 저장되어 있고 액세스할 수 없는 숨겨진 위치에 있습니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

== 외부 키 관리

외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다. 외부 키 관리를 구현하려면 다음 단계를 수행하십시오.

. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
. 서명된 클라이언트 인증서 파일을 가져옵니다. 클라이언트 인증서가 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP 요청을 신뢰할 수 있습니다.
+
.. 먼저 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 설정 [인증서 > 키 관리 > CSR 완료] 메뉴로 이동합니다.
.. 그런 다음 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다. (CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다.)
.. 클라이언트 인증서 파일이 있는 경우 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.

. 키 관리 서버에서 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트에 해당 파일을 복사합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.
. 키 관리 서버의 IP 주소와 KMIP 통신에 사용되는 포트 번호를 정의하는 데 사용되는 외부 키를 생성합니다. 이 프로세스 중에 인증서 파일도 로드합니다. 외부 키를 만들려면 설정 [시스템 > 보안 키 관리 > 외부 키 만들기] 메뉴로 이동합니다.

입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

```
[[ID3da02ca749d122eb17a0f5f336856fd4]]
= 드라이브 보안 용어
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
드라이브 보안 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명


 a|
드라이브 보안 기능
 a|
드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.


 a|
FDE 드라이브
 a|
FDE(전체 디스크 암호화) 드라이브는 하드웨어 레벨의 디스크 드라이브에서 암호화를 수행합니다. 하드 드라이브에는 쓰기 중에 데이터를 암호화한 다음 읽기 중에 데이터를 해독하는 ASIC 칩이 포함되어 있습니다.


 a|
FIPS 드라이브
 a|
FIPS 드라이브는 FIPS(Federal Information Processing Standards) 140-2 레벨 2를 사용합니다. 이러한 드라이브는 강력한 암호화 알고리즘 및 방법을 보장하는 미국 정부 표준을 준수하는 FDE 드라이브입니다. FIPS 드라이브는 FDE 드라이브보다 보안 표준이 더 높습니다.
```

a|
관리 클라이언트
a|
System Manager 액세스를 위한 브라우저가 포함된 로컬 시스템(컴퓨터, 태블릿 등)

a|
암호 구문
a|
암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 드라이브 마이그레이션 또는 헤드 스왑의 결과로 백업된 보안 키를 가져올 때 보안 키를 암호화하는 데 사용된 것과 동일한 암호를 제공해야 합니다. 암호문은 8자에서 32자 사이여야 합니다.

[NOTE]
====
Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.

====

a|
보안 지원 드라이브
a|
보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있으며, 이 드라이브는 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이러한 드라이브는 드라이브 보안 기능을 사용하여 추가 보안을 위해 사용할 수 있으므로 보안 -_가능_으로 간주됩니다. 드라이브 보안 기능이 이러한 드라이브에 사용된 볼륨 그룹 및 풀에 대해 활성화된 경우 드라이브는 secure-_enabled_가 됩니다.

a|
보안 지원 드라이브
a|
보안 지원 드라이브는 드라이브 보안 기능과 함께 사용됩니다. 드라이브 보안 기능을 활성화한 다음 보안 -_가능_ 드라이브의 풀 또는 볼륨 그룹에 드라이브 보안을 적용하면 드라이브는 보안__-사용__ 상태가 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.

a|
보안 키
a|

보안 키는 스토리지 어레이에서 보안 지원 드라이브와 컨트롤러 간에 공유되는 문자의 문자열입니다. 드라이브 전원을 껐다가 켤 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다. 다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

* 내부 키 관리 -- 컨트롤러의 영구 메모리에 보안 키를 만들고 관리합니다.
* 외부 키 관리 -- 외부 키 관리 서버에 보안 키를 만들고 유지 관리합니다.

a|
보안 키 식별자입니다
a|
보안 키 식별자는 키를 생성하는 동안 보안 키와 연결된 문자열입니다. 식별자는 컨트롤러와 보안 키와 연결된 모든 드라이브에 저장됩니다.

|===

:leveloffset: -1

= 보안 키를 구성합니다

:leveloffset: +1

[[ID35fd84ab8e27092413a6a6fb9bb43ba9]]
= 내부 보안 키를 생성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
드라이브 보안 기능을 사용하려면 스토리지 어레이에서 컨트롤러와 보안 가능 드라이브에서 공유하는 내부 보안 키를 생성해야 합니다. 내부 키는 컨트롤러의 영구 메모리에 유지됩니다.

.시작하기 전에
* 스토리지 배열에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard)

드라이브일 수 있습니다.
* 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.

[NOTE]
====
FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

====
.이 작업에 대해
이 작업에서는 내부 보안 키와 연결할 식별자와 암호를 정의합니다.

[NOTE]
====
Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.

====
.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 내부 키 생성 * 을 선택합니다.
+
아직 보안 키를 생성하지 않은 경우 보안 키 만들기 대화 상자가 열립니다.

. 다음 필드에 정보를 입력합니다.
+
** * 보안 키 식별자 정의 * -- 기본값(컨트롤러 펌웨어에 의해 생성되는 스토리지 배열 이름 및 타임 스탬프)을 그대로 사용하거나 값을 직접 입력할 수 있습니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.
+
[NOTE]
====
입력한 문자열의 양쪽 끝에 추가된 추가 문자가 자동으로 생성됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

====
** * 암호문 정의/암호문 다시 입력 * -- 암호문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
+
*** 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
*** 숫자(하나 이상)
*** !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.

+
[CAUTION]
====
* 나중에 사용할 수 있도록 항목을 기록해 두십시오 *. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터의 잠금을 해제하려면 식별자와 암호를 알아야 합니다.

====
. Create * 를 클릭합니다.
+
보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 실제 키와 함께 암호화된 키 파일이 브라우저에서 다운로드됩니다.

+
[NOTE]
====
다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

====
. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

.결과
이제 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

[NOTE]
====
드라이브 전원을 껐다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안 잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

====
.작업을 마친 후
키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

[[ID96cd89f1c94eb131a81b192ac606c61b]]
= 외부 보안 키를 만듭니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
키 관리 서버에서 드라이브 보안 기능을 사용하려면 스토리지 어레이에서 키 관리 서버와 보안 가능 드라이브가 공유하는 외부 키를 만들어야 합니다.

.시작하기 전에
* 스토리지에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
+
[NOTE]
====
FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

====
* 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
* 스토리지 배열 컨트롤러의 서명된 클라이언트 인증서 파일이 있고, System Manager에 액세스하는 호스트에 해당 파일을 복사했습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.
* 키 관리 서버에서 인증서 파일을 검색한 다음 System Manager에 액세스할 호스트에 해당 파일을 복사해야 합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.
+
[NOTE]
====
서버 인증서에 대한 자세한 내용은 키 관리 서버 설명서를 참조하십시오.

====

.이 작업에 대해
이 작업에서는 키 관리 서버의 IP 주소와 사용하는 포트 번호를 정의한 다음 외부 키 관리를 위해 인증서를 로드합니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 외부 키 생성 * 을 선택합니다.
+
[NOTE]
====
현재 내부 키 관리가 구성되어 있으면 대화 상자가 열리고 외부 키 관리로 전환할지 확인하는 메시지가 표시됩니다.

====
+
외부 보안 키 만들기 대화 상자가 열립니다.

. 키 서버에 연결 * 에서 다음 필드에 정보를 입력합니다.
+
** * 키 관리 서버 주소 * -- 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
** * 키 관리 포트 번호 * -- KMIP 통신에 사용되는 포트 번호를 입력합니다. 키 관리 서버 통신에 사용되는 가장 일반적인 포트 번호는 5696입니다.
+
* 선택 사항: * 백업 키 서버를 구성하려면 * 키 서버 추가 * 를 클릭한 다음 해당 서버의 정보를 입력합니다. 기본 키 서버에 연결할 수 없는 경우 두 번째 키 서버가 사용됩니다. 각 키 서버가 동일한 키 데이터베이스에 액세스할 수 있는지 확인합니다. 그렇지 않으면 어레이에서 오류를 게시하고 백업 서버를 사용할 수 없습니다.

+

NOTE: 한 번에 하나의 키 서버만 사용됩니다. 스토리지 배열이 기본 키 서버에 도달할 수 없는 경우, 스토리지는 백업 키 서버에 접속하게 됩니다. 두 서버 간에 패리티를 유지해야 합니다. 그렇지 않으면 오류가 발생할 수 있습니다.

** * 클라이언트 인증서 선택 * -- 첫 번째 * 찾아보기 * 버튼을 클릭하여 스토리지 배열 컨트롤러의 인증서 파일을 선택합니다.
** * 키 관리 서버의 서버 인증서 선택 * -- 두 번째 * 찾아보기 * 버튼을 클릭하여 키 관리 서버의 인증서 파일을 선택합니다. 키 관리 서버에 대한 루트, 중간 또는 서버 인증서를 선택할 수 있습니다.

. 다음 * 을 클릭합니다.
. Create/Backup Key * 에서 보안을 위해 백업 키를 생성할 수 있습니다.
+
** (권장) 백업 키를 만들려면 확인란을 선택한 상태로 두고 암호를 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
+
*** 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
*** 숫자(하나 이상)
*** !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.

+
[CAUTION]
====
* 나중에 사용할 수 있도록 항목을 기록해 두십시오 *. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터를 잠금 해제하려면 암호를 알아야 합니다.

====
+
** 백업 키를 생성하지 않으려면 확인란을 선택 취소합니다.
+
[CAUTION]
====
외부 키 서버에 액세스할 수 없고 백업 키가 없는 경우 다른 스토리지 어레이로 마이그레이션하면 드라이브의 데이터에 액세스할 수 없게 됩니다. 이 옵션은 System Manager에서 백업 키를 생성하는 유일한 방법입니다.

====

. 마침 * 을 클릭합니다.
+
입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안 키의 복사본이 로컬 시스템에 저장됩니다.

+
[NOTE]
====
다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

====
. 다운로드한 키 파일의 위치와 암호를 기록한 다음 * 닫기 * 를 클릭합니다.
+
외부 키 관리를 위한 추가 링크가 포함된 다음 메시지가 페이지에 표시됩니다.

+
`Current key management method: External`

. 테스트 통신 * 을 선택하여 스토리지 어레이와 키 관리 서버 간의 연결을 테스트합니다.
+
대화 상자에 검사 결과가 표시됩니다.

.결과
외부 키 관리를 사용하도록 설정하면 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

[NOTE]
====
드라이브 전원을 껐다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안

잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

====
.작업을 마친 후
키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

:leveloffset: -1

= 보안 키 관리

:leveloffset: +1

[[ID958b6440ffbe3deb270b085d0c6dffb1]]
= 보안 키를 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
언제든지 보안 키를 새 키로 바꿀 수 있습니다. 회사에서 보안 위반이 발생할 수 있으며 권한이 없는 직원이 드라이브 데이터에 액세스하지 못하도록 하려면 보안 키를 변경해야 할 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 키 변경 * 을 선택합니다.
+
보안 키 변경 대화 상자가 열립니다.

. 다음 필드에 정보를 입력합니다.
+
** * 보안 키 식별자 정의 * --(내부 보안 키에만 해당) 기본값(컨트롤러 펌웨어에 의해 생성되는 스토리지 배열 이름 및 타임스탬프)을 적용하거나 고유한 값을 입력합니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.
+
[NOTE]
====
추가 문자는 자동으로 생성되며 입력하는 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인하는 데 도움이 됩니다.

====

** * 암호문 정의/암호문 다시 입력 * -- 이러한 각 필드에 암호문을 입력합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
+
*** 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
*** 숫자(하나 이상)
*** !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.

. 외부 보안 키의 경우 새 보안 키를 만들 때 이전 보안 키를 삭제하려면 대화 상자 아래쪽에 있는 "현재 보안 키 삭제..." 확인란을 선택합니다.
+
[CAUTION]
====
* 나중에 사용할 수 있도록 항목을 기록해 두십시오. * -- 보안 지원 드라이브를 스토리지 배열에서 이동해야 하는 경우, 드라이브 데이터를 잠금 해제하려면 식별자와 암호를 알아야 합니다.

====
. 변경 * 을 클릭합니다.
+
새 보안 키는 더 이상 유효하지 않은 이전 키를 덮어씁니다.

+
[NOTE]
====
다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

====
. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

.작업을 마친 후
키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

[[IDbcd29c418c28c8377c673561ace7107c]]
= 외부에서 내부 키 관리로 전환합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

외부 키 서버에서 스토리지 배열에 사용되는 내부 방법으로 Drive Security의 관리 방법을 변경할 수 있습니다. 그런 다음 외부 키 관리를 위해 이전에 정의된 보안 키를 내부 키 관리에 사용합니다.

.이 작업에 대해
이 작업에서는 외부 키 관리를 사용하지 않도록 설정하고 새 백업 복사본을 로컬 호스트에 다운로드합니다. 기존 키는 드라이브 보안에 계속 사용되지만 스토리지 시스템에서 내부적으로 관리됩니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 외부 키 관리 비활성화 * 를 선택합니다.
+
외부 키 관리 비활성화 대화 상자가 열립니다.

. 암호 정의/암호 다시 입력 * 에서 키 백업에 대한 암호 구문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
+
** 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
** 숫자(하나 이상)
** !, *, @(하나 이상)와 같은 영숫자 이외의 문자입니다.

+
[CAUTION]
====
나중에 사용할 수 있도록 항목을 기록해 두십시오 _. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터의 잠금을 해제하려면 식별자와 암호를 알아야 합니다.

====
. 비활성화 * 를 클릭합니다.
+
백업 키가 로컬 호스트에 다운로드됩니다.

. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

.결과
이제 드라이브 보안이 스토리지 어레이를 통해 내부적으로 관리됩니다.

.작업을 마친 후
키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

[[IDf9a6912bc061f357713e26b936c5748b]]
= 키 관리 서버 설정을 편집합니다

```
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
외부 키 관리를 구성한 경우 언제든지 키 관리 서버 설정을 보고 편집할 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 키 관리 서버 설정 보기/편집 * 을 선택합니다.
. 다음 필드에서 정보를 편집합니다.
+
** * 키 관리 서버 주소 * -- 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP
주소(IPv4 또는 IPv6)를 입력합니다.
** * 키 관리 포트 번호 * -- KMIP(Key Management Interoperability Protocol)
통신에 사용되는 포트 번호를 입력합니다.
+
* 선택 사항: * 키 서버 추가 * 를 클릭하여 다른 키 서버를 포함할 수 있습니다.



. 저장 * 을 클릭합니다.




[[ID14952faa791078af8b09f73e75edf6ad]]
= 보안 키를 백업합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
보안 키를 만들거나 변경한 후에는 원본이 손상되는 경우에 대비하여 키 파일의 백업 복사본을 만들 수 있습니다.

.이 작업에 대해
이 작업에서는 이전에 만든 보안 키를 백업하는 방법에 대해 설명합니다. 이 절차를 수행하는 동안 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.
```

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 백업 키 * 를 선택합니다.
+
보안 키 백업 대화 상자가 열립니다.

. 암호 구문 정의/암호 구문 다시 입력 * 필드에 이 백업의 암호 구문을 입력하고 확인합니다.
+
값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

+
** 대문자(하나 이상)
** 숫자(하나 이상)
** 영숫자 이외의 문자(예:!, *, @(하나 이상)

+
[CAUTION]
====
* 나중에 사용할 수 있도록 항목을 기록해 두십시오 *. 이 보안 키의 백업에 액세스하려면
암호문이 필요합니다.

====
. 백업 * 을 클릭합니다.
+
보안 키의 백업이 로컬 호스트에 다운로드되고 * 보안 키 백업 확인/기록 * 대화 상자가 열립니다.

+
[NOTE]
====
다운로드한 보안 키 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

====
. 암호를 안전한 위치에 기록한 다음 * 닫기 * 를 클릭합니다.

.작업을 마친 후
백업 보안 키의 유효성을 확인해야 합니다.

[[ID5a11e5d9f57825f019e232d0b27cb70a]]
= 보안 키를 확인합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/

:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
보안 키가 손상되지 않았는지 확인하고 올바른 암호문이 있는지 확인할 수 있습니다.

.이 작업에 대해
이 작업에서는 이전에 만든 보안 키의 유효성을 검사하는 방법을 설명합니다. 이 단계는 키 파일이 손상되지 않고 암호 구문이 올바른지 확인하는 중요한 단계입니다. 이렇게 하면 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 나중에 드라이브 데이터에 액세스할 수 있습니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 키 확인 * 을 선택합니다.
+
보안 키 유효성 검사 대화 상자가 열립니다.

. 찾아보기 * 를 클릭한 다음 키 파일(예:)을 `drivesecurity.slk` 선택합니다.
. 선택한 키와 관련된 암호를 입력합니다.
+
유효한 키 파일과 암호를 선택하면 * Validate * 버튼을 사용할 수 있게 됩니다.

. Validate * 를 클릭합니다.
+
유효성 검사 결과가 대화 상자에 표시됩니다.

. 결과에 "보안 키 유효성 확인 성공"이 표시되면 * 닫기 * 를 클릭합니다. 오류 메시지가 나타나면 대화 상자에 표시되는 권장 지침을 따릅니다.

[[IDc8ac6c47220aaa0c6b0a025be8fe5d4b]]
= 내부 키 관리 사용 시 드라이브 잠금을 해제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
내부 키 관리를 구성한 다음 나중에 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우, 드라이브의 암호화된 데이터에 액세스하려면 보안 키를 새 스토리지 배열에 다시 할당해야 합니다.

.시작하기 전에
* 소스 스토리지(드라이브를 제거할 스토리지)에서 볼륨 그룹을 내보내고 드라이브를 제거했습니다. 대상 어레이에서 드라이브를 다시 설치했습니다.
+

NOTE: 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

+
볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 https://kb.netapp.com/["NetApp 기술 자료"^]참조하십시오. System Manager 또는 기존 시스템에서 관리하는 최신 어레이에 대한 적절한 지침을 따라야 합니다.

* 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
* 잠금을 해제할 드라이브와 연결된 보안 키를 알아야 합니다.
* 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있습니다. 드라이브를 다른 시스템에서 관리하는 스토리지 어레이로 이동하는 경우 보안 키 파일을 해당 관리 클라이언트로 이동해야 합니다.

.이 작업에 대해
내부 키 관리를 사용하면 보안 키가 스토리지 배열에 로컬로 저장됩니다. 보안 키는 읽기/쓰기 액세스를 위해 컨트롤러와 드라이브에서 공유하는 일련의 문자입니다. 드라이브가 어레이에서 물리적으로 제거되어 다른 드라이브에 설치된 경우 올바른 보안 키를 제공할 때까지 드라이브가 작동할 수 없습니다.

[NOTE]
====
컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 이 항목에서는 _INTERNAL_KEY 관리 사용 시 데이터 잠금 해제를 설명합니다. _EXTERNAL_KEY 관리를 사용한 경우 을 참조하십시오link:unlock-drives-using-an-external-security-key.html["외부 키 관리 사용 시 드라이브 잠금을 해제합니다"]. 컨트롤러 업그레이드를 수행하고 모든 컨트롤러를 최신 하드웨어로 교체하는 경우 E-Series 및 SANtricity 설명서 센터의 에 설명된 대로 서로 다른 단계를 수행해야 합니다.link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["드라이브 잠금을 해제합니다"]

====
다른 어레이에 보안 활성 드라이브를 재설치하면 해당 배열이 드라이브를 검색하고 "보안 키 필요" 상태와 함께 "주의 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 선택하고 키에 대한 암호를 입력합니다. (이 암호는 스토리지 배열의 관리자 암호와 같지 않습니다.)

다른 보안 지원 드라이브가 새 스토리지 배열에 설치되어 있는 경우 가져오는 것과 다른 보안 키를 사용할 수 있습니다. 가져오기 프로세스 중에 이전 보안 키는 설치 중인 드라이브의 데이터 잠금을 해제하는 데만 사용됩니다. 잠금 해제 프로세스가 성공하면 새로 설치된 드라이브가 대상 스토리지 배열의 보안 키에 다시 입력됩니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 보안 드라이브 잠금 해제 * 를 선택합니다.
+
보안 드라이브 잠금 해제 대화 상자가 열립니다. 보안 키가 필요한 모든 드라이브가 표에 나와 있습니다.

. * 선택 사항: * 드라이브 번호 위로 마우스를 가져가면 드라이브 위치(쉘프 번호 및 베이 번호)가 표시됩니다.
. 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다.
+
선택한 키 파일이 대화 상자에 나타납니다.

. 이 키 파일과 관련된 암호를 입력합니다.
+
입력한 문자는 마스크됩니다.

. 잠금 해제 * 를 클릭합니다.
+
잠금 해제 작업이 성공하면 대화 상자에 "연결된 보안 드라이브가 잠금 해제되었습니다."라는 메시지가 표시됩니다.

.결과
모든 드라이브가 잠겼다가 잠금 해제되면 스토리지 배열의 각 컨트롤러가 재부팅됩니다. 그러나 대상 스토리지 배열에 이미 일부 잠금 해제된 드라이브가 있는 경우 컨트롤러는 재부팅되지 않습니다.

.작업을 마친 후
이제 대상 배열(새로 설치된 드라이브가 있는 배열)에서 볼륨 그룹을 가져올 수 있습니다.

NOTE: 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 https://kb.netapp.com/["NetApp 기술 자료"^]참조하십시오.

```
[[IDfe5d961817ec9700d6296504120a6eea]]
= 외부 키 관리 사용 시 드라이브 잠금을 해제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
외부 키 관리를 구성한 다음 나중에 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우, 드라이브의 암호화된 데이터에 액세스하려면 보안 키를 새 스토리지 배열에 다시 할당해야 합니다.

.시작하기 전에
* 소스 스토리지(드라이브를 제거할 스토리지)에서 볼륨 그룹을 내보내고 드라이브를 제거했습니다. 대상 어레이에서 드라이브를 다시 설치했습니다.
+

NOTE: 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

+
볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 https://kb.netapp.com/["NetApp 기술 자료"^]참조하십시오. System Manager 또는 기존 시스템에서 관리하는 최신 어레이에 대한 적절한 지침을 따라야 합니다.

* 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
* 키 관리 서버의 IP 주소와 포트 번호를 알고 있어야 합니다.
* 스토리지 배열 컨트롤러의 서명된 클라이언트 인증서 파일이 있고, System Manager에 액세스하는 호스트에 해당 파일을 복사했습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.
* 키 관리 서버에서 인증서 파일을 검색한 다음 System Manager에 액세스할 호스트에 해당 파일을 복사해야 합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.


[NOTE]
====
서버 인증서에 대한 자세한 내용은 키 관리 서버 설명서를 참조하십시오.
```

====
.이 작업에 대해
외부 키 관리를 사용하는 경우 보안 키는 보안 키를 안전하게 보호하도록 설계된 서버에 외부에 저장됩니다. 보안 키는 읽기/쓰기 액세스를 위해 컨트롤러와 드라이브에서 공유하는 일련의 문자입니다. 드라이브가 어레이에서 물리적으로 제거되어 다른 드라이브에 설치된 경우 올바른 보안 키를 제공할 때까지 드라이브가 작동할 수 없습니다.

[NOTE]
====
컨트롤러의 영구 메모리에서 내부 키를 만들거나 키 관리 서버에서 외부 키를 만들 수 있습니다. 이 항목에서는 _EXTERNAL_KEY 관리 사용 시 데이터 잠금 해제를 설명합니다. internal_key 관리를 사용한 경우 를 참조하십시오link:unlock-drives-using-an-internal-security-key.html["내부 키 관리 사용 시 드라이브 잠금을 해제합니다"]. 컨트롤러 업그레이드를 수행하고 모든 컨트롤러를 최신 하드웨어로 교체하는 경우 E-Series 및 SANtricity 설명서 센터의 에 설명된 대로 서로 다른 단계를 수행해야 합니다.link:https://docs.netapp.com/us-en/e-series/upgrade-controllers/upgrade-unlock-drives-task.html["드라이브 잠금을 해제합니다"]

====
다른 어레이에 보안 활성 드라이브를 재설치하면 해당 배열이 드라이브를 검색하고 "보안 키 필요" 상태와 함께 "주의 필요" 상태를 표시합니다. 드라이브 데이터의 잠금을 해제하려면 보안 키 파일을 가져오고 키에 대한 암호를 입력합니다. (이 암호는 스토리지 배열의 관리자 암호와 같지 않습니다.) 이 프로세스 중에 외부 키 관리 서버를 사용하도록 스토리지 배열을 구성하면 보안 키에 액세스할 수 있습니다. 보안 키를 연결 및 검색하려면 스토리지 배열에 대한 서버의 연락처 정보를 제공해야 합니다.

다른 보안 지원 드라이브가 새 스토리지 배열에 설치되어 있는 경우 가져오는 것과 다른 보안 키를 사용할 수 있습니다. 가져오기 프로세스 중에 이전 보안 키는 설치 중인 드라이브의 데이터 잠금을 해제하는 데만 사용됩니다. 잠금 해제 프로세스가 성공하면 새로 설치된 드라이브가 대상 스토리지 배열의 보안 키에 다시 입력됩니다.

.단계
. 설정 [시스템] 메뉴를 선택합니다.
. 보안 키 관리 * 에서 * 외부 키 생성 * 을 선택합니다.
. 필수 연결 정보 및 인증서를 사용하여 마법사를 완료합니다.
. 외부 키 관리 서버에 액세스하려면 * 통신 테스트 * 를 클릭합니다.
. 보안 드라이브 잠금 해제 * 를 선택합니다.
+
보안 드라이브 잠금 해제 대화 상자가 열립니다. 보안 키가 필요한 모든 드라이브가 표에 나와 있습니다.

. * 선택 사항: * 드라이브 번호 위로 마우스를 가져가면 드라이브 위치(쉘프 번호 및 베이 번호)가 표시됩니다.
. 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다.
+
선택한 키 파일이 대화 상자에 나타납니다.

. 이 키 파일과 관련된 암호를 입력합니다.
+
입력한 문자는 마스크됩니다.

. 잠금 해제 * 를 클릭합니다.
+
잠금 해제 작업이 성공하면 대화 상자에 "연결된 보안 드라이브가 잠금 해제되었습니다."라는 메시지가 표시됩니다.

.결과
모든 드라이브가 잠겼다가 잠금 해제되면 스토리지 배열의 각 컨트롤러가 재부팅됩니다. 그러나 대상 스토리지 배열에 이미 일부 잠금 해제된 드라이브가 있는 경우 컨트롤러는 재부팅되지 않습니다.

.작업을 마친 후
이제 대상 배열(새로 설치된 드라이브가 있는 배열)에서 볼륨 그룹을 가져올 수 있습니다.

NOTE: 내보내기/가져오기 기능은 System Manager 사용자 인터페이스에서 지원되지 않습니다. 볼륨 그룹을 다른 스토리지 어레이로 내보내기/가져오려면 CLI(Command Line Interface)를 사용해야 합니다.

볼륨 그룹을 마이그레이션하는 방법에 대한 자세한 지침은 을 https://kb.netapp.com/["NetApp 기술 자료"^]참조하십시오.

:leveloffset: -1

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDb7e1076124c7e85948a665e311cd0d5c]]
= 보안 키를 생성하기 전에 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

보안 키는 스토리지 시스템 내의 컨트롤러 및 보안 지원 드라이브에서 공유됩니다. 스토리지 배열에서 보안 지원 드라이브를 제거하면 보안 키가 무단 액세스로부터 데이터를 보호합니다.

다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

* 컨트롤러의 영구 메모리에서 내부 키 관리.
* 외부 키 관리 서버의 외부 키 관리.

== 내부 키 관리

내부 키는 컨트롤러의 영구 메모리에 액세스할 수 없는 위치에 유지되고 "숨김"됩니다. 내부 보안 키를 생성하기 전에 다음을 수행해야 합니다.

. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.

그런 다음 식별자 및 암호 구문을 정의하는 내부 보안 키를 만들 수 있습니다. 식별자는 보안 키와 연결된 문자열이며, 컨트롤러와 키에 연결된 모든 드라이브에 저장됩니다. 암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 작업을 마치면 보안 키가 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

== 외부 키 관리

외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다. 외부 보안 키를 만들기 전에 다음을 수행해야 합니다.

. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
. 서명된 클라이언트 인증서 파일을 가져옵니다. 클라이언트 인증서가 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP 요청을 신뢰할 수 있습니다.
+
.. 먼저 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 설정 [인증서 > 키 관리 > CSR 완료] 메뉴로 이동합니다.
.. 그런 다음 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다.

(다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다.)
.. 클라이언트 인증서 파일이 있는 경우 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.

. 키 관리 서버에서 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트에 해당 파일을 복사합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.

그런 다음 외부 키를 생성하여 키 관리 서버의 IP 주소와 KMIP 통신에 사용되는 포트 번호를 정의할 수 있습니다. 이 프로세스 중에 인증서 파일도 로드합니다. 작업을 마치면 입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

[[ID68e06d7f7c89b03aec3713af9d93d3ed]]
= 암호문을 정의해야 하는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
암호 구문은 로컬 관리 클라이언트에 저장된 보안 키 파일을 암호화하고 해독하는 데 사용됩니다. 암호 구문이 없으면 보안 키를 해독할 수 없으며 다른 스토리지 배열에 다시 설치한 경우 보안 활성 드라이브에서 데이터의 잠금을 해제하는 데 사용할 수 없습니다.

[[ID32a69649fee2b93d57cebe6e9952399a]]
= 보안 키 정보를 기록하는 것이 중요한 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
보안 키 정보가 손실되고 백업이 없는 경우, 보안 지원 드라이브를 재배치하거나 컨트롤러를 업그레이드할 때 데이터가 손실될 수 있습니다. 드라이브에서 데이터를 잠금 해제하려면 보안 키가 필요합니다.

보안 키 식별자, 연결된 암호 구문 및 보안 키 파일이 저장된 로컬 호스트의 위치를 기록해야 합니다.

[[ID2324d20ceef2b4acc5e36e831fccf317]]
= 보안 키를 백업하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
원래 보안 키가 손상되고 백업이 없는 경우, 한 스토리지 어레이에서 다른 스토리지 어레이로 마이그레이션할 경우 드라이브의 데이터에 액세스할 수 없게 됩니다.

보안 키를 백업하기 전에 다음 지침을 염두에 두십시오.

* 원본 키 파일의 보안 키 식별자 및 암호를 알고 있어야 합니다.
+
[NOTE]
====
내부 키만 식별자를 사용합니다. 식별자를 만들면 추가 문자가 자동으로 생성되고 식별자 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

====
* 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.
+
[NOTE]
====
드라이브 보안의 암호를 스토리지 배열의 관리자 암호와 혼동해서는 안 됩니다. Drive Security의 암호 구문은 보안 키의 백업을 보호합니다. 관리자 암호를 사용하면 전체 스토리지 시스템이 무단으로 액세스하지 못하도록 보호할 수 있습니다.

====
* 백업 보안 키 파일이 관리 클라이언트에 다운로드됩니다. 다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다. 보안 키 정보가 저장된 위치를 기록해 두십시오.

[[IDa515a6506e6525a65ca12e0aad3b1faf]]
= 보안 드라이브를 잠금 해제하기 전에 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:icons: font

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
보안 지원 드라이브에서 데이터의 잠금을 해제하려면 해당 보안 키를 가져와야 합니다.

보안 지원 드라이브를 잠금 해제하기 전에 다음 지침을 염두에 두십시오.

* 스토리지 배열에 이미 보안 키가 있어야 합니다. 마이그레이션된 드라이브는 대상 스토리지 배열에 다시 연결됩니다.
* 마이그레이션하는 드라이브의 경우 보안 키 식별자와 보안 키 파일에 해당하는 암호 구문을 알아야 합니다.
* 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있어야 합니다.
* 잠긴 NVMe 드라이브를 재설정하는 경우 드라이브의 보안 ID를 입력해야 합니다. 보안 ID를 찾으려면 드라이브를 물리적으로 제거하고 드라이브 레이블에서 PSID 문자열(최대 32자)을 찾아야 합니다. 작업을 시작하기 전에 드라이브를 다시 설치해야 합니다.




[[ID0c7837d8a972fc5c6260d1c587be079f]]
= 읽기/쓰기 접근성이란 무엇입니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
드라이브 설정 창에는 드라이브 보안 속성에 대한 정보가 포함되어 있습니다. "읽기/쓰기 액세스 가능"은 드라이브의 데이터가 잠겨 있는지 여부를 표시하는 속성 중 하나입니다.

드라이브 보안 속성을 보려면 하드웨어 페이지로 이동합니다. 드라이브를 선택하고 * 설정 보기 * 를 클릭한 다음 * 추가 설정 표시 * 를 클릭합니다. 드라이브의 잠금이 해제될 때 페이지 하단에서 읽기/쓰기 액세스 가능 속성 값은 * 예 * 입니다. 읽기/쓰기 액세스 가능 속성 값은 드라이브가 잠겨 있을 때 * 아니오, 유효하지 않은 보안 키 * 입니다. 보안 키를 가져와 보안 드라이브의 잠금을 해제할 수 있습니다(설정 [시스템 > 보안 드라이브 잠금 해제] 메뉴로 이동).



[[ID902d173f3cdda7e221ebdae9fb5ef26c]]
= 보안 키 유효성 검사에 대해 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
```

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
보안 키를 만든 후에는 키 파일이 손상되지 않았는지 확인해야 합니다.

유효성 검사에 실패하면 다음을 수행합니다.

* 보안 키 식별자가 컨트롤러의 식별자와 일치하지 않는 경우 올바른 보안 키 파일을 찾은 다음 확인을 다시 시도하십시오.
* 컨트롤러가 유효성 검사를 위해 보안 키를 해독할 수 없는 경우 암호 구문을 잘못 입력했을 수 있습니다. 암호를 다시 확인하고 필요한 경우 다시 입력한 다음 확인을 다시 시도하십시오. 오류 메시지가 다시 나타나면 키 파일의 백업을 선택하고(있는 경우) 유효성 검사를 다시 시도하십시오.
* 여전히 보안 키의 유효성을 검사할 수 없는 경우 원본 파일이 손상되었을 수 있습니다. 키의 새 백업을 생성하고 해당 복사본을 확인합니다.

```
[[ID40096fa0c33a0c5aa3971589b44d6553]]
```
= 내부 보안 키와 외부 보안 키 관리의 차이점은 무엇입니까?
```
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
드라이브 보안 기능을 구현할 때 스토리지 배열에서 보안 지원 드라이브를 제거할 때 내부 보안 키 또는 외부 보안 키를 사용하여 데이터를 잠글 수 있습니다.

보안 키는 문자열을 말합니다. 이 문자열은 스토리지 어레이에서 보안이 설정된 드라이브와 컨트롤러 간에 공유됩니다. 내부 키는 컨트롤러의 영구 메모리에 유지됩니다. 외부 키는 KMIP(Key Management Interoperability Protocol)를 사용하여 별도의 키 관리 서버에 유지됩니다.

```
:leveloffset: -1


:leveloffset: -1


```
= 액세스 관리
```
:leveloffset: +1
```

```
[[IDfb8d5ca2e036faa976bd4d234d85e982]]
= 액세스 관리 개요
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
액세스 관리는 SANtricity 시스템 관리자에서 사용자 인증을 설정하는 방법입니다.



== 어떤 인증 방법을 사용할 수 있습니까?

인증 방법에는 RBAC(역할 기반 액세스 제어), 디렉터리 서비스 및 SAML(Security Assertion Markup Language)이 포함됩니다.

* * RBAC/로컬 사용자 역할 * -- 스토리지 어레이에 적용된 RBAC 기능을 통해 인증이 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다.
* * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다.
* * SAML * -- 인증은 SAML 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다.


자세한 내용:

* xref:{relative_path}how-access-management-works.html["액세스 관리 작동 방식"]
* xref:{relative_path}access-management-terminology.html["Access Management(액세스 관리) 용어"]
* xref:{relative_path}permissions-for-mapped-roles.html["매핑된 역할에 대한 권한"]
* xref:{relative_path}access-management-with-local-user-roles.html["로컬 사용자 역할"]
* xref:{relative_path}access-management-with-directory-services.html["디렉터리 서비스"]
* xref:{relative_path}access-management-with-saml.html["SAML"]



== 인증을 구성하려면 어떻게 합니까?
```

스토리지 어레이는 RBAC 기능이 구현된 로컬 사용자 역할을 사용하도록 사전 구성되어 있습니다. 다른 방법을 구성하려면 설정 [Access Management] 메뉴로 이동합니다.

자세한 내용:

* xref:{relative_path}add-directory-server.html["LDAP 디렉토리 서버를 추가합니다"]
* xref:{relative_path}configure-saml.html["SAML를 구성합니다"]

== 관련 정보

액세스 관리 관련 작업에 대해 자세히 알아보십시오.

* xref:{relative_path}change-passwords.html["암호를 변경합니다"]
* xref:{relative_path}view-audit-log-activity.html["감사 로그 활동을 봅니다"]
* xref:{relative_path}configure-syslog-server-for-audit-logs.html["감사 로그를 위해 syslog 서버를 구성합니다"]

= 개념

:leveloffset: +1

[[IDe1e9735a29ccac00c1f159d147faf2e3]]
= 액세스 관리 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리는 SANtricity 시스템 관리자에서 사용자 인증을 설정하는 방법입니다.

구성 및 사용자 인증은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.
+
[NOTE]

====
처음 로그인하는 경우 사용자 이름이 `admin` 자동으로 표시되며 변경할 수 없습니다. `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 사용자 인터페이스에서 Access Management(액세스 관리)로 이동합니다. 스토리지 어레이는 RBAC(역할 기반 액세스 제어) 기능을 구현하는 로컬 사용자 역할을 사용하도록 사전 구성됩니다.
. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
+
** * 로컬 사용자 역할 * -- 스토리지 어레이에 적용된 RBAC 기능을 통해 인증이 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다. 관리자는 이러한 로컬 사용자 역할을 단일 인증 방법으로 사용하거나 디렉터리 서비스와 함께 사용할 수 있습니다. 사용자 암호 설정 이외의 구성은 필요하지 않습니다.
** * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다. 관리자는 LDAP 서버에 연결한 다음 LDAP 사용자를 스토리지 배열에 포함된 로컬 사용자 역할에 매핑합니다.
** * SAML * -- 인증은 SAML(Security Assertion Markup Language) 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다. 관리자는 IdP 시스템과 스토리지 어레이 간의 통신을 설정한 다음 IdP 사용자를 스토리지 어레이에 포함된 로컬 사용자 역할에 매핑합니다.

. 관리자는 사용자에게 System Manager에 대한 로그인 자격 증명을 제공합니다.
. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다.
+
[NOTE]
====
SAML 및 SSO(Single Sign-On)로 인증이 관리되는 경우 시스템은 System Manager 로그인 대화 상자를 건너뛸 수 있습니다.

====
+
로그인 중에 시스템은 다음과 같은 백그라운드 작업을 수행합니다.

+
** 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
** 할당된 역할에 따라 사용자의 권한을 결정합니다.
** 사용자에게 사용자 인터페이스의 작업에 대한 액세스 권한을 제공합니다.
** 인터페이스의 오른쪽 위에 사용자 이름을 표시합니다.

== System Manager에서 사용 가능한 작업

작업에 대한 액세스 권한은 사용자가 할당한 역할에 따라 다르며, 여기에는 다음이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용할 수 없는 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다. 예를 들어 Monitor 역할을 가진 사용자는 볼륨에 대한 모든 정보를 볼 수 있지만 해당 볼륨을 수정하기 위한 기능에는 액세스할 수 없습니다. Copy Services * 및 * Add to Workload * 와 같은 기능에 대한 탭은 회색으로 표시되고 * View/Edit Settings * 만 사용할 수 있습니다.

== Unified Manager 및 Storage Manager의 제한 사항

스토리지에 대해 SAML이 구성된 경우 사용자는 Unified Manager 또는 기존 Storage Manager 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

로컬 사용자 역할 및 디렉터리 서비스가 구성된 경우 사용자는 다음 기능을 수행하기 전에 자격 증명을 입력해야 합니다.

* 스토리지 배열의 이름을 바꿉니다
* 컨트롤러 펌웨어 업그레이드 중
* 스토리지 배열 구성을 로드하는 중입니다
* 스크립트 실행
* 사용하지 않는 세션이 시간 초과된 경우 활성 작업을 수행하려고 합니다

[[ID07a6a45273bcdef94a5f29637d8de1ba]]
= Access Management(액세스 관리) 용어
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

액세스 관리 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

```
[cols="25h,~"]
|===
| 기간 | 설명


 a|
액세스 토큰
 a|
액세스 토큰은 사용자 이름과 암호 대신 REST API 또는 CLI(Command Line Interface)를 사용하여 인증하는 데 사용됩니다. 토큰은 특정 사용자(LDAP 사용자 포함)에 연결되며 권한 집합 및 만료가 포함됩니다.



 a|
Active Directory를 클릭합니다
 a|
AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.



 a|
바인딩
 a|
바인딩 작업은 클라이언트를 디렉토리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명이 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.



 a|
CA
 a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.



 a|
인증서
 a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.
```

a|
IDP
a|
IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.

a|
LDAP를 지원합니다
a|
LDAP(Lightweight Directory Access Protocol)는 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하면 다양한 응용 프로그램 및 서비스를 LDAP 서버에 연결하여 사용자의 유효성을 검사할 수 있습니다.

a|
RBAC
a|
역할 기반 액세스 제어(RBAC)는 개별 사용자의 역할에 따라 컴퓨터 또는 네트워크 리소스에 대한 액세스를 제어하는 방법입니다. RBAC 제어는 스토리지 어레이에 적용되고 사전 정의된 역할을 포함합니다.

a|
SAML
a|
SAML(Security Assertion Markup Language)은 두 개체 간의 인증 및 승인을 위한 XML 기반 표준입니다. SAML을 사용하면 다중 요소 인증을 수행할 수 있습니다. 사용자는 ID를 입증하기 위해 두 개 이상의 항목(예: 암호 및 지문)을 제공해야 합니다. 스토리지에 포함된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.

a|
SP
a|
서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다.

```
 a|
SSO
 a|
SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

|===



[[IDf89b75c92af62bfdf029bda14ab967f1]]
= 매핑된 역할에 대한 권한
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자 프로필이 포함됩니다. 각 역할에는 SANtricity 시스템 관리자의 작업에 액세스할 수 있는 권한이 포함되어 있습니다.

사용자 프로필 및 매핑된 역할은 System Manager의 사용자 인터페이스에서 설정 [액세스 관리 > 로컬 사용자 역할] 메뉴에서 액세스할 수 있습니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

* * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.


사용자에게 특정 작업에 대한 권한이 없는 경우 해당 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.
```

```
[[ID879e268c060146b12c7e00a86e239b6f]]
= 로컬 사용자 역할을 사용하여 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
액세스 관리의 경우 관리자는 스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.



== 구성 워크플로우

로컬 사용자 역할은 스토리지에 대해 사전 구성됩니다. 로컬 사용자 역할을 인증에 사용하려면 관리자가 다음을 수행할 수 있습니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 사용자 프로파일을 검토합니다. 사용자 프로필은 미리 정의되어 있으며 수정할 수 없습니다.
. 필요에 따라 관리자는 각 사용자 프로필에 대해 새 암호를 할당합니다.
. 사용자는 할당된 자격 증명을 사용하여 시스템에 로그인합니다.



== 관리

인증에 로컬 사용자 역할만 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 암호를 변경합니다.
* 암호의 최소 길이를 설정합니다.
* 사용자가 암호 없이 로그인할 수 있도록 허용합니다.



[[ID8ac800e5a9cf860b81c0fc19924d06c6]]
```

= 디렉토리 서비스를 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리의 경우 관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉토리 서비스를 사용할 수 있습니다.

== 구성 워크플로우

네트워크에서 LDAP 서버 및 디렉토리 서비스를 사용하는 경우 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 LDAP 서버에 대한 구성 설정을 입력합니다. 설정에는 도메인 이름, URL 및 바인딩 계정 정보가 포함됩니다.
. LDAP 서버가 보안 프로토콜(LDAPS)을 사용하는 경우 관리자는 LDAP 서버와 스토리지 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
. 서버 연결이 설정되면 관리자는 사용자 그룹을 스토리지 시스템의 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
. 관리자는 LDAP 서버와 스토리지 시스템 간의 연결을 테스트합니다.
. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 디렉터리 서비스를 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 디렉토리 서버를 추가합니다.
* 디렉토리 서버 설정을 편집합니다.
* LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
* 디렉토리 서버를 제거합니다.

```
[[IDd9ecd8f75855605ba78d26dd083c9a5e]]
= SAML을 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Access Management의 경우 관리자는 스토리지에 포함된 SAML(Security Assertion
Markup Language) 2.0 기능을 사용할 수 있습니다.



== 구성 워크플로우

SAML 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에
로그인합니다.
+
[NOTE]
====
 `admin`사용자는 System Manager의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 액세스 관리 아래의 * SAML * 탭으로 이동합니다.
. 관리자는 ID 공급자(IDP)와의 통신을 구성합니다. IDP는 사용자의 자격 증명을 요청하고
사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 스토리지 어레이와의
통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 System
Manager를 사용하여 파일을 스토리지 어레이에 업로드합니다.
. 관리자는 서비스 공급자와 IDP 간의 신뢰 관계를 설정합니다. 서비스 공급자는 사용자 인증을
제어합니다. 이 경우 스토리지 배열의 컨트롤러는 서비스 공급자 역할을 합니다. 통신을 구성하기
위해 관리자는 System Manager를 사용하여 각 컨트롤러에 대한 서비스 공급자 메타데이터 파일을
내보냅니다. 그런 다음 관리자는 IDP 시스템에서 해당 메타데이터 파일을 IDP로 가져옵니다.
+
[NOTE]
====
또한 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하는지 확인해야 합니다.

====
. 관리자는 스토리지 어레이의 역할을 IDP에 정의된 사용자 속성에 매핑합니다. 이렇게 하려면
관리자가 System Manager를 사용하여 매핑을 생성합니다.
. 관리자는 IDP URL에 대한 SSO 로그인을 테스트합니다. 이 테스트는 스토리지 배열 및 IDP가
통신할 수 있도록 보장합니다.
```

+
[CAUTION]
====
SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
. System Manager에서 관리자는 스토리지 배열에 대해 SAML을 활성화합니다.
. 사용자는 SSO 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 SAML을 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 새 역할 매핑을 수정하거나 작성합니다
* 서비스 공급자 파일을 내보냅니다

== 액세스 제한

SAML이 활성화된 경우 사용자는 Unified Manager 또는 기존 Storage Manager 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

또한 다음 클라이언트는 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

* 엔터프라이즈 관리 창(EMW)
* CLI(Command-Line Interface)
* SDK(소프트웨어 개발자 키트) 클라이언트
* 대역내 클라이언트
* HTTP 기본 인증 REST API 클라이언트
* 표준 REST API 끝점을 사용하여 로그인합니다

[[IDcae49ebe5e5309cc68fe29d0c90b45e4]]
= 액세스 토큰
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 토큰은 사용자 이름과 암호를 노출하지 않고 REST API 또는 CLI(Command Line Interface)를 사용하여 인증 방법을 제공합니다. 토큰은 특정 사용자(LDAP 사용자 포함)에 연결되며 권한 집합 및 만료가 포함됩니다.

== SAML 및 JSON 웹 토큰 액세스

기본적으로 SAML이 활성화된 시스템은 기존 명령줄 도구에 대한 액세스를 허용하지 않습니다. MFA 워크플로우에서 인증을 위해 ID 공급자 서버로 리디렉션해야 하므로 REST API 및 CLI가 효과적으로 작동하지 않습니다. 따라서 사용자는 MFA를 통해 인증을 받아야 하는 토큰을 System Manager에서 생성해야 합니다.

NOTE: SAML이 웹 토큰을 사용하도록 설정할 필요는 없지만 최고 수준의 보안을 위해 SAML이 권장됩니다.

== 토큰 생성 및 사용 워크플로

. System Manager에서 토큰을 생성하고 해당 만료일을 확인합니다.
. 토큰 텍스트를 클립보드에 복사하거나 파일로 다운로드한 다음 안전한 위치에 토큰 텍스트를 저장합니다.
. 다음과 같이 토큰을 사용합니다.
+
** * REST API *: REST API 요청에서 토큰을 사용하려면 요청에 HTTP 헤더를 추가하십시오. 예를 들면 다음과 같습니다.
`Authorization: Bearer _<access-token-value>_`
** * Secure CLI *: CLI에서 토큰을 사용하려면 명령줄에 토큰 값을 추가하거나 토큰 값이 포함된 파일의 경로를 사용합니다. 예를 들면 다음과 같습니다.
+
*** 명령줄의 토큰 값: `-t _access-token-value_`
*** 토큰 값이 포함된 파일의 경로: `-T _access-token-file_`

자세한 내용:

* xref:{relative_path}access-management-tokens-create.html["액세스 토큰을 생성합니다"]

```
* xref:{relative_path}access-management-tokens-edit.html["액세스 토큰을
편집합니다"]
* xref:{relative_path}access-management-tokens-revoke.html["액세스 토큰을
취소합니다"]




:leveloffset: -1


= 로컬 사용자 역할을 사용합니다

:leveloffset: +1


[[ID8899b7cc1f49bb45251247e7883916c3]]
= 로컬 사용자 역할을 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
로컬 사용자 역할 탭에서 사용자 프로필의 매핑을 기본 역할에 표시할 수 있습니다. 이러한 매핑은
스토리지 어레이에서 적용되는 RBAC(역할 기반 액세스 제어)의 일부입니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access
Management 기능이 나타나지 않습니다.

.이 작업에 대해
사용자 프로파일과 매핑은 변경할 수 없습니다. 암호만 수정할 수 있습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
+
사용자 프로파일이 표에 표시됩니다.

+
** * 루트 관리자 * (admin) -- 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이
사용자 프로필에는 모든 역할이 포함되어 있습니다.
** * 스토리지 관리자 * (스토리지) -- 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자
프로필에는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다.
```

** * 보안 관리자 * (보안) -- 액세스 관리, 인증서 관리 및 보안 활성화 드라이브 기능을 비롯한 보안 구성을 담당하는 사용자입니다. 이 사용자 프로필에는 보안 관리 및 모니터 역할이 포함되어 있습니다.
** * 지원 관리자 * (지원) -- 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자 프로필에는 지원 관리자 및 모니터 역할이 포함되어 있습니다.
** * 모니터 * (모니터) -- 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자 프로필에는 Monitor 역할만 포함됩니다.

[[IDc19544e7055919b342d33a9351393587]]
= 암호를 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management에서 각 사용자 프로필에 대한 사용자 암호를 변경할 수 있습니다.

.시작하기 전에
* 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
* 로컬 관리자 암호를 알아야 합니다.

.이 작업에 대해
암호를 선택할 때는 다음 지침을 염두에 두십시오.

* 새 로컬 사용자 암호는 최소 암호(보기/편집 설정)에 대한 현재 설정을 충족하거나 초과해야 합니다.
* 암호는 대/소문자를 구분합니다.
* 후행 공백이 설정된 경우 암호에서 제거되지는 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
* 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

[NOTE]
====
System Manager에서 암호를 변경하면 CLI(Command Line Interface)에서도 암호가 변경됩니다. 또한 암호를 변경하면 사용자의 활성 세션이 종료됩니다.

====

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 테이블에서 사용자를 선택합니다.
+
암호 변경 단추를 사용할 수 있게 됩니다.

. 암호 변경 * 을 선택합니다.
+
암호 변경 대화 상자가 열립니다.

. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 선택한 사용자가 스토리지 배열에 액세스하기 위해 암호를 입력하도록 확인란을 선택한 다음 선택한 사용자의 새 암호를 입력할 수 있습니다.
. 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

.결과
사용자가 현재 로그인한 경우 암호 변경으로 인해 사용자의 활성 세션이 종료됩니다.

[[ID282bf98d2a064fa87386365629f1cc15]]
= 로컬 사용자 암호 설정을 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 배열의 새 로컬 사용자 암호 또는 업데이트된 로컬 사용자 암호의 최소 길이를 설정할 수 있습니다. 또한 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 허용할 수 있습니다.

.시작하기 전에
루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.

.이 작업에 대해
로컬 사용자 암호의 최소 길이를 설정할 때는 다음 지침을 염두에 두십시오.

* 설정을 변경해도 기존 로컬 사용자 암호에는 영향을 주지 않습니다.
* 로컬 사용자 암호에 필요한 최소 길이 설정은 0자에서 30자 사이여야 합니다.
* 새 로컬 사용자 암호는 현재 최소 길이 설정을 충족하거나 초과해야 합니다.
* 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 하려면 암호의 최소 길이를 설정하지 마십시오.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 설정 보기/편집 * 버튼을 선택합니다.
+
로컬 사용자 암호 설정 대화 상자가 열립니다.

. 다음 중 하나를 수행합니다.
+
** 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스할 수 있도록 하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란의 선택을 취소합니다.
** 모든 로컬 사용자 암호에 대해 최소 암호 길이를 설정하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란을 선택한 다음 spinner 상자를 사용하여 모든 로컬 사용자 암호에 필요한 최소 길이를 설정합니다.
+
새 로컬 사용자 암호는 현재 설정을 충족하거나 초과해야 합니다.

. 저장 * 을 클릭합니다.

:leveloffset: -1

= 디렉토리 서비스를 사용합니다

:leveloffset: +1

[[IDa7b4df30bc7358f36a145228114ce8af]]
= LDAP 디렉토리 서버를 추가합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리에 대한 인증을 구성하려면 스토리지 어레이와 LDAP 서버 간의 통신을 설정한 다음 LDAP 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

.이 작업에 대해
디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관에서 서명한 경우 인증을 위한 CA 인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명이 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 그런 다음 LDAP 서버의 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑합니다.

[NOTE]
====
LDAP 서버를 추가하는 절차 중에는 레거시 관리 인터페이스가 비활성화됩니다. 기존 관리 인터페이스(symbol)는 스토리지 배열과 관리 클라이언트 간의 통신 방법입니다. 이 기능을 해제하면 스토리지 어레이와 관리 클라이언트에서 더욱 안전한 통신 방법(https를 통한 REST API)을 사용합니다.

====
.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 디렉터리 서비스 탭에서 * 디렉터리 서버 추가 * 를 선택합니다.
+
디렉토리 서버 추가 대화 상자가 열립니다.

. 서버 설정 탭에서 LDAP 서버의 자격 증명을 입력합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 구성 설정 *

 a|

도메인

a|
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.

a|
서버 URL입니다

a|
LDAP 서버에 액세스하기 위한 URL을 의 형식으로 `ldap[s]://*host*:*port*` 입력합니다.

a|
인증서 업로드(선택 사항)

a|

NOTE: 이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.

찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.

a|
BIND ACCOUNT(선택 사항)

a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어 바인딩 사용자가 "bindacct"라고 하는 경우 "CN=bindacct, CN=Users, DC=CPoC, DC=local"과 같은 값을 입력할 수 있습니다.

a|
바인딩 암호(선택 사항)

a|

NOTE: 이 필드는 위에 바인딩 계정을 입력할 때 나타납니다.

바인딩 계정의 암호를 입력합니다.

a|
추가하기 전에 서버 연결을 테스트합니다

a|
스토리지 배열이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다. 이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.

a|
** 권한 설정**

a|
검색 기준 DN
a|
사용자를 검색할 LDAP 컨텍스트를 입력합니다(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`).

a|
사용자 이름 특성입니다
a|
인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들면 다음과 `sAMAccountName`같습니다.

a|
그룹 속성
a|
그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들면 다음과 `memberOf, managedObjects`같습니다.

|===
====
. [역할 매핑]** 탭을 클릭합니다.
. 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 매핑 *

a|
그룹 DN
a|
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다

a|
역할
a|
필드를 클릭하고 그룹 DN에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity 시스템 관리자에 로그인하려면 모니터 역할이 다른 역할과 함께 필요합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+
[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

====
. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 매핑을 마쳤으면 * 추가 * 를 클릭합니다.
+
시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

```
[[IDc21b062ffb5834e9a9caa5214cec06d9]]
= 디렉토리 서버 설정 및 역할 매핑을 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
이전에 Access Management에서 디렉터리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수 있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 디렉토리 서버를 정의해야 합니다.


.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 디렉터리 서비스 * 탭을 선택합니다.
. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
. 설정 보기/편집 * 을 선택합니다.
+
Directory Server Settings(디렉터리 서버 설정) 대화 상자가 열립니다.

. 서버 설정 탭에서 원하는 설정을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명


 a|
* 구성 설정 *



 a|
```

도메인
a|
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.

a|
서버 URL입니다
a|
의 형식으로 LDAP 서버에 액세스하기 위한 URL `ldap[s]://host:port`입니다.

a|
BIND ACCOUNT(선택 사항)
a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.

a|
바인딩 암호(선택 사항)
a|
바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)

a|
저장하기 전에 서버 연결을 테스트합니다
a|
스토리지 배열이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 이 테스트는 대화 상자 아래쪽에 있는 * Save * 를 클릭하면 발생합니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 다시 편집할 수 있습니다.

a|
* 권한 설정 *

a|
검색 기준 DN
a|

사용자를 검색하는 LDAP 컨텍스트(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`)

a|
사용자 이름 특성입니다
a|
인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들면 다음과 `sAMAccountName`같습니다.

a|
그룹 속성
a|
그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들면 다음과 `memberOf, managedObjects`같습니다.

|===
====
. 역할 매핑 탭에서 원하는 매핑을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 매핑 *

a|
그룹 DN
a|
매핑할 LDAP 사용자 그룹의 도메인 이름입니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다

a|
역할
a|
그룹 DN에 매핑할 스토리지 시스템의 역할입니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity 시스템 관리자에 로그인하려면 모니터 역할이 다른 역할과 함께

필요합니다. 스토리지 시스템의 역할은 다음과 같습니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+
[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

====
. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.

.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

[[ID5c0fd8775f0020d8ae9aac4b90bdad68]]
= 디렉토리 서버를 제거합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
디렉토리 서버와 스토리지 시스템 간의 접속을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access

Management 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 디렉터리 서비스 * 탭을 선택합니다.
. 목록에서 삭제할 디렉토리 서버를 선택합니다.
. 제거 * 를 클릭합니다.
+
디렉터리 서버 제거 대화 상자가 열립니다.

. 필드에 입력한 `remove` 다음 * 제거 * 를 클릭합니다.
+
디렉토리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.

:leveloffset: -1

= SAML을 사용합니다

:leveloffset: +1

[[ID109ba9e88b1dba8b4cd4e3527559b31d]]
= SAML를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리에 대한 인증을 구성하려면 스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용할 수 있습니다. 이 구성은 ID 공급자와 스토리지 공급자 간의 연결을 설정합니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

* 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알아야 합니다.
* IDP 관리자가 IDP 시스템을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.

.이 작업에 대해
IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다. 서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다. IDP와 스토리지 어레이 간의 연결을 설정하려면 이 두 엔터티 간에 메타데이터 파일을 공유합니다. 다음으로 IDP 사용자 엔터티를 스토리지 어레이 역할에 매핑합니다. 마지막으로 SAML을 활성화하기 전에 연결 및 SSO 로그인을 테스트합니다.

[NOTE]
====
* SAML 및 디렉토리 서비스 *. 디렉터리 서비스가 인증 방법으로 구성되어 있을 때 SAML을 설정하면 SAML이 System Manager의 디렉터리 서비스를 대체합니다. 나중에 SAML을 사용하지 않도록 설정하면 Directory Services 구성이 이전 구성으로 돌아갑니다.

====
[CAUTION]
====
* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
SAML 인증 구성은 다단계 절차입니다.

== 1단계: IDP 메타데이터 파일을 업로드합니다

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 System Manager로 가져옵니다. IDP 시스템은 인증 요청을 올바른 URL로 리디렉션하고 받은 응답을 검증하려면 이 메타데이터가 필요합니다. 두 개의 컨트롤러가 있더라도 스토리지 어레이에 대해 하나의 메타데이터 파일만 업로드하면 됩니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.

+
구성 단계의 개요가 페이지에 표시됩니다.

. IdP(ID 공급자 가져오기) 파일 * 링크를 클릭합니다.
+
ID 공급자 파일 가져오기 대화 상자가 열립니다.

. 로컬 시스템에 복사한 IDP 메타데이터 파일을 선택하여 업로드하려면 * 찾아보기 * 를 클릭합니다.
+
파일을 선택하면 IDP 엔티티 ID가 표시됩니다.

. 가져오기 * 를 클릭합니다.

== 2단계: 서비스 제공업체 파일 내보내기

IDP와 스토리지 어레이 간의 신뢰 관계를 설정하려면 서비스 공급자 메타데이터를 IDP로 가져옵니다. IDP는 컨트롤러와 신뢰 관계를 설정하고 승인 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 서비스 공급자와 통신할 수 있도록 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. Export Service Provider files *(서비스 제공자 파일 내보내기 *) 링크를 클릭합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 컨트롤러 A * 필드에 컨트롤러 IP 주소 또는 DNS 이름을 입력한 다음 * 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다. 스토리지 배열에 두 개의 컨트롤러가 포함된 경우, * Controller B * 필드의 두 번째 컨트롤러에 대해 이 단계를 반복합니다.
+
내보내기 * 를 클릭하면 서비스 공급자 메타데이터가 로컬 시스템에 다운로드됩니다. 파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.
+
각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져와 트러스트 관계를 설정합니다. 파일을 직접 가져오거나 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.

== 3단계: 역할 매핑

사용자에게 System Manager에 대한 권한 부여 및 액세스 권한을 제공하려면 IDP 사용자 특성 및 그룹 멤버쉽을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

.시작하기 전에
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* IDP 메타데이터 파일을 System Manager로 가져옵니다.
* 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

.단계
. System Manager * 역할 매핑 링크를 클릭합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 매핑 *

a|
사용자 속성
a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.

a|
속성 값
a|
매핑할 그룹의 속성 값을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다

a|
역할
a|
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 System Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 하나 이상의 그룹에 보안 관리자 역할도 필요합니다.

매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+
[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

====
. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
+
[NOTE]
====
역할 매핑은 SAML이 활성화된 후에 수정할 수 있습니다.

====
. 매핑을 마치면 * 저장 * 을 클릭합니다.

== 4단계: SSO 로그인을 테스트합니다

IDP 시스템 및 스토리지 어레이가 통신할 수 있도록 SSO 로그인을 선택적으로 테스트할 수 있습니다. 이 테스트는 SAML을 활성화하기 위한 마지막 단계에서도 수행됩니다.

.시작하기 전에

* IDP 메타데이터 파일을 System Manager로 가져옵니다.
* 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

.단계
. Test SSO Login * 링크를 선택합니다.
+
SSO 자격 증명을 입력하기 위한 대화 상자가 열립니다.

. 보안 관리자 권한과 모니터 권한이 모두 있는 사용자의 로그인 자격 증명을 입력합니다.
+
시스템에서 로그인을 테스트하는 동안 대화 상자가 열립니다.

. 테스트 성공 메시지를 찾습니다. 테스트가 성공적으로 완료되면 SAML 활성화를 위한 다음 단계로 이동합니다.
+
테스트가 성공적으로 완료되지 않으면 추가 정보와 함께 오류 메시지가 나타납니다. 다음을 확인합니다.

+
** 사용자는 보안 관리자 및 모니터 권한이 있는 그룹에 속합니다.
** IDP 서버에 대해 업로드한 메타데이터가 정확합니다.
** SP 메타데이터 파일의 컨트롤러 주소가 올바릅니다.

== 5단계: SAML을 활성화합니다

마지막 단계는 사용자 인증을 위해 SAML 구성을 완료하는 것입니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.

.시작하기 전에
* IDP 메타데이터 파일을 System Manager로 가져옵니다.
* 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.
* 하나 이상의 Monitor 및 Security Admin 역할 매핑이 구성되어 있습니다.

[CAUTION]
====
* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술

지원 부서에 지원을 요청하십시오.

====
.단계
. SAML * 탭에서 * SAML * 활성화 링크를 선택합니다.
+
Confirm Enable SAML(SAML 활성화 확인) 대화 상자가 열립니다.

. 을 입력하고 `enable` * 사용 * 을 클릭합니다.
. SSO 로그인 테스트에 대한 사용자 자격 증명을 입력합니다.

.결과
시스템에서 SAML을 활성화하면 모든 활성 세션이 종료되고 SAML을 통해 사용자 인증이 시작됩니다.

[[ID285bf71e66e5d218eeb174f213a7197f]]
= SAML 역할 매핑을 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 Access Management에 SAML을 구성한 경우 IDP 그룹과 스토리지 배열의 사전 정의된 역할 간의 역할 매핑을 변경할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* SAML이 구성 및 활성화되었습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 역할 매핑 * 을 선택합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

+
[CAUTION]
====
SAML이 활성화되어 있는 동안에는 권한을 제거하지 않도록 주의하십시오. 그렇지 않으면 System Manager에 액세스할 수 없게 됩니다.

====
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 매핑 *

 a|
사용자 속성
 a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.

 a|
속성 값
 a|
매핑할 그룹의 속성 값을 지정합니다.

 a|
역할
 a|
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 System Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 보안 관리자 역할은 하나 이상의 그룹에 할당해야 합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.

** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

. 선택적으로 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.

.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

[[ID2f16dc407ce63f0a587f124116416375]]
= SAML 서비스 공급자 파일을 내보냅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
필요한 경우 스토리지 배열에 대한 서비스 공급자 메타데이터를 내보내고 해당 파일을 IdP(Identity Provider) 시스템으로 다시 가져올 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* SAML이 구성 및 활성화되었습니다.

.이 작업에 대해
이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다(각 컨트롤러에 대해 파일 1개). IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 요청을 보내는 데 사용할 수 있는 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 내보내기 * 를 선택합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 각 컨트롤러에 대해 * Export * (내보내기 *)를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.
+
[NOTE]
====
각 컨트롤러의 도메인 이름 필드는 읽기 전용입니다.

====
+
파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.
+
각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져옵니다. 파일을 직접 가져오거나 해당 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.
. 닫기 * 를 클릭합니다.

:leveloffset: -1

= 액세스 토큰을 사용합니다

:leveloffset: +1

[[IDe3ca896d6611d3d12ef91a951661b69e]]
= 액세스 토큰을 생성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
사용자 이름과 암호 대신 REST API 또는 CLI(Command Line Interface)를 사용하여 인증할 액세스 토큰을 생성할 수 있습니다.

NOTE: 토큰에는 암호가 없으므로 주의해서 관리해야 합니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. Access Tokens * 탭을 선택합니다.
. 액세스 토큰 설정 보기/편집 * 을 선택합니다. 대화 상자에서 * 액세스 토큰 사용 * 확인란이 선택되어 있는지 확인합니다. 대화 상자를 닫으려면 * 저장 * 을 클릭합니다.
. 액세스 토큰 만들기 * 를 선택합니다.
. 대화 상자에서 토큰이 유효할 기간을 선택합니다.
+

NOTE: 토큰이 만료되면 사용자의 인증 시도가 실패합니다.

. 생성 * 을 클릭합니다
. 대화 상자에서 다음 중 하나를 선택합니다.
+
** * 복사 * 를 눌러 토큰 텍스트를 클립보드에 저장합니다.
** * 토큰 텍스트를 파일에 저장하려면 * 다운로드 * 를 클릭합니다.
+

NOTE: 토큰 텍스트를 저장해야 합니다. 대화 상자를 닫기 전에 텍스트를 볼 수 있는 유일한 기회입니다.

. 닫기 * 를 클릭합니다.
. 다음과 같이 토큰을 사용합니다.
+
** * REST API *: REST API 요청에서 토큰을 사용하려면 요청에 HTTP 헤더를 추가하십시오. 예를 들면 다음과 같습니다.
`Authorization: Bearer _<access-token-value>_`
** * Secure CLI *: CLI에서 토큰을 사용하려면 명령줄에 토큰 값을 추가하거나 토큰 값이 포함된 파일의 경로를 사용합니다. 예를 들면 다음과 같습니다.
+
*** 명령줄의 토큰 값: `-t _access-token-value_`
*** 토큰 값이 포함된 파일의 경로: `-T _access-token-file_`
+

NOTE: 사용자 이름, 암호 또는 토큰이 지정되지 않은 경우 CLI에서 명령줄에 액세스 토큰 값을 입력하라는 메시지를 표시합니다.

[[IDe0103b56833d36abf085047fd012171c]]
= 액세스 토큰 설정을 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
만료 시간 및 새 토큰 생성 기능이 포함된 액세스 토큰의 설정을 편집할 수 있습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. Access Tokens * 탭을 선택합니다.
. 액세스 토큰 설정 보기/편집 * 을 선택합니다.
. 대화 상자에서 다음 작업 중 하나 또는 모두를 수행할 수 있습니다.
+
** 토큰 생성을 활성화 또는 비활성화합니다.
** 기존 토큰의 만료를 변경합니다.
+

NOTE: 액세스 토큰 사용 * 설정을 선택 취소하면 토큰 생성 및 토큰 인증이 모두 방지됩니다. 나중에 이 설정을 다시 활성화하면 만료되지 않은 토큰을 다시 사용할 수 있습니다. 기존 토큰을 모두 영구적으로 취소하려면 를 참조하십시오link:access-management-tokens-revoke.html["액세스 토큰을 취소합니다"].

. 저장 * 을 클릭합니다.

[[ID94891f30e717c851a78e20ec649468e1]]
= 액세스 토큰을 취소합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
토큰이 손상되었거나 액세스 토큰의 서명 및 확인에 사용되는 암호화 키에 대해 수동 키 회전을 수행하려는 경우 모든 액세스 토큰을 취소할 수 있습니다.

이 작업을 수행하면 토큰에 서명하는 데 사용되는 키가 재생성됩니다. 키가 재설정되면 _ALL_DENDED 토큰이 즉시 무효화됩니다. 스토리지 배열이 토큰을 추적하지 않으므로 개별 토큰을 취소할 수 없습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. Access Tokens * 탭을 선택합니다.
. 모든 액세스 토큰 해지 * 를 선택합니다.
. 대화 상자에서 * 예 * 를 클릭합니다.


모든 토큰을 해지한 후 새 토큰을 생성하고 즉시 사용할 수 있습니다.



:leveloffset: -1


= syslog를 관리합니다

:leveloffset: +1


[[ID6dba51388f519ca0d6333cdbffe5925d]]
= 감사 로그 활동을 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
보안 관리자 권한이 있는 사용자는 감사 로그를 보고 사용자 작업, 인증 실패, 잘못된 로그인 시도 및 사용자 세션 수명을 모니터링할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
```

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. ** 감사 로그** 탭을 선택합니다.
+
감사 로그 작업은 다음과 같은 정보 열이 포함된 표 형식으로 표시됩니다.

+
** * 날짜/시간 * -- 스토리지 배열이 이벤트를 감지한 때의 타임스탬프(GMT).
** * 사용자 이름 * -- 이벤트와 연결된 사용자 이름입니다. 스토리지 시스템에서 인증되지 않은 작업의 경우 "N/A"가 사용자 이름으로 나타납니다. 인증되지 않은 작업은 내부 프록시 또는 다른 메커니즘에 의해 트리거될 수 있습니다.
** * 상태 코드 * -- 작업의 HTTP 상태 코드(200, 400 등) 및 이벤트와 관련된 설명 텍스트입니다.
** * URL 액세스 * -- 전체 URL(호스트 포함) 및 쿼리 문자열
** * 클라이언트 IP 주소 * -- 이벤트와 연결된 클라이언트의 IP 주소입니다.
** * 소스 * -- 이벤트와 연결된 로깅 소스로, System Manager, CLI, 웹 서비스 또는 지원 셸이 될 수 있습니다.
** * 설명 * -- 해당되는 경우 이벤트에 대한 추가 정보

. 감사 로그 페이지의 선택 항목을 사용하여 이벤트를 보고 관리할 수 있습니다.
+
.선택 세부 사항
[%collapsible]
====
[cols="25h,~"]
|===
| 선택 | 설명

 a|
이벤트 표시...
 a|
날짜 범위별로 표시되는 이벤트 제한(지난 24시간, 지난 7일, 지난 30일 또는 사용자 지정 날짜 범위)

 a|
필터
 a|
필드에 입력한 문자로 표시되는 이벤트를 제한합니다. 정확히 일치하는 단어를 찾으려면 따옴표("")를 사용하고, 하나 이상의 단어를 반환하려면 을 `OR` 입력하고, 단어를 생략하려면 대시(--)를 입력합니다.

a|
새로 고침
a|
페이지를 최신 이벤트로 업데이트하려면 * Refresh * 를 선택합니다.

a|
설정 보기/편집
a|
설정 보기/편집 * 을 선택하여 전체 로그 정책 및 기록할 작업 수준을 지정할 수 있는 대화 상자를 엽니다.

a|
이벤트를 삭제합니다
a|
페이지에서 이전 이벤트를 제거할 수 있는 대화 상자를 열려면 * 삭제 * 를 선택합니다.

a|
열 표시/숨기기
a|
표시/숨기기 * 열 아이콘을 image:../media/sam-1140-ss-access-columns.gif[""] 클릭하여 테이블에 표시할 추가 열을 선택합니다. 추가 열은 다음과 같습니다.

** * Method * -- HTTP 메서드(예: POST, GET, DELETE 등).
** * CLI 명령 실행됨 * -- Secure CLI 요청에 대해 실행되는 CLI 명령(문법)
** * CLI return Status * -- CLI 상태 코드 또는 클라이언트의 입력 파일 요청입니다.
** * 기호 프로시저 * -- 기호 프로시저가 실행됩니다.
** * SSH 이벤트 유형 * -- 로그인, 로그아웃 및 login_fail과 같은 SSH(Secure Shell) 이벤트 유형
** * SSH 세션 PID * -- SSH 세션의 프로세스 ID 번호입니다.
** * SSH 세션 지속 시간 * -- 사용자가 로그인한 시간(초)입니다.
** * 인증 유형 * -- 유형에는 로컬 사용자, LDAP, SAML 및 액세스 토큰이 포함될 수 있습니다.
** * 인증 ID * -- 인증된 세션의 ID입니다.

a|
열 필터를 전환합니다
a|
각 열의 필터링 필드를 열려면 * 전환 * 아이콘을 image:../media/sam-1140-ss-access-

toggle.gif[""]클릭합니다. 열 필드에 문자를 입력하여 해당 문자로 표시되는 이벤트를 제한합니다. 필터링 필드를 닫으려면 아이콘을 다시 클릭합니다.

a|
변경 내용을 취소합니다
a|
테이블을 기본 구성으로 되돌리려면 * 실행 취소 * 아이콘을 image:../media/sam-1140-ss-access-undo.gif[""]클릭합니다.

a|
내보내기
a|
내보내기 * 를 클릭하여 테이블 데이터를 CSV(쉼표로 구분된 값) 파일에 저장합니다.

|===
====

[[ID7867c78ce8f78a9205ed49d90425cbde]]
= 감사 로그 정책을 정의합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
덮어쓰기 정책과 감사 로그에 기록된 이벤트 유형을 변경할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업에서는 이전 이벤트를 덮어쓰는 정책과 이벤트 유형을 기록하는 정책을 비롯한 감사 로그 설정을 변경하는 방법에 대해 설명합니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. Audit Log(감사 로그) * 탭을 선택합니다.

. 설정 보기/편집 * 을 선택합니다.
+
감사 로그 설정 대화 상자가 열립니다.

. 기록된 이벤트 유형 또는 덮어쓰기 정책을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
정책 덮어쓰기
 a|
최대 용량에 도달할 때 이전 이벤트를 덮어쓰는 정책을 결정합니다.

** * 감사 로그가 가득 차면 감사 로그의 가장 오래된 이벤트를 덮어쓰도록 허용 * -- 감사 로그가 50,000개 레코드에 도달할 때 이전 이벤트를 덮어씁니다.
** * 감사 로그 이벤트를 수동으로 삭제해야 함 * -- 이벤트가 자동으로 삭제되지 않도록 지정합니다. 대신 설정된 백분율로 임계값 경고가 표시됩니다. 이벤트는 수동으로 삭제해야 합니다.
+

NOTE: 덮어쓰기 정책을 사용하지 않도록 설정하고 감사 로그 항목이 최대 한도에 도달하면 보안 관리자 권한이 없는 사용자는 System Manager에 액세스할 수 없습니다. 보안 관리자 권한이 없는 사용자에 대한 시스템 액세스를 복원하려면 보안 관리자 역할에 할당된 사용자가 이전 이벤트 레코드를 삭제해야 합니다.

+

NOTE: 감사 로그 보관을 위해 syslog 서버가 구성된 경우 덮어쓰기 정책은 적용되지 않습니다.

 a|
기록할 작업 수준입니다
 a|
기록할 이벤트 유형을 결정합니다.

** * 수정 이벤트만 기록 * -- 사용자 작업이 시스템에서 변경을 수행하는 이벤트만 표시합니다.
** * 모든 수정 및 읽기 전용 이벤트 기록 * -- 정보를 읽거나 다운로드하는 사용자 작업을 포함한 모든 이벤트를 표시합니다.

```
|===
====
```
. 저장 * 을 클릭합니다.

```
[[IDe447711d3ef23e7c46a802a051ad7947]]
= 감사 로그에서 이벤트를 삭제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
이전 이벤트의 감사 로그를 지울 수 있으므로 이벤트 검색을 보다 쉽게 관리할 수 있습니다. 삭제 시 이전 이벤트를 CSV(쉼표로 구분된 값) 파일에 저장할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. Audit Log(감사 로그) * 탭을 선택합니다.
. 삭제 * 를 선택합니다.
+
감사 로그 삭제 대화 상자가 열립니다.

. 삭제할 가장 오래된 이벤트 수를 선택하거나 입력합니다.
. 삭제된 이벤트를 CSV 파일로 내보내려면(권장) 확인란을 선택한 상태로 유지합니다. 다음 단계에서 * 삭제 * 를 클릭하면 파일 이름과 위치를 입력하라는 메시지가 표시됩니다. 그렇지 않으면 이벤트를 CSV 파일에 저장하지 않으려면 확인란을 클릭하여 선택을 취소합니다.
. 삭제 * 를 클릭합니다.
+
확인 대화 상자가 열립니다.

. 필드를 입력한 `delete` 다음 * 삭제 * 를 클릭합니다.
+
가장 오래된 이벤트는 감사 로그 페이지에서 제거됩니다.

```
[[ID3630d1b60190957a33c2d7f71f55ee99]]
= 감사 로그를 위해 syslog 서버를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
감사 로그를 외부 syslog 서버에 보관하려는 경우 해당 서버와 스토리지 시스템 간의 통신을 구성할 수 있습니다. 연결이 설정되면 감사 로그가 syslog 서버에 자동으로 저장됩니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
* 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.


.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 감사 로그 탭에서 * Syslog 서버 구성 * 을 선택합니다.
+
Configure Syslog Servers 대화 상자가 열립니다.

. 추가 * 를 클릭합니다.
+
Add Syslog Server 대화 상자가 열립니다.

. 서버에 대한 정보를 입력한 다음 * 추가 * 를 클릭합니다.
+
** * 서버 주소 * -- 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
** * 프로토콜 * -- 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
** * 인증서 업로드(선택 사항) * -- TLS 프로토콜을 선택했지만 아직 서명된 CA 인증서를 업로드하지 않은 경우 * 찾아보기 * 를 클릭하여 인증서 파일을 업로드합니다. 감사 로그는 신뢰할 수 있는 인증서가 없는 syslog 서버에 보관되지 않습니다.
+
[NOTE]
====
나중에 인증서가 유효하지 않게 되면 TLS 핸드셰이크가 실패합니다. 따라서 오류 메시지가 감사 로그에 게시되고 메시지가 더 이상 syslog 서버로 전송되지 않습니다. 이 문제를 해결하려면
```

syslog 서버의 인증서를 수정한 다음 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] 메뉴로 이동해야 합니다.

====
** * Port * -- syslog 수신기의 포트 번호를 입력합니다. Add * 를 클릭하면 Configure Syslog Servers 대화 상자가 열리고 구성된 syslog 서버가 페이지에 표시됩니다.

. 스토리지 배열과의 서버 연결을 테스트하려면 * Test All * 을 선택합니다.

.결과
구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다. 경고에 대한 syslog 설정을 추가로 구성하려면 를 참조하십시오 https://docs.netapp.com/us-en/e-series-santricity/sm-settings/configure-syslog-server-for-alerts.html["경고에 대한 syslog 서버를 구성합니다"].

NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

[[ID00c6eb3dbd7572c74ef855e06744b561]]
= 감사 로그 레코드에 대한 syslog 서버 설정을 편집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
감사 로그 아카이빙에 사용되는 syslog 서버의 설정을 변경하고 서버에 대한 새 CA(인증 기관) 인증서를 업로드할 수도 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
* 새 CA 인증서를 업로드하는 경우 로컬 시스템에서 인증서를 사용할 수 있어야 합니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. 감사 로그 탭에서 * Syslog 서버 구성 * 을 선택합니다.
+

구성된 syslog 서버가 페이지에 표시됩니다.

. 서버 정보를 편집하려면 서버 이름 오른쪽에 있는 * Edit * (연필) 아이콘을 선택한 후 다음 필드에서 원하는 대로 변경합니다.
+
** * 서버 주소 * -- 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
** * 프로토콜 * -- 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
** * Port * -- syslog 수신기의 포트 번호를 입력합니다.

. 프로토콜을 보안 TLS 프로토콜(UDP 또는 TCP)으로 변경한 경우 * 신뢰할 수 있는 인증서 가져오기 * 를 클릭하여 CA 인증서를 업로드합니다.
. 스토리지 배열과의 새 연결을 테스트하려면 * Test All * 을 선택합니다.

.결과
구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

:leveloffset: -1

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDea182ac499c15688c3c002720c96c44f]]
= 로그인할 수 없는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity 시스템 관리자에 로그인하려고 할 때 오류가 발생하면 가능한 원인을 검토하십시오.

다음 이유 중 하나로 System Manager에 로그인 오류가 발생할 수 있습니다.

* 잘못된 사용자 이름 또는 암호를 입력했습니다.
* 권한이 부족합니다.
* 디렉토리 서버(구성된 경우)를 사용할 수 없습니다. 이 경우 로컬 사용자 역할로 로그인을 시도하십시오.
* 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 다시 로그인하려면 10분 정도 기다립니다.

* 잠금 조건이 트리거되었고 감사 로그가 꽉 찼을 수 있습니다. Access Management(액세스 관리)로 이동하여 감사 로그에서 이전 이벤트를 삭제합니다.
* SAML 인증이 활성화되었습니다. 로그인하려면 브라우저를 새로 고치십시오.

미러링 작업을 위해 원격 스토리지 어레이에 로그인 오류가 발생하는 원인은 다음과 같습니다.

* 잘못된 암호를 입력했습니다.
* 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 10분 정도 기다린 후 다시 로그인하십시오.
* 컨트롤러에 사용된 최대 클라이언트 연결 수에 도달했습니다. 여러 사용자 또는 클라이언트를 확인합니다.

[[ID569c378d45add473ef6604945f5906ae]]
= 디렉토리 서버를 추가하기 전에 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management에서 디렉터리 서버를 추가하기 전에 다음 요구 사항을 충족하는지 확인합니다.

* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

[[IDddec5a61c9a3e3d068fa38d5f9f27d4f]]
= 스토리지 어레이 역할에 매핑하는 방법에 대해 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
그룹을 역할에 매핑하기 전에 다음 지침을 검토하십시오.

스토리지 시스템의 내장 RBAC(역할 기반 액세스 제어) 기능에는 다음과 같은 역할이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

== 디렉터리 서비스

LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스를 사용하는 경우 다음 사항을 확인하십시오.

* 관리자가 디렉토리 서비스에 사용자 그룹을 정의했습니다.
* LDAP 사용자 그룹의 그룹 도메인 이름을 알고 있습니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다.
+
[listing]

\.[]{}()<>*+-=!?^$|
----
* Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

== SAML

스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하는 경우 다음 사항을 확인하십시오.

* IDP(Identity Provider) 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* 그룹 구성원 이름을 알고 있습니다.
* 매핑할 그룹의 속성 값을 알고 있습니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다.
+
[listing]

```
----
\.[]{}()<>*+-=!?^$|
----
```
* Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

[[ID5ea9eb53baf68c14bec979c39da2ef70]]
= 이 변경의 영향을 받을 수 있는 외부 관리 도구는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리 인터페이스 전환이나 인증 방법을 위해 SAML을 사용하는 등 SANtricity System Manager에서 특정 변경 사항을 적용하면 일부 외부 툴과 기능의 사용이 제한될 수 있습니다.

== 관리 인터페이스

레거시 관리 인터페이스 설정이 활성화되어 있지 않으면 SANtricity SMI-S Provider 또는 OnCommand Insight(OCI)와 같은 기존 관리 인터페이스(기호)와 직접 통신하는 도구가 작동하지 않습니다. 또한 이 설정이 비활성화되어 있으면 레거시 CLI 명령을 사용하거나 미러링 작업을 수행할 수 없습니다.

자세한 내용은 기술 지원 부서에 문의하십시오.

== SAML 인증

SAML이 활성화되면 다음 클라이언트가 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

* 엔터프라이즈 관리 창(EMW)
* CLI(Command-Line Interface)
* SDK(소프트웨어 개발자 키트) 클라이언트
* 대역내 클라이언트
* HTTP 기본 인증 REST API 클라이언트
* 표준 REST API 끝점을 사용하여 로그인합니다

자세한 내용은 기술 지원 부서에 문의하십시오.

```
[[ID8f59cb68c926c8058d744516f4278f7a]]
= SAML을 구성 및 활성화하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증을 위해 SAML(Security Assertion Markup Language) 기능을 구성 및 활성화하기 전에 다음 요구 사항을 충족하고 SAML 제한 사항을 이해해야 합니다.



== 요구 사항

시작하기 전에 다음 사항을 확인하십시오.

* ID 공급자(IDP)가 네트워크에 구성되어 있습니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.
* 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알고 있습니다.



== 제한 사항

위의 요구 사항 외에 다음과 같은 제한 사항을 이해해야 합니다.

* SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오. 최종 구성 단계에서 SAML을 활성화하기 전에 SSO 로그인을 테스트하는 것이 좋습니다. (SAML을 활성화하기 전에 SSO 로그인 테스트도 수행합니다.)
* 나중에 SAML을 사용하지 않도록 설정하면 이전 구성(로컬 사용자 역할 및/또는 디렉터리 서비스)이 자동으로 복원됩니다.
* 디렉토리 서비스가 현재 사용자 인증을 위해 구성된 경우 SAML은 해당 구성을 재정의합니다.
* SAML이 구성된 경우 다음 클라이언트가 스토리지 시스템 리소스에 액세스할 수 없습니다.
```

+
** 엔터프라이즈 관리 창(EMW)
** CLI(Command-Line Interface)
** SDK(소프트웨어 개발자 키트) 클라이언트
** 대역내 클라이언트
** HTTP 기본 인증 REST API 클라이언트
** 표준 REST API 끝점을 사용하여 로그인합니다

[[IDf10c41414d04fffa81f77b5d022f3849]]
= 감사 로그에 기록되는 이벤트 유형은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
감사 로그는 수정 이벤트 또는 수정 이벤트와 읽기 전용 이벤트를 모두 기록할 수 있습니다.

정책 설정에 따라 다음과 같은 유형의 이벤트가 표시됩니다.

* * 수정 이벤트 * -- 시스템 변경(예: 스토리지 프로비저닝)이 포함된 System Manager 내 사용자 조치.
* * 수정 및 읽기 전용 이벤트 * -- 볼륨 할당 보기와 같은 정보 보기 또는 다운로드와 관련된 이벤트뿐만 아니라 시스템에 대한 변경 사항을 포함하는 사용자 작업입니다.

[[ID7b1e6d056ce42888f84ebd972734bcb4]]
= syslog 서버를 구성하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
외부 syslog 서버에 감사 로그를 보관할 수 있습니다.

syslog 서버를 구성하기 전에 다음 지침을 염두에 두십시오.

* 서버 주소, 프로토콜 및 포트 번호를 알고 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
* 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.
* 구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.
* 덮어쓰기 정책 설정(* 보기/편집 설정 * 에서 사용 가능)은 syslog 서버 구성을 사용하여 로그를 관리하는 방법에 영향을 주지 않습니다.
* 감사 로그는 RFC 5424 메시징 형식을 따릅니다.

[[ID49d2c8bab7a84d7efb2218ef6c89699f]]
= syslog 서버가 더 이상 감사 로그를 수신하지 않습니다. 어떻게 해야 합니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
TLS 프로토콜을 사용하여 syslog 서버를 구성한 경우 어떤 이유로든 인증서가 유효하지 않으면 서버에서 메시지를 수신할 수 없습니다. 유효하지 않은 인증서에 대한 오류 메시지가 감사 로그에 게시됩니다.

이 문제를 해결하려면 먼저 syslog 서버의 인증서를 수정해야 합니다. 유효한 인증서 체인이 배치되면 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] 메뉴로 이동합니다.

:leveloffset: -1

:leveloffset: -1

= 인증서

:leveloffset: +1

[[ID45c5f7a25f9cfbec3b788c2c5735da98]]
= 인증서 개요
:allow-uri-read:
:icons: font

```
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SANtricity 시스템 관리자를 사용하여 CSR(인증서 서명 요청)을 만들고, 인증서를 가져오고, 기존 인증서를 관리할 수 있습니다.



== 인증서란 무엇입니까?

_Certificates_는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다. 인증서 유형에는 두 가지가 있습니다. CA(인증 기관)에서 _signed certificate_를 검증하고, 타사 대신 엔터티의 소유자가 _self-signed certificate_를 확인합니다.

자세한 내용:

* xref:{relative_path}how-certificates-work-sam.html["인증서 작동 방식"]
* xref:{relative_path}certificate-terminology.html["인증서 용어"]



== 서명된 인증서를 구성하려면 어떻게 합니까?

먼저 System Manager에서 서명 요청을 생성한 다음 파일을 CA로 보냅니다. CA가 인증서 파일을 반환하면 System Manager를 사용하여 인증서 파일을 가져옵니다.

자세한 내용:

* xref:{relative_path}use-ca-signed-certificates-for-controllers.html["컨트롤러에 CA 서명 인증서를 사용합니다"]
* xref:{relative_path}use-ca-signed-certificates-for-authentication-with-a-key-management-server.html["키 관리 서버에서 인증에 CA 서명 인증서를 사용합니다"]



== 관련 정보

인증서 관련 작업에 대해 자세히 알아보기:

* xref:{relative_path}view-imported-certificates.html["가져온 인증서 정보를 봅니다"]
* xref:{relative_path}enable-certificate-revocation-checking.html["인증서
```

해지 확인을 사용합니다"]

= 개념

:leveloffset: +1

[[ID971af8164f8f0cf922391b4b36127fff]]
= 인증서 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다.

인증서는 웹 통신이 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지 않도록 합니다. System Manager를 사용하면 호스트 관리 시스템의 브라우저(클라이언트 역할)와 스토리지 시스템의 컨트롤러(서버 역할) 간에 인증서를 관리할 수 있습니다.

인증서는 신뢰할 수 있는 기관에서 서명할 수도 있고 자체 서명할 수도 있습니다. "서명"은 단순히 누군가가 소유자의 신원을 확인하고 자신의 장치를 신뢰할 수 있다는 것을 확인하는 것을 의미합니다. 스토리지 어레이에는 각 컨트롤러에서 자동으로 생성된 자체 서명 인증서가 함께 제공됩니다. 자체 서명된 인증서를 계속 사용하거나 컨트롤러와 호스트 시스템 간의 보다 안전한 연결을 위해 CA 서명 인증서를 얻을 수 있습니다.

[NOTE]
====
CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간의 공격 방지) 대규모 네트워크를 사용하는 경우 비용이 많이 들 수 있습니다. 반면 자체 서명된 인증서는 보안성이 떨어지지만 무료입니다. 따라서 자체 서명된 인증서는 프로덕션 환경이 아닌 내부 테스트 환경에 가장 많이 사용됩니다.

====

== 서명된 인증서

서명된 인증서는 신뢰할 수 있는 타사 조직인 CA(인증 기관)에서 유효성을 검사합니다. 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보, 인증서 발급 및 만료 날짜, 엔터티에 대한 유효한 도메인 및 문자와 숫자로 구성된 디지털 서명이 포함됩니다.

브라우저를 열고 웹 주소를 입력하면 시스템은 백그라운드에서 인증서 확인 프로세스를 수행하여 유효한 CA 서명 인증서가 포함된 웹 사이트에 연결 중인지 확인합니다. 일반적으로 서명된 인증서로 보호되는 사이트에는 자물쇠 아이콘과 주소에 https 지정이 포함되어 있습니다. CA 서명 인증서가 없는 웹 사이트에 연결하려고 하면 브라우저에 사이트가 안전하지 않음을 알리는 경고가 표시됩니다.

CA는 응용 프로그램 프로세스 중에 ID를 확인하는 단계를 수행합니다. 등록된 회사에 이메일을 보내고, 회사 주소를 확인하고, HTTP 또는 DNS 확인을 수행할 수 있습니다. 응용 프로그램 프로세스가 완료되면 CA는 호스트 관리 시스템에 로드할 디지털 파일을 보냅니다. 일반적으로 이러한 파일에는 다음과 같은 신뢰 체인이 포함됩니다.

* * 루트 * -- 계층 구조의 맨 위에 루트 인증서가 있으며, 이 인증서에는 다른 인증서에 서명하는 데 사용되는 개인 키가 들어 있습니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
* * 중급 * -- 루트에서 오프하는 것은 중간 인증서입니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
* * 서버 * -- 체인 하단에 있는 서버 인증서는 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 어레이의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

== 자체 서명된 인증서

스토리지 어레이의 각 컨트롤러에는 사전 설치된 자체 서명된 인증서가 포함되어 있습니다. 자체 서명된 인증서는 타사 대신 개체 소유자가 유효성을 검사한다는 점을 제외하면 CA 서명 인증서와 비슷합니다. CA 서명 인증서와 마찬가지로 자체 서명된 인증서에는 자체 개인 키가 포함되어 있으며, 서버와 클라이언트 간의 HTTPS 연결을 통해 데이터가 암호화되고 전송되도록 합니다. 그러나 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않습니다.

자체 서명된 인증서는 브라우저에서 "신뢰할 수 있는" 인증서가 아닙니다. 자체 서명된 인증서만 포함된 웹 사이트에 연결할 때마다 브라우저에 경고 메시지가 표시됩니다. 웹 사이트로 이동할 수 있는 경고 메시지의 링크를 클릭해야 합니다. 이렇게 하면 자체 서명된 인증서를 기본적으로 수락하게 됩니다.

== 키 관리 서버에 사용되는 인증서

드라이브 보안 기능이 있는 외부 키 관리 서버를 사용하는 경우 해당 서버와 컨트롤러 간의 인증을 위한 인증서를 관리할 수도 있습니다.

[[IDeebcd68a39d4a0e5e479645450a7055f]]
= 인증서 용어

```
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
다음 용어는 인증서 관리에 적용됩니다.

[cols="25h,~"]
|===
| 기간 | 설명


 a|
CA
 a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.



 a|
CSR
 a|
CSR(인증서 서명 요청)은 신청자가 CA(인증 기관)로 보내는 메시지입니다. CSR은 CA가 인증서를 발급하는 데 필요한 정보를 확인합니다.



 a|
인증서
 a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.



 a|
인증서 체인
 a|
인증서에 보안 계층을 추가하는 파일의 계층 구조입니다. 일반적으로 체인은 계층 맨 위에 루트 인증서 하나, 중간 인증서 하나 이상 및 엔터티를 식별하는 서버 인증서를 포함합니다.
```

a|
클라이언트 인증서
a|
보안 키 관리를 위해 클라이언트 인증서는 스토리지 배열의 컨트롤러를 검증하므로 키 관리 서버가 해당 IP 주소를 신뢰할 수 있습니다.

a|
중간 인증서
a|
하나 이상의 중간 인증서가 인증서 체인의 루트에서 분기됩니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.

a|
키 관리 서버 인증서입니다
a|
보안 키 관리를 위해 키 관리 서버 인증서는 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다.

a|
키 저장소
a|
키 저장소는 해당 공개 키 및 인증서와 함께 개인 키가 들어 있는 호스트 관리 시스템의 리포지토리입니다. 이러한 키와 인증서는 컨트롤러와 같은 사용자 고유의 엔터티를 식별합니다.

a|
OCSP 서버
a|
OCSP(Online Certificate Status Protocol) 서버는 CA(인증 기관)가 예약된 만료 날짜 이전에 인증서를 취소할지 여부를 확인한 다음 인증서가 해지되면 사용자가 서버에 액세스하지 못하도록 차단합니다.

a|
루트 인증서입니다
a|
루트 인증서는 인증서 체인의 계층 구조 맨 위에 있으며 다른 인증서에 서명하는 데 사용되는 개인 키를 포함합니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는

경우 하나의 루트 인증서만 있으면 됩니다.

 a|
서명된 인증서
 a|
CA(인증 기관)에서 유효성을 검사하는 인증서입니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 또한 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보와 문자와 숫자로 구성된 디지털 서명이 포함됩니다. 서명된 인증서는 신뢰 체인을 사용하므로 프로덕션 환경에서 가장 많이 사용됩니다. "CA 서명 인증서" 또는 "관리 인증서"라고도 합니다.

 a|
자체 서명된 인증서
 a|
자체 서명된 인증서는 해당 엔터티의 소유자에 의해 유효성이 검사됩니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 문자와 숫자로 구성된 디지털 서명도 포함되어 있습니다. 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않으므로 테스트 환경에서 가장 많이 사용됩니다. "사전 설치된" 인증서라고도 합니다.

 a|
서버 인증서
 a|
서버 인증서는 인증서 체인의 맨 아래에 있습니다. 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 시스템의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

|===

:leveloffset: -1

= 인증서를 사용합니다

:leveloffset: +1

[[ID81f51bf66c0e866ce46055dc49584fb2]]
= 컨트롤러에 CA 서명 인증서를 사용합니다
:allow-uri-read:

```
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
SANtricity System Manager에 액세스하는 데 사용되는 컨트롤러와 브라우저 간에 안전한 통신을 위해 CA 서명 인증서를 얻을 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* 각 컨트롤러의 IP 주소 또는 DNS 이름을 알아야 합니다.


.이 작업에 대해
CA 서명 인증서를 사용하는 것은 3단계 절차입니다.



== 1단계: CSR을 컨트롤러에 대해 완료합니다

먼저 스토리지 배열의 각 컨트롤러에 대해 CSR(인증서 서명 요청) 파일을 생성해야 합니다.

.이 작업에 대해
이 작업은 System Manager에서 CSR 파일을 생성하는 방법을 설명합니다. CSR은 조직에 대한 정보와 컨트롤러의 IP 주소 또는 DNS 이름을 제공합니다. 이 작업 중에 스토리지 어레이에 컨트롤러가 1개 있고 CSR 파일이 2개 있는 경우 CSR 파일 1개가 생성됩니다.

[NOTE]
====
또는 OpenSSL과 같은 도구를 사용하여 CSR 파일을 생성할 수 있으며 로 건너뛸 수 있습니다 <<2단계: CSR 파일을 제출합니다>>.

====
.단계
. 설정 [인증서] 메뉴를 선택합니다.
. Array Management(어레이 관리) 탭에서 * Complete CSR * 을 선택합니다.
+
[NOTE]
====
두 번째 컨트롤러에 대해 자체 서명된 인증서를 수락하라는 대화 상자가 표시되면 * 자체 서명된 인증서 수락 * 을 클릭하여 계속 진행합니다.

====
. 다음 정보를 입력하고 * 다음 * 을 클릭합니다.
```

+
** * 조직 * -- 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
** * 조직 단위(선택 사항) * -- 인증서를 처리하는 조직의 사업부입니다.
** * 시/군/구 * -- 스토리지 배열 또는 비즈니스가 위치한 시/군/구.
** * 주/지역(선택 사항) * -- 스토리지 배열 또는 비즈니스가 위치한 주 또는 지역입니다.
** * 국가 ISO 코드 * -- 미국 등 해당 국가의 2자리 ISO(International Organization for Standardization) 코드입니다.

+
[CAUTION]
====
일부 필드는 컨트롤러의 IP 주소와 같은 적절한 정보로 미리 채워질 수 있습니다. 값이 올바르지 않다고 확신하지 않는 한 미리 채워진 값을 변경하지 마십시오. 예를 들어 CSR을 아직 완료하지 않은 경우 컨트롤러 IP 주소는 ""localhost""로 설정됩니다. 이 경우 "localhost"를 컨트롤러의 DNS 이름 또는 IP 주소로 변경해야 합니다.

====
. 스토리지 어레이에서 컨트롤러 A에 대한 다음 정보를 확인하거나 입력합니다.
+
** * Controller a common name * -- 컨트롤러 A의 IP 주소 또는 DNS 이름이 기본적으로 표시됩니다. 이 주소가 올바른지 확인합니다. 입력한 주소와 정확하게 일치해야 브라우저에서 System Manager에 액세스할 수 있습니다. DNS 이름은 와일드카드로 시작할 수 없습니다.
** *Controller a alternate IP addresses* -- 공통 이름이 IP 주소인 경우 선택적으로 컨트롤러 A에 대한 추가 IP 주소나 별칭을 입력할 수 있습니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용하십시오.
** * Controller A alternate DNS names * -- 일반적인 이름이 DNS 이름인 경우 컨트롤러 A에 대한 추가 DNS 이름을 입력합니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용하십시오. 대체 DNS 이름이 없지만 첫 번째 필드에 DNS 이름을 입력한 경우 여기에 해당 이름을 복사합니다. DNS 이름은 와일드카드로 시작할 수 없습니다. 스토리지 배열에 컨트롤러가 하나만 있는 경우 * Finish * (마침 *) 버튼을 사용할 수 있습니다.
+
스토리지 배열에 컨트롤러가 두 개 있는 경우 * Next * (다음 *) 버튼을 사용할 수 있습니다.

+
[NOTE]
====
CSR 요청을 처음 생성할 때 * 이 단계 건너뛰기 * 링크를 클릭하지 마십시오. 이 링크는 오류 복구 상황에서 제공됩니다. 드문 경우지만 한 컨트롤러에서 CSR 요청이 실패할 수 있지만 다른 컨트롤러에서는 그렇지 않습니다. 이 링크를 사용하면 컨트롤러 A에서 CSR 요청을 생성하는 단계를 건너뛸 수 있습니다(이미 정의된 경우). 컨트롤러 B에서 CSR 요청을 다시 생성하기 위한 다음 단계를 계속 진행할 수 있습니다

====
. 하나의 컨트롤러만 있는 경우 * 마침 * 을 클릭합니다. 두 개의 컨트롤러가 있는 경우 * 다음 * 을 클릭하여 컨트롤러 B에 대한 정보(위와 동일)를 입력한 다음 * 마침 * 을 클릭합니다.
+
단일 컨트롤러의 경우 하나의 CSR 파일이 로컬 시스템에 다운로드됩니다. 이중 컨트롤러의 경우 두 개의 CSR 파일이 다운로드됩니다. 다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

. 로 이동합니다. <<2단계: CSR 파일을 제출합니다>>

== 2단계: CSR 파일을 제출합니다

CSR(인증서 서명 요청) 파일을 생성한 후 CA(인증 기관)에 파일을 보냅니다. E-Series 시스템에는 PEM, .CRT, .CER 또는 .key 파일 형식이 포함된 서명된 인증서에 대한 PEM 형식(Base64 ASCII 인코딩)이 필요합니다.

.단계
. 다운로드한 CSR 파일을 찾습니다.
. CSR 파일을 CA(예: VeriSign 또는 DigiCert)에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.
+
[CAUTION]
====
* CSR 파일을 CA에 제출한 후에는 다른 CSR 파일을 다시 생성하지 마십시오. * CSR을 생성할 때마다 시스템은 개인 키 및 공개 키 쌍을 생성합니다. 공개 키는 CSR의 일부이며 개인 키는 시스템의 키 저장소에 보관됩니다. 서명된 인증서를 받아서 가져오면 시스템에서 개인 키와 공개 키가 모두 원래 쌍이 되도록 합니다. 키가 일치하지 않으면 서명된 인증서가 작동하지 않으므로 CA에서 새 인증서를 요청해야 합니다.

====
. CA가 서명된 인증서를 반환하면 로 이동합니다<<3단계: 컨트롤러의 서명된 인증서 가져오기>>.

== 3단계: 컨트롤러의 서명된 인증서 가져오기

CA(인증 기관)에서 서명된 인증서를 받은 후 컨트롤러의 파일을 가져옵니다.

.시작하기 전에
* CA가 서명된 인증서 파일을 반환했습니다. 이러한 파일에는 루트 인증서, 하나 이상의 중간 인증서 및 서버 인증서가 포함됩니다.
* CA가 체인 인증서 파일(예: .p7b 파일)을 제공한 경우, 연결된 파일의 압축을 개별 파일(루트 인증서, 하나 이상의 중간 인증서, 컨트롤러를 식별하는 서버 인증서)에 풀어야 합니다. Windows 유틸리티를 사용하여 파일의 압축을 풀 수 `certmgr` 있습니다(마우스 오른쪽 버튼을 클릭하고

메뉴: 모든 작업 [내보내기] 선택). base-64 인코딩이 권장됩니다. 내보내기가 완료되면 체인의 각 인증서 파일에 대해 CER 파일이 표시됩니다.
* 인증서 파일을 System Manager에 액세스하는 호스트 시스템에 복사했습니다.

.단계
. 메뉴 선택: 설정 [인증서]
. Array Management 탭에서 * Import * 를 선택합니다.
+
인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

. 찾아보기 * 단추를 클릭하여 먼저 루트 및 중간 인증서 파일을 선택한 다음 컨트롤러의 각 서버 인증서를 선택합니다. 루트 파일과 중간 파일은 두 컨트롤러 모두에 대해 동일합니다. 서버 인증서만 각 컨트롤러에 대해 고유합니다. 외부 도구에서 CSR을 생성한 경우 CSR과 함께 생성된 개인 키 파일도 가져와야 합니다.
+
파일 이름이 대화 상자에 표시됩니다.

. 가져오기 * 를 클릭합니다.
+
파일이 업로드되고 검증됩니다.

.결과
세션이 자동으로 종료됩니다. 인증서를 적용하려면 다시 로그인해야 합니다. 다시 로그인하면 새 CA 서명 인증서가 세션에 사용됩니다.

[[ID05e8bf807d8dddb01042969cd5d0deb8]]
= 관리 인증서를 재설정합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
CA 서명 인증서를 사용하는 것이 아니라 자체 서명된 인증서를 공장 출하시 설정된 인증서로 되돌릴 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* CA 서명 인증서는 이전에 가져와야 합니다.

.이 작업에 대해
재설정 기능은 각 컨트롤러에서 현재 CA 서명 인증서 파일을 삭제합니다. 그런 다음 컨트롤러는 자체 서명 인증서를 사용하여 로 돌아갑니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. Array Management 탭에서 * Reset * 을 선택합니다.
+
관리 인증서 재설정 확인 대화 상자가 열립니다.

. 필드에 입력한 `reset` 다음 * 재설정 * 을 클릭합니다.
+
브라우저가 새로 고쳐지면 브라우저가 대상 사이트에 대한 액세스를 차단하고 사이트가 HTTP Strict Transport Security를 사용하고 있다고 보고할 수 있습니다. 이 조건은 자체 서명된 인증서로 다시 전환하면 발생합니다. 대상에 대한 액세스를 차단하는 조건을 지우려면 브라우저에서 탐색 데이터를 지워야 합니다.

.결과
컨트롤러는 자체 서명된 인증서 사용으로 되돌아갑니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.

[[ID8eef855b8968a709a52bfca41f00d949]]
= 가져온 인증서 정보를 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서 페이지에서 인증서 유형, 발급 기관 및 스토리지 배열에 대한 유효한 인증서 날짜 범위를 볼 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 인증서에 대한 정보를 보려면 탭 중 하나를 선택합니다.

```
+
[cols="25h,~"]
|===
| 탭을 클릭합니다 | 설명


 a|
어레이 관리
 a|
루트 파일, 중간 파일 및 서버 파일을 포함하여 각 컨트롤러에 대해 가져온 CA 서명 인증서에 대한 정보를 봅니다.



 a|
신뢰성
 a|
컨트롤러에 대해 가져온 다른 모든 유형의 인증서에 대한 정보를 봅니다. 사용자가 설치한 인증서 또는 사전 설치된 인증서를 보려면 * 다음 인증서 표시 * 아래의 필터 필드를 사용하십시오.

** * 사용자 설치 * -- 컨트롤러가 서버 대신 클라이언트, LDAPS 인증서 및 ID 페더레이션 인증서를 사용할 때 신뢰할 수 있는 인증서를 포함할 수 있는 사용자가 스토리지 배열에 업로드한 인증서입니다.
** * 사전 설치 * -- 스토리지 배열에 포함된 자체 서명된 인증서.



 a|
키 관리
 a|
외부 키 관리 서버에 대해 가져온 CA 서명 인증서에 대한 정보를 봅니다.

|===



[[IDaee650f046653fb5edc20bcc878c6fff]]
= 클라이언트로 작동할 때 컨트롤러의 인증서를 가져옵니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
네트워크 서버에 대한 신뢰 체인을 확인할 수 없기 때문에 컨트롤러가 연결을 거부하면 신뢰할 수 있는 탭에서 인증서를 가져올 수 있습니다. 그러면 컨트롤러(클라이언트 역할)가 해당 서버의 통신을 수락할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* 인증서 파일이 로컬 시스템에 설치됩니다.

.이 작업에 대해
다른 서버가 컨트롤러(예: TLS를 사용하는 LDAP 서버 또는 syslog 서버)에 접속하도록 허용하려면 신뢰할 수 있는 탭에서 인증서를 가져와야 할 수 있습니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 신뢰할 수 있는 탭에서 * 가져오기 * 를 선택합니다.
+
신뢰할 수 있는 인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

. 컨트롤러의 인증서 파일을 선택하려면 * 찾아보기 * 를 클릭합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 가져오기 * 를 클릭합니다.

.결과
파일이 업로드되고 검증됩니다.

[[IDf435b4dd38133c1ba6201ef935226e22]]
= 인증서 해지 확인을 사용합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
OCSP(Online Certificate Status Protocol) 서버가 비보안 연결을 만드는 사용자를 차단하도록 해지된 인증서를 자동으로 검사할 수 있습니다.

.시작하기 전에

* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* DNS 서버는 두 컨트롤러 모두에 구성되어 OCSP 서버에 정규화된 도메인 이름을 사용할 수 있습니다. 이 작업은 하드웨어 페이지에서 사용할 수 있습니다.
* 사용자 고유의 OCSP 서버를 지정하려면 해당 서버의 URL을 알아야 합니다.

.이 작업에 대해
CA에서 인증서를 잘못 발급했거나 개인 키가 손상된 경우 자동 해지 확인을 사용하는 것이 좋습니다.

이 작업 중에 OCSP 서버를 구성하거나 인증서 파일에 지정된 서버를 사용할 수 있습니다. OCSP 서버는 CA가 예약된 만료 날짜 이전에 인증서를 취소할지 여부를 확인한 다음 인증서가 해지될 경우 사용자가 사이트에 액세스하지 못하도록 차단합니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
[NOTE]
====
키 관리 * 탭에서 해지 확인을 활성화할 수도 있습니다.

====
. Uncommon Tasks * 를 클릭한 다음 드롭다운 메뉴에서 * Enable Revocation Checking * 을 선택합니다.
. 해지 확인을 활성화하겠습니다 * 를 선택하면 확인란에 확인 표시가 나타나고 대화 상자에 추가 필드가 나타납니다.
. OCSP 응답자 주소* 필드에 OCSP 응답자 서버의 URL을 선택적으로 입력할 수 있습니다. 주소를 입력하지 않으면 시스템에서 인증서 파일의 OCSP 서버 URL을 사용합니다.
. Test Address * 를 클릭하여 시스템이 지정된 URL에 대한 연결을 열 수 있는지 확인합니다.
. 저장 * 을 클릭합니다.

.결과
스토리지 배열이 인증서가 해지된 서버에 연결을 시도하면 연결이 거부되고 이벤트가 기록됩니다.

[[IDe3cf5d9e54153216458a55f78b182b21]]
= 신뢰할 수 있는 인증서를 삭제합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
신뢰할 수 있는 탭에서 이전에 가져온 사용자 설치 인증서를 삭제할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* 신뢰할 수 있는 인증서를 새 버전으로 업데이트하는 경우 이전 인증서를 삭제하기 전에 업데이트된 인증서를 가져와야 합니다.

[CAUTION]
====
대체 인증서를 가져오기 전에 컨트롤러 및 LDAP 서버와 같은 다른 서버를 인증하는 데 사용되는 인증서를 삭제하면 시스템에 대한 액세스가 끊어질 수 있습니다.

====
.이 작업에 대해
이 작업은 사용자가 설치한 인증서를 삭제하는 방법을 설명합니다. 사전 설치된 자체 서명된 인증서는 삭제할 수 없습니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
아래 표에는 스토리지 배열의 신뢰할 수 있는 인증서가 나와 있습니다.

. 테이블에서 제거할 인증서를 선택합니다.
. Uncommon Tasks[드문 작업][Delete] 메뉴를 클릭합니다.
+
신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

. 필드를 입력한 `delete` 다음 * 삭제 * 를 클릭합니다.

[[IDb07495668d290fced1b335c6126866be]]
= 키 관리 서버에서 인증에 CA 서명 인증서를 사용합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

키 관리 서버와 스토리지 어레이 컨트롤러 간의 보안 통신을 위해 적절한 인증서 세트를 구성해야 합니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.이 작업에 대해
컨트롤러와 키 관리 서버 간의 인증은 2단계 절차입니다.

== 1단계: 키 관리 서버를 사용하여 인증을 위해 CSR을 작성하여 제출합니다

먼저 CSR(인증서 서명 요청) 파일을 생성한 다음 CSR을 사용하여 키 관리 서버에서 신뢰할 수 있는 CA(인증 기관)로부터 서명된 클라이언트 인증서를 요청해야 합니다. 다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 키 관리 탭에서 * CSR 완료 * 를 선택합니다.
. 다음 정보를 입력합니다.
+
** * 공통 이름 * -- 인증서 파일에 표시될 스토리지 배열 이름과 같이 이 CSR을 식별하는 이름입니다.
** * 조직 * -- 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
** * 조직 단위(선택 사항) * -- 인증서를 처리하는 조직의 사업부입니다.
** * 시/군/구 * -- 조직이 위치한 시/군/구.
** * 시/도(선택 사항) * -- 조직이 위치한 시/도 또는 지역입니다.
** * 국가 ISO 코드 * -- 귀하의 조직이 위치한 미국과 같은 두 자리 ISO(국제 표준화 기구) 코드입니다.

. 다운로드 * 를 클릭합니다.
+
CSR 파일이 로컬 시스템에 저장됩니다.

. 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다.
. 클라이언트 인증서가 있으면 로 이동합니다<<2단계: 키 관리 서버의 인증서를 가져옵니다>>.

== 2단계: 키 관리 서버의 인증서를 가져옵니다

다음 단계에서는 스토리지 어레이와 키 관리 서버 간에 인증을 위한 인증서를 가져옵니다. 인증서 유형에는 두 가지가 있습니다. 클라이언트 인증서는 스토리지 시스템의 컨트롤러를 검증하는 반면 키 관리 서버 인증서는 서버를 검증합니다. 컨트롤러의 클라이언트 인증서 파일과 키 관리 서버의 서버 인증서 파일을 모두 로드해야 합니다.

.시작하기 전에
* 서명된 클라이언트 인증서 파일(참조<<1단계: 키 관리 서버를 사용하여 인증을 위해 CSR을 작성하여 제출합니다>>)이 있고 System Manager에 액세스하는 호스트에 해당 파일을 복사했습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.
* 키 관리 서버에서 인증서 파일을 검색한 다음 System Manager에 액세스할 호스트에 해당 파일을 복사해야 합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에 루트, 중간 또는 서버 인증서를 사용할 수 있습니다.
+
[NOTE]
====
서버 인증서에 대한 자세한 내용은 키 관리 서버 설명서를 참조하십시오.

====

.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 키 관리 탭에서 * 가져오기 * 를 선택합니다.
+
인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

. Select client certificate * 옆에 있는 * Browse * 버튼을 클릭하여 스토리지 배열 컨트롤러의 클라이언트 인증서 파일을 선택합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 키 관리 서버의 서버 인증서 선택 * 옆에 있는 * 찾아보기 * 버튼을 클릭하여 키 관리 서버의 서버 인증서 파일을 선택합니다. 키 관리 서버에 대한 루트, 중간 또는 서버 인증서를 선택할 수 있습니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 가져오기 * 를 클릭합니다.
+
파일이 업로드되고 검증됩니다.

```
[[ID3737f31ee74303a52a4f87e26803f6d1]]
= 키 관리 서버 인증서를 내보냅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
키 관리 서버의 인증서를 로컬 컴퓨터에 저장할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
* 인증서를 이전에 가져와야 합니다.


.단계
. 설정 [인증서] 메뉴를 선택합니다.
. 키 관리 * 탭을 선택합니다.
. 테이블에서 내보낼 인증서를 선택한 다음 * 내보내기 * 를 클릭합니다.
+
저장 대화 상자가 열립니다.

. 파일 이름을 입력하고 * 저장 * 을 클릭합니다.




:leveloffset: -1


= FAQ 를 참조하십시오

:leveloffset: +1


[[ID1b897e9273315d9d9c37c313b86013dc]]
= 다른 컨트롤러에 액세스할 수 없음 대화 상자가 나타나는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
인증서 가져오기 등의 CA 인증서와 관련된 특정 작업을 수행할 때 두 번째 컨트롤러에 대해 자체 서명된 인증서를 수락하라는 대화 상자가 나타날 수 있습니다.

두 개의 컨트롤러가 있는 스토리지 배열(이중 구성)에서 이 대화 상자는 SANtricity 시스템 관리자가 두 번째 컨트롤러와 통신할 수 없거나 브라우저가 특정 작업 중에 인증서를 수락할 수 없는 경우에 나타납니다.

이 대화 상자가 열리면 * 자체 서명된 인증서 수락 * 을 클릭하여 계속 진행합니다. 암호를 묻는 다른 대화 상자가 나타나면 System Manager 액세스에 사용되는 관리자 암호를 입력합니다.

이 대화 상자가 다시 나타나고 인증서 작업을 완료할 수 없는 경우 다음 절차 중 하나를 수행합니다.

* 다른 브라우저 유형을 사용하여 이 컨트롤러에 액세스하고, 인증서를 수락하고, 계속합니다.
* System Manager에서 두 번째 컨트롤러에 액세스하고, 자체 서명된 인증서를 수락한 다음 첫 번째 컨트롤러로 돌아가 계속합니다.

[[IDe39f21447a3eda6f9a7fbe3d62a97769]]
= 외부 키 관리를 위해 SANtricity System Manager에 업로드해야 하는 인증서는 어떻게 알 수 있습니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
외부 키 관리의 경우 두 엔터티가 서로 신뢰할 수 있도록 스토리지 배열과 키 관리 서버 간에 인증을 위해 두 가지 유형의 인증서를 가져옵니다.

클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다. 클라이언트 인증서를 얻으려면 System Manager를 사용하여 스토리지 배열에 대한 CSR을 완료합니다. 그런 다음 CSR을 키 관리 서버에 업로드하고 여기서 클라이언트 인증서를 생성할 수 있습니다. 클라이언트 인증서가 있으면 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.

키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에서 서버 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트로 해당 파일을 복사합니다.

[[ID599e97fb335b524c15e5526ee029aa2a]]

= 인증서 해지 확인에 대해 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity 시스템 관리자를 사용하면 CRL(인증서 해지 목록)을 업로드하는 대신 OCSP(온라인 인증서 상태 프로토콜) 서버를 사용하여 해지된 인증서를 확인할 수 있습니다.

해지된 인증서는 더 이상 신뢰할 수 없습니다. 인증서를 잘못 발급했거나 개인 키가 손상되었거나 식별된 엔터티가 정책 요구 사항을 준수하지 않은 경우와 같이 여러 가지 이유로 인증서가 해지될 수 있습니다.

시스템 관리자에서 OCSP 서버에 대한 연결을 설정한 후 스토리지 어레이는 AutoSupport 서버, EKMS(외부 키 관리 서버), LDAPS(Lightweight Directory Access Protocol over SSL) 서버 또는 Syslog 서버에 연결할 때마다 해지 확인을 수행합니다. 스토리지 배열은 이러한 서버의 인증서가 해지되지 않았는지 확인하기 위해 유효성을 검사합니다. 그런 다음 서버는 해당 인증서에 대해 "양호", "취소됨" 또는 "알 수 없음" 값을 반환합니다. 인증서가 해지되었거나 어레이가 OCSP 서버에 연결할 수 없는 경우 연결이 거부됩니다.

[NOTE]
====
System Manager 또는 CLI(Command Line Interface)에서 OCSP 응답자 주소를 지정하면 인증서 파일에 있는 OCSP 주소가 재정의됩니다.

====

[[IDc98fae80a1064e35de153dbc3dd7938b]]
= 어떤 유형의 서버에 대해 해지 확인을 사용할 수 있습니까?
:allow-uri-read:
:icons: font
:relative_path: ./sm-settings/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
스토리지 시스템은 AutoSupport 서버, EKMS(외부 키 관리 서버), LDAPS(Lightweight Directory Access Protocol over SSL) 서버 또는 Syslog 서버에 연결할 때마다 해지 확인을 수행합니다.

:leveloffset: -1

```
:leveloffset: -1


= 지원

:leveloffset: +1


[[IDa07a675cbe060f90b94f0593478d14d0]]
= 지원 개요
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
지원 페이지에서는 기술 지원 리소스에 액세스할 수 있습니다.



== 어떤 지원 작업을 사용할 수 있습니까?

지원 에서 기술 지원 연락처를 보고, 진단을 수행하고, AutoSupport를 구성하고, 이벤트 로그를 보고, 소프트웨어 업그레이드를 수행할 수 있습니다.

자세한 내용:

* xref:{relative_path}autosupport-feature-overview.html["AutoSupport 기능 개요"]
* xref:{relative_path}overview-event-log.html["이벤트 로그 개요"]
* xref:{relative_path}overview-upgrade-center.html["업그레이드 센터 개요"]



== 기술 지원 부서에 어떻게 문의합니까?

기본 페이지에서 지원 [지원 센터 > 지원 리소스 탭] 메뉴를 클릭합니다. 기술 지원 연락처 정보는 인터페이스의 오른쪽 위에 나와 있습니다.



= 정보 및 진단 정보를 봅니다
```

```
:leveloffset: +1


[[ID2d13a60f3b21c6ae85c8a485bab7123d]]
= 스토리지 배열 프로파일을 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
스토리지 배열 프로파일은 스토리지 배열의 모든 구성 요소와 속성에 대한 설명을 제공합니다.

.이 작업에 대해
스토리지 배열 프로파일을 복구 과정에서 보조 도구로 사용하거나 스토리지 배열의 현재 구성에 대한 개요로 사용할 수 있습니다. 스토리지 배열 프로파일의 복사본을 관리 클라이언트에 저장하고 스토리지 배열 프로파일의 하드 복사본을 스토리지 배열에 보관할 수 있습니다. 구성이 변경되는 경우 스토리지 배열 프로파일의 새 복사본을 생성합니다.

.단계
. 지원 [지원 센터 > 지원 리소스] 탭을 선택합니다.
. 아래로 스크롤하여 * 자세한 스토리지 배열 정보 시작 * 을 선택한 다음 * 스토리지 배열 프로파일 * 을 선택합니다.
+
보고서가 화면에 나타납니다.

+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 섹션을 참조하십시오 | 설명


 a|
스토리지
 a|
에는 구성할 수 있는 모든 옵션과 스토리지 배열에 대한 시스템 정적 옵션이 나와 있습니다. 이러한 옵션에는 컨트롤러 수, 드라이브 쉘프, 드라이브, 디스크 풀, 볼륨 그룹, 볼륨 및 핫 스페어 드라이브, 허용되는 최대 드라이브 쉘프, 드라이브, SSD(Solid State Disk) 및 볼륨 수, 스냅샷 그룹 수, 스냅샷 이미지, 스냅샷 볼륨 및 일관성 그룹, 기능에 대한 정보, 펌웨어 버전에 대한 정보, 섀시 일련 번호에 대한 정보, AutoSupport 상태 및 AutoSupport 일정 정보 자동 지원 데이터 수집 및 예약된 지원 데이터 수집 설정, 스토리지 어레이 WWID(World-
```

Wide Identifier), 미디어 검색 및 캐시 설정

a|
스토리지
a|
에는 스토리지 배열의 모든 스토리지 장치 목록이 나와 있습니다. 스토리지 배열 구성에 따라 Storage 섹션에 이러한 하위 섹션이 표시될 수 있습니다.

** * 디스크 풀 * -- 스토리지 배열의 모든 디스크 풀 목록을 표시합니다.
** * 볼륨 그룹 * -- 스토리지 배열의 모든 볼륨 그룹 목록을 표시합니다. 볼륨 및 사용 가능한 용량이 생성된 순서대로 나열됩니다.
** * Volumes * -- 스토리지 배열의 모든 볼륨 목록을 표시합니다. 나열된 정보에는 볼륨 이름, 볼륨 상태, 용량, RAID 레벨, 볼륨 그룹 또는 디스크 풀, 드라이브 유형 및 추가 세부 정보가 포함됩니다.
** * Missing Volumes * -- 현재 누락된 상태가 있는 스토리지 배열의 모든 볼륨 목록을 표시합니다. 나열된 정보에는 누락된 각 볼륨에 대한 WWID(World Wide Identifier)가 포함됩니다.

a|
복사 서비스
a|
에는 스토리지 시스템에 사용되는 모든 복제본 서비스 목록이 나와 있습니다. 스토리지 배열 구성에 따라 Copy Services 섹션에 다음과 같은 하위 섹션이 표시될 수 있습니다.

** * Volume Copies * -- 스토리지 배열의 모든 복제 쌍 목록을 표시합니다. 나열된 정보에는 복사본 수, 복사본 쌍 이름, 상태, 시작 타임스탬프 및 추가 세부 정보가 포함됩니다.
** * 스냅샷 그룹 * -- 스토리지 배열의 모든 스냅샷 그룹 목록을 표시합니다.
** * 스냅샷 이미지 * -- 스토리지 배열의 모든 스냅샷 목록을 표시합니다.
** * Snapshot Volumes * -- 스토리지 배열의 모든 스냅샷 볼륨 목록을 표시합니다.
** * 정합성 보장 그룹 * -- 스토리지 배열의 모든 정합성 보장 그룹 목록을 표시합니다.
** * 구성원 볼륨 * -- 스토리지 배열의 모든 정합성 보장 그룹 구성원 볼륨 목록을 표시합니다.
** * 미러 그룹 * -- 미러링된 모든 볼륨의 목록을 표시합니다.
** * Reserved Capacity * -- 스토리지 배열의 모든 예약된 용량 볼륨 목록을 표시합니다.

a|
호스트 할당
a|
에는 스토리지 배열의 호스트 할당 목록이 나와 있습니다. 나열된 정보에는 볼륨 이름, LUN(논리 유닛 번호), 컨트롤러 ID, 호스트 이름 또는 호스트 클러스터 이름, 볼륨 상태가 포함됩니다.

여기에 나열된 추가 정보에는 토폴로지 정의 및 호스트 유형 정의가 포함됩니다.

a|
하드웨어
a|
에는 스토리지 배열의 모든 하드웨어 목록이 나와 있습니다. 스토리지 배열 구성에 따라 Hardware 섹션에 이러한 하위 섹션이 표시될 수 있습니다.

** * 컨트롤러 * -- 스토리지 어레이에 있는 모든 컨트롤러의 목록을 표시하며 컨트롤러 위치, 상태 및 구성을 포함합니다. 또한 드라이브 채널 정보, 호스트 채널 정보 및 이더넷 포트 정보도 포함됩니다.
** * 드라이브 * -- 스토리지 배열의 모든 드라이브 목록을 표시합니다. 쉘프 ID, 문서함 ID, 슬롯 ID 순서로 드라이브가 나열됩니다. 나열된 정보에는 쉘프 ID, 문서함 ID, 슬롯 ID, 상태, 물리적 용량, 미디어 유형, 인터페이스 유형, 현재 데이터 속도, 제품 ID 및 각 드라이브의 펌웨어 버전입니다. 드라이브 섹션에는 드라이브 채널 정보, 핫 스페어 적용 범위 정보 및 마모 수명 정보(SSD 드라이브 전용)도 포함되어 있습니다. 마모 수명 정보에는 사용된 내구성 비율, 즉 현재까지 SSD 드라이브에 기록된 데이터의 양을 이론적인 드라이브의 총 쓰기 한계로 나눈 값이 포함됩니다.
** * 드라이브 채널 * -- 스토리지 배열의 모든 드라이브 채널에 대한 정보를 표시합니다. 나열된 정보에는 채널 상태, 링크 상태(해당하는 경우), 드라이브 수 및 누적 오류 수가 포함됩니다.
** * 쉘프 * -- 스토리지 어레이의 모든 쉘프에 대한 정보를 표시합니다. 드라이브 유형과 쉘프의 각 구성 요소에 대한 상태 정보가 표시됩니다. 쉘프 구성 요소에는 배터리 팩, SFP(Small Form-factor Pluggable) 트랜시버, 전원 팬 캐니스터 또는 IOM(Input/Output Module) 캐니스터가 포함될 수 있습니다. 스토리지 배열에 보안 키를 사용하는 경우 하드웨어 섹션에는 보안 키 식별자도 표시됩니다.

a|
피처
a|
에는 설치된 기능 팩 목록과 호스트 또는 호스트 클러스터당 허용되는 최대 스냅샷 그룹, 스냅샷(레거시) 및 볼륨 수가 나와 있습니다. Features(기능) 섹션에 있는 정보에는 Drive Security(드라이브 보안), 즉 스토리지 어레이가 보안이 설정되어 있는지 또는 보안이 비활성화되어 있는지 여부도 포함됩니다.

|===
====
. 스토리지 배열 프로파일을 검색하려면 * 찾기 * 텍스트 상자에 검색어를 입력한 다음 * 찾기 * 를 클릭합니다.
+
일치하는 모든 용어가 강조 표시됩니다. 모든 결과를 한 번에 하나씩 스크롤하려면 * 찾기 * 를 계속 클릭합니다.

. 스토리지 배열 프로파일을 저장하려면 * 저장 * 을 클릭합니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `storage-array-profile.txt`저장됩니다.

[[ID76cffb08368f0a2c214f14da6e316e3c]]
= 소프트웨어 및 펌웨어 인벤토리를 봅니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
소프트웨어 및 펌웨어 인벤토리는 스토리지 배열의 각 구성 요소에 대한 펌웨어 버전을 나열합니다.

.이 작업에 대해
스토리지 어레이는 컨트롤러, 드라이브, 서랍 및 IOM(Input/Output Module)을 비롯한 여러 구성 요소로 구성됩니다. 이러한 각 구성 요소에는 펌웨어가 포함되어 있습니다. 일부 펌웨어 버전은 다른 펌웨어 버전에 따라 다릅니다. 스토리지 배열의 모든 펌웨어 버전에 대한 정보를 캡처하려면 소프트웨어 및 펌웨어 인벤토리를 확인합니다. 기술 지원 부서에서는 소프트웨어 및 펌웨어 인벤토리를 분석하여 펌웨어 불일치를 감지할 수 있습니다.

.단계
. 지원 [지원 센터 > 지원 리소스] 탭을 선택합니다.
. 아래로 스크롤하여 * 자세한 스토리지 배열 정보 시작 * 을 선택한 다음 * 소프트웨어 및 펌웨어 인벤토리 * 를 선택합니다.
+
소프트웨어 및 펌웨어 인벤토리 보고서가 화면에 나타납니다.

. 소프트웨어 및 펌웨어 인벤토리를 저장하려면 * 저장 * 을 클릭합니다.
+
파일은 브라우저의 다운로드 폴더에 파일 이름과 함께 `firmware-inventory.txt` 저장됩니다.

. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

:leveloffset: -1

= 진단 데이터를 수집합니다

```
:leveloffset: +1


[[IDa5adc56514dcf3430fbe9dc250833058]]
= 지원 데이터를 수동으로 수집합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./sm-support/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
단일 파일에서 스토리지 어레이에 대한 다양한 유형의 인벤토리, 상태 및 성능 데이터를 수집할 수 있습니다. 기술 지원 부서에서는 이 파일을 사용하여 문제 해결 및 추가 분석을 수행할 수 있습니다.

.이 작업에 대해
```

AutoSupport 기능이 활성화된 경우 * AutoSupport * 탭으로 이동하여 * AutoSupport 디스패치 전송 * 을 선택하여 이 데이터를 수집할 수도 있습니다.

한 번에 하나의 수집 작업만 실행할 수 있습니다. 다른 작업을 시작하려고 하면 오류 메시지가 나타납니다.

기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 지원 데이터 수집 * 을 선택합니다.
3. 수집 * 을 클릭합니다.

   파일이 브라우저의 다운로드 폴더에 이름으로 `support-data.7z`저장됩니다. 선반에 서랍이 포함된 경우 해당 선반에 대한 진단 데이터는 라는 별도의 압축 파일에 보관됩니다. `tray-component-state-capture.7z`

4. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

구성 데이터를 수집합니다

볼륨 그룹 및 디스크 풀에 대한 모든 데이터가 포함된 RAID 구성 데이터를 컨트롤러에서 저장할 수 있습니다. 그런 다음 기술 지원 부서에 문의하여 데이터 복원에 대한 지원을 받을 수 있습니다.

이 작업에 대해

이 작업은 RAID 구성 데이터베이스의 현재 상태를 저장하는 방법을 설명합니다. 이 데이터는 컨트롤러의 RPA 메모리 위치에서 검색됩니다.

구성 데이터 수집 기능은 의 CLI 명령과 동일한 정보를 `save storageArray dbmDatabase` 저장합니다.

Recovery Guru 운영 또는 기술 지원 부서의 지시가 있는 경우에만 이 작업을 수행해야 합니다.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 구성 데이터 수집 * 을 선택합니다.
3. 대화 상자에서 * 수집 * 을 클릭합니다.

   파일,은(`configurationData-<arrayName>-<dateTime>.7z`는) 브라우저의 다운로드 폴더에 저장됩니다.

4. 파일을 보내는 방법 및 데이터를 시스템에 다시 로드하는 방법에 대한 자세한 내용은 기술 지원 부서에 문의하십시오.

복구 지원 파일을 검색합니다

기술 지원 부서에서는 복구 지원 파일을 사용하여 문제를 해결할 수 있습니다. SANtricity 시스템 관리자는 이러한 파일을 자동으로 저장합니다.

시작하기 전에

기술 지원 부서에서 문제 해결을 위해 추가 파일을 보내도록 요청했습니다.

이 작업에 대해

복구 지원 파일에는 다음과 같은 파일 유형이 포함되어 있습니다.

- 데이터 파일을 지원합니다
- AutoSupport 기록
- AutoSupport 로그
- SAS/RLS 진단 파일
- 복구 프로필 데이터
- 데이터베이스 캡처 파일

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 복구 지원 파일 검색 * 을 선택합니다.

   스토리지 배열이 수집한 모든 복구 지원 파일이 대화 상자에 나열됩니다. 특정 파일을 찾으려면 * 필터 * 상자에 원하는 열을 정렬하거나 문자를 입력하면 됩니다.

3. 파일을 선택한 다음 * 다운로드 * 를 클릭합니다.

   파일은 브라우저의 다운로드 폴더에 저장됩니다.

4. 추가 파일을 저장해야 할 경우 이전 단계를 반복합니다.

5. 닫기 * 를 클릭합니다.
6. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

추적 버퍼를 검색합니다

컨트롤러에서 추적 버퍼를 검색하여 기술 지원 부서에 파일을 보내 분석할 수 있습니다.

이 작업에 대해

펌웨어는 추적 버퍼를 사용하여 디버깅에 유용한 처리, 특히 예외 조건을 기록합니다. 스토리지 배열의 작동을 중단하지 않고 성능에 미치는 영향을 최소화하면서 추적 버퍼를 검색할 수 있습니다.

기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 추적 버퍼 검색 * 을 선택합니다.
3. 추적 버퍼를 검색할 각 컨트롤러 옆의 확인란을 선택합니다.

   하나 또는 두 컨트롤러를 모두 선택할 수 있습니다. 확인란 오른쪽에 있는 컨트롤러 상태 메시지가 Failed(실패) 또는 Disabled(비활성화) 인 경우 확인란이 비활성화됩니다.

4. 예 * 를 클릭합니다.

   파일은 브라우저의 다운로드 폴더에 파일 이름과 함께 `trace-buffers.7z` 저장됩니다.

5. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

입출력 경로 통계를 수집합니다

I/O 경로 통계 파일을 저장하고 기술 지원 부서에 보내 분석할 수 있습니다.

이 작업에 대해

기술 지원 부서에서는 I/O 경로 통계를 사용하여 성능 문제를 진단합니다. 메모리 사용률, CPU 사용률, 네트워크 지연 시간, I/O 지연 시간 또는 기타 문제로 인해 애플리케이션 성능 문제가 발생할 수 있습니다. 입출력 경로 통계는 지원 데이터 수집 중에 자동으로 수집되거나 사용자가 수동으로 수집할 수 있습니다. 또한 AutoSupport가 켜져 있는 경우 입출력 경로 통계가 자동으로 수집되어 기술 지원 부서에 전송됩니다.

입출력 경로 통계를 수집할지 확인한 후에 입출력 경로 통계에 대한 카운터가 재설정됩니다. 나중에 작업을 취소해도 카운터가 재설정됩니다. 컨트롤러가 재설정(재부팅)되면 카운터도 재설정됩니다.

기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. Collect I/O Path Statistics * 를 선택합니다.
3. 을 입력하여 작업을 수행할지 확인한 `collect` 다음 * Collect * 를 클릭합니다.

파일은 브라우저의 다운로드 폴더에 파일 이름과 함께 `io-path-statistics.7z` 저장됩니다.

4. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

상태 이미지를 검색합니다

컨트롤러의 상태 이미지를 검토할 수 있습니다. 상태 이미지는 기술 지원 부서에서 컨트롤러 문제를 진단하는 데 사용할 수 있는 컨트롤러 프로세서 메모리의 원시 데이터 덤프입니다.

이 작업에 대해

펌웨어는 특정 오류를 감지하면 자동으로 상태 이미지를 생성합니다. 상태 이미지가 생성되고 나면 오류가 발생한 컨트롤러가 재부팅되고 이벤트가 이벤트 로그에 기록됩니다.

AutoSupport를 켜면 상태 이미지가 기술 지원 부서에 자동으로 전송됩니다. AutoSupport가 켜져 있지 않은 경우 기술 지원 부서에 문의하여 상태 이미지를 검색하고 분석할 수 있도록 이미지를 보내야 합니다.

기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 상태 이미지 검색 * 을 선택합니다.

   파일을 다운로드하기 전에 세부 정보 섹션에서 상태 이미지의 크기를 확인할 수 있습니다.

3. 수집 * 을 클릭합니다.

   파일이 브라우저의 다운로드 폴더에 이름으로 `health-image.7z`저장됩니다.

4. 기술 지원 부서에서 제공하는 지침에 따라 파일을 보냅니다.

복구 작업을 수행합니다

읽을 수 없는 섹터 로그를 봅니다

읽을 수 없는 섹터 로그를 저장하고 기술 지원 부서에 파일을 보내 분석할 수 있습니다.

이 작업에 대해

읽을 수 없는 섹터 로그에는 복구할 수 없는 미디어 오류를 보고하는 드라이브로 인해 읽을 수 없는 섹터의 자세한 기록이 포함되어 있습니다. 정상적인 I/O 및 재구성 등의 수정 작업 중에 읽을 수 없는 섹터가 감지됩니다. 스토리지 어레이에서 읽을 수 없는 섹터가 감지되면 스토리지 어레이에 대한 주의 필요 경고가 나타납니다. Recovery Guru는 주의가 필요한 읽을 수 없는 섹터 상태를 구분합니다. 읽을 수 없는 섹터에 포함된 모든 데이터는 복구할 수 없으며 유실된 것으로 간주해야 합니다.

읽을 수 없는 섹터 로그는 최대 1,000개의 읽을 수 없는 섹터를 저장할 수 있습니다. 읽을 수 없는 섹터 로그가 1,000개 항목에 도달하면 다음 조건이 적용됩니다.

- 재구성 중에 읽을 수 없는 새로운 섹터가 감지되면 재구성이 실패하고 아무 항목도 기록되지 않습니다.
- I/O 중에 읽을 수 없는 새로운 섹터가 감지되면 I/O에 장애가 발생하고 항목이 기록되지 않습니다.

이러한 동작에는 오버플로가 발생하기 전에 성공한 RAID 5 쓰기 및 RAID 6 쓰기가 포함됩니다.

- 데이터 손실 가능성 * — 읽을 수 없는 섹터로부터 복구하는 것은 여러 가지 다른 방법이 수반될 수 있는 복잡한 절차입니다. 기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 읽을 수 없는 섹터 보기/지우기 * 를 선택합니다.
3. 읽을 수 없는 섹터 로그 저장하기:

   a. 표의 첫 번째 열에서 읽을 수 없는 섹터 로그를 저장할 개별 볼륨을 선택하거나(각 볼륨 옆의 확인란을 클릭) 모든 볼륨을 선택합니다(표 머리글에서 확인란 선택).

      특정 볼륨을 찾으려면 * Filter * (필터 *) 상자에 원하는 열을 정렬하거나 문자를 입력합니다.

   b. 저장 * 을 클릭합니다.

   파일이 브라우저의 다운로드 폴더에 이름으로 `unreadable-sectors.txt`저장됩니다.

4. 기술 지원 부서에서 읽을 수 없는 섹터 로그를 지우라고 지시하는 경우 다음 단계를 수행하십시오.

   a. 표의 첫 번째 열에서 읽을 수 없는 섹터 로그를 지우려는 개별 볼륨을 선택하거나(각 볼륨 옆의 확인란을 클릭) 모든 볼륨을 선택합니다(표 머리글에서 확인란 선택).

   b. 지우기 * 를 클릭하고 작업을 수행할지 확인합니다.

드라이브 포트를 다시 활성화합니다

오류 상태의 복구를 위해 수정 조치가 취해졌음을 컨트롤러에 표시할 수 있습니다.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 드라이브 포트 다시 활성화 * 를 선택하고 작업을 수행할지 확인합니다.

   이 옵션은 스토리지 배열에 드라이브 포트가 비활성화된 경우에만 나타납니다.

   잘못된 배선이 감지될 경우 컨트롤러가 비활성화된 모든 SAS 포트를 다시 활성화합니다.

복구 모드를 해제합니다

스토리지 배열 구성을 복원한 후 복구 모드 지우기 작업을 사용하여 스토리지 배열의 I/O를 재개하고 정상 작업으로 되돌립니다.

시작하기 전에

- 스토리지 배열을 이전 구성으로 되돌리려면 복구 모드를 지우기 전에 백업에서 구성을 복원해야 합니다.
- 복원 성공 여부를 확인하려면 유효성 검사를 수행하거나 기술 지원 부서에 확인해야 합니다. 복원이 성공적이었는 것을 확인한 후 복구 모드를 지울 수 있습니다.

이 작업에 대해

스토리지 어레이에는 논리적 구성(풀, 볼륨 그룹, 볼륨 등)의 레코드가 포함된 구성 데이터베이스가 포함되어 있습니다. 스토리지 배열 구성을 의도적으로 지우거나 구성 데이터베이스가 손상된 경우 스토리지 배열은 복구 모드로 전환됩니다. 복구 모드는 입출력을 중지하고 구성 데이터베이스를 중지하므로 다음 중 하나를 수행할 수 있습니다.

- 컨트롤러의 플래시 장치에 저장된 자동 백업에서 구성을 복원합니다. 이 작업을 수행하려면 기술 지원 부서에 문의해야 합니다.
- 이전 구성 데이터베이스 저장 작업에서 구성을 복원합니다. 구성 저장 데이터베이스 작업은 CLI(Command Line Interface)를 통해 수행됩니다.
- 스토리지 배열을 처음부터 다시 구성합니다.

스토리지 배열 구성을 복원하거나 재정의하고 모두 잘 되었는지 확인한 후에는 복구 모드를 수동으로 지워야 합니다.

복구 모드 지우기 작업을 시작한 후에는 취소할 수 없습니다. 복구 모드를 지우는 데 시간이 오래 걸릴 수 있습니다. 기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 지원 [지원 센터 > 진단] 탭을 선택합니다.
2. 복구 모드 지우기 * 를 선택하고 이 작업을 수행할지 확인합니다.

   이 옵션은 스토리지 배열이 복구 모드에 있는 경우에만 나타납니다.

AutoSupport 관리

AutoSupport 기능 개요

AutoSupport 기능은 스토리지 배열의 상태를 모니터링하고 자동 디스패치를 기술 지원 부서에 보냅니다.

기술 지원 부서에서는 AutoSupport 데이터를 적극적으로 활용하여 고객의 문제를 더욱 신속하게 진단 및 해결하고 사전에 잠재적 문제를 감지하고 해결합니다.

AutoSupport 데이터에는 스토리지 배열의 구성, 상태, 성능 및 시스템 이벤트에 대한 정보가 포함됩니다. AutoSupport 데이터에 사용자 데이터가 없습니다. 디스패치는 즉시 또는 일정(매일 및 매주)으로 보낼 수 있습니다.

주요 이점

AutoSupport 기능의 몇 가지 주요 이점은 다음과 같습니다.

- 신속한 케이스 해결 시간
- 보다 빠른 인시던트 관리를 위한 정교한 모니터링
- 일정에 따라 보고 자동화 및 중요 이벤트에 대한 자동 보고 기능
- 드라이브와 같은 선택한 구성 요소에 대한 자동 하드웨어 교체 요청
- 운영 환경에 영향을 주지 않는 경고 기능을 통해 문제를 알리고 기술 지원 부서에서 수정 조치를 취할 수 있도록 정보를 제공합니다
- 알려진 구성 문제에 대한 디스패치를 모니터링하는 AutoSupport 분석 도구입니다

개별 **AutoSupport** 기능

AutoSupport 기능은 사용자가 별도로 사용하는 세 가지 개별 기능으로 구성됩니다.

- * 기본 AutoSupport * — 스토리지 어레이에서 자동으로 데이터를 수집하여 기술 지원 부서에 전송할 수 있습니다.
- * AutoSupport OnDemand * — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 이전 AutoSupport 디스패치의 재전송을 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 재전송 요청이 있는지 확인하고 그에 따라 응답합니다.
- * 원격 진단* — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 새로운 최신 AutoSupport 디스패치를 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 새 요청이 있는지 확인하고 그에 따라 응답합니다.

AutoSupport와 지원 데이터 수집의 차이

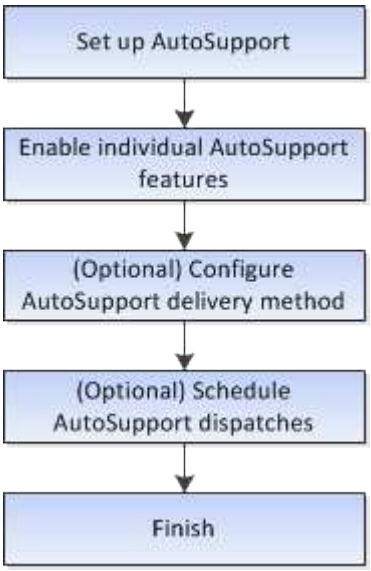
스토리지 시스템에 두 가지 방법으로 지원 데이터를 수집할 수 있습니다.

- * AutoSupport Feature * — 데이터가 자동으로 수집됩니다.
- * 지원 데이터 수집 옵션 * — 데이터를 수동으로 수집 및 전송해야 합니다.

AutoSupport 기능은 데이터가 자동으로 수집되고 전송되므로 사용이 간편합니다. AutoSupport 데이터를 사전에 사용하여 문제가 발생하기 전에 방지할 수 있습니다. AutoSupport 기능은 기술 지원 부서에서 이미 데이터에 액세스할 수 있기 때문에 문제 해결 시간이 단축됩니다. 이러한 이유로 AutoSupport 기능은 사용하는 기본 데이터 수집 방법입니다.

AutoSupport 기능의 워크플로

SANtricity 시스템 관리자에서 다음 단계를 수행하여 AutoSupport 기능을 구성합니다.



AutoSupport 기능을 활성화 또는 비활성화합니다

초기 설정 중에 AutoSupport 기능 및 개별 AutoSupport 기능을 활성화하거나 나중에 활성화하거나 비활성화할 수 있습니다.

시작하기 전에

AutoSupport OnDemand 또는 원격 진단을 활성화하려면 AutoSupport 전송 방법을 HTTPS로 설정해야 합니다.

이 작업에 대해

언제든지 AutoSupport 기능을 사용하지 않도록 설정할 수 있지만, 이 기능을 활성 상태로 두는 것이 좋습니다. AutoSupport 기능을 사용하면 스토리지 어레이에서 문제가 발생할 경우 문제 확인 및 해결 속도를 크게 높일 수 있습니다.

AutoSupport 기능은 사용자가 별도로 사용하는 세 가지 개별 기능으로 구성됩니다.

- * 기본 AutoSupport * — 스토리지 어레이에서 자동으로 데이터를 수집하여 기술 지원 부서에 전송할 수 있습니다.
- * AutoSupport OnDemand * — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 이전 AutoSupport 디스패치의 재전송을 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 재전송 요청이 있는지 확인하고 그에 따라 응답합니다.
- * 원격 진단* — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 새로운 최신 AutoSupport 디스패치를 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 새 요청이 있는지 확인하고 그에 따라 응답합니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 기능 활성화/비활성화 * 를 선택합니다.
3. 활성화할 AutoSupport 기능 옆의 확인란을 선택합니다.

   피처는 대화 상자의 항목 들여쓰기로 표시되는 대로 서로 다릅니다. 예를 들어 원격 진단을 활성화하려면 AutoSupport OnDemand를 활성화해야 합니다.

4. 저장 * 을 클릭합니다.

   AutoSupport를 사용하지 않도록 설정하면 홈 페이지에 알림이 표시됩니다. 무시 * 를 클릭하여 알림을 해제할 수 있습니다.

AutoSupport 전달 방법을 구성합니다

AutoSupport 기능은 기술 지원 부서에 디스패치를 제공하기 위해 HTTPS, HTTP 및 SMTP 프로토콜을 지원합니다.

시작하기 전에

- AutoSupport 기능을 활성화해야 합니다. AutoSupport 페이지에서 활성화되어 있는지 여부를 확인할 수 있습니다.
- 네트워크에 DNS 서버가 설치 및 구성되어 있어야 합니다. DNS 서버 주소는 System Manager에서 구성해야 합니다(이 작업은 하드웨어 페이지에서 사용 가능).

이 작업에 대해

다양한 프로토콜을 검토합니다.

- * HTTPS * — HTTPS를 사용하여 대상 기술 지원 서버에 직접 연결할 수 있습니다. AutoSupport OnDemand 또는 원격 진단을 활성화하려면 AutoSupport 전송 방법을 HTTPS로 설정해야 합니다.

- * HTTP * — HTTP를 사용하여 대상 기술 지원 서버에 직접 연결할 수 있습니다.
- * 이메일 * — 이메일 서버를 AutoSupport 디스패치 전송 방법으로 사용할 수 있습니다.

- HTTPS/HTTP와 이메일 방법의 차이점 *. SMTP를 사용하는 이메일 전송 방법은 HTTPS 및 HTTP 전송 방법과 몇 가지 중요한 차이점이 있습니다. 먼저, 이메일 방법에 대한 디스패치 크기는 5MB로 제한되며, 이는 일부 ASUP 데이터 수집이 디스패치되지 않음을 의미합니다. 둘째, AutoSupport OnDemand 기능은 HTPP 및 HTTPS 방법에서만 사용할 수 있습니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 제공 방법 구성 * 을 선택합니다.

   디스패치 제공 방법이 나열된 대화 상자가 나타납니다.

3. 원하는 전달 방법을 선택한 다음 해당 전달 방법에 대한 매개 변수를 선택합니다. 다음 중 하나를 수행합니다.
   - HTTPS 또는 HTTP를 선택한 경우 다음 전송 매개 변수 중 하나를 선택합니다.
     - * 직접 * — 이 전달 매개 변수는 기본 선택 항목입니다. 이 옵션을 선택하면 HTTPS 또는 HTTP 프로토콜을 사용하여 대상 기술 지원 시스템에 직접 연결할 수 있습니다.
     - * 프록시 서버를 통해 * — 이 옵션을 선택하면 대상 기술 지원 시스템과의 연결을 설정하는 데 필요한 HTTP 프록시 서버 세부 정보를 지정할 수 있습니다. 호스트 주소와 포트 번호를 지정해야 합니다. 그러나 필요한 경우 호스트 인증 세부 정보(사용자 이름 및 암호)만 입력하면 됩니다.
     - * 프록시 자동 구성 스크립트(PAC)를 통해 * — 프록시 자동 구성(PAC) 스크립트 파일의 위치를 지정합니다. PAC 파일을 사용하면 시스템이 대상 기술 지원 시스템과의 연결을 설정할 적절한 프록시 서버를 자동으로 선택할 수 있습니다.
   - 이메일 을 선택한 경우 다음 정보를 입력합니다.
     - 메일 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소입니다.
     - AutoSupport 디스패치 이메일의 보낸 사람 필드에 나타나는 이메일 주소입니다.
     - * 선택 사항. 구성 테스트를 수행하려면 *: AutoSupport 시스템이 테스트 디스패치를 받을 때 확인을 보내는 이메일 주소입니다.
     - 메시지를 암호화하려면 암호화 유형으로 * SMTPS * 또는 * STARTTLS * 를 선택한 다음 암호화된 메시지의 포트 번호를 선택합니다. 그렇지 않으면 * 없음 * 을 선택합니다.
     - 필요한 경우 보내는 보낸 사람과 메일 서버에서 인증을 위한 사용자 이름과 암호를 입력합니다.
4. 이러한 ASUP 디스패치의 전달을 차단하는 방화벽이 있는 경우 화이트리스트에 다음 URL을 추가합니다. `https://support.netapp.com/put/AsupPut/`
5. 지정된 전달 매개 변수를 사용하여 기술 지원 서버에 대한 연결을 테스트하려면 * Test Configuration * 을 클릭합니다. AutoSupport 온디맨드 기능을 활성화한 경우 AutoSupport OnDemand 디스패치 전달에 대한 연결도 테스트합니다.

   구성 테스트에 실패하면 구성 설정을 확인하고 테스트를 다시 실행하십시오. 테스트가 계속 실패하면 기술 지원 부서에 문의하십시오.

6. 저장 * 을 클릭합니다.

AutoSupport 디스패치를 예약합니다

SANtricity System Manager에서 AutoSupport 디스패치에 대한 기본 일정을 자동으로 생성합니다. 원하는 경우 자신의 일정을 지정할 수 있습니다.

시작하기 전에

AutoSupport 기능을 활성화해야 합니다. AutoSupport 페이지에서 활성화되어 있는지 여부를 확인할 수 있습니다.

이 작업에 대해

- * 일일 시간 * — 매일 디스패치는 사용자가 지정한 시간 범위 동안 수집되어 매일 발송됩니다. System Manager는 범위 내에서 임의의 시간을 선택합니다. 모든 시간은 UTC(협정 세계시)로 스토리지의 현지 시간과 다를 수 있습니다. 스토리지의 현지 시간을 UTC로 변환해야 합니다.
- * Weekly Day * — 매주 디스패치가 수집되어 일주일에 한 번 발송됩니다. System Manager는 사용자가 지정한 일 중에서 임의의 날짜를 선택합니다. 주별 디스패치를 허용하지 않을 요일을 선택 취소합니다. System Manager는 허용되는 일 중에서 임의의 일을 선택합니다.
- * Weekly Time * — 매주 디스패치는 사용자가 지정한 시간 범위 동안 매주 한 번 수집 및 전송됩니다. System Manager는 범위 내에서 임의의 시간을 선택합니다. 모든 시간은 UTC(협정 세계시)로 스토리지의 현지 시간과 다를 수 있습니다. 스토리지의 현지 시간을 UTC로 변환해야 합니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 디스패치 예약 * 을 선택합니다.

   AutoSupport 디스패치 예약 마법사가 나타납니다.

3. 마법사의 단계를 따릅니다.

AutoSupport 디스패치를 보냅니다

SANtricity 시스템 관리자를 사용하면 예약된 디스패치가 필요해질 때까지 기다리지 않고 AutoSupport 디스패치를 기술 지원으로 보낼 수 있습니다.

시작하기 전에

AutoSupport 기능을 활성화해야 합니다. AutoSupport 페이지에서 활성화되어 있는지 여부를 확인할 수 있습니다.

이 작업에 대해

이 작업은 지원 데이터를 수집하여 기술 지원 부서에 자동으로 전송하므로 문제를 해결할 수 있습니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. Send AutoSupport Dispatch(디스패치 전송) * 를 선택합니다.

   AutoSupport 디스패치 보내기 대화 상자가 나타납니다.

3. Send * 를 선택하여 작업을 확인합니다.

AutoSupport 상태를 봅니다

AutoSupport 페이지에는 AutoSupport 기능 및 개별 AutoSupport 기능이 현재 활성화되어 있는지 여부가 표시됩니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. 탭 바로 아래의 페이지 오른쪽에서 기본 AutoSupport 기능이 활성화되어 있는지 확인합니다.
3. 커서를 물음표 위로 가져가면 개별 AutoSupport 기능이 활성화되었는지 확인할 수 있습니다.

AutoSupport 로그를 봅니다

AutoSupport 로그는 AutoSupport 디스패치 제공 중 발생한 상태, 디스패치 기록 및 오류에 대한 정보를 제공합니다.

이 작업에 대해

여러 로그 파일이 있을 수 있습니다. 현재 로그 파일이 200KB에 도달하면 보관되고 새 로그 파일이 생성됩니다. 보관된 로그 파일 이름은 `ASUPMessages.n`입니다. 여기서 _n_은 1에서 9 사이의 정수입니다. 로그 파일이 여러 개 있는 경우 최신 로그 또는 이전 로그를 보도록 선택할 수 있습니다.

- * 현재 로그 * — 최근 캡처된 이벤트 목록을 표시합니다.
- * Archived log * — 이전 이벤트 목록을 표시합니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 로그 보기 * 를 선택합니다.

   현재 AutoSupport 로그를 나열하는 대화 상자가 나타납니다.

3. 이전 AutoSupport 로그를 보려면 * Archived * 라디오 버튼을 선택한 다음 * AutoSupport 로그 선택 * 드롭다운 목록에서 로그를 선택합니다.

   아카이브된 로그는 스토리지 배열에 있는 경우에만 Archived(보관됨) 옵션이 나타납니다.

   선택한 AutoSupport 로그가 대화 상자에 나타납니다.

4. * 선택 사항: * AutoSupport 로그를 검색하려면 * 찾기 * 상자에 용어를 입력하고 * 찾기 * 를 클릭합니다.

   검색어를 추가로 검색하려면 * 찾기 * 를 다시 클릭합니다.

AutoSupport 유지 관리 창을 활성화합니다

AutoSupport 유지 관리 창을 활성화하여 오류 이벤트 시 티켓 자동 생성을 억제합니다. 정상 작동 모드에서 스토리지 어레이는 AutoSupport를 사용하여 문제가 있는 경우 지원 케이스를 엽니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 유지 관리 창 활성화 * 를 선택합니다.
3. 유지보수 윈도우 요청이 처리되었다는 확인 메시지를 받으려면 이메일 주소를 입력하십시오.

   구성에 따라 최대 5개의 이메일 주소를 입력할 수 있습니다. 둘 이상의 주소를 추가하려면 * 다른 이메일 추가 * 를 선택하여 다른 필드를 엽니다.

4. 유지 보수 창을 활성화할 기간(시간)을 지정합니다.

   최대 지원 시간은 72시간입니다.

5. 예 * 를 클릭합니다.

   오류 이벤트에 대한 AutoSupport 자동 티켓 생성이 지정된 기간 동안 일시적으로 억제됩니다.

작업을 마친 후

스토리지 어레이의 요청이 AutoSupport 서버에 의해 처리될 때까지 유지보수 윈도우가 시작되지 않습니다. 스토리지 시스템에서 유지 관리 작업을 수행하기 전에 확인 이메일을 받을 때까지 기다립니다.

AutoSupport 유지 보수 창을 비활성화합니다

AutoSupport 유지 관리 창을 비활성화하여 오류 이벤트에 대한 티켓 자동 생성을 허용합니다. AutoSupport 유지 관리 창이 비활성화된 경우 스토리지 어레이는 AutoSupport를 사용하여 문제가 있는 경우 지원 케이스를 엽니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 유지 관리 창 비활성화 * 를 선택합니다.
3. 유지보수 윈도우 비활성화 요청이 처리되었다는 확인 메시지를 받으려면 이메일 주소를 입력하십시오.

   구성에 따라 최대 5개의 이메일 주소를 입력할 수 있습니다. 둘 이상의 주소를 추가하려면 * 다른 이메일 추가 * 를 선택하여 다른 필드를 엽니다.

4. 예 * 를 클릭합니다.

   오류 이벤트에 대한 AutoSupport 자동 티켓 생성이 활성화됩니다.

작업을 마친 후

AutoSupport 서버에서 스토리지 어레이의 요청을 처리할 때까지 유지 관리 기간이 종료되지는 않습니다. 계속하기 전에 확인 이메일을 받을 때까지 기다리십시오.

이벤트를 봅니다

이벤트 로그 개요

이벤트 로그는 스토리지 어레이에서 발생한 이벤트에 대한 기록 기록을 제공하여 기술 지원 부서에서 장애가 발생할 수 있는 이벤트 문제를 해결하는 데 도움이 됩니다.

스토리지 배열 이벤트를 추적하기 위해 Recovery Guru에 이벤트 로그를 보조 진단 도구로 사용할 수 있습니다. 스토리지 어레이의 구성 요소 장애로부터 복구하려고 할 때 항상 Recovery Guru를 먼저 참조하십시오.

이벤트 범주

이벤트 로그의 이벤트는 다양한 상태로 분류됩니다. 조치를 취해야 하는 이벤트에는 다음과 같은 상태가 있습니다.

- 심각
- 경고

정보 제공이며 즉각적인 조치가 필요하지 않은 이벤트는 다음과 같습니다.

- 정보 제공

중요 이벤트

중요 이벤트는 스토리지 배열에 문제가 있음을 나타냅니다. 중요한 이벤트를 즉시 해결할 경우 데이터 액세스 손실을 방지할 수 있습니다.

중요한 이벤트가 발생하면 이벤트 로그에 기록됩니다. 모든 중요 이벤트는 SNMP 관리 콘솔 또는 경고 알림을 수신하도록 구성된 e-메일 수신자에게 전송됩니다. 이벤트 발생 시 쉘프 ID를 모를 경우 쉘프 ID가 "쉘프 알 수 없음"으로 표시됩니다.

중요한 이벤트를 수신할 경우 Recovery Guru 절차를 참조하여 중요한 이벤트에 대한 자세한 설명을 확인하십시오. Recovery Guru 절차를 완료하여 중요한 이벤트를 해결하십시오. 특정 중요 이벤트를 해결하려면 기술 지원 부서에 문의해야 할 수 있습니다.

이벤트 로그를 사용하여 이벤트를 봅니다

스토리지 어레이에서 발생한 이벤트의 기록 레코드를 제공하는 이벤트 로그를 볼 수 있습니다.

단계

1. 메뉴 선택: 지원 [이벤트 로그].

   이벤트 로그 페이지가 나타납니다.

페이지 세부 정보

항목	설명
모두 보기 필드	모든 이벤트와 위험 이벤트 및 경고 이벤트만 전환합니다.
필터 필드	이벤트를 필터링합니다. 특정 구성 요소, 특정 이벤트 등과 관련된 이벤트만 표시하는 데 유용합니다
열 선택 아이콘	볼 다른 열을 선택할 수 있습니다. 다른 열은 이벤트에 대한 추가 정보를 제공합니다.
확인란을 선택합니다	저장할 이벤트를 선택할 수 있습니다. 표 머리글의 확인란을 선택하면 모든 이벤트가 선택됩니다.
날짜/시간 열	컨트롤러 시계에 따라 이벤트의 날짜 및 시간 스탬프입니다. 이벤트 로그는 처음에 시퀀스 번호를 기반으로 이벤트를 정렬합니다. 일반적으로 이 순서는 날짜 및 시간과 일치합니다. 그러나 스토리지 어레이에서 두 컨트롤러 클럭의 동기화가 해제됩니다. 이 경우, 이벤트 및 표시된 날짜 및 시간과 관련하여 일부 인지된 비일관성이 이벤트 로그에 나타날 수 있습니다.
우선 순위 열	이러한 우선순위 값은 다음과 같습니다. • * Critical * — 스토리지 배열에 문제가 있습니다. 그러나 즉각적인 조치를 취하는 경우 데이터에 대한 액세스가 손실되는 것을 방지할 수 있습니다. 중요 이벤트는 경고 알림에 사용됩니다. 모든 중요 이벤트는 네트워크 관리 클라이언트(SNMP 트랩 사용) 또는 구성한 전자 메일 수신자에게 전송됩니다. • * 경고 * — 스토리지 배열의 성능과 복구 기능이 다른 오류에서 저하되어 오류가 발생했습니다. • * 정보 * — 스토리지 어레이와 관련된 중요하지 않은 정보입니다.
부품 유형 열	이벤트의 영향을 받는 구성 요소입니다. 구성 요소는 드라이브 또는 컨트롤러와 같은 하드웨어이거나 컨트롤러 펌웨어와 같은 소프트웨어일 수 있습니다.
부품 위치 열	스토리지 배열에 있는 구성 요소의 물리적 위치입니다.
설명 열	이벤트에 대한 설명입니다. • 예제 * — `Drive write failure - retries exhausted`
시퀀스 번호 열	스토리지 배열의 특정 로그 항목을 고유하게 식별하는 64비트 번호입니다. 이 숫자는 모든 새 이벤트 로그 항목에 대해 하나씩 증가합니다. 이 정보를 표시하려면 * 열 선택 * 아이콘을 클릭합니다.

항목	설명
이벤트 유형 열	기록된 이벤트의 각 유형을 식별하는 4자리 숫자 이 정보를 표시하려면 * 열 선택 * 아이콘을 클릭합니다.
이벤트 특정 코드 열	이 정보는 기술 지원 부서에서 사용합니다. 이 정보를 표시하려면 * 열 선택 * 아이콘을 클릭합니다.
이벤트 범주 열	• 오류 – 스토리지 배열의 구성요소에 장애가 발생했습니다(예: 드라이브 장애 또는 배터리 장애). • 상태 변경 – 상태가 변경된 스토리지 배열의 요소(예: 볼륨이 최적 상태로 전환되었거나 컨트롤러가 오프라인 상태로 전환된 경우) • 내부 – 사용자 작업이 필요하지 않은 내부 컨트롤러 작업(예: 컨트롤러가 당일 시작을 완료함) • 명령 – 스토리지 배열에 대해 실행된 명령(예: 핫 스페어가 할당되었습니다. • 오류 – 스토리지 배열에서 오류 상태가 감지되었습니다. 예를 들어, 컨트롤러가 캐시를 동기화 및 제거할 수 없거나 스토리지 배열에서 중복 오류가 감지되었습니다. • 일반 – 다른 범주에 적합하지 않은 모든 이벤트. 이 정보를 표시하려면 칼럼 선택 아이콘을 클릭합니다.
로그자 열	이벤트를 기록한 컨트롤러의 이름입니다. 이 정보를 표시하려면 칼럼 선택 아이콘을 클릭합니다.

2. 스토리지 배열에서 새 이벤트를 검색하려면 새로 고침 을 클릭합니다.

   이벤트가 로깅되고 이벤트 로그 페이지에 표시되려면 몇 분 정도 걸릴 수 있습니다.

3. 이벤트 로그를 파일에 저장하려면 다음을 수행합니다.
   a. 저장할 각 이벤트 옆에 있는 확인란을 선택합니다.
   b. 저장 * 을 클릭합니다.

      파일이 브라우저의 다운로드 폴더에 이름으로 `major-event-log-timestamp.log`저장됩니다.

4. 이벤트 로그에서 이벤트를 지우려면 다음을 수행합니다.

   이벤트 로그는 이벤트를 새 이벤트로 바꾸기 전에 약 8,000개의 이벤트를 저장합니다. 이벤트를 유지하려면 이벤트를 저장하고 이벤트 로그에서 해당 이벤트를 지울 수 있습니다.

   a. 먼저 이벤트 로그를 저장합니다.
   b. 모두 지우기 * 를 클릭하고 작업을 수행할지 확인합니다.

업그레이드 관리

Upgrade Center를 사용하여 최신 소프트웨어 및 펌웨어를 다운로드하고 컨트롤러와 드라이브를 업그레이드합니다.

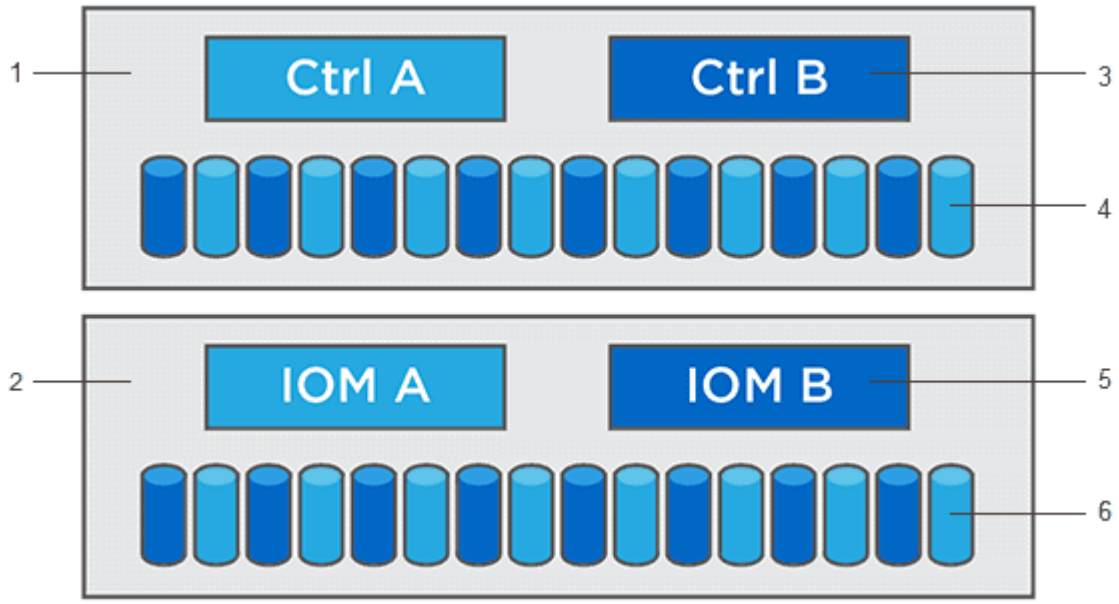
컨트롤러 업그레이드 개요

모든 최신 기능 및 버그 픽스에 대해 스토리지 어레이의 소프트웨어 및 펌웨어를 업그레이드할 수 있습니다.

OS 컨트롤러 업그레이드에 포함된 구성 요소

여러 스토리지 배열 구성 요소에는 가끔 업그레이드하려는 소프트웨어나 하드웨어가 포함되어 있습니다.

- * 관리 소프트웨어 * — System Manager는 스토리지 배열을 관리하는 소프트웨어입니다.
- * 컨트롤러 펌웨어 * — 컨트롤러 펌웨어는 호스트와 볼륨 간의 I/O를 관리합니다.
- * 컨트롤러 NVSRAM * — 컨트롤러 NVSRAM은 컨트롤러의 기본 설정을 지정하는 컨트롤러 파일입니다.
- * IOM 펌웨어 * — I/O 모듈(IOM) 펌웨어는 컨트롤러와 드라이브 쉘프 간의 연결을 관리합니다. 또한 구성 요소의 상태를 모니터링합니다.
- * Supervisor 소프트웨어 * — Supervisor 소프트웨어는 소프트웨어가 실행되는 컨트롤러의 가상 머신입니다.



[1]컨트롤러 쉘프;[2]드라이브 쉘프;[3]소프트웨어, 컨트롤러 펌웨어, 컨트롤러 NVSRAM, 감독자 소프트웨어;[4]드라이브 펌웨어;[5]IOM 펌웨어;[6]드라이브 펌웨어

소프트웨어 및 펌웨어 인벤토리 대화 상자에서 현재 소프트웨어 및 펌웨어 버전을 볼 수 있습니다. 지원 [업그레이드 센터] 메뉴로 이동한 다음 * 소프트웨어 및 펌웨어 인벤토리 * 링크를 클릭합니다.

업그레이드 프로세스의 일부로 호스트의 다중 경로/페일오버 드라이버 및/또는 HBA 드라이버도 업그레이드해야 호스트가 컨트롤러와 올바르게 상호 작용할 수 있습니다. 이 경우에 해당하는지 확인하려면 을 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

I/O 중지 시기

스토리지 어레이에 2개의 컨트롤러가 포함되어 있고 다중 경로 드라이버가 설치되어 있는 경우 업그레이드가 진행되는 동안 스토리지 어레이가 I/O 처리를 계속할 수 있습니다. 업그레이드 중에 컨트롤러 A가 모든 볼륨을 컨트롤러 B로 페일오버하고, 업그레이드하고, 해당 볼륨과 모든 컨트롤러 B의 볼륨을 되찾은 다음 컨트롤러 B를 업그레이드합니다

업그레이드 전 상태 점검

업그레이드 전 상태 점검이 업그레이드 프로세스의 일부로 실행됩니다. 업그레이드 전 상태 점검을 통해 모든 스토리지 시스템 구성 요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다. 다음 조건에서는 업그레이드가 되지 않을 수 있습니다.

- 할당된 드라이브에 오류가 발생했습니다
- 핫 스페어가 사용 중입니다
- 볼륨 그룹이 불완전합니다
- 단독 운영 실행 중
- 볼륨이 누락되었습니다
- 컨트롤러가 최적화되지 않은 상태입니다
- 이벤트 로그 이벤트의 수가 너무 넘습니다
- 구성 데이터베이스 유효성 검사에 실패했습니다
- DACstore의 이전 버전이 있는 드라이브입니다

업그레이드를 수행하지 않고 업그레이드 전 상태 점검을 별도로 실행할 수도 있습니다.

드라이브 업그레이드 개요

드라이브 펌웨어는 드라이브의 낮은 수준의 작동 특성을 제어합니다. 드라이브 제조업체는 주기적으로 드라이브 펌웨어의 업데이트를 릴리스하여 새로운 기능을 추가하고 성능을 개선하며 결함을 수정합니다.

드라이브 펌웨어의 온라인 및 오프라인 업그레이드

드라이브 펌웨어의 업그레이드 방법에는 온라인 및 오프라인 두 가지가 있습니다.

온라인

온라인 업그레이드 중에 드라이브는 한 번에 하나씩 순차적으로 업그레이드됩니다. 스토리지 시스템은 업그레이드가 진행되는 동안 입출력을 계속 처리합니다. I/O를 중지할 필요가 없습니다 드라이브에서 온라인 업그레이드를 수행할 수 있는 경우 온라인 방법이 자동으로 사용됩니다.

온라인 업그레이드를 수행할 수 있는 드라이브는 다음과 같습니다.

- 드라이브가 최적의 풀에 있을 때
- 최적의 중복 볼륨 그룹의 드라이브(RAID 1, RAID 5 및 RAID 6)
- 할당되지 않은 드라이브
- 대기 핫 스페어 드라이브

드라이브 펌웨어의 온라인 업그레이드를 수행하는 데 몇 시간이 걸릴 수 있으며, 스토리지 어레이가 잠재적인 볼륨

장애에 노출될 수 있습니다. 다음과 같은 경우 볼륨 장애가 발생할 수 있습니다.

- RAID 1 또는 RAID 5 볼륨 그룹에서 볼륨 그룹의 다른 드라이브가 업그레이드되는 동안 하나의 드라이브에 장애가 발생합니다.
- RAID 6 풀 또는 볼륨 그룹에서 풀 또는 볼륨 그룹의 다른 드라이브가 업그레이드되는 동안 두 개의 드라이브에 장애가 발생합니다.

오프라인(병렬)

오프라인 업그레이드 중에 동일한 드라이브 유형의 모든 드라이브가 동시에 업그레이드됩니다. 이 방법을 사용하려면 선택한 드라이브와 연결된 볼륨에 대한 I/O 작업을 중단해야 합니다. 여러 드라이브를 동시에 업그레이드할 수 있으므로(병렬로) 전체 다운타임이 크게 줄어듭니다. 드라이브에서 오프라인 업그레이드만 수행할 수 있는 경우 오프라인 방법이 자동으로 사용됩니다.

다음 드라이브는 오프라인 방법을 사용해야 합니다.

- 비중복 볼륨 그룹의 드라이브(RAID 0)
- 최적화되지 않은 풀 또는 볼륨 그룹의 드라이브입니다
- SSD 캐시 내 드라이브

호환성

각 드라이브 펌웨어 파일에는 펌웨어가 실행되는 드라이브 유형에 대한 정보가 들어 있습니다. 지정된 펌웨어 파일은 호환되는 드라이브에만 다운로드할 수 있습니다. System Manager는 업그레이드 프로세스 중에 호환성을 자동으로 확인합니다.

컨트롤러 소프트웨어 및 펌웨어를 업그레이드합니다

스토리지 어레이의 소프트웨어 및 선택적으로 IOM 펌웨어 및 NVSRAM(Nonvolatile Static Random Access Memory)을 업그레이드하여 최신 기능 및 버그 수정을 가할 수 있습니다.

시작하기 전에

- IOM 펌웨어를 업그레이드할지 여부를 알고 있습니다.

  일반적으로 모든 구성 요소를 동시에 업그레이드해야 합니다. 하지만 SANtricity OS 소프트웨어 업그레이드의 일부로 업그레이드하지 않으려는 경우 또는 기술 지원 부서에서 IOM 펌웨어를 다운그레이드하도록 지시한 경우(명령줄 인터페이스를 사용하여 펌웨어를 다운그레이드할 수만 있음) IOM 펌웨어를 업그레이드하지 않을 수도 있습니다.

- 컨트롤러 NVSRAM 파일을 업그레이드할지 여부를 알 수 있습니다.

  일반적으로 모든 구성 요소를 동시에 업그레이드해야 합니다. 그러나 파일이 패치되었거나 사용자 정의 버전이고 덮어쓰지 않으려는 경우 컨트롤러 NVSRAM 파일을 업그레이드하지 않을 수 있습니다.

- 지금 또는 나중에 OS 업그레이드를 활성화할지 여부를 알 수 있습니다.

  나중에 활성화하는 이유는 다음과 같습니다.

  ◦ * 시간 * — 소프트웨어 및 펌웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 로드가 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.

◦ * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

- 보안이 설정되지 않은 드라이브로부터 전환할지 또는 드라이브 보안을 위해 외부 키 관리 서버(KMS)를 사용하기 위해 내부적으로 보안된 드라이브로부터 전환할지 여부를 알 수 있습니다.
- 스토리지 시스템에서 역할 기반 액세스 제어를 사용할지 여부를 알 수 있습니다.

이 작업에 대해

OS 소프트웨어 파일만 업그레이드하거나 컨트롤러 NVSRAM 파일만 업그레이드하도록 선택할 수 있으며 두 파일을 모두 업그레이드하도록 선택할 수도 있습니다.

기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

- 데이터 손실 또는 스토리지 배열 손상 위험 * — 업그레이드 중에 스토리지 배열을 변경하지 마십시오. 스토리지 어레이에 대한 전원을 유지합니다.

단계

1. 스토리지 배열에 컨트롤러가 하나만 포함되어 있거나 다중 경로 드라이버가 설치되어 있지 않은 경우, 어플리케이션 오류를 방지하기 위해 스토리지 배열에 대한 I/O 작업을 중지합니다. 스토리지 어레이에 2개의 컨트롤러가 있는데 다중 경로 드라이버가 설치되어 있는 경우 I/O 작업을 중지할 필요가 없습니다.
2. 메뉴 선택: 지원 [업그레이드 센터].
3. Support 사이트에서 관리 클라이언트로 새 파일을 다운로드합니다.
   a. 지원 웹 사이트를 시작하려면 * NetApp Support * 를 클릭합니다.
   b. 지원 웹 사이트에서 * 다운로드 * 탭을 클릭한 다음 * 다운로드 * 를 선택합니다.
   c. E-Series SANtricity OS 컨트롤러 소프트웨어 * 를 선택합니다.
   d. 나머지 지침을 따릅니다.

   버전 8.42 이상에서는 디지털 서명된 펌웨어가 필요합니다. 서명되지 않은 펌웨어를 다운로드하려고 하면 오류가 표시되고 다운로드가 중단됩니다.
4. 현재 IOM 펌웨어를 업그레이드하지 않으려면 * IOM 자동 동기화 일시 중지 * 를 클릭합니다.

   단일 컨트롤러가 있는 스토리지 어레이를 사용하는 경우 IOM 펌웨어가 업그레이드되지 않습니다.
5. SANtricity OS 소프트웨어 업그레이드 아래에서 * 업그레이드 시작 * 을 클릭합니다.

   SANtricity OS 소프트웨어 업그레이드 대화 상자가 나타납니다.
6. 업그레이드 프로세스를 시작하려면 하나 이상의 파일을 선택하십시오.
   a. 찾아보기 * 를 클릭하고 지원 웹 사이트에서 다운로드한 OS 소프트웨어 파일을 탐색하여 SANtricity OS 소프트웨어 파일을 선택합니다.
   b. [찾아보기] * 를 클릭하고 지원 사이트에서 다운로드한 NVSRAM 파일로 이동하여 컨트롤러 NVSRAM 파일을 선택합니다. 컨트롤러 NVSRAM 파일의 파일 이름은 과 `N2800-830000-000.dlp`유사합니다.

      이러한 작업은 다음과 같이 수행됩니다.

      - 기본적으로 현재 스토리지 배열 구성과 호환되는 파일만 표시됩니다.

- 업그레이드할 파일을 선택하면 파일 이름과 크기가 나타납니다.

7. * 선택 사항: * 업그레이드할 SANtricity OS 소프트웨어 파일을 선택한 경우 지금 파일 전송 * 확인란을 선택하여 활성화하지 않고 컨트롤러로 파일을 전송할 수 있습니다(나중에 업그레이드 활성화) *.
8. 시작 * 을 클릭하고 작업을 수행할지 확인합니다.

   업그레이드 전 상태 점검 중에는 작업을 취소할 수 있지만 전송 또는 활성화 중에는 취소할 수 없습니다.

9. * 선택 사항: * 업그레이드된 항목 목록을 보려면 * 로그 저장 * 을 클릭합니다.

   파일이 브라우저의 다운로드 폴더에 이름으로 `drive_upgrade_log-timestamp.txt`저장됩니다.

작업을 마친 후

- 하드웨어 페이지에 모든 구성 요소가 나타나는지 확인합니다.
- 소프트웨어 및 펌웨어 인벤토리 대화 상자(지원 [업그레이드 센터] 메뉴로 이동한 다음 * 소프트웨어 및 펌웨어 인벤토리 * 링크를 클릭하여 소프트웨어 및 펌웨어 버전을 확인합니다.
- 컨트롤러 NVSRAM을 업그레이드한 경우 기존 NVSRAM에 적용한 모든 사용자 정의 설정은 활성화 과정 중에 손실됩니다. 활성화 프로세스가 완료된 후 NVSRAM에 사용자 정의 설정을 다시 적용해야 합니다.

컨트롤러 소프트웨어 및 펌웨어를 활성화합니다

업그레이드 파일을 즉시 활성화하거나 더 편리한 시간이 될 때까지 기다릴 수 있습니다.

이 작업에 대해

파일을 활성화하지 않고 다운로드 및 전송할 수 있습니다. 다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

- * 시간 * — 소프트웨어 및 펌웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 로드가 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
- * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

전송되었지만 활성화되지 않은 소프트웨어 또는 펌웨어가 있는 경우 System Manager 홈 페이지의 알림 영역과 업그레이드 센터 페이지에서 알림이 표시됩니다.

활성화 프로세스가 시작된 후에는 중지할 수 없습니다.

단계

1. 메뉴 선택: 지원 [업그레이드 센터].
2. SANtricity OS 컨트롤러 소프트웨어 업그레이드 영역에서 * 활성화 * 를 클릭하고 작업을 수행할지 확인합니다.

   업그레이드 전 상태 점검 중에는 작업을 취소할 수 있지만 활성화하는 동안에는 취소할 수 없습니다.

   업그레이드 전 상태 점검이 시작됩니다. 업그레이드 전 상태 점검을 통과하면 업그레이드 프로세스에서 파일 활성화를 진행합니다. 업그레이드 전 상태 점검에 실패하면 Recovery Guru를 사용하거나 기술 지원 부서에 문의하여 문제를 해결하십시오. 일부 유형의 경우, 기술 지원 부서에서는 오류 발생 시 * 업그레이드 허용 * 확인란을 선택하여 업그레이드를 계속하도록 조언할 수 있습니다.

업그레이드 전 상태 점검이 성공적으로 완료되면 활성화가 발생합니다. 활성화하는 데 걸리는 시간은 스토리지 배열 구성과 활성화 중인 구성 요소에 따라 달라집니다.

3. * 선택 사항: * 업그레이드된 항목 목록을 보려면 * 로그 저장 * 을 클릭합니다.

   파일이 브라우저의 다운로드 폴더에 이름으로 `drive_upgrade_log-timestamp.txt`저장됩니다.

작업을 마친 후

- 하드웨어 페이지에 모든 구성 요소가 나타나는지 확인합니다.
- 소프트웨어 및 펌웨어 인벤토리 대화 상자(지원 [업그레이드 센터] 메뉴로 이동한 다음 * 소프트웨어 및 펌웨어 인벤토리 * 링크를 클릭하여 소프트웨어 및 펌웨어 버전을 확인합니다.
- 컨트롤러 NVSRAM을 업그레이드한 경우 기존 NVSRAM에 적용한 모든 사용자 정의 설정은 활성화 과정 중에 손실됩니다. 활성화 프로세스가 완료된 후 NVSRAM에 사용자 정의 설정을 다시 적용해야 합니다.

드라이브 펌웨어를 업그레이드합니다

드라이브 펌웨어를 업그레이드하여 최신 기능 및 버그 수정 사항이 모두 있는지 확인할 수 있습니다.

시작하기 전에

- 디스크 간 백업, 볼륨 복사(계획된 펌웨어 업그레이드의 영향을 받지 않는 볼륨 그룹에) 또는 원격 미러를 사용하여 데이터를 백업했습니다.
- 스토리지 배열의 상태는 Optimal(최적) 입니다.
- 모든 드라이브가 최적 상태입니다.
- 스토리지 시스템에서 구성 변경이 실행되고 있지 않습니다.
- 드라이브가 오프라인 업그레이드만 가능한 경우 드라이브와 연결된 모든 볼륨에 대한 I/O 작업이 중지됩니다.

단계

1. 메뉴 선택: 지원 [업그레이드 센터].
2. Support 사이트에서 관리 클라이언트로 새 파일을 다운로드합니다.
   a. 드라이브 펌웨어 업그레이드 에서 * NetApp 지원 * 을 클릭합니다.
   b. NetApp Support 웹 사이트에서 * Downloads * 탭을 클릭합니다.
   c. 디스크 드라이브 및 펌웨어 매트릭스 * 를 선택합니다.
   d. 나머지 지침을 따릅니다.
3. 드라이브 펌웨어 업그레이드 에서 * 업그레이드 시작 * 을 클릭합니다.

   현재 사용 중인 드라이브 펌웨어 파일이 나열된 대화 상자가 나타납니다.

4. 지원 사이트에서 다운로드한 파일의 압축을 풉니다.
5. 찾아보기 * 를 클릭하고 Support 사이트에서 다운로드한 새 드라이브 펌웨어 파일을 선택합니다.

   드라이브 펌웨어 파일에는 확장자와 유사한 파일 이름이 `D_HUC101212CSS600_30602291_MS01_2800_0002` 있습니다 `.dlp`.

한 번에 하나씩 최대 4개의 드라이브 펌웨어 파일을 선택할 수 있습니다. 둘 이상의 드라이브 펌웨어 파일이 동일한 드라이브와 호환되는 경우 파일 충돌 오류가 발생합니다. 업그레이드에 사용할 드라이브 펌웨어 파일을 결정하고 다른 드라이브 펌웨어 파일을 제거합니다.

6. 다음 * 을 클릭합니다.

   선택한 파일로 업그레이드할 수 있는 드라이브가 나열된 * 드라이브 선택 * 대화 상자가 나타납니다.

   호환되는 드라이브만 나타납니다.

   드라이브의 선택한 펌웨어가 제안된 펌웨어 정보 영역에 나타납니다. 펌웨어를 변경해야 하는 경우 * Back * 을 클릭하여 이전 대화 상자로 돌아갑니다.

7. 수행할 업그레이드 유형을 선택합니다.

   ◦ * 온라인(기본값) * — 스토리지 어레이가 I/O_를 처리하는 동안 펌웨어 다운로드를 지원할 수 있는 드라이브를 표시합니다. 이 업그레이드 방법을 선택할 때 이러한 드라이브를 사용하여 연결된 볼륨에 대한 I/O를 중지할 필요가 없습니다. 이러한 드라이브는 스토리지 어레이가 해당 드라이브에 대한 I/O를 처리하는 동안 한 번에 하나씩 업그레이드됩니다.

   ◦ * 오프라인(병렬) * — 드라이브를 사용하는 볼륨에서 모든 I/O 작업이 중지되는 동안 펌웨어 다운로드를 지원할 수 있는 드라이브를 표시합니다. 이 업그레이드 방법을 선택할 때 업그레이드 중인 드라이브를 사용하는 모든 볼륨에서 모든 I/O 작업을 중지해야 합니다. 중복성이 없는 드라이브는 오프라인 작업으로 처리해야 합니다. 이 요구사항에는 SSD 캐시와 연결된 드라이브, RAID 0 볼륨 그룹 또는 성능이 저하된 풀 또는 볼륨 그룹이 포함됩니다. 오프라인(병렬) 업그레이드는 일반적으로 온라인(기본) 방법보다 빠릅니다.

8. 테이블의 첫 번째 열에서 업그레이드할 드라이브를 선택합니다.

9. 시작 * 을 클릭하고 작업을 수행할지 확인합니다.

   업그레이드를 중지해야 하는 경우 * Stop * (중지 *)을 클릭합니다. 현재 진행 중인 모든 펌웨어 다운로드가 완료되었습니다. 시작되지 않은 모든 펌웨어 다운로드는 취소됩니다.

   > 드라이브 펌웨어 업그레이드를 중지하면 데이터가 손실되거나 드라이브를 사용할 수 없게 될 수 있습니다.

10. * 선택 사항: * 업그레이드된 항목 목록을 보려면 * 로그 저장 * 을 클릭합니다.

    파일이 브라우저의 다운로드 폴더에 이름으로 `drive_upgrade_log-timestamp.txt`저장됩니다.

11. 업그레이드 절차 중에 다음 오류가 발생하는 경우 적절한 권장 조치를 취하십시오.

이 펌웨어 다운로드 오류가 발생하는 경우…	그런 다음 다음을 수행합니다.
할당된 드라이브에 오류가 발생했습니다	이 오류가 발생하는 한 가지 이유는 드라이브에 적절한 서명이 없을 수 있기 때문입니다. 영향을 받는 드라이브가 승인된 드라이브인지 확인합니다. 자세한 내용은 기술 지원 부서에 문의하십시오. 드라이브를 교체할 때 교체 드라이브의 용량이 교체 중인 드라이브의 용량보다 크거나 같은지 확인하십시오. 스토리지 배열이 I/O를 수신하는 동안 오류가 발생한 드라이브를 교체할 수 있습니다
스토리지 배열을 확인합니다	• 각 컨트롤러에 IP 주소가 할당되었는지 확인합니다. • 컨트롤러에 연결된 모든 케이블이 손상되지 않았는지 확인합니다. • 모든 케이블이 단단히 연결되어 있는지 확인합니다.
내장형 핫 스페어 드라이브	펌웨어를 업그레이드하기 전에 이 오류 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
볼륨 그룹이 불완전합니다	하나 이상의 볼륨 그룹 또는 디스크 풀이 불완전하면 펌웨어를 업그레이드하기 전에 이 오류 조건을 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
현재 모든 볼륨 그룹에서 실행 중인 단독 작업\(백그라운드 미디어/패리티 검사 제외\	하나 이상의 배타적 작업이 진행 중인 경우 펌웨어를 업그레이드하기 전에 작업을 완료해야 합니다. System Manager를 사용하여 작업 진행률을 모니터링합니다.
볼륨이 누락되었습니다	펌웨어를 업그레이드하기 전에 누락된 볼륨 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
두 컨트롤러 중 하나가 Optimal(최적) 이외의 상태입니다	스토리지 어레이 컨트롤러 중 하나에 주의가 필요합니다. 펌웨어를 업그레이드하기 전에 이 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
컨트롤러 오브젝트 그래프 간에 스토리지 파티션 정보가 일치하지 않습니다	컨트롤러의 데이터를 검증하는 동안 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
SPM 데이터베이스 컨트롤러 확인 실패	컨트롤러에서 스토리지 파티션 매핑 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

이 펌웨어 다운로드 오류가 발생하는 경우...	그런 다음 다음을 수행합니다.
구성 데이터베이스 유효성 검사\(스토리지 배열의 컨트롤러 버전에서 지원되는 경우\)	컨트롤러에서 구성 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
Mel 관련 검사	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
지난 7일 동안 10개 이상의 DDE 정보 또는 중요 MEL 이벤트가 보고되었습니다	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
지난 7일 동안 2개 이상의 2c 페이지 주요 MEL 이벤트가 보고되었습니다	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
최근 7일 동안 성능이 저하된 드라이브 채널 중요 MEL 이벤트가 2개 이상 보고되었습니다	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
지난 7일 동안 4개 이상의 중요한 MEL 항목이 있습니다	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

작업을 마친 후

드라이브 펌웨어 업그레이드가 완료되었습니다. 일반 작업을 다시 시작할 수 있습니다.

가능한 소프트웨어 및 펌웨어 업그레이드 오류를 검토합니다

컨트롤러 소프트웨어 업그레이드 또는 드라이브 펌웨어 업그레이드 중에 오류가 발생할 수 있습니다.

펌웨어 다운로드 오류입니다	설명	권장 조치
할당된 드라이브에 오류가 발생했습니다	스토리지 배열에 할당된 드라이브를 업그레이드하지 못했습니다.	이 오류가 발생하는 한 가지 이유는 드라이브에 적절한 서명이 없을 수 있기 때문입니다. 영향을 받는 드라이브가 승인된 드라이브인지 확인합니다. 자세한 내용은 기술 지원 부서에 문의하십시오. 드라이브를 교체할 때 교체 드라이브의 용량이 교체 중인 드라이브의 용량보다 크거나 같은지 확인하십시오. 스토리지 배열이 I/O를 수신하는 동안 오류가 발생한 드라이브를 교체할 수 있습니다

펌웨어 다운로드 오류입니다	설명	권장 조치
내장형 핫 스페어 드라이브	드라이브가 핫 스페어로 표시되어 있고 볼륨 그룹에서 사용 중인 경우 펌웨어 업그레이드 프로세스가 실패합니다.	펌웨어를 업그레이드하기 전에 이 오류 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
볼륨 그룹이 불완전합니다	볼륨 그룹의 일부인 드라이브가 무시되거나 제거되거나 응답하지 않는 경우 불완전한 볼륨 그룹으로 간주됩니다. 볼륨 그룹이 불완전하면 펌웨어 업그레이드가 방지됩니다.	하나 이상의 볼륨 그룹 또는 디스크 풀이 불완전하면 펌웨어를 업그레이드하기 전에 이 오류 조건을 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
현재 모든 볼륨 그룹에서 실행 중인 단독 작업(백그라운드 미디어/패리티 검사 제외	볼륨에서 배타적 작업이 진행 중인 경우 펌웨어를 업그레이드할 수 없습니다.	하나 이상의 배타적 작업이 진행 중인 경우 펌웨어를 업그레이드하기 전에 작업을 완료해야 합니다. System Manager를 사용하여 작업 진행률을 모니터링합니다.
볼륨이 누락되었습니다	볼륨이 없는 경우 펌웨어를 업그레이드할 수 없습니다.	펌웨어를 업그레이드하기 전에 누락된 볼륨 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
두 컨트롤러 중 하나가 Optimal(최적) 이외의 상태입니다	두 컨트롤러 중 하나가 Optimal(최적) 이외의 상태인 경우 펌웨어를 업그레이드할 수 없습니다.	스토리지 어레이 컨트롤러 중 하나에 주의가 필요합니다. 펌웨어를 업그레이드하기 전에 이 상태를 수정해야 합니다. System Manager를 시작하고 Recovery Guru를 사용하여 문제를 해결합니다.
SPM 데이터베이스 컨트롤러 확인 실패	스토리지 파티션 매핑 데이터베이스가 손상되어 펌웨어를 업그레이드할 수 없습니다.	컨트롤러에서 스토리지 파티션 매핑 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
구성 데이터베이스 유효성 검사(스토리지 배열의 컨트롤러 버전에서 지원되는 경우)	구성 데이터베이스가 손상되어 펌웨어를 업그레이드할 수 없습니다.	컨트롤러에서 구성 데이터베이스 오류가 발생했습니다. 이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
Mel 관련 검사	이벤트 로그에 오류가 있어 펌웨어를 업그레이드할 수 없습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
지난 7일 동안 10개 이상의 DDE 정보 또는 중요 MEL 이벤트가 보고되었습니다	최근 7일 동안 보고된 DDE 정보 또는 중요 MEL 이벤트가 10개를 초과하여 펌웨어를 업그레이드할 수 없습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.

펌웨어 다운로드 오류입니다	설명	권장 조치
지난 7일 동안 2개 이상의 2c 페이지 주요 MEL 이벤트가 보고되었습니다	최근 7일 동안 보고된 2페이지 이상의 2c 중요 MEL 이벤트가 있으므로 펌웨어를 업그레이드할 수 없습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
최근 7일 동안 성능이 저하된 드라이브 채널 중요 MEL 이벤트가 2개 이상 보고되었습니다	최근 7일 동안 성능이 저하된 드라이브 채널 중요 MEL 이벤트가 2개 이상 보고되었기 때문에 펌웨어를 업그레이드할 수 없습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
지난 7일 동안 4개 이상의 중요한 MEL 항목이 있습니다	최근 7일 동안 보고된 중요 이벤트 로그 항목이 4개 이상 있으므로 펌웨어를 업그레이드할 수 없습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
유효한 관리 IP 주소가 필요합니다.	이 작업을 수행하려면 유효한 컨트롤러 IP 주소가 필요합니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
명령을 사용하려면 각 컨트롤러에 대한 액티브 관리 IP 주소가 필요합니다.	이 작업을 수행하려면 스토리지 어레이와 연결된 각 컨트롤러의 컨트롤러 IP 주소가 필요합니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
처리되지 않은 다운로드 파일 형식이 반환되었습니다.	지정된 다운로드 파일이 지원되지 않습니다.	이 문제를 해결하려면 기술 지원 부서에 문의하십시오.
펌웨어 다운로드 업로드 절차 중 오류가 발생했습니다.	컨트롤러가 요청을 처리할 수 없기 때문에 펌웨어를 다운로드하지 못했습니다. 스토리지 배열이 적합한지 확인하고 작업을 다시 시도하십시오.	스토리지 어레이가 최적화되었는지 확인한 후 이 오류가 다시 발생하면 기술 지원 부서에 문의하여 이 문제를 해결하십시오.
펌웨어 활성화 절차 중 오류가 발생했습니다.	컨트롤러가 요청을 처리할 수 없기 때문에 펌웨어를 활성화하지 못했습니다. 스토리지 배열이 적합한지 확인하고 작업을 다시 시도하십시오.	스토리지 어레이가 최적화되었는지 확인한 후 이 오류가 다시 발생하면 기술 지원 부서에 문의하여 이 문제를 해결하십시오.
컨트롤러 {0}의 재부팅을 기다리는 동안 시간 제한에 도달했습니다.	재부팅 후 관리 소프트웨어가 컨트롤러 {0}에 다시 연결할 수 없습니다. 스토리지 시스템에 대한 운영 접속 경로가 있는지 확인하고 성공적으로 완료되지 않은 경우 작업을 다시 시도하십시오.	스토리지 어레이가 최적화되었는지 확인한 후 이 오류가 다시 발생하면 기술 지원 부서에 문의하여 이 문제를 해결하십시오.

System Manager의 Recovery Guru를 사용하여 이러한 조건 중 일부를 해결할 수 있습니다. 그러나 일부 조건에서는 기술 지원 팀에 문의해야 할 수 있습니다. 최신 컨트롤러 펌웨어 다운로드에 대한 정보는 스토리지 어레이에서 확인할 수 있습니다. 이 정보는 기술 지원 부서에서 펌웨어 업그레이드 및 다운로드를 방해하는 오류 조건을 이해하는 데 도움이 됩니다.

FAQ 를 참조하십시오

어떤 데이터를 수집하고 있습니까?

AutoSupport 기능 및 수동 지원 데이터 수집 기능은 고객 지원 번들에서 데이터를 수집하는 방법을 제공하여 기술 지원 팀의 원격 문제 해결 및 문제 분석을 지원합니다.

고객 지원 번들은 스토리지 어레이에 대한 모든 유형의 정보를 압축된 단일 파일로 수집합니다. 수집되는 정보에는 물리적 구성, 논리적 구성, 버전 정보, 이벤트, 로그 파일, 성능 데이터입니다. 이 정보는 기술 지원 부서에서 스토리지 어레이 관련 문제를 해결하는 데 사용됩니다.

읽을 수 없는 섹터 데이터는 무엇을 보여 줍니까?

스토리지 배열의 드라이브에서 검색된 읽을 수 없는 섹터에 대한 자세한 데이터를 표시할 수 있습니다.

읽을 수 없는 섹터 로그는 가장 최근의 읽을 수 없는 섹터를 먼저 보여줍니다. 이 로그에는 읽을 수 없는 섹터가 포함된 볼륨에 대한 다음 정보가 포함되어 있습니다. 필드를 정렬할 수 있습니다.

필드에 입력합니다	설명
영향을 받는 볼륨	볼륨의 레이블을 표시합니다. 누락된 볼륨에 읽을 수 없는 섹터가 포함된 경우, 누락 볼륨에 대한 월드 와이드 식별자가 표시됩니다.
논리 단위 번호(LUN)	에는 볼륨의 LUN이 나와 있습니다. 볼륨에 LUN이 없으면 대화 상자에 NA가 표시됩니다.
할당 대상	에는 볼륨에 대한 액세스 권한이 있는 호스트 또는 호스트 클러스터가 나와 있습니다. 호스트, 호스트 클러스터 또는 기본 클러스터에서 볼륨에 액세스할 수 없는 경우 대화 상자에 NA가 표시됩니다.

읽을 수 없는 섹터에 대한 추가 정보를 보려면 볼륨 옆에 있는 더하기 기호(+)를 클릭합니다.

필드에 입력합니다	설명
날짜/시간입니다	읽을 수 없는 섹터가 감지된 날짜와 시간을 표시합니다.
볼륨 논리적 블록 주소입니다	볼륨의 LBA(논리 블록 주소)를 표시합니다.
드라이브 위치	에는 드라이브 쉘프, 서랍(드라이브 쉘프에 서랍이 있는 경우) 및 베이 위치가 나와 있습니다.
드라이브 논리 블록 주소	에서는 드라이브의 LBA를 보여 줍니다.

필드에 입력합니다	설명
실패 유형	에서는 다음 오류 유형 중 하나를 보여 줍니다. • * 물리적 * — 물리적 미디어 오류입니다. • * 논리 * — 스트라이프의 다른 위치에서 읽기 오류가 발생하여 데이터를 읽을 수 없습니다. 예를 들어, 볼륨의 다른 위치에서 미디어 오류로 인해 읽을 수 없는 섹터가 있습니다. • * 불일치 * — 일관성 없는 중복 데이터. • * Data Assurance * — Data Assurance 오류입니다.

건강 이미지란 무엇입니까**?**

상태 이미지는 기술 지원 부서에서 컨트롤러 문제를 진단하는 데 사용할 수 있는 컨트롤러 프로세서 메모리의 원시 데이터 덤프입니다.

펌웨어는 특정 오류를 감지하면 자동으로 상태 이미지를 생성합니다. 특정 문제 해결 시나리오에서 기술 지원 부서에서는 사용자가 상태 이미지 파일을 검색하여 해당 파일로 보내도록 요청할 수 있습니다.

AutoSupport 기능은 어떤 기능을 합니까**?**

AutoSupport 기능은 사용자가 별도로 사용하는 세 가지 개별 기능으로 구성됩니다.

- * 기본 AutoSupport * — 스토리지 어레이에서 자동으로 데이터를 수집하여 기술 지원 부서에 전송할 수 있습니다.
- * AutoSupport OnDemand * — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 이전 AutoSupport 디스패치의 재전송을 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 재전송 요청이 있는지 확인하고 그에 따라 응답합니다.
- * 원격 진단* — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 새로운 최신 AutoSupport 디스패치를 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 새 요청이 있는지 확인하고 그에 따라 응답합니다.

AutoSupport 기능을 통해 수집되는 데이터 유형은 무엇입니까**?**

AutoSupport 기능에는 이벤트 디스패치, 예약된 디스패치, 주문형 및 원격 진단 디스패치의 세 가지 표준 디스패치 유형이 있습니다.

AutoSupport 데이터에 사용자 데이터가 없습니다.

- * 이벤트 디스패치 *

  기술 지원에 사전 알림이 필요한 이벤트가 시스템에서 발생할 경우 AutoSupport 기능은 자동으로 이벤트 트리거 디스패치를 보냅니다.

  - 관리되는 스토리지 어레이에서 지원 이벤트가 발생할 때 발송됩니다.
  - 이벤트가 발생한 시점의 스토리지 어레이에 대한 포괄적인 스냅샷이 포함됩니다.
- * 예약된 디스패치 *

AutoSupport 기능은 정기적으로 여러 개의 디스패치를 자동으로 전송합니다.

  - * 일일 디스패치 * — 사용자가 구성할 수 있는 시간 간격 동안 매일 한 번 발송됩니다. 현재 시스템 이벤트 로그 및 성능 데이터가 포함됩니다.
  - * 주별 디스패치 * — 사용자가 구성할 수 있는 시간 간격 및 일 동안 매주 한 번 발송됩니다. 구성 및 시스템 상태 정보를 포함합니다.

- * AutoSupport OnDemand 및 원격 진단 디스패치 *
  - * AutoSupport OnDemand * — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 이전 AutoSupport 디스패치의 재전송을 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 재전송 요청이 있는지 확인하고 그에 따라 응답합니다.
  - * 원격 진단* — 문제 해결을 위해 필요한 경우 기술 지원 부서에서 새로운 최신 AutoSupport 디스패치를 요청할 수 있습니다. 모든 전송은 AutoSupport 서버가 아니라 스토리지 시스템에서 시작됩니다. 스토리지 어레이는 AutoSupport 서버와 주기적으로 확인하여 보류 중인 새 요청이 있는지 확인하고 그에 따라 응답합니다.

AutoSupport 기능의 전달 방법을 구성하려면 어떻게 합니까**?**

AutoSupport 기능은 기술 지원 부서에 AutoSupport 디스패치를 제공하기 위한 HTTPS, HTTP 및 SMTP 프로토콜을 지원합니다.

시작하기 전에

- AutoSupport 기능을 활성화해야 합니다. AutoSupport 페이지에서 활성화되어 있는지 여부를 확인할 수 있습니다.
- 네트워크에 DNS 서버가 설치 및 구성되어 있어야 합니다. DNS 서버 주소는 System Manager에서 구성해야 합니다(이 작업은 하드웨어 페이지에서 사용 가능).

이 작업에 대해

다양한 프로토콜을 검토합니다.

- * HTTPS * — HTTPS를 사용하여 대상 기술 지원 서버에 직접 연결할 수 있습니다. AutoSupport OnDemand 또는 원격 진단을 활성화하려면 AutoSupport 전송 방법을 HTTPS로 설정해야 합니다.
- * HTTP * — HTTP를 사용하여 대상 기술 지원 서버에 직접 연결할 수 있습니다.
- * 이메일 * — 이메일 서버를 AutoSupport 디스패치 전송 방법으로 사용할 수 있습니다.

- HTTPS/HTTP와 이메일 방법의 차이점 *. SMTP를 사용하는 이메일 전송 방법은 HTTPS 및 HTTP 전송 방법과 몇 가지 중요한 차이점이 있습니다. 먼저, 이메일 방법에 대한 디스패치 크기는 5MB로 제한되며, 이는 일부 ASUP 데이터 수집이 디스패치되지 않음을 의미합니다. 둘째, AutoSupport OnDemand 기능은 HTPP 및 HTTPS 방법에서만 사용할 수 있습니다.

단계

1. 지원 [지원 센터 > AutoSupport] 탭을 선택합니다.
2. AutoSupport 제공 방법 구성 * 을 선택합니다.

   디스패치 제공 방법이 나열된 대화 상자가 나타납니다.

3. 원하는 전달 방법을 선택한 다음 해당 전달 방법에 대한 매개 변수를 선택합니다. 다음 중 하나를 수행합니다.
   - HTTPS 또는 HTTP를 선택한 경우 다음 전송 매개 변수 중 하나를 선택합니다.

- * 직접 * — 이 전달 매개 변수는 기본 선택 항목입니다. 이 옵션을 선택하면 HTTPS 또는 HTTP 프로토콜을 사용하여 대상 기술 지원 시스템에 직접 연결할 수 있습니다.
- * 프록시 서버를 통해 * — 이 옵션을 선택하면 대상 기술 지원 시스템과의 연결을 설정하는 데 필요한 HTTP 프록시 서버 세부 정보를 지정할 수 있습니다. 호스트 주소와 포트 번호를 지정해야 합니다. 그러나 필요한 경우 호스트 인증 세부 정보(사용자 이름 및 암호)만 입력하면 됩니다.
- * 프록시 자동 구성 스크립트(PAC)를 통해 * — 프록시 자동 구성(PAC) 스크립트 파일의 위치를 지정합니다. PAC 파일을 사용하면 시스템이 대상 기술 지원 시스템과의 연결을 설정할 적절한 프록시 서버를 자동으로 선택할 수 있습니다.

◦ 이메일 을 선택한 경우 다음 정보를 입력합니다.

- 메일 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소입니다.
- AutoSupport 디스패치 이메일의 보낸 사람 필드에 나타나는 이메일 주소입니다.
- 선택 사항**;** 구성 테스트를 수행하려면**.** AutoSupport 시스템이 테스트 디스패치를 받을 때 확인을 보내는 이메일 주소입니다.
- 메시지를 암호화하려면 암호화 유형으로 * SMTPS * 또는 * STARTTLS * 를 선택한 다음 암호화된 메시지의 포트 번호를 선택합니다. 그렇지 않으면 * 없음 * 을 선택합니다.
- 필요한 경우 보내는 보낸 사람과 메일 서버에서 인증을 위한 사용자 이름과 암호를 입력합니다.

4. 지정된 전달 매개 변수를 사용하여 기술 지원 서버에 대한 연결을 테스트하려면 * Test Configuration * 을 클릭합니다. AutoSupport 온디맨드 기능을 활성화한 경우 AutoSupport OnDemand 디스패치 전달에 대한 연결도 테스트합니다.

   구성 테스트에 실패하면 구성 설정을 확인하고 테스트를 다시 실행하십시오. 테스트가 계속 실패하면 기술 지원 부서에 문의하십시오.

5. 저장 * 을 클릭합니다.

구성 데이터란 무엇입니까**?**

구성 데이터 수집 을 선택하면 시스템이 RAID 구성 데이터베이스의 현재 상태를 저장합니다.

RAID 구성 데이터베이스에는 컨트롤러의 볼륨 그룹 및 디스크 풀에 대한 모든 데이터가 포함됩니다. 구성 데이터 수집 기능은 의 CLI 명령과 동일한 정보를 `save storageArray dbmDatabase` 저장합니다.

SANtricity OS 소프트웨어를 업그레이드하기 전에 알아야 할 내용은 무엇입니까**?**

컨트롤러의 소프트웨어 및 펌웨어를 업그레이드하기 전에 이러한 항목을 숙지하십시오.

- 문서와 파일을 읽었으며 `readme.txt` 업그레이드를 수행하기로 결정했습니다.
- IOM 펌웨어를 업그레이드할지 여부를 알고 있습니다.

  일반적으로 모든 구성 요소를 동시에 업그레이드해야 합니다. 하지만 SANtricity OS 컨트롤러 소프트웨어 업그레이드의 일부로 업그레이드하지 않으려는 경우 또는 기술 지원 부서에서 IOM 펌웨어를 다운그레이드하도록 지시한 경우(명령줄 인터페이스를 사용하여 펌웨어를 다운그레이드할 수만 있음) IOM 펌웨어를 업그레이드하지 않을 수도 있습니다.

- 컨트롤러 NVSRAM 파일을 업그레이드할지 여부를 알 수 있습니다.

  일반적으로 모든 구성 요소를 동시에 업그레이드해야 합니다. 그러나 파일이 패치되었거나 사용자 정의 버전이고

덮어쓰지 않으려는 경우 컨트롤러 NVSRAM 파일을 업그레이드하지 않을 수 있습니다.

- 지금 활성화할지 아니면 나중에 활성화할지 알 수 있습니다.

  나중에 활성화하는 이유는 다음과 같습니다.

  - * 시간 * — 소프트웨어 및 펌웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 로드가 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
  - * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

이러한 구성요소는 SANtricity OS 컨트롤러 소프트웨어 업그레이드의 일부입니다.

- * 관리 소프트웨어 * — System Manager는 스토리지 배열을 관리하는 소프트웨어입니다.
- * 컨트롤러 펌웨어 * — 컨트롤러 펌웨어는 호스트와 볼륨 간의 I/O를 관리합니다.
- * 컨트롤러 NVSRAM * — 컨트롤러 NVSRAM은 컨트롤러의 기본 설정을 지정하는 컨트롤러 파일입니다.
- * IOM 펌웨어 * — I/O 모듈(IOM) 펌웨어는 컨트롤러와 드라이브 쉘프 간의 연결을 관리합니다. 또한 구성 요소의 상태를 모니터링합니다.
- * Supervisor 소프트웨어 * — Supervisor 소프트웨어는 소프트웨어가 실행되는 컨트롤러의 가상 머신입니다.

업그레이드 프로세스의 일부로 호스트의 다중 경로/페일오버 드라이버 및/또는 HBA 드라이버도 업그레이드해야 호스트가 컨트롤러와 올바르게 상호 작용할 수 있습니다.

이 경우에 해당하는지 확인하려면 을 "NetApp 상호 운용성 매트릭스 툴"참조하십시오.

스토리지 배열에 컨트롤러가 하나만 포함되어 있거나 다중 경로 드라이버가 설치되어 있지 않은 경우, 어플리케이션 오류를 방지하기 위해 스토리지 배열에 대한 I/O 작업을 중지합니다. 스토리지 어레이에 2개의 컨트롤러가 있는데 다중 경로 드라이버가 설치되어 있는 경우 I/O 작업을 중지할 필요가 없습니다.

업그레이드가 진행되는 동안 스토리지 배열을 변경하지 마십시오.

IOM 자동 동기화를 일시 중단하기 전에 알아야 할 내용은 무엇입니까**?**

IOM 자동 동기화를 일시 중단하면 다음에 SANtricity OS 컨트롤러 소프트웨어 업그레이드가 발생할 때 IOM 펌웨어가 업그레이드되지 않습니다.

일반적으로 컨트롤러 소프트웨어 및 IOM 펌웨어는 번들로 업그레이드됩니다. 인클로저에 보존하려는 IOM 펌웨어의 특수 빌드를 가지고 있는 경우 IOM 자동 동기화를 일시 중지할 수 있습니다. 그렇지 않으면 다음 번에 컨트롤러 소프트웨어 업그레이드를 수행할 때 컨트롤러 소프트웨어와 함께 번들로 제공되는 IOM 펌웨어로 되돌아갑니다.

펌웨어 업그레이드가 너무 느리게 진행되는 이유는 무엇입니까**?**

펌웨어 업그레이드 진행 상황은 시스템의 전체 로드에 따라 다릅니다.

드라이브 펌웨어의 온라인 업그레이드 중에 빠른 재구성 프로세스 중에 볼륨 전송이 발생하면 시스템은 전송된 볼륨에서 전체 재구성을 시작합니다. 이 작업에는 상당한 시간이 걸릴 수 있습니다. 실제 전체 재구성 시간은 재구성 작업 중 발생하는 I/O 활동 양, 볼륨 그룹의 드라이브 수, 리빌드 우선순위 설정 및 드라이브 성능 등 여러 요소에 따라

달라집니다.

드라이브 펌웨어를 업그레이드하기 전에 알아야 할 내용은 무엇입니까**?**

드라이브 펌웨어를 업그레이드하기 전에 다음 항목을 숙지하십시오.

- 예방 조치로 디스크 간 백업, 볼륨 복사(계획된 펌웨어 업그레이드의 영향을 받지 않는 볼륨 그룹에) 또는 원격 미러를 사용하여 데이터를 백업합니다.
- 새 펌웨어의 동작을 테스트하여 올바른 작동을 확인하기 위해 드라이브를 몇 개만 업그레이드할 수 있습니다. 새 펌웨어가 제대로 작동하는 경우 나머지 드라이브를 업그레이드하십시오.
- 오류가 발생한 드라이브가 있는 경우 펌웨어 업그레이드를 시작하기 전에 해결하십시오.
- 드라이브에서 오프라인 업그레이드를 수행할 수 있는 경우 드라이브와 연결된 모든 볼륨에 대한 I/O 작업을 중지합니다. I/O 작업이 중지되면 해당 볼륨과 관련된 구성 작업이 수행되지 않습니다.
- 드라이브 펌웨어를 업그레이드하는 동안 드라이브를 제거하지 마십시오.
- 드라이브 펌웨어를 업그레이드하는 동안 스토리지 배열의 구성을 변경하지 마십시오.

수행할 업그레이드 유형을 선택하려면 어떻게 해야 합니까**?**

풀 또는 볼륨 그룹의 상태에 따라 드라이브에서 수행할 업그레이드 유형을 선택합니다.

- * 온라인 *

  풀 또는 볼륨 그룹이 중복성을 지원하고 최적의 경우 Online(온라인) 방법을 사용하여 드라이브 펌웨어를 업그레이드할 수 있습니다. 온라인 메소드는 스토리지 어레이가 I/O를 처리하는 동안 _ 펌웨어를 이러한 드라이브를 사용하여 연결된 볼륨에 다운로드합니다. 이러한 드라이브를 사용하여 연결된 볼륨에 대한 I/O를 중지할 필요가 없습니다. 이러한 드라이브는 드라이브에 연결된 볼륨으로 한 번에 하나씩 업그레이드됩니다. 드라이브가 풀 또는 볼륨 그룹에 할당되지 않은 경우 온라인 또는 오프라인 방법으로 해당 펌웨어를 업데이트할 수 있습니다. 드라이브 펌웨어를 업그레이드하는 온라인 방법을 사용할 경우 시스템 성능에 영향을 줄 수 있습니다.

- * 오프라인 *

  풀 또는 볼륨 그룹이 이중화(RAID 0)를 지원하지 않거나 성능이 저하된 경우, 드라이브 펌웨어를 업그레이드하려면 오프라인 방법을 사용해야 합니다. Offline 방법은 모든 I/O 작업이 중지되어 있는 동안 _ 펌웨어를 해당 드라이브를 사용하는 연결된 볼륨으로 업그레이드합니다. 이러한 드라이브를 사용하여 연결된 볼륨에 대한 모든 I/O를 중지해야 합니다. 드라이브가 풀 또는 볼륨 그룹에 할당되지 않은 경우 온라인 또는 오프라인 방법으로 해당 펌웨어를 업데이트할 수 있습니다.

SANtricity Unified Manager 6을 통한 다중 어레이 관리

기본 인터페이스

SANtricity Unified Manager 인터페이스 개요

SANtricity Unified Manager는 여러 스토리지 어레이를 단일 뷰에서 관리할 수 있는 웹 기반 인터페이스입니다.

기본 페이지

Unified Manager에 로그인하면 기본 페이지가 열리고 * Manage - All * 가 표시됩니다. 이 페이지에서는 네트워크에서 검색된 스토리지 배열의 목록을 스크롤하고, 해당 상태를 보고, 단일 배열 또는 어레이 그룹에서 작업을 수행할 수 있습니다.

탐색 사이드바

탐색 사이드바에서 Unified Manager 기능에 액세스할 수 있습니다.

영역	설명
관리	네트워크에서 스토리지 시스템을 검색하고, 어레이에 대한 SANtricity 시스템 관리자를 시작하고, 한 어레이에서 여러 어레이로 설정을 가져오고, 어레이 그룹을 관리합니다. 설정 가져오기 및 스토리지 그룹 생성과 같은 작업을 수행할 스토리지 이름 옆의 확인란을 선택합니다. 각 행의 끝에 있는 줄임표는 이름 바꾸기와 같은 단일 배열의 작업에 대한 인라인 메뉴를 제공합니다.
운영	한 어레이에서 다른 어레이로 설정을 가져오는 것과 같은 배치 작업의 진행률을 봅니다. 스토리지 배열의 상태가 최적이 아닌 경우 일부 작업을 사용할 수 없습니다.
인증서 관리	브라우저와 클라이언트 간 인증을 위한 인증서를 관리합니다.
액세스 관리	Unified Manager 인터페이스에 대한 사용자 인증 설정
지원	기술 지원 옵션, 리소스 및 연락처를 봅니다.

인터페이스 설정 및 도움말

인터페이스 오른쪽 상단에서 도움말 및 기타 설명서에 액세스할 수 있습니다. 로그인 이름 옆의 드롭다운에서 사용할 수 있는 관리 옵션에 액세스할 수도 있습니다.

사용자 로그인 및 암호

시스템에 로그인한 현재 사용자가 인터페이스의 오른쪽 상단에 표시됩니다.

사용자 및 암호에 대한 자세한 내용은 다음을 참조하십시오.

- "관리자 암호 보호를 설정합니다"
- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

지원되는 브라우저

SANtricity Unified Manager는 다양한 유형의 브라우저에서 액세스할 수 있습니다.

다음 브라우저 및 버전이 지원됩니다.

브라우저	최소 버전
Google Chrome	89
Mozilla Firefox	80
사파리	14
Microsoft Edge를 참조하십시오	90

웹 서비스 프록시는 설치되어 브라우저에서 사용할 수 있어야 합니다.

관리자 암호 보호를 설정합니다

관리자 암호를 사용하여 SANtricity Unified Manager를 무단 액세스로부터 보호해야 합니다.

관리자 암호 및 사용자 프로필

Unified Manager를 처음 시작하면 관리자 암호를 설정하라는 메시지가 표시됩니다. admin 암호를 가진 모든 사용자는 스토리지 배열에 대한 구성을 변경할 수 있습니다.

관리자 암호 외에도 Unified Manager 인터페이스에는 하나 이상의 역할이 매핑되어 있는 사전 구성된 사용자 프로필이 포함되어 있습니다. 자세한 내용은 을 "액세스 관리 작동 방식"참조하십시오.

사용자 및 매핑을 변경할 수 없습니다. 암호만 수정할 수 있습니다. 암호를 변경하려면 다음을 참조하십시오.

- "admin 암호를 변경합니다"
- "로컬 사용자 프로필에 대한 암호를 변경합니다"

세션 시간 초과

단일 관리 세션 중에 암호를 입력하라는 메시지가 한 번만 표시됩니다. 기본적으로 30분 동안 활동이 없으면 세션 시간이 초과되며, 이 경우 암호를 다시 입력해야 합니다. 다른 사용자가 다른 관리 클라이언트에서 소프트웨어에 액세스하고 세션이 진행되는 동안 암호를 변경하는 경우 다음에 구성 작업 또는 보기 작업을 시도할 때 암호를 입력하라는 메시지가 표시됩니다.

보안상의 이유로 소프트웨어가 "잠금" 상태가 되기 5회만 암호를 입력할 수 있습니다. 이 상태에서는 소프트웨어가 후속 암호 시도를 거부합니다. 암호를 다시 입력하기 전에 10분 정도 기다린 후 "정상" 상태로 재설정해야 합니다.

세션 시간 초과를 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다. 자세한 내용은 을 "세션 시간 제한을 관리합니다"참조하십시오.

admin 암호를 변경합니다

SANtricity Unified Manager에 액세스하는 데 사용되는 admin 암호를 변경할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
- 현재 관리자 암호를 알아야 합니다.

이 작업에 대해

암호를 선택할 때는 다음 지침을 염두에 두십시오.

- 암호는 대/소문자를 구분합니다.
- 후행 공백은 암호가 설정되어 있을 때 암호에서 제거되지 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
- 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 * 탭을 선택합니다.
3. 표에서 * admin * 사용자를 선택합니다.

   암호 변경 단추를 사용할 수 있게 됩니다.

4. 암호 변경 * 을 선택합니다.

   암호 변경 대화 상자가 열립니다.

5. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 사용자가 시스템에 액세스하기 위해 암호를 입력하도록 확인란을 선택합니다.
6. 두 필드에 새 암호를 입력합니다.
7. 이 작업을 확인하려면 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

세션 시간 제한을 관리합니다

SANtricity Unified Manager의 시간 제한을 구성하여 지정된 시간이 지나면 사용자 비활성 세션의 연결을 끊을 수 있습니다.

이 작업에 대해

기본적으로 Unified Manager의 세션 제한 시간은 30분입니다. 이 시간을 조정하거나 세션 시간 초과를 모두 비활성화할 수 있습니다.

> 스토리지에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하여 액세스 관리를 구성하는 경우 사용자의 SSO 세션이 최대 제한에 도달하면 세션 시간 초과가 발생할 수 있습니다. 이 문제는 System Manager 세션 시간이 초과되기 전에 발생할 수 있습니다.

단계

1. 메뉴 표시줄에서 사용자 로그인 이름 옆에 있는 드롭다운 화살표를 선택합니다.
2. Enable/Disable session timeout * 을 선택합니다.

   Enable/Disable Session Timeout(세션 시간 제한 활성화/비활성화) 대화 상자가 열립니다.
3. 스피너 컨트롤을 사용하여 시간을 분 단위로 늘리거나 줄입니다.

   설정할 수 있는 최소 시간 초과는 15분입니다.

   > 세션 시간 초과를 비활성화하려면 * 시간 길이 설정… * 확인란의 선택을 취소합니다.
4. 저장 * 을 클릭합니다.

지원합니다

검색 개요

스토리지 리소스를 관리하려면 먼저 네트워크에서 스토리지 어레이를 검색해야 합니다.

어레이를 어떻게 검색합니까**?**

추가/검색 페이지를 사용하여 조직의 네트워크에서 관리할 스토리지 어레이를 찾아서 추가합니다. 여러 어레이를 검색할 수도 있고 단일 어레이를 검색할 수도 있습니다. 이렇게 하려면 네트워크 IP 주소를 입력한 다음 Unified Manager가 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다.

자세한 내용:

- "스토리지 검색 시 고려 사항"
- "여러 스토리지 시스템을 검색합니다"
- "단일 스토리지를 검색합니다"

어레이를 어떻게 관리해야 합니까?

어레이를 검색하고 나면 * Manage - All * 페이지로 이동합니다. 이 페이지에서는 네트워크에서 검색된 스토리지 배열의 목록을 스크롤하고, 해당 상태를 보고, 단일 배열 또는 어레이 그룹에서 작업을 수행할 수 있습니다.

단일 어레이를 관리하려면 어레이를 선택하고 System Manager를 열 수 있습니다.

자세한 내용:

- "System Manager 액세스에 대한 고려 사항"
- "개별 스토리지 어레이를 관리합니다"
- "스토리지 배열 상태를 봅니다"

개념

스토리지 검색 시 고려 사항

SANtricity Unified Manager가 스토리지 리소스를 표시하고 관리하기 전에 먼저 조직의 네트워크에서 관리할 스토리지 어레이를 검색해야 합니다. 여러 어레이를 검색할 수도 있고 단일 어레이를 검색할 수도 있습니다.

여러 스토리지 시스템을 검색하는 중입니다

여러 어레이를 검색하도록 선택한 경우 네트워크 IP 주소 범위를 입력한 다음 Unified Manager가 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다. 성공적으로 도달한 스토리지 배열이 검색 페이지에 표시되고 관리 도메인에 추가될 수 있습니다.

단일 스토리지 시스템 검색

단일 어레이를 검색하도록 선택한 경우 스토리지 어레이에서 컨트롤러 중 하나에 대한 단일 IP 주소를 입력한 다음 개별 스토리지 어레이가 추가됩니다.

> Unified Manager는 컨트롤러에 할당된 범위 내에서 단일 IP 주소 또는 IP 주소만 검색하여 표시합니다. 이 단일 IP 주소 또는 IP 주소 범위를 벗어나는 컨트롤러에 할당된 대체 컨트롤러 또는 IP 주소가 있는 경우 Unified Manager는 이를 검색 또는 표시하지 않습니다. 그러나 스토리지 배열을 추가하면 연결된 모든 IP 주소가 검색되어 관리 보기에 표시됩니다.

사용자 자격 증명

검색 프로세스 중에 추가할 각 스토리지 배열에 대해 관리자 암호를 제공해야 합니다.

웹 서비스 인증서

검색 프로세스의 일부로 Unified Manager는 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. Unified Manager에서는 브라우저에 설정한 모든 연결에 대해 두 가지 유형의 인증서 기반 인증을 사용합니다.

- * 신뢰할 수 있는 인증서 *

  Unified Manager에서 검색된 스토리지의 경우 인증 기관에서 제공하는 신뢰할 수 있는 인증서를 추가로 설치해야

할 수 있습니다.

이러한 인증서를 가져오려면 * 가져오기 * 버튼을 사용합니다. 이전에 이 어레이에 연결한 경우 하나 또는 두 컨트롤러 인증서 중 하나가 만료되었거나 해지되었거나 인증서 체인에 루트 인증서 또는 중간 인증서가 누락되었습니다. 스토리지 배열을 관리하기 전에 만료되었거나 해지된 인증서를 교체하거나 누락된 루트 인증서 또는 중간 인증서를 추가해야 합니다.

- * 자체 서명된 인증서 *

  자체 서명된 인증서도 사용할 수 있습니다. 관리자가 서명된 인증서를 가져오지 않고 어레이를 검색하려고 하면 Unified Manager에 관리자가 자체 서명된 인증서를 수락할 수 있는 오류 대화 상자가 표시됩니다. 스토리지 시스템의 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 시스템이 Unified Manager에 추가됩니다.

  스토리지 배열에 대한 연결을 신뢰하지 않는 경우, Unified Manager에 스토리지 배열을 추가하기 전에 * Cancel * 을 선택하고 스토리지 배열의 보안 인증서 전략을 확인합니다.

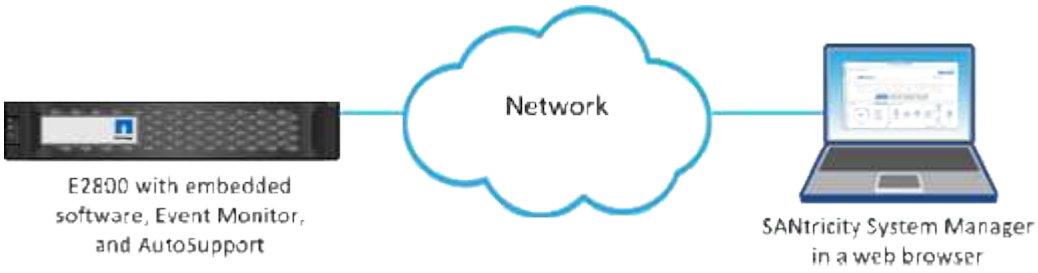
SANtricity 시스템 관리자에 액세스할 때의 고려 사항

스토리지 어레이를 구성 및 관리하려는 경우 하나 이상의 스토리지 어레이를 선택하고 시작 옵션을 사용하여 SANtricity System Manager를 엽니다.

System Manager는 이더넷 관리 포트를 통해 네트워크에 연결되는 컨트롤러에 내장된 애플리케이션입니다. 모든 스토리지 기반 기능이 포함되어 있습니다.

System Manager에 액세스하려면 다음이 있어야 합니다.

- 여기에 나열된 어레이 모델 중 하나: "E-Series 하드웨어 개요"
- 웹 브라우저를 사용하여 네트워크 관리 클라이언트에 대한 대역외 연결.



스토리지를 검색합니다

여러 스토리지 시스템을 검색합니다

여러 어레이를 검색하여 관리 서버가 있는 서브넷에서 모든 스토리지 어레이를 검색하고 검색된 어레이를 관리 도메인에 자동으로 추가합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 System Manager의 액세스 관리 타일을 사용하여 설정해야 합니다.

- 신뢰할 수 없는 인증서를 해결하려면 CA(인증 기관)의 신뢰할 수 있는 인증서 파일이 있어야 하며 로컬 시스템에서 인증서 파일을 사용할 수 있어야 합니다.

어레이 검색 절차는 여러 단계로 이루어진 절차입니다.

1단계**:** 네트워크 주소를 입력합니다

로컬 하위 네트워크에서 검색할 네트워크 주소 범위를 입력합니다. 성공적으로 도달한 스토리지 배열이 검색 페이지에 표시되고 관리 도메인에 추가될 수 있습니다.

어떤 이유로든 검색 작업을 중지해야 하는 경우 * 검색 중지 * 를 클릭합니다.

단계

1. 관리 페이지에서 * 추가/검색 * 을 선택합니다.

   추가/검색 대화 상자가 나타납니다.

2. 네트워크 범위 내의 모든 스토리지 배열 검색 * 라디오 버튼을 선택합니다.
3. 로컬 하위 네트워크를 검색할 시작 네트워크 주소와 끝 네트워크 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   검색 프로세스가 시작됩니다. 이 검색 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 스토리지 배열이 검색되면 검색 페이지의 테이블이 채워집니다.

   관리 가능한 어레이가 검색되지 않으면 스토리지 어레이가 네트워크에 올바르게 연결되어 있고 할당된 주소가 범위 내에 있는지 확인합니다. 추가/검색 페이지로 돌아가려면 * New Discovery Parameters * 를 클릭합니다.

4. 검색된 스토리지 시스템의 목록을 검토합니다.
5. 관리 도메인에 추가할 스토리지 배열 옆의 확인란을 선택하고 * 다음 * 을 클릭합니다.

   Unified Manager는 관리 도메인에 추가할 각 어레이에서 자격 증명 검사를 수행합니다. 해당 배열과 연결된 자체 서명된 인증서 및 신뢰할 수 없는 인증서를 확인해야 할 수 있습니다.

6. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

2단계**:** 검색 중에 자체 서명된 인증서 해결

검색 프로세스의 일부로 시스템은 스토리지 어레이가 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다.

단계

1. 다음 중 하나를 수행합니다.
   - 검색된 스토리지 배열에 대한 접속을 신뢰할 수 있는 경우 마법사의 다음 카드로 계속 진행합니다. 자체 서명된 인증서는 신뢰할 수 있는 인증서로 표시되며 스토리지 시스템이 Unified Manager에 추가됩니다.
   - 스토리지 어레이에 대한 연결을 신뢰할 수 없는 경우 * Cancel * 을 선택하고 각 스토리지 어레이의 보안 인증서 전략을 확인한 다음 Unified Manager에 추가합니다.
2. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

3단계**:** 검색 중에 신뢰할 수 없는 인증서를 해결합니다

신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 어레이 검색 프로세스 중에 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서 또는 CA 서명 인증서를 가져와 신뢰할 수 없는 인증서를 해결할 수 있습니다.

다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

- 최근에 스토리지 배열을 추가했습니다.
- 하나 이상의 인증서가 만료되었습니다.
- 하나 이상의 인증서가 해지되었습니다.
- 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

단계

1. 신뢰할 수 없는 인증서를 확인할 스토리지 배열 옆의 확인란을 선택한 다음 가져오기 버튼을 선택합니다.

   신뢰할 수 있는 인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

2. Browse * 를 클릭하여 스토리지 배열에 대한 인증서 파일을 선택합니다.

   대화 상자에 파일 이름이 표시됩니다.

3. 가져오기 * 를 클릭합니다.

   파일이 업로드되고 검증됩니다.

   신뢰할 수 없는 인증서 문제가 해결되지 않은 스토리지 어레이는 Unified Manager에 추가되지 않습니다.

4. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

4단계**:** 암호를 입력합니다

관리 도메인에 추가할 스토리지 배열에 대한 암호를 입력해야 합니다.

단계

1. Unified Manager에 추가할 각 스토리지 어레이의 암호를 입력합니다.
2. * 선택 사항: * 그룹에 스토리지 어레이 연결: 드롭다운 목록에서 선택한 스토리지 어레이와 연결할 그룹을 선택합니다.
3. 마침 * 을 클릭합니다.

작업을 마친 후

스토리지 배열이 관리 도메인에 추가되고 선택한 그룹에 연결됩니다(지정된 경우).

Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

단일 스토리지 배열 추가/검색 옵션을 사용하여 조직의 네트워크에 단일 스토리지 배열을 수동으로 검색하고 추가합니다.

시작하기 전에

- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.
- 스토리지 배열 암호는 System Manager의 액세스 관리 타일을 사용하여 설정해야 합니다.

단계

1. 관리 페이지에서 * 추가/검색 * 을 선택합니다.

   추가/검색 대화 상자가 나타납니다.

2. Discover a single storage array * 라디오 버튼을 선택합니다.
3. 스토리지 배열에 있는 컨트롤러 중 하나의 IP 주소를 입력한 다음 * 검색 시작 * 을 클릭합니다.

   Unified Manager가 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

   지정된 컨트롤러의 IP 주소에 대한 연결이 실패하면 스토리지 어레이에 액세스할 수 없음 메시지가 나타납니다.

4. 메시지가 표시되면 자체 서명된 인증서를 모두 해결합니다.

   검색 프로세스의 일부로 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. 스토리지 배열에 대한 디지털 인증서를 찾을 수 없는 경우 보안 예외를 추가하여 CA(인증 기관)에서 서명하지 않은 인증서를 확인하라는 메시지가 표시됩니다.

5. 메시지가 나타나면 신뢰할 수 없는 인증서를 모두 확인합니다.

   신뢰할 수 없는 인증서는 스토리지 어레이에서 Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 신뢰할 수 있는 제3자가 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 해결합니다.

6. 다음 * 을 클릭합니다.
7. * 선택 사항: * 검색된 스토리지 배열을 그룹에 연결: 드롭다운 목록에서 스토리지 배열에 연결할 그룹을 선택합니다.

   기본적으로 "모두" 그룹이 선택됩니다.

8. 관리 도메인에 추가할 스토리지 배열의 관리자 암호를 입력한 다음 * 확인 * 을 클릭합니다.

작업을 마친 후

스토리지 시스템이 Unified Manager에 추가되고 지정된 경우 선택한 그룹에 추가됩니다.

자동 지원 데이터 수집이 설정된 경우 추가하는 스토리지 배열에 대한 지원 데이터가 자동으로 수집됩니다.

스토리지 관리

스토리지 배열 상태를 봅니다

SANtricity Unified Manager는 검색된 각 스토리지 어레이의 상태를 표시합니다.

Manage - All * 페이지로 이동합니다. 이 페이지에서는 웹 서비스 프록시와 해당 스토리지 배열 간의 연결 상태를 볼 수 있습니다.

상태 표시기는 다음 표에 설명되어 있습니다.

상태	를 나타냅니다
최적	스토리지 배열이 Optimal(최적) 상태에 있습니다. 인증서 문제가 없으며 암호가 유효합니다.
암호가 잘못되었습니다	잘못된 스토리지 배열 암호가 제공되었습니다.
신뢰할 수 없는 인증서입니다	HTTPS 인증서가 자체 서명되어 있고 가져오지 않았거나 인증서가 CA 서명되었으며 루트 및 중간 CA 인증서를 가져오지 않았기 때문에 스토리지 배열과의 연결을 하나 이상 신뢰할 수 없습니다.
주의가 필요합니다	스토리지 어레이에 문제가 있어 수정하려면 스토리지 시스템의 개입이 필요합니다.
잠금	스토리지 배열이 잠김 상태에 있습니다.
알 수 없음	스토리지 배열에 연결된 적이 없습니다. 웹 서비스 프록시가 시작되고 아직 스토리지 배열과 연결되지 않았거나, 스토리지 배열이 오프라인 상태이고 웹 서비스 프록시가 시작된 이후 연락되지 않은 경우에 이 문제가 발생할 수 있습니다.
오프라인	웹 서비스 프록시가 이전에 스토리지 어레이에 연결했지만 이제 모든 연결이 끊어졌습니다.

개별 스토리지 어레이를 관리합니다

실행 옵션을 사용하면 관리 작업을 수행하려는 경우 하나 이상의 스토리지 어레이에 대한 브라우저 기반 SANtricity System Manager를 열 수 있습니다.

단계

1. 관리 페이지에서 관리할 스토리지 어레이를 하나 이상 선택합니다.
2. 시작 * 을 클릭합니다.

   새 창이 열리고 System Manager 로그인 페이지가 표시됩니다.

3. 사용자 이름과 암호를 입력한 다음 * 로그인 * 을 클릭합니다.

스토리지 배열 암호를 변경합니다

SANtricity Unified Manager에서 스토리지 어레이를 보고 액세스하는 데 사용되는 암호를

업데이트할 수 있습니다.

시작하기 전에

- 스토리지 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
- System Manager에서 설정된 스토리지 어레이의 현재 암호를 알아야 합니다.

이 작업에 대해

이 작업에서는 Unified Manager에서 스토리지 어레이에 액세스할 수 있도록 스토리지 어레이의 현재 암호를 입력합니다. System Manager에서 어레이 암호를 변경했으므로 이제는 Unified Manager에서 어레이 암호를 변경해야 할 수도 있습니다.

단계

1. 관리 페이지에서 하나 이상의 스토리지 배열을 선택합니다.
2. SELECT MENU: Uncommon Tasks[스토리지 배열 암호 제공].
3. 각 스토리지 배열의 암호 또는 암호를 입력한 다음 * 저장 * 을 클릭합니다.

SANtricity Unified Manager에서 스토리지 어레이를 제거합니다

SANtricity Unified Manager에서 더 이상 스토리지 어레이를 관리하지 않으려는 경우 하나 이상의 스토리지 어레이를 제거할 수 있습니다.

이 작업에 대해

제거하는 스토리지 시스템은 액세스할 수 없습니다. 그러나 브라우저를 IP 주소 또는 호스트 이름에 직접 연결하여 제거된 스토리지 배열에 대한 연결을 설정할 수 있습니다.

스토리지 배열을 제거해도 스토리지 배열 또는 해당 데이터에는 어떤 식으로든 영향을 주지 않습니다. 스토리지 배열이 실수로 제거된 경우 다시 추가할 수 있습니다.

단계

1. Manage * 페이지를 선택합니다.
2. 제거할 스토리지 배열을 하나 이상 선택합니다.
3. Uncommon Tasks [Remove storage array] 메뉴를 선택합니다.

   스토리지 어레이가 SANtricity Unified Manager의 모든 보기에서 제거됩니다.

설정을 가져옵니다

설정 가져오기 개요

설정 가져오기 기능을 사용하면 한 어레이에서 여러 어레이로 설정을 가져오기 위한 일괄 작업을 수행할 수 있습니다. 이 기능을 사용하면 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약할 수 있습니다.

가져올 수 있는 설정은 무엇입니까**?**

알림 방법, AutoSupport 구성, 디렉토리 서비스 구성, 스토리지 구성(예: 볼륨 그룹 및 풀) 및 시스템 설정(예: 자동 로드 밸런싱)을 가져올 수 있습니다.

자세한 내용:

- "가져오기 설정 작동 방식"
- "스토리지 구성 복제 요구 사항"

일괄 불러오기는 어떻게 수행합니까**?**

소스로 사용할 스토리지 배열에서 System Manager를 열고 원하는 설정을 구성합니다. 그런 다음 Unified Manager에서 관리 페이지로 이동하여 설정을 하나 이상의 어레이로 가져옵니다.

자세한 내용:

- "알림 설정을 가져옵니다"
- "AutoSupport 설정을 가져옵니다"
- "디렉터리 서비스 설정을 가져옵니다"
- "스토리지 구성 설정을 가져옵니다"
- "시스템 설정을 가져옵니다"

개념

가져오기 설정 작동 방식

SANtricity Unified Manager를 사용하여 한 스토리지 어레이에서 여러 스토리지 어레이로 설정을 가져올 수 있습니다. 설정 가져오기 기능은 네트워크에 여러 어레이를 구성해야 할 때 시간을 절약할 수 있는 일괄 작업입니다.

가져올 수 있는 설정입니다

다음 구성을 여러 어레이로 가져올 수 있습니다.

- * Alerts * — e-메일, syslog 서버 또는 SNMP 서버를 사용하여 중요한 이벤트를 관리자에게 보내는 경고 방법입니다.
- * AutoSupport * — 스토리지 어레이의 상태를 모니터링하고 자동 디스패치를 기술 지원 부서에 보내는 기능입니다.
- * 디렉터리 서비스 * — LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스(예: Microsoft의 Active Directory)를 통해 관리되는 사용자 인증 방법입니다.
- * 스토리지 구성 * — 다음과 관련된 구성:
  - 볼륨(일반 및 비리포지토리 볼륨만 해당)
  - 볼륨 그룹 및 풀
  - 핫 스페어 드라이브 할당
- * 시스템 설정 * — 다음과 관련된 구성:

- 볼륨에 대한 미디어 스캔 설정입니다
- SSD 설정
- 자동 로드 밸런싱(호스트 연결 보고 포함 안 함)

구성 워크플로우

설정을 가져오려면 다음 워크플로를 따릅니다.

1. 소스로 사용할 스토리지 배열에서 System Manager를 사용하여 설정을 구성합니다.
2. 타겟으로 사용할 스토리지 어레이에서 System Manager를 사용하여 구성을 백업합니다.
3. Unified Manager에서 * 관리 * 페이지로 이동하여 설정을 가져옵니다.
4. Operations * 페이지에서 설정 가져오기 작업의 결과를 검토합니다.

스토리지 구성 복제 요구 사항

스토리지 시스템 간에 스토리지 구성을 가져오기 전에 요구 사항 및 지침을 검토하십시오.

쉘프

- 컨트롤러가 상주하는 쉘프는 소스 및 타겟 어레이에서 동일해야 합니다.
- 소스 및 타겟 스토리지에서 쉘프 ID가 동일해야 합니다.
- 확장 쉘프가 동일한 드라이브 유형으로 동일한 슬롯에 설치되어야 합니다(구성에서 드라이브를 사용하는 경우, 사용되지 않은 드라이브의 위치는 중요하지 않음).

컨트롤러

- 컨트롤러 유형은 소스 어레이와 타겟 어레이 간에 다를 수 있지만(예: E2800에서 E5700으로 가져오기) RBOD 케이스 유형은 동일해야 합니다.
- 호스트의 DA 기능을 포함한 HIC는 소스와 타겟 스토리지 간에 동일해야 합니다.
- 양면 인쇄에서 단면 인쇄로 가져오는 것은 지원되지 않지만 단면 인쇄에서 양면 인쇄로 가져오는 것은 허용됩니다.
- FDE 설정은 가져오기 프로세스에 포함되지 않습니다.

상태

- 타겟 스토리지가 최적 상태여야 합니다.
- 소스 스토리지가 최적 상태가 아니어야 합니다.

스토리지

- 타겟의 볼륨 용량이 소스보다 큰 경우 소스 스토리지와 타겟 스토리지 간에 드라이브 용량이 다를 수 있습니다. (타겟 스토리지에는 복제 작업에 의해 볼륨으로 완전히 구성되지 않는 더 큰 최신 용량 드라이브가 있을 수 있습니다.)
- 소스 스토리지에서 64TB 이상의 디스크 풀 볼륨으로 인해 타겟의 가져오기 프로세스가 실행되지 않습니다.
- 씬 볼륨은 가져오기 프로세스에 포함되지 않습니다.

일괄 가져오기를 사용합니다

알림 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 경고 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 알림은 소스로 사용할 스토리지 어레이에 대해 System Manager에서 구성됩니다(메뉴: 설정 [경고]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져오기 작업에 대한 e-메일, SNMP 또는 syslog 알림을 선택할 수 있습니다. 가져온 설정은 다음과 같습니다.

- * 이메일 경고 * — 메일 서버 주소 및 경고 수신자의 이메일 주소입니다.
- Syslog 경고 * — syslog 서버 주소와 UDP 포트입니다.
- SNMP 경고 * — SNMP 서버의 커뮤니티 이름 및 IP 주소입니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 이메일 경고 *, * SNMP 경고 * 또는 * Syslog 경고 * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   > 8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 e-메일, SNMP 또는 syslog를 통해 관리자에게 알림을 보내도록 타겟 스토리지 시스템을 구성할 수 있습니다.

AutoSupport 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 AutoSupport 구성을 가져올 수 있습니다. 이

배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 소스로 사용할 스토리지 어레이에 대한 AutoSupport가 시스템 관리자에 구성됩니다(메뉴: 지원 [지원 센터]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 별도 기능(기본 AutoSupport, AutoSupport OnDemand 및 원격 진단), 유지 관리 창, 제공 방법, 및 발송 일정을 참조하십시오.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * AutoSupport * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 AutoSupport 설정으로 구성됩니다.

디렉터리 서비스 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 디렉토리 서비스 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 디렉토리 서비스는 소스로 사용할 스토리지 어레이에 대해 System Manager에서 구성됩니다(메뉴: 설정 [액세스 관리]).
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 LDAP(Lightweight Directory Access Protocol) 서버의 도메인 이름과 URL, LDAP 서버의 사용자

그룹에 대한 매핑과 스토리지 배열의 사전 정의된 역할에 대한 URL이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 디렉터리 서비스 * 를 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 디렉토리 서비스로 구성됩니다.

시스템 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 시스템 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 시스템 설정은 소스로 사용할 스토리지 배열에 대해 System Manager에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.

이 작업에 대해

가져온 설정에는 볼륨에 대한 미디어 스캔 설정, 컨트롤러에 대한 SSD 설정, 자동 로드 밸런싱(호스트 연결 보고 제외)이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 시스템 * 을 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

> 8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 시스템 설정으로 구성됩니다.

스토리지 구성 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 스토리지 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

- 스토리지는 소스로 사용할 스토리지 배열에 대해 SANtricity System Manager에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.
- 소스 및 타겟 스토리지가 다음 요구 사항을 충족해야 합니다.
  - 컨트롤러가 상주하는 쉘프는 동일해야 합니다.
  - 쉘프 ID는 동일해야 합니다.
  - 확장 셸프는 동일한 드라이브 유형으로 동일한 슬롯에 설치되어야 합니다.
  - RBOD 케이스 유형은 동일해야 합니다.
  - 호스트의 Data Assurance 기능을 비롯한 HIC는 동일해야 합니다.
  - 타겟 스토리지가 최적 상태여야 합니다.
  - 타겟 스토리지의 볼륨 용량이 소스 스토리지의 용량보다 큽니다.
- 다음과 같은 제한 사항을 이해합니다.
  - 양면 인쇄에서 단면 인쇄로 가져오는 것은 지원되지 않지만 단면 인쇄에서 양면 인쇄로 가져오는 것은 허용됩니다.
  - 소스 스토리지에서 64TB 이상의 디스크 풀 볼륨으로 인해 타겟의 가져오기 프로세스가 실행되지 않습니다.
  - 씬 볼륨은 가져오기 프로세스에 포함되지 않습니다.

이 작업에 대해

가져온 설정에는 구성된 볼륨(일반 및 비리포지토리 볼륨만 해당), 볼륨 그룹, 풀 및 핫 스페어 드라이브 할당이 포함됩니다.

단계

1. 관리 페이지에서 * 설정 가져오기 * 를 클릭합니다.

   설정 가져오기 마법사가 열립니다.

2. 설정 선택 대화 상자에서 * 스토리지 구성 * 을 선택한 후 * 다음 * 을 클릭합니다.

   소스 스토리지를 선택할 수 있는 대화 상자가 열립니다.

3. 소스 선택 대화 상자에서 가져올 설정이 있는 배열을 선택하고 * 다음 * 을 클릭합니다.
4. 대상 선택 대화 상자에서 새 설정을 받을 하나 이상의 배열을 선택합니다.

   8.50 미만의 펌웨어를 사용하는 스토리지 어레이는 선택할 수 없습니다. 또한 Unified Manager가 해당 어레이와 통신할 수 없는 경우(예: 오프라인 상태이거나 인증서, 암호 또는 네트워킹 문제가 있는 경우) 이 대화 상자에 어레이가 표시되지 않습니다.

5. 마침 * 을 클릭합니다.

   작업 페이지에는 가져오기 작업의 결과가 표시됩니다. 작업이 실패하면 해당 행을 클릭하여 자세한 정보를 볼 수 있습니다.

결과

이제 타겟 스토리지 시스템이 소스 스토리지와 동일한 스토리지 구성으로 구성됩니다.

FAQ 를 참조하십시오

가져올 설정은 무엇입니까?

설정 가져오기 기능은 하나의 스토리지 어레이에서 여러 스토리지 어레이로 구성을 로드하는 일괄 작업입니다. 이 작업 중에 가져온 설정은 SANtricity 시스템 관리자에서 소스 스토리지 배열이 구성된 방식에 따라 다릅니다.

다음 설정을 여러 스토리지 어레이로 가져올 수 있습니다.

- * 이메일 경고 * — 설정에는 메일 서버 주소와 경고 받는 사람의 이메일 주소가 포함됩니다.
- * Syslog alerts * — 설정에는 syslog 서버 주소와 UDP 포트가 포함됩니다.
- SNMP 경고 * — 설정에는 SNMP 서버에 대한 커뮤니티 이름과 IP 주소가 포함됩니다.
- * AutoSupport * — 설정에는 별도 기능(기본 AutoSupport, AutoSupport OnDemand 및 원격 진단), 유지보수 윈도우, 제공 방법, 및 발송 일정을 참조하십시오.
- * 디렉토리 서비스 * — 구성에는 LDAP(Lightweight Directory Access Protocol) 서버의 도메인 이름 및 URL과 LDAP 서버의 사용자 그룹에 대한 스토리지 배열의 사전 정의된 역할에 대한 매핑이 포함됩니다.
- * 스토리지 구성 * — 구성에는 볼륨(일반 및 비리포지토리 볼륨만), 볼륨 그룹, 풀 및 핫 스페어 드라이브 할당이 포함됩니다.
- * 시스템 설정 * — 구성에는 볼륨에 대한 미디어 스캔 설정, 컨트롤러에 대한 SSD 캐시, 자동 로드 밸런싱(호스트 연결 보고 제외)이 포함됩니다.

내 스토리지 어레이가 모두 보이지 않는 이유는 무엇입니까**?**

설정 가져오기 작업 중에 일부 스토리지 배열을 대상 선택 대화 상자에서 사용하지 못할 수 있습니다.

다음과 같은 이유로 스토리지 어레이가 나타나지 않을 수 있습니다.

- 펌웨어 버전이 8.50 미만입니다.
- 스토리지 배열이 오프라인입니다.
- 시스템이 해당 어레이와 통신할 수 없습니다(예: 어레이에 인증서, 암호 또는 네트워킹 문제가 있음).

스토리지 그룹

그룹 개요

Manage Groups 페이지에서 스토리지 어레이 그룹 세트를 생성하여 관리를 간소화할 수 있습니다.

어레이 그룹이란 무엇입니까**?**

스토리지 시스템 세트를 그룹화하여 물리적 인프라와 가상화 인프라를 관리할 수 있습니다. 모니터링 또는 보고 작업을 보다 쉽게 실행할 수 있도록 스토리지 어레이를 그룹화할 수 있습니다.

두 가지 유형의 그룹이 있습니다.

- * All group * — all 그룹은 기본 그룹이며 조직에서 검색된 모든 스토리지 어레이를 포함합니다. All(모두) 그룹은 기본 보기에서 액세스할 수 있습니다.
- * 사용자 생성 그룹 * — 사용자 생성 그룹에는 해당 그룹에 추가하기 위해 수동으로 선택한 스토리지 배열이 포함됩니다. 사용자 생성 그룹은 기본 보기에서 액세스할 수 있습니다.

그룹을 구성하려면 어떻게 합니까**?**

그룹 관리 페이지에서 그룹을 생성한 다음 해당 그룹에 어레이를 추가할 수 있습니다.

자세한 내용:

- "스토리지 어레이 그룹을 구성합니다"

스토리지 어레이 그룹을 구성합니다

스토리지 그룹을 생성한 다음 스토리지 시스템을 그룹에 추가합니다.

그룹 구성은 2단계 절차입니다.

1단계**:** 그룹 만들기

먼저 그룹을 만듭니다. 스토리지 그룹은 볼륨을 구성하는 스토리지를 제공하는 드라이브를 정의합니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [스토리지 그룹 생성]을 선택합니다.
2. 이름 * 필드에 새 그룹의 이름을 입력합니다.
3. 새 그룹에 추가할 스토리지 배열을 선택합니다.
4. Create * 를 클릭합니다.

2단계**:** 스토리지 배열을 그룹에 추가합니다

사용자가 생성한 그룹에 하나 이상의 스토리지 어레이를 추가할 수 있습니다.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 스토리지 배열을 추가할 그룹을 선택합니다.
2. 메뉴: Manage Groups [Add storage arrays to group]를 선택합니다.
3. 그룹에 추가할 스토리지 배열을 선택합니다.
4. 추가 * 를 클릭합니다

그룹에서 스토리지 배열을 제거합니다

특정 스토리지 그룹에서 더 이상 관리 대상 스토리지 어레이를 관리하지 않으려는 경우 그룹에서 하나 이상의 관리되는 스토리지 어레이를 제거할 수 있습니다.

이 작업에 대해

그룹에서 스토리지 배열을 제거해도 스토리지 배열 또는 해당 데이터에는 어떤 식으로든 영향을 주지 않습니다. System Manager에서 스토리지 어레이를 관리하는 경우에도 브라우저를 사용하여 관리할 수 있습니다. 스토리지 배열이 그룹에서 실수로 제거된 경우 다시 추가할 수 있습니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [그룹에서 스토리지 배열 제거]를 선택합니다.
2. 드롭다운에서 제거할 스토리지 배열이 포함된 그룹을 선택한 다음 그룹에서 제거할 각 스토리지 배열 옆의 확인란을 클릭합니다.
3. 제거 * 를 클릭합니다.

스토리지 어레이 그룹을 삭제합니다

더 이상 필요하지 않은 스토리지 그룹을 하나 이상 제거할 수 있습니다.

이 작업에 대해

이 작업은 스토리지 어레이 그룹만 삭제합니다. 삭제된 그룹과 연결된 스토리지 배열은 모두 관리 보기 또는 연결된 다른 그룹을 통해 액세스할 수 있습니다.

단계

1. 관리 페이지에서 메뉴 관리 그룹 [스토리지 어레이 그룹 삭제]를 선택합니다.
2. 삭제할 스토리지 그룹을 하나 이상 선택합니다.
3. 삭제 * 를 클릭합니다.

스토리지 그룹 이름을 바꿉니다

현재 이름이 더 이상 의미가 없거나 적용할 수 없는 경우 스토리지 어레이 그룹의 이름을 변경할 수 있습니다.

이 작업에 대해

이 지침을 염두에 두십시오.

- 이름은 문자, 숫자 및 밑줄(_), 하이픈(-) 및 파운드(#)로 구성될 수 있습니다. 다른 문자를 선택하면 오류 메시지가 나타납니다. 다른 이름을 선택하라는 메시지가 표시됩니다.
- 이름을 30자로 제한합니다. 이름의 선행 및 후행 공백이 삭제됩니다.
- 쉽게 이해하고 기억할 수 있는 독특하고 의미 있는 이름을 사용합니다.
- 나중에 그 의미를 금방 잊어버릴 수 있는 임의 이름이나 이름을 피하십시오.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 이름을 바꿀 스토리지 어레이 그룹을 선택합니다.
2. 메뉴 선택: Manage Groups [Rename storage array group](그룹 관리 [스토리지 배열 그룹 이름 바꾸기]).
3. 그룹 이름 * 필드에 그룹의 새 이름을 입력합니다.
4. 이름 바꾸기 * 를 클릭합니다

업그레이드

업그레이드 센터 개요

업그레이드 센터에서 여러 스토리지 어레이에 대한 SANtricity OS 소프트웨어 및 NVSRAM 업그레이드를 관리할 수 있습니다.

업그레이드는 어떻게 작동합니까**?**

최신 OS 소프트웨어를 다운로드한 다음 하나 이상의 어레이를 업그레이드합니다.

워크플로우 업그레이드

다음 단계에서는 소프트웨어 업그레이드를 수행하기 위한 높은 수준의 워크플로우를 제공합니다.

1. Support 사이트에서 최신 SANtricity OS 소프트웨어 파일을 다운로드합니다(지원 페이지의 Unified Manager에서 링크 사용 가능). 관리 호스트 시스템(브라우저에서 Unified Manager에 액세스하는 호스트)에 파일을 저장한 다음 파일의 압축을 풉니다.
2. Unified Manager에서 SANtricity OS 소프트웨어 파일과 NVSRAM 파일을 리포지토리(파일이 저장되는 웹 서비스 프록시 서버 영역)에 로드합니다. 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드 또는 업그레이드 센터 > 소프트웨어 저장소 관리] 메뉴에서 파일을 추가할 수 있습니다.
3. 저장소에 파일이 로드되면 업그레이드에 사용할 파일을 선택할 수 있습니다. SANtricity OS 소프트웨어 업그레이드 페이지(메뉴: 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드])에서 SANtricity OS 소프트웨어 파일과 NVSRAM 파일을 선택합니다. 소프트웨어 파일을 선택하면 호환되는 스토리지 배열 목록이 이 페이지에 표시됩니다. 그런 다음 새 소프트웨어로 업그레이드할 스토리지 어레이를 선택합니다. (호환되지 않는 어레이는 선택할 수 없습니다.)

4. 그런 다음 즉시 소프트웨어 전송 및 활성화를 시작하거나 나중에 활성화할 파일을 준비하도록 선택할 수 있습니다. 업그레이드 프로세스 중에 Unified Manager는 다음 작업을 수행합니다.

   a. 스토리지 배열의 상태 점검을 수행하여 업그레이드가 완료되지 못할 수 있는 조건이 있는지 확인합니다. 상태 확인에 실패한 어레이가 있으면 해당 특정 어레이를 건너뛰고 다른 어레이를 계속 업그레이드할 수 있습니다. 또는 전체 프로세스를 중지하고 통과하지 못한 어레이의 문제를 해결할 수 있습니다.

   b. 각 컨트롤러로 업그레이드 파일을 전송합니다.

   c. 컨트롤러를 재부팅하여 한 번에 하나의 컨트롤러인 새로운 SANtricity OS 소프트웨어를 활성화합니다. 활성화 중에 기존 SANtricity OS 파일이 새 파일로 대체됩니다.

      나중에 소프트웨어가 활성화되도록 지정할 수도 있습니다.

즉시 또는 단계별 업그레이드

업그레이드를 즉시 활성화하거나 나중에 스테이징할 수 있습니다. 다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

- * 시간 * — 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더 가벼워질 때까지 기다려야 할 수 있습니다. I/O 로드 및 캐시 크기에 따라 컨트롤러 업그레이드를 완료하는 데 일반적으로 15~25분 정도 걸릴 수 있습니다. 활성화 중에 컨트롤러가 재부팅되고 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
- * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.

스테이징된 소프트웨어를 활성화하려면 메뉴 [업그레이드 센터]로 이동한 후 SANtricity OS 컨트롤러 소프트웨어 업그레이드라고 표시된 영역에서 * 활성화 * 를 클릭합니다.

상태 점검

상태 점검은 업그레이드 프로세스의 일부로 실행되지만 시작하기 전에 별도로 상태 점검을 실행할 수도 있습니다(메뉴: 업그레이드 센터 [사전 업그레이드 상태 점검]).

상태 점검을 통해 모든 스토리지 시스템 구성요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다. 다음 조건에서는 업그레이드가 되지 않을 수 있습니다.

- 할당된 드라이브에 오류가 발생했습니다
- 핫 스페어가 사용 중입니다
- 볼륨 그룹이 불완전합니다
- 단독 운영 실행 중
- 볼륨이 누락되었습니다
- 컨트롤러가 최적화되지 않은 상태입니다
- 이벤트 로그 이벤트의 수가 너무 넘습니다
- 구성 데이터베이스 유효성 검사에 실패했습니다
- DACstore의 이전 버전이 있는 드라이브입니다

업그레이드하기 전에 알아야 할 사항은 무엇입니까?

여러 스토리지 시스템을 업그레이드하기 전에 계획의 일환으로 주요 고려 사항을 검토하십시오.

현재 버전

검색된 각 스토리지 시스템에 대해 Unified Manager의 관리 페이지에서 현재 SANtricity OS 소프트웨어 버전을 확인할 수 있습니다. 이 버전은 SANtricity OS 소프트웨어 열에 표시됩니다. 각 행에서 SANtricity OS 버전을 클릭하면 컨트롤러 펌웨어 및 NVSRAM 정보를 팝업 대화 상자에서 사용할 수 있습니다.

업그레이드가 필요한 기타 구성 요소

업그레이드 프로세스 중에 호스트가 컨트롤러와 올바르게 상호 작용할 수 있도록 호스트의 다중 경로/페일오버 드라이버 또는 HBA 드라이버를 업그레이드해야 할 수도 있습니다.

호환성 정보는 을 "NetApp 상호 운용성 매트릭스"참조하십시오. 또한 운영 체제의 Express Guide에 있는 절차를 참조하십시오. Express 가이드는 에서 "E-Series 및 SANtricity 설명서"제공됩니다.

듀얼 컨트롤러

스토리지 어레이에 2개의 컨트롤러가 포함되어 있고 다중 경로 드라이버가 설치되어 있는 경우, 업그레이드가 진행되는 동안 스토리지 어레이에서 I/O를 계속 처리할 수 있습니다. 업그레이드 중에 다음 프로세스가 발생합니다.

1. 컨트롤러 A는 모든 LUN을 컨트롤러 B로 페일오버합니다
2. 컨트롤러 A에서 업그레이드가 발생합니다
3. 컨트롤러 A는 LUN과 모든 컨트롤러 B의 LUN을 백업합니다.
4. 컨트롤러 B에서 업그레이드가 발생합니다

업그레이드가 완료된 후 컨트롤러 간에 볼륨을 수동으로 재배포하여 볼륨이 올바른 소유 컨트롤러로 돌아가도록 해야 할 수 있습니다.

소프트웨어 및 펌웨어를 업그레이드합니다

업그레이드 전 상태 점검을 수행합니다

상태 점검은 업그레이드 프로세스의 일부로 실행되지만 시작하기 전에 상태 점검을 별도로 실행할 수도 있습니다. 상태 점검을 통해 스토리지 시스템의 구성 요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [업그레이드 전 상태 점검] 을 선택합니다.

   업그레이드 전 상태 점검 대화 상자가 열리고 검색된 모든 스토리지 시스템이 나열됩니다.

2. 필요한 경우 현재 최적의 상태가 아닌 모든 시스템을 볼 수 있도록 목록에서 스토리지 시스템을 필터링하거나 정렬합니다.
3. 상태 점검을 통해 실행할 스토리지 시스템의 확인란을 선택합니다.
4. 시작 * 을 클릭합니다.

상태 점검이 수행되는 동안 대화 상자에 진행 상황이 표시됩니다.

5. 상태 점검이 완료되면 각 행의 오른쪽에 있는 줄임표(...)를 클릭하여 추가 정보를 보고 다른 작업을 수행할 수 있습니다.

상태 확인에 실패한 어레이가 있으면 해당 특정 어레이를 건너뛰고 다른 어레이를 계속 업그레이드할 수 있습니다. 또는 전체 프로세스를 중지하고 통과하지 못한 어레이의 문제를 해결할 수 있습니다.

SANtricity OS를 업그레이드합니다

최신 소프트웨어 및 NVSRAM으로 하나 이상의 스토리지 어레이를 업그레이드하여 모든 최신 기능과 버그 수정을 확인할 수 있습니다. 컨트롤러 NVSRAM은 컨트롤러의 기본 설정을 지정하는 컨트롤러 파일입니다.

시작하기 전에

- 최신 SANtricity OS 파일은 SANtricity 웹 서비스 프록시 및 Unified Manager가 실행 중인 호스트 시스템에서 사용할 수 있습니다.
- 소프트웨어 업그레이드를 지금 또는 나중에 활성화할지 여부를 알 수 있습니다.

  다음과 같은 이유로 나중에 정품 인증을 선택할 수 있습니다.

  - * 시간 * — 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더 가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 페일오버되므로 업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
  - * 패키지 유형 * — 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지 어레이에서 새 OS 소프트웨어를 테스트할 수 있습니다.

11.80.x 이상으로 업그레이드하려면 시스템에서 SANtricity OS 11.70.5 를 실행해야 합니다.

이 작업에 대해

```
[NOTE]
====
데이터 손실 또는 스토리지 어레이 손상 위험 - 업그레이드가 진행되는 동안 스토리지 어레이를 변경하지 마십시오. 스토리지 어레이에 대한 전원을 유지합니다.

====
.단계
. 스토리지 어레이에 컨트롤러가 하나만 포함되어 있거나 다중 경로 드라이버를 사용하지 않는 경우 스토리지 어레이에 대한 I/O 작업을 중지하여 응용 프로그램 오류를 방지합니다. 스토리지 어레이에 2개의 컨트롤러가 있는데 다중 경로 드라이버가 설치되어 있는 경우 I/O 작업을 중지할 필요가 없습니다.
. 기본 보기에서 * 관리 * 를 선택한 다음 업그레이드할 스토리지 어레이를 하나 이상 선택합니다.
. 메뉴: 업그레이드 센터 [SANtricity OS 소프트웨어 업그레이드]를 선택합니다.
+
SANtricity OS 소프트웨어 업그레이드 페이지가 나타납니다.
```

. NetApp Support 사이트에서 로컬 시스템으로 최신 SANtricity OS 소프트웨어 패키지를 다운로드하십시오.
+
.. 소프트웨어 리포지토리에 새 파일 추가 * 를 클릭합니다.
.. 최신 * SANtricity OS 다운로드 * 를 찾는 링크를 클릭합니다.
.. 최신 릴리스 다운로드 * 링크를 클릭합니다.
.. 나머지 지침에 따라 SANtricity OS 파일 및 NVSRAM 파일을 로컬 컴퓨터에 다운로드합니다.

+
[NOTE]
====
버전 8.42 이상에서는 디지털 서명된 펌웨어가 필요합니다. 서명되지 않은 펌웨어를 다운로드하려고 하면 오류가 표시되고 다운로드가 중단됩니다.

====
. 컨트롤러를 업그레이드하는 데 사용할 OS 소프트웨어 파일과 NVSRAM 파일을 선택합니다.
+
.. SANtricity OS 소프트웨어 파일 선택 * 드롭다운에서 로컬 컴퓨터에 다운로드한 OS 파일을 선택합니다.
+
여러 개의 파일을 사용할 수 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.

+
[NOTE]
====
소프트웨어 리포지토리는 웹 서비스 프록시와 연결된 모든 소프트웨어 파일을 나열합니다. 사용할 파일이 표시되지 않으면 * 소프트웨어 리포지토리에 새 파일 추가 * 링크를 클릭하여 추가할 OS 파일이 있는 위치를 찾을 수 있습니다.

====
.. NVSRAM 파일 선택 * 드롭다운에서 사용할 컨트롤러 파일을 선택합니다.
+
파일이 여러 개 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.

. Compatible Storage Array 표에서 선택한 OS 소프트웨어 파일과 호환되는 스토리지 배열을 검토한 다음 업그레이드할 스토리지를 선택합니다.
+
** 관리 보기에서 선택했으며 선택한 펌웨어 파일과 호환되는 스토리지 배열은 기본적으로 호환 가능한 스토리지 배열 테이블에서 선택됩니다.
** 선택한 펌웨어 파일로 업데이트할 수 없는 스토리지 배열은 * 호환되지 않음 * 상태로 표시된 호환 가능한 스토리지 배열 테이블에서 선택할 수 없습니다.

. * 선택 사항: * 소프트웨어 파일을 활성화하지 않고 스토리지 어레이로 전송하려면 * OS 소프트웨어를 스토리지 어레이로 전송, 스테이징으로 표시 및 나중에 활성화 * 확인란을 선택합니다.
. 시작 * 을 클릭합니다.
. 지금 활성화할지 아니면 나중에 활성화할지 여부에 따라 다음 중 하나를 수행합니다.
+
** 업그레이드하려는 어레이에서 제안된 OS 소프트웨어 버전을 전송할지 확인하려면 * TRANSFER * 를 입력하고 * TRANSFER * 를 클릭합니다.
+
전송된 소프트웨어를 활성화하려면 업그레이드 센터 [스테이징된 OS 소프트웨어 활성화] 메뉴를 선택합니다.

** 업그레이드 * 를 입력하여 업그레이드하도록 선택한 어레이에서 제안된 OS 소프트웨어 버전을 전송 및 활성화한 다음 * 업그레이드 * 를 클릭합니다.
+
시스템은 업그레이드를 위해 선택한 각 스토리지 어레이로 소프트웨어 파일을 전송한 다음 재부팅을 시작하여 해당 파일을 활성화합니다.

+
업그레이드 작업 중에 다음 작업이 수행됩니다.

+
** 업그레이드 전 상태 점검이 업그레이드 프로세스의 일부로 실행됩니다. 업그레이드 전 상태 점검을 통해 모든 스토리지 시스템 구성 요소를 평가하여 업그레이드를 진행할 수 있는지 확인합니다.
** 스토리지 배열에 대한 상태 검사에 실패하면 업그레이드가 중지됩니다. 줄임표(...)를 클릭하고 * 로그 저장 * 을 선택하여 오류를 검토할 수 있습니다. 상태 점검 오류를 재정의하도록 선택한 다음 * 계속 * 을 클릭하여 업그레이드를 진행할 수도 있습니다.
** 업그레이드 전 상태 점검 후 업그레이드 작업을 취소할 수 있습니다.

. * 선택 사항: * 업그레이드가 완료되면 줄임표(...)를 클릭한 다음 * Save Log * 를 선택하여 특정 스토리지 배열에 대해 업그레이드된 항목 목록을 볼 수 있습니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `upgrade_log-<date>.json`저장됩니다.

[[ID6ff874791c3649fa72bead05fd9f4ee7]]
= 스테이징된 OS 소프트웨어를 활성화합니다
:allow-uri-read:
:experimental:
:icons: font

```
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
소프트웨어 파일을 즉시 활성화하거나 더 편리한 시간이 될 때까지 기다릴 수 있습니다. 이
절차에서는 나중에 소프트웨어 파일을 활성화하도록 선택한 것으로 가정합니다.

.이 작업에 대해
펌웨어 파일을 활성화하지 않고 전송할 수 있습니다. 다음과 같은 이유로 나중에 정품 인증을
선택할 수 있습니다.

* * 시간 * -- 소프트웨어를 활성화하는 데 시간이 오래 걸릴 수 있으므로 I/O 부하가 더
가벼워질 때까지 기다려야 할 수 있습니다. 활성화 중에 컨트롤러가 재부팅되고 페일오버되므로
업그레이드가 완료될 때까지 성능이 평소보다 저하될 수 있습니다.
* * 패키지 유형 * -- 다른 스토리지 어레이의 파일을 업그레이드하기 전에 한 스토리지
어레이에서 새 소프트웨어 및 펌웨어를 테스트할 수 있습니다.


[NOTE]
====
활성화 프로세스가 시작된 후에는 중지할 수 없습니다.

====
.단계
. 기본 보기에서 * 관리 * 를 선택합니다. 필요한 경우 페이지 맨 위에서 Status 열을 클릭하여
"OS Upgrade(활성화 대기 중)" 상태의 모든 스토리지 어레이를 정렬합니다.
. 소프트웨어를 활성화할 스토리지 어레이를 하나 이상 선택한 다음 메뉴: 업그레이드 센터
[스테이징된 OS 소프트웨어 활성화] 를 선택합니다.
+
업그레이드 작업 중에 다음 작업이 수행됩니다.

+
** 업그레이드 전 상태 점검이 활성화 프로세스의 일부로 실행됩니다. 업그레이드 전 상태 점검을
통해 모든 스토리지 시스템 구성 요소를 평가하여 활성화를 진행할 수 있는지 확인합니다.
** 스토리지 배열에 대한 상태 검사에 실패하면 활성화가 중지됩니다. 줄임표(...)를 클릭하고 *
로그 저장 * 을 선택하여 오류를 검토할 수 있습니다. 상태 점검 오류를 재정의하도록 선택한 다음
* 계속 * 을 클릭하여 활성화를 계속 진행할 수도 있습니다.
** 업그레이드 전 상태 점검 후 활성화 작업을 취소할 수 있습니다. 업그레이드 전 상태 점검이
성공적으로 완료되면 활성화가 발생합니다. 활성화하는 데 걸리는 시간은 스토리지 배열 구성과
활성화 중인 구성 요소에 따라 달라집니다.


. * 선택 사항: * 활성화가 완료된 후 줄임표(...)를 클릭한 다음 * Save Log * 를 선택하여
특정 스토리지 배열에 대해 활성화된 항목 목록을 볼 수 있습니다.
+
파일이 브라우저의 다운로드 폴더에 이름으로 `activate_log-<date>.json`저장됩니다.
```

```
[[ID927a137764facc6b7211ef5f14e42097]]
= 소프트웨어 저장소를 관리합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
소프트웨어 리포지토리는 웹 서비스 프록시와 연결된 모든 소프트웨어 파일을 나열합니다.

사용할 파일이 표시되지 않으면 소프트웨어 저장소 관리 옵션을 사용하여 하나 이상의 SANtricity OS 파일을 웹 서비스 프록시 및 Unified Manager가 실행 중인 호스트 시스템으로 가져올 수 있습니다. 소프트웨어 저장소에서 사용 가능한 하나 이상의 SANtricity OS 파일을 삭제하도록 선택할 수도 있습니다.

.시작하기 전에
SANtricity OS 파일을 추가하는 경우 로컬 시스템에서 OS 파일을 사용할 수 있는지 확인합니다.

.단계
. 기본 보기에서 * 관리 * 를 선택한 다음 업그레이드 센터 [소프트웨어 리포지토리 관리] 메뉴를 선택합니다.
+
Manage Software Repository 대화상자가 나타납니다.

. 다음 작업 중 하나를 수행합니다.
+
[cols="25h,~"]
|===
| 옵션을 선택합니다 | 이렇게 하세요


 a|
가져오기
 a|
.. 가져오기 * 를 클릭합니다
.. 찾아보기 * 를 클릭한 다음 추가할 OS 파일이 있는 위치로 이동합니다.
+
OS 파일의 파일 이름은 과 `N2800-830000-000.dlp`유사합니다.

.. 추가할 OS 파일을 하나 이상 선택한 다음 * 가져오기 * 를 클릭합니다.
```

a|
삭제
a|
.. 소프트웨어 저장소에서 제거할 OS 파일을 하나 이상 선택합니다.
.. 삭제 * 를 클릭합니다.

|===

.결과
가져오기를 선택한 경우 파일이 업로드되고 확인됩니다. 삭제를 선택하면 소프트웨어 저장소에서 파일이 제거됩니다.

[[IDbcd2d17dc8c0c0f867887b1929411961]]
= 스테이징된 OS 소프트웨어를 지웁니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
대기 중인 버전이 나중에 실수로 활성화되지 않도록 스테이징된 OS 소프트웨어를 제거할 수 있습니다. 스테이징된 OS 소프트웨어를 제거해도 스토리지 어레이에서 실행 중인 현재 버전에는 영향을 주지 않습니다.

.단계
. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [스테이징된 OS 소프트웨어 지우기] 를 선택합니다.
+
준비된 OS 소프트웨어 지우기 대화 상자가 열리고 보류 중인 소프트웨어 또는 NVSRAM이 있는 검색된 모든 스토리지 시스템이 나열됩니다.

. 필요한 경우 스테이징된 소프트웨어가 있는 모든 시스템을 볼 수 있도록 목록에서 스토리지 시스템을 필터링하거나 정렬합니다.
. 선택 취소할 보류 중인 소프트웨어가 있는 스토리지 시스템의 확인란을 선택합니다.
. 지우기 * 를 클릭합니다.
+
작업 상태가 대화 상자에 표시됩니다.

```
:leveloffset: -1


:leveloffset: -1


= 미러링

:leveloffset: +1


[[ID6452109c03023a568dc531a59a2db35e]]
= 미러링 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미러링 기능을 사용하여 로컬 스토리지 시스템과 원격 스토리지 시스템 간에 데이터를 비동기식으로 또는 동기식으로 복제합니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====


== 미러링이란 무엇입니까?

SANtricity 애플리케이션에는 두 가지 유형의 미러링, 즉 비동기식과 동기식이 있습니다. 비동기식 미러링은 데이터 볼륨을 필요 시 또는 일정에 따라 복제하여 데이터 손상 또는 손실로 인한 다운타임을 최소화 또는 방지합니다. 동기식 미러링은 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다.

자세한 내용:

* xref:{relative_path}mirroring-overview.html["미러링의 작동 방식"]
* xref:{relative_path}mirroring-terminology.html["미러링 용어"]
```

== 미러링을 구성하려면 어떻게 합니까?

Unified Manager에서 비동기식 또는 동기식 미러링을 구성한 다음 System Manager를 사용하여 동기화를 관리합니다.

자세한 내용:

* xref:{relative_path}mirroring-configuration-workflow.html["미러링 구성 워크플로우"]
* xref:{relative_path}requirements-for-using-mirroring.html["미러링 사용에 대한 요구사항"]
* xref:{relative_path}create-asynchronous-mirrored-pair-um.html["비동기 미러링 쌍을 생성합니다"]
* xref:{relative_path}create-synchronous-mirrored-pair-um.html["동기식 미러링 쌍을 생성합니다"]

= 개념

:leveloffset: +1

[[ID827ea7007d098cf0c20e23a09b03880e]]
= 미러링의 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity Unified Manager에는 SANtricity 미러링 기능을 위한 구성 옵션이 포함되어 있어 관리자가 데이터 보호를 위해 두 스토리지 어레이 간에 데이터를 복제할 수 있습니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

== 미러링 유형

SANtricity 애플리케이션에는 두 가지 유형의 미러링, 즉 비동기식과 동기식이 있습니다.

비동기식 미러링은 데이터 볼륨을 필요 시 또는 일정에 따라 복제하여 데이터 손상 또는 손실로 인한 다운타임을 최소화 또는 방지합니다. 비동기식 미러링은 특정 시점에 기본 볼륨의 상태를 캡처하고 마지막 이미지 캡처 이후 변경된 데이터만 복사합니다. 운영 사이트를 즉시 업데이트할 수 있으며 대역폭이 허용할 경우 보조 사이트를 업데이트할 수 있습니다. 네트워크 리소스를 사용할 수 있게 되면 정보가 캐시되어 나중에 전송됩니다. 이러한 유형의 미러링은 백업 및 아카이빙과 같은 주기적인 프로세스에 이상적입니다.

동기식 미러링은 데이터 볼륨을 실시간으로 복제하여 지속적인 가용성을 보장합니다. 두 스토리지 어레이 중 하나에서 재해가 발생할 경우 중요 데이터의 복사본을 사용할 수 있으므로 RPO(복구 시점 목표)를 달성할 수 있습니다. 복제본은 운영 볼륨에 쓸 때마다 보조 볼륨에 쓰기가 수행되므로 항상 운영 데이터와 동일합니다. 보조 볼륨이 운영 볼륨에서 수행된 변경 사항으로 업데이트될 때까지 호스트에 쓰기가 성공했다는 확인 메시지가 표시되지 않습니다. 이러한 유형의 미러링은 재해 복구와 같은 비즈니스 연속성 목적으로 이상적입니다.

== 미러링 유형의 차이점

다음 표에서는 두 미러링 유형의 주요 차이점을 설명합니다.

[cols="1a,1a,1a"]
|===
| 속성 | 비동기식 | 동기식이다

a|
복제 방법입니다
a|
시점 -- 미러링은 사용자 정의 일정에 따라 필요 시 또는 자동으로 수행됩니다.
a|
연속 -- 미러링은 모든 호스트 쓰기에서 데이터를 복사하여 지속적으로 자동 실행됩니다.

a|
거리
a|
어레이 간 장거리 지원. 일반적으로 거리는 네트워크 및 채널 확장 기술의 성능에 의해서만 제한됩니다.
a|
어레이 간 거리가 짧아집니다. 일반적으로 지연 시간 및 애플리케이션 성능 요구 사항을 충족하려면 로컬 스토리지 어레이에서 약 10km(6.2마일) 이내에 있어야 합니다.

 a|
통신 방법
 a|
표준 IP 또는 Fibre Channel 네트워크
 a|
Fibre Channel 네트워크만 해당.

 a|
볼륨 유형
 a|
표준 또는 얇은.
 a|
표준 전용.

|===

[[ID320fe4f933350da8e0eb786393c39fb3]]
= 미러링 구성 워크플로우
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity Unified Manager에서 비동기식 또는 동기식 미러링을 구성한 다음 SANtricity System Manager를 사용하여 동기화를 관리합니다.

== 비동기식 미러링 워크플로우

비동기식 미러링에는 다음 워크플로우가 포함됩니다.

. Unified Manager에서 초기 구성을 수행합니다.
+
.. 로컬 스토리지 배열을 데이터 전송 소스로 선택합니다.
.. 로컬 스토리지의 운영 볼륨과 원격 스토리지의 보조 볼륨을 위한 컨테이너인 기존 미러 정합성 보장 그룹을 생성하거나 선택합니다. 운영 볼륨과 보조 볼륨을 "미러링된 페어"라고 합니다. 미러 정합성 보장 그룹을 처음으로 생성하는 경우 수동 동기화 또는 예약된 동기화를 수행할지 여부를 지정합니다.
.. 로컬 스토리지 어레이에서 운영 볼륨을 선택한 다음 예약된 용량을 확인합니다. 예약된 용량은

복제 작업에 사용할 물리적 할당 용량입니다.
.. 원격 스토리지 시스템을 전송 대상, 보조 볼륨으로 선택한 다음 예약된 용량을 결정합니다.
.. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기 전송에 몇 시간이 걸릴 수 있습니다.

. 초기 동기화 진행률을 확인합니다.
+
.. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
.. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다.

. 선택적으로 System Manager에서 후속 데이터 전송을 다시 예약하거나 수동으로 수행할 수 있습니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.
+
[NOTE]
====
비동기식 복제는 정기적으로 수행되므로 시스템에서 변경된 블록을 통합하고 네트워크 대역폭을 보존할 수 있습니다. 쓰기 처리량과 쓰기 지연 시간에 미치는 영향은 미미합니다.

====

== 동기 미러링 워크플로우

동기식 미러링에는 다음 워크플로우가 포함됩니다.

. Unified Manager에서 초기 구성을 수행합니다.
+
.. 데이터 전송을 위한 소스로 로컬 스토리지 배열을 선택합니다.
.. 로컬 스토리지 어레이에서 운영 볼륨을 선택합니다.
.. 데이터 전송 대상으로 원격 스토리지 시스템을 선택한 다음 보조 볼륨을 선택합니다.
.. 동기화 및 재동기화 우선 순위를 선택합니다.
.. 운영 볼륨에서 보조 볼륨으로 초기 데이터 전송을 시작합니다. 볼륨 크기에 따라 이 초기 전송에 몇 시간이 걸릴 수 있습니다.

. 초기 동기화 진행률을 확인합니다.
+
.. Unified Manager에서 로컬 어레이에 대한 System Manager를 시작합니다.
.. System Manager에서 미러링 작업의 상태를 봅니다. 미러링이 완료되면 미러링된 쌍의 상태가 "Optimal(최적)"입니다. 두 배열은 정상적인 작업을 통해 동기화 상태를 유지하려고 합니다. 운영 볼륨에서 2차 볼륨으로 새 블록과 변경된 블록만 전송합니다.

. 선택적으로 System Manager에서 동기화 설정을 변경할 수 있습니다.
+
[NOTE]
====
동기식 복제는 지속적이기 때문에 두 사이트 간의 복제 링크는 충분한 대역폭 기능을 제공해야 합니다.

====

[[ID56fe168fdca23c12549be36c90f13218]]
= 미러링 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
미러링 조건이 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명

a|
로컬 스토리지 시스템입니다
a|
로컬 스토리지 배열은 사용자가 수행하는 스토리지 배열입니다.

a|
미러 정합성 보장 그룹
a|
미러 정합성 보장 그룹은 하나 이상의 미러링된 쌍에 대한 컨테이너입니다. 비동기식 미러링 작업의 경우 미러 정합성 보장 그룹을 생성해야 합니다. 그룹의 모든 미러링된 쌍이 동시에 재동기화되므로 일관된 복구 지점이 유지됩니다.

동기식 미러링은 미러 정합성 보장 그룹을 사용하지 않습니다.

a|
미러링 쌍

a|
미러링된 쌍은 기본 볼륨 및 보조 볼륨이라는 두 개의 볼륨으로 구성됩니다.

비동기식 미러링에서는 미러링된 쌍이 항상 미러 정합성 보장 그룹에 속합니다. 쓰기 작업은 먼저 운영 볼륨에 대해 수행된 다음 보조 볼륨에 복제됩니다. 미러 정합성 보장 그룹의 미러링된 각 쌍은 동일한 동기화 설정을 공유합니다.

a|
운영 볼륨

a|
미러링된 쌍의 기본 볼륨은 미러링될 소스 볼륨입니다.

a|
원격 스토리지 시스템

a|
원격 스토리지 시스템은 일반적으로 미러링 구성의 데이터 복제본을 보관하는 보조 사이트로 지정됩니다.

a|
예약된 용량입니다

a|
예약된 용량은 복제 서비스 작업 및 스토리지 객체에 사용되는 물리적 할당 용량입니다. 호스트에서 직접 읽을 수 없습니다.

이러한 볼륨은 컨트롤러가 운영 상태에서 미러링을 유지하는 데 필요한 정보를 지속적으로 저장할 수 있도록 하기 위해 필요합니다. 여기에는 델타 로그 및 쓰기 시 복사 데이터와 같은 정보가 포함됩니다.

a|
2차 볼륨

a|
미러링된 쌍의 보조 볼륨은 일반적으로 보조 사이트에 위치하며 데이터 복제본을 보관합니다.

a|
동기화

```
 a|
동기화는 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화에서 수행됩니다. 동기화는 통신
중단 후 운영 볼륨과 2차 볼륨의 동기화가 중단된 경우에도 발생합니다. 통신 링크가 다시
작동되면 복제되지 않은 모든 데이터가 보조 볼륨의 스토리지 시스템에 동기화됩니다.

|===



[[ID1623b18157f15324690f4612ab3f674b]]
= 미러링 사용에 대한 요구사항
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
미러링을 구성하려는 경우 다음 요구사항을 염두에 두십시오.



== Unified Manager를 참조하십시오

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체
서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로
이동하여 자체 보안 인증서를 설치할 수 있습니다.



== 지원합니다

[NOTE]
====
동기식 미러링은 EF600 또는 EF300 스토리지 어레이에서 사용할 수 없습니다.

====
* 두 개의 스토리지 어레이가 있어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며
네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
```

* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 비동기 미러링은 FC(파이버 채널) 또는 iSCSI 호스트 포트가 있는 컨트롤러에서 지원되며, 동기식 미러링은 FC 호스트 포트가 있는 컨트롤러에서만 지원됩니다.

== 연결 요구 사항

FC 인터페이스(비동기식 또는 동기식)를 통해 미러링하려면 다음이 필요합니다.

* 스토리지 어레이의 각 컨트롤러는 가장 높은 번호가 지정된 FC 호스트 포트를 미러링 작업에 사용합니다.
* 컨트롤러에 기본 FC 포트와 HIC(호스트 인터페이스 카드) FC 포트가 모두 있는 경우 가장 높은 번호가 지정된 포트가 HIC에 있습니다. 전용 포트에 로그온한 호스트는 로그아웃되며 호스트 로그인 요청은 허용되지 않습니다. 이 포트의 I/O 요청은 미러링 작업에 사용되는 컨트롤러에서만 허용됩니다.
* 전용 미러링 포트는 디렉토리 서비스 및 네임 서비스 인터페이스를 지원하는 FC 패브릭 환경에 연결해야 합니다. 특히 FC-AL 및 지점 간 연결 옵션은 미러 관계에 참여하는 컨트롤러 간의 연결 옵션으로 지원되지 않습니다.

iSCSI 인터페이스를 통한 미러링(비동기식만 해당)에는 다음이 필요합니다.

* FC와 달리 iSCSI에는 전용 포트가 필요하지 않습니다. iSCSI 환경에서 비동기 미러링을 사용하는 경우 비동기 미러링에 사용하기 위해 스토리지 어레이의 프런트 엔드 iSCSI 포트 중 하나를 전용으로 지정할 필요가 없습니다. 이러한 포트는 비동기 미러 트래픽과 호스트-스토리지 I/O 연결을 위해 모두 공유됩니다.
* 컨트롤러는 iSCSI 이니시에이터가 세션을 설정하려고 시도하는 원격 스토리지 시스템의 목록을 유지합니다. iSCSI 연결을 성공적으로 설정하는 첫 번째 포트는 해당 원격 스토리지 시스템과의 이후의 모든 통신에 사용됩니다. 통신이 실패하면 사용 가능한 모든 포트를 사용하여 새 세션이 시도됩니다.
* iSCSI 포트는 포트별로 어레이 레벨에서 구성됩니다. 구성 메시징 및 데이터 전송을 위한 컨트롤러 간 통신은 다음 설정을 포함한 글로벌 설정을 사용합니다.
+
** VLAN: 로컬 시스템과 원격 시스템 모두 동일한 VLAN 설정을 사용하여 통신해야 합니다
** iSCSI 수신 포트입니다
** 점보 프레임
** 이더넷 우선 순위

[NOTE]
====

iSCSI 인터컨트롤러 통신은 관리 이더넷 포트가 아닌 호스트 연결 포트를 사용해야 합니다.

====

== 미러링 볼륨 후보

* RAID 레벨, 캐싱 매개 변수 및 세그먼트 크기는 미러링된 쌍의 운영 볼륨과 2차 볼륨에서 서로 다를 수 있습니다.
+

NOTE: EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.
* 볼륨은 하나의 미러 관계에만 참여할 수 있습니다.
* 동기식 미러링 쌍의 경우 운영 볼륨과 2차 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨 또는 스냅샷 볼륨일 수 없습니다.
* 동기식 미러링의 경우 지정된 스토리지 어레이에서 지원되는 볼륨 수에 제한이 있습니다. 스토리지 배열에 구성된 볼륨 수가 지원되는 제한보다 적었는지 확인합니다. 동기식 미러링이 활성 상태인 경우 생성된 2개의 예약된 용량 볼륨이 볼륨 제한에 대해 계산됩니다.
* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨의 드라이브 보안 기능이 동일해야 합니다.
+
** 기본 볼륨이 FIPS를 지원할 수 있는 경우 보조 볼륨은 FIPS를 지원할 수 있어야 합니다.
** 기본 볼륨이 FDE를 지원할 수 있는 경우 보조 볼륨은 FDE를 지원할 수 있어야 합니다.
** 주 볼륨이 드라이브 보안을 사용하지 않는 경우 보조 볼륨이 드라이브 보안을 사용하지 않아야 합니다.

== 예약된 용량입니다

비동기식 미러링:

* 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 미러링된 쌍의 보조 볼륨과 운영 볼륨에 예약된 용량 볼륨이 필요합니다.
* 미러링 쌍의 운영 볼륨과 2차 볼륨 모두에 추가 예약 용량이 필요하므로 미러 관계의 두 스토리지 어레이에서 사용 가능한 용량이 있는지 확인해야 합니다.

동기식 미러링:

* 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위해 쓰기 정보를 로깅하기 위해 운영

볼륨과 보조 볼륨에 예약된 용량이 필요합니다.
* 예약된 용량 볼륨은 동기식 미러링이 활성화될 때 자동으로 생성됩니다. 미러링된 쌍의 운영 볼륨과 2차 볼륨 모두에 예약된 용량이 필요하므로 동기 미러 관계에 참여하는 두 스토리지 시스템에서 사용 가능한 용량이 충분한지 확인해야 합니다.

== 드라이브 보안 기능

* 보안 가능 드라이브를 사용하는 경우 기본 볼륨 및 보조 볼륨에 호환되는 보안 설정이 있어야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
* 보안 가능 드라이브를 사용하는 경우 기본 볼륨과 보조 볼륨은 동일한 드라이브 유형을 사용해야 합니다. 이 제한은 적용되지 않으므로 직접 확인해야 합니다.
* DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.

:leveloffset: -1

= 미러링을 구성합니다

:leveloffset: +1

[[IDa81673b7bf1424632e658e2145d5e580]]
= 비동기 미러링 쌍을 생성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
비동기식 미러링을 구성하려면 로컬 스토리지의 기본 볼륨과 원격 스토리지의 보조 볼륨을 포함하는 미러링된 쌍을 생성합니다.

.시작하기 전에
미러링된 쌍을 생성하기 전에 Unified Manager에 대한 다음 요구사항을 충족해야 합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로

이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이 및 볼륨에 대한 다음 요구 사항도 충족해야 합니다.

* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.
* 비동기식 미러 관계에 사용할 운영 볼륨과 2차 볼륨을 모두 생성했습니다.
* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.

.이 작업에 대해
비동기 미러링 쌍을 만드는 프로세스는 다단계 절차입니다.

== 1단계: 미러 정합성 보장 그룹을 생성하거나 선택합니다

이 단계에서는 새 미러 일관성 그룹을 생성하거나 기존 미러 일관성 그룹을 선택합니다. 미러 정합성 보장 그룹은 운영 볼륨과 2차 볼륨(미러링된 페어)의 컨테이너로, 그룹의 모든 페어에 대해 원하는 재동기화 방법(수동 또는 자동)을 지정합니다.

.단계
. Manage * 페이지에서 소스에 사용할 로컬 스토리지 배열을 선택합니다.
. 메뉴 선택: 작업 [비동기 미러링 쌍 만들기].
+
Create Asynchronous Mirrored Pair 마법사가 열립니다.

. 기존 미러 정합성 보장 그룹을 선택하거나 새 미러 정합성 보장 그룹을 생성합니다.
+
기존 그룹을 선택하려면 * 기존 미러 정합성 보장 그룹 * 이 선택되어 있는지 확인한 다음 테이블에서 그룹을 선택합니다. 일관성 그룹에는 여러 개의 미러링된 쌍이 포함될 수 있습니다.

+
새 그룹을 만들려면 다음을 수행합니다.

+
.. 새 미러 정합성 보장 그룹 * 을 선택한 후 * 다음 * 을 클릭합니다.
.. 두 스토리지 배열 간에 미러링될 볼륨의 데이터를 가장 잘 설명하는 고유한 이름을 입력합니다.

이름은 문자, 숫자 및 밑줄(_), 대시(-) 및 해시 기호(#)로만 구성될 수 있습니다. 이름은 30자를 초과할 수 없으며 공백을 포함할 수 없습니다.
.. 로컬 스토리지 시스템과 미러 관계를 설정할 원격 스토리지 시스템을 선택합니다.
+
[NOTE]
====
원격 스토리지 배열이 암호로 보호되어 있는 경우 암호를 입력하라는 메시지가 표시됩니다.

====
.. 미러링된 쌍을 수동으로 동기화할지 또는 자동으로 동기화할지 여부를 선택합니다.
+
*** * 수동 * -- 이 그룹 내에서 미러링된 모든 쌍의 동기화를 수동으로 시작하려면 이 옵션을 선택합니다. 나중에 재동기화를 수행하려면 운영 스토리지 시스템에 대해 System Manager를 시작한 다음 메뉴(Storage [Asynchronous Mirroring])로 이동하여 * Mirror Consistency Groups * 탭에서 그룹을 선택한 다음 menu: More [Manually resyncize]를 선택합니다.
*** * 자동 * - 이전 업데이트 시작에서 다음 업데이트 시작까지 원하는 간격을 * 분 *, * 시간 * 또는 * 일 * 으로 선택합니다. 예를 들어 동기화 간격이 30분으로 설정되어 있고 동기화 프로세스가 오후 4시에 시작되면 다음 프로세스는 오후 4시 30분에 시작됩니다

.. 원하는 알림 설정을 선택합니다.
+
*** 수동 동기화의 경우 알림을 받을 때의 임계값(남은 용량 백분율로 정의)을 지정합니다.
*** 자동 동기화의 경우 세 가지 알림 방법을 설정할 수 있습니다. 특정 시간 동안 동기화가 완료되지 않은 경우, 원격 스토리지의 복구 지점 데이터가 특정 시간 제한보다 오래되고 예약된 용량이 특정 임계값(남은 용량 백분율로 정의)에 근접하는 경우

. 다음 * 을 선택하고 로 이동합니다<<2단계: 운영 볼륨을 선택합니다>>.
+
새 미러 정합성 보장 그룹을 정의한 경우 Unified Manager는 먼저 로컬 스토리지 시스템에 미러 정합성 보장 그룹을 생성한 다음 원격 스토리지 시스템에 미러 정합성 보장 그룹을 생성합니다. 각 어레이에 대해 System Manager를 시작하여 미러 정합성 보장 그룹을 보고 관리할 수 있습니다.

+
[NOTE]
====
Unified Manager가 로컬 스토리지 시스템에 미러 정합성 보장 그룹을 생성했지만 원격 스토리지 시스템에 생성하지 못한 경우 로컬 스토리지 시스템에서 미러 정합성 보장 그룹이 자동으로 삭제됩니다. Unified Manager에서 미러 정합성 보장 그룹을 삭제하려는 동안 오류가 발생하면 수동으로 삭제해야 합니다.

====

== 2단계: 운영 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 운영 볼륨을 선택하고 예약된 용량을 할당합니다. 로컬 스토리지 배열에서 운영 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다.

로컬 스토리지 시스템의 미러 정합성 보장 그룹에 추가하는 모든 볼륨은 미러 관계에서 기본 역할을 유지합니다.

.단계
. 사용 가능한 볼륨 목록에서 운영 볼륨으로 사용할 볼륨을 선택한 후 * Next * 를 클릭하여 예약된 용량을 할당합니다.
. 적합한 후보 목록에서 운영 볼륨에 대해 예약된 용량을 선택합니다.
+
다음 지침을 염두에 두십시오.

+
** 예약된 용량의 기본 설정은 기본 볼륨 용량의 20%이며 일반적으로 이 용량이면 충분합니다. 비율을 변경한 경우 * 후보 새로 고침 * 을 클릭합니다.
** 필요한 용량은 운영 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 용량을 유지하는 데 필요한 기간에 따라 달라집니다.
** 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.
+
*** 미러링 쌍을 장기간 유지하려고 합니다.
*** 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

. 다음 * 을 선택하고 로 이동합니다<<3단계: 보조 볼륨을 선택합니다>>.

== 3단계: 보조 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 보조 볼륨을 선택하고 예약된 용량을 할당합니다. 원격 스토리지 어레이에서 보조 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다.

원격 스토리지 시스템의 미러 정합성 보장 그룹에 추가하는 모든 볼륨은 미러 관계에서 2차 역할을

유지합니다.

.단계
. 적합한 볼륨 목록에서 미러링된 쌍의 보조 볼륨으로 사용할 볼륨을 선택한 후 * Next * 를 클릭하여 예약된 용량을 할당합니다.
. 적합한 후보 목록에서 2차 볼륨에 대해 예약된 용량을 선택합니다.
+
다음 지침을 염두에 두십시오.

+
** 예약된 용량의 기본 설정은 기본 볼륨 용량의 20%이며 일반적으로 이 용량이면 충분합니다. 비율을 변경한 경우 * 후보 새로 고침 * 을 클릭합니다.
** 필요한 용량은 운영 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 용량을 유지하는 데 필요한 기간에 따라 달라집니다.
** 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 용량을 선택합니다.
+
*** 미러링 쌍을 장기간 유지하려고 합니다.
*** 입출력 작업이 많은 경우 운영 볼륨에서 데이터 블록의 비율이 크게 변경됩니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

. 비동기 미러링 시퀀스를 완료하려면 * Finish * 를 선택합니다.

.결과
Unified Manager는 다음 작업을 수행합니다.

* 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화를 시작합니다.
* 로컬 스토리지 시스템 및 원격 스토리지 시스템에서 미러링된 쌍에 대한 예약된 용량을 생성합니다.

NOTE: 미러링되는 볼륨이 씬 볼륨인 경우 초기 동기화 중에 프로비저닝된 블록(보고된 용량이 아닌 할당된 용량)만 보조 볼륨으로 전송됩니다. 이렇게 하면 초기 동기화를 완료하기 위해 전송해야 하는 데이터의 양이 줄어듭니다.

[[ID834de0fb7a23508db7a7bc72b370a03b]]
= 동기식 미러링 쌍을 생성합니다
:allow-uri-read:
:experimental:

```
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
동기식 미러링을 구성하려면 로컬 스토리지의 기본 볼륨과 원격 스토리지의 보조 볼륨을 포함하는 미러링된 쌍을 생성합니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

====
.시작하기 전에
미러링된 쌍을 생성하기 전에 Unified Manager에 대한 다음 요구사항을 충족해야 합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.


또한 스토리지 어레이 및 볼륨에 대한 다음 요구 사항도 충족해야 합니다.

* 미러링에 사용할 두 스토리지 어레이가 Unified Manager에서 검색됩니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭을 통해 연결됩니다.
* 동기식 미러 관계에 사용할 운영 볼륨과 2차 볼륨을 모두 생성했습니다.
* 운영 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨이거나 스냅샷 볼륨일 수 없습니다.
* 2차 볼륨은 표준 볼륨이어야 합니다. 씬 볼륨이거나 스냅샷 볼륨일 수 없습니다.
* 2차 볼륨의 크기는 운영 볼륨만큼 크지 않아야 합니다.


.이 작업에 대해
동기식 미러링 쌍을 생성하는 프로세스는 여러 단계로 이루어집니다.



== 1단계: 운영 볼륨을 선택합니다

이 단계에서는 동기식 미러 관계에 사용할 운영 볼륨을 선택합니다. 로컬 스토리지 배열에서 운영
```

볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 선택한 볼륨은 미러 관계에서 1차 역할을 보유합니다.

.단계
. Manage * 페이지에서 소스에 사용할 로컬 스토리지 배열을 선택합니다.
. 메뉴 선택: 작업 [동기식 미러링 쌍 생성].
+
동기식 미러링 쌍 생성 마법사가 열립니다.

. 적합한 볼륨 목록에서 미러의 운영 볼륨으로 사용할 볼륨을 선택합니다.
. 다음 * 을 선택하고 로 이동합니다<<2단계: 보조 볼륨을 선택합니다>>.

== 2단계: 보조 볼륨을 선택합니다

이 단계에서는 미러 관계에 사용할 보조 볼륨을 선택합니다. 원격 스토리지 어레이에서 보조 볼륨을 선택하면 해당 미러링된 쌍에 대해 적합한 모든 볼륨 목록이 표시됩니다. 사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 선택한 볼륨은 미러 관계에서 2차 역할을 유지합니다.

.단계
. 로컬 스토리지 시스템과 미러 관계를 설정할 원격 스토리지 시스템을 선택합니다.
+
[NOTE]
====
원격 스토리지 배열이 암호로 보호되어 있는 경우 암호를 입력하라는 메시지가 표시됩니다.

====
+
** 스토리지 배열은 해당 스토리지 배열 이름으로 나열됩니다. 스토리지 배열의 이름을 지정하지 않은 경우 이름이 "UNNAMED(명명되지 않음)"으로 표시됩니다.
** 사용하려는 스토리지 어레이가 목록에 없는 경우 Unified Manager에서 검색된 스토리지인지 확인합니다.

. 적합한 볼륨 목록에서 미러의 2차 볼륨으로 사용할 볼륨을 선택합니다.
+
[NOTE]
====
운영 볼륨보다 큰 용량으로 2차 볼륨을 선택하는 경우 사용 가능한 용량이 운영 볼륨의 크기로 제한됩니다.

====
. 다음 * 을 클릭하고 로 이동합니다<<3단계: 동기화 설정을 선택합니다>>.

== 3단계: 동기화 설정을 선택합니다

이 단계에서는 통신 중단 후 데이터 동기화 방법을 결정하는 설정을 선택합니다. 통신이 중단된 후 기본 볼륨의 컨트롤러 소유자가 데이터를 보조 볼륨과 재동기화하는 우선 순위를 설정할 수 있습니다. 수동 또는 자동 재동기화 정책도 선택해야 합니다.

.단계
. 슬라이더 막대를 사용하여 동기화 우선 순위를 설정합니다.
+
동기화 우선 순위는 서비스 입출력 요청과 비교하여 통신 중단 후 초기 동기화 및 재동기화 작업을 완료하는 데 사용되는 시스템 리소스의 양을 결정합니다.

+
이 대화 상자에 설정된 우선 순위는 운영 볼륨과 2차 볼륨 모두에 적용됩니다. 나중에 System Manager로 이동하여 메뉴에서 스토리지 [동기식 미러링 > 자세히 > 설정 편집]을 선택하여 기본 볼륨의 속도를 수정할 수 있습니다.

+
동기화 우선 순위는 5가지입니다.

+
** 최저
** 낮음
** 중간
** 높음
** 최고
+
동기화 우선 순위가 가장 낮은 속도로 설정된 경우 입출력 작업의 우선 순위가 지정되고 재동기화 작업이 더 오래 걸립니다. 동기화 우선 순위가 가장 높은 속도로 설정된 경우 재동기화 작업의 우선 순위가 지정되지만 스토리지 시스템의 입출력 작업이 영향을 받을 수 있습니다.

. 원격 스토리지 시스템에서 미러링된 쌍을 수동 또는 자동으로 재동기화할지 여부를 선택합니다.
+
** * 수동 * (권장 옵션) -- 미러링된 쌍으로 통신이 복구된 후 수동으로 동기화를 재개하려면 이 옵션을 선택합니다. 이 옵션은 데이터를 복구할 수 있는 최적의 기회를 제공합니다.
** * 자동 * -- 통신이 미러링된 쌍으로 복구된 후 재동기화를 자동으로 시작하려면 이 옵션을 선택합니다.
+
동기화를 수동으로 재개하려면 System Manager로 이동하여 메뉴에서 Storage [Synchronous Mirroring](저장소 [Synchronous Mirroring])을 선택하고 표에서 미러링된 쌍을 강조 표시한 다음 * More *(기타 *) * 에서 * Resume * 을 선택합니다.

. 동기식 미러링 시퀀스를 완료하려면 * Finish * 를 클릭합니다.

.결과
미러링이 활성화되면 시스템은 다음 작업을 수행합니다.

* 로컬 스토리지와 원격 스토리지 시스템 간의 초기 동기화를 시작합니다.
* 동기화 우선 순위 및 재동기화 정책을 설정합니다.
* 미러 데이터 전송을 위해 컨트롤러 HIC에서 가장 높은 번호의 포트를 예약합니다.
+
이 포트에서 수신된 I/O 요청은 미러링된 쌍에 있는 보조 볼륨의 원격 기본 컨트롤러 소유자만이 허용됩니다. (기본 볼륨에 대한 예약이 허용됩니다.)

* 각 컨트롤러에 대해 하나씩, 예약된 용량 볼륨 2개를 생성합니다. 이 볼륨은 컨트롤러 재설정 및 기타 임시 중단으로부터 복구하기 위한 쓰기 정보를 로깅하는 데 사용됩니다.
+
각 볼륨의 용량은 128MiB입니다. 하지만 볼륨이 풀에 배치되면 4GiB가 각 볼륨에 대해 예약됩니다.

.작업을 마친 후
System Manager로 이동하여 Home [View Operations in Progress] 메뉴를 선택하여 동기 미러링 작업의 진행률을 확인합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

:leveloffset: -1

= FAQ 를 참조하십시오

:leveloffset: +1

[[ID1368d58027310a8761abe92db744fd3d]]
= 미러 정합성 보장 그룹을 생성하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

미러 일관성 그룹을 생성하기 전에 다음 지침을 따르십시오.

Unified Manager에 대한 다음 요구사항을 충족합니다.

* 웹 서비스 프록시 서비스가 실행되고 있어야 합니다.
* Unified Manager는 HTTPS 연결을 통해 로컬 호스트에서 실행되고 있어야 합니다.
* Unified Manager에 스토리지 시스템에 대한 유효한 SSL 인증서가 표시되어야 합니다. 자체 서명된 인증서를 수락하거나 Unified Manager를 사용하여 인증서 [인증서 관리] 메뉴로 이동하여 자체 보안 인증서를 설치할 수 있습니다.

또한 스토리지 어레이에 대한 다음 요구 사항도 충족해야 합니다.

* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.
* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 로컬 및 원격 스토리지 어레이는 파이버 채널 패브릭 또는 iSCSI 인터페이스를 통해 연결됩니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

[[IDbf5a4b6b9de36da8448b752b6fb91ca1]]
= 미러링된 쌍을 만들기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
대칭 복사된 쌍을 만들기 전에 다음 지침을 따릅니다.

* 두 개의 스토리지 어레이가 있어야 합니다.
* 각 스토리지 어레이에는 2개의 컨트롤러가 필요합니다.
* Unified Manager에서 2개의 스토리지 어레이가 검색되어야 합니다.
* 기본 어레이와 보조 어레이의 각 컨트롤러에는 이더넷 관리 포트가 구성되어 있어야 하며 네트워크에 연결되어 있어야 합니다.

* 스토리지 어레이의 펌웨어 버전은 최소 7.84입니다. (각 OS 버전은 서로 다를 수 있음)
* 로컬 및 원격 스토리지 배열의 암호를 알아야 합니다.
* 미러링할 운영 볼륨과 같거나 더 큰 보조 볼륨을 생성하려면 원격 스토리지 시스템에 사용 가능한 용량이 충분해야 합니다.
* 비동기 미러링은 FC(파이버 채널) 또는 iSCSI 호스트 포트가 있는 컨트롤러에서 지원되며, 동기식 미러링은 FC 호스트 포트가 있는 컨트롤러에서만 지원됩니다.

[NOTE]
====
EF600 또는 EF300 스토리지 시스템에서는 동기식 미러링을 사용할 수 없습니다.

====

[[ID0cdc702f30cbc173f4c0faf8adf5f1f4]]
= 이 비율을 변경하는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
일반적으로 예약된 용량은 비동기식 미러링 작업을 위한 기본 볼륨의 20%입니다. 일반적으로 이 용량이면 충분합니다.

필요한 용량은 기본 볼륨에 대한 I/O 쓰기의 빈도 및 크기와 스토리지 오브젝트의 복사 서비스 작업을 사용할 기간에 따라 달라집니다. 일반적으로 다음 조건 중 하나 또는 둘 다 존재할 경우 예약된 용량에 더 큰 비율을 선택합니다.

* 특정 스토리지 오브젝트의 복사 서비스 작업 수명이 매우 긴 경우
* 입출력 작업이 많은 경우 기본 볼륨에서 데이터 블록의 비율이 크게 변경될 수 있습니다. 기간별 성능 데이터 또는 기타 운영 체제 유틸리티를 사용하여 기본 볼륨에 대한 일반적인 I/O 작업을 결정할 수 있습니다.

[[ID27a640f72cffa39299f6929c5c6822a7]]
= 예약된 용량이 두 개 이상 표시되는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
풀 또는 볼륨 그룹에 스토리지 객체에 대해 선택한 용량 비율을 충족하는 볼륨이 두 개 이상 있는 경우 여러 후보가 표시됩니다.

복사 서비스 작업을 위해 기본 볼륨에 예약할 물리적 드라이브 공간의 비율을 변경하여 권장되는 후보 목록을 새로 고칠 수 있습니다. 선택한 내용에 따라 가장 적합한 후보가 표시됩니다.

[[ID130e595f6fd78a09bf0167b6ac149505]]
= 내 볼륨이 모두 표시되지 않는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
미러링된 쌍의 기본 볼륨을 선택하면 목록에 모든 적격 볼륨이 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

* 볼륨이 최적이 아닙니다.
* 볼륨이 이미 미러링 관계에 있습니다.
* 동기식 미러링의 경우 미러링된 쌍의 운영 볼륨과 2차 볼륨이 표준 볼륨이어야 합니다. 씬 볼륨 또는 스냅샷 볼륨일 수 없습니다.
* 비동기식 미러링의 경우 씬 볼륨에 자동 확장이 설정되어 있어야 합니다.

NOTE: EF600 및 EF300 컨트롤러의 경우 비동기식 미러링 쌍의 운영 볼륨과 2차 볼륨이 동일한 프로토콜, 트레이 레벨, 세그먼트 크기, 보안 유형 및 RAID 레벨과 일치해야 합니다. 사용 가능한 볼륨 목록에 비적격한 비동기 미러링 쌍이 나타나지 않습니다.

[[ID5eacbf397af349a138eea30708e19bab]]
= 원격 스토리지 어레이에 볼륨이 모두 표시되지 않는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]

원격 스토리지 어레이에서 보조 볼륨을 선택할 경우 목록에 해당 미러링된 쌍에 대해 적합한 볼륨이 모두 표시됩니다.

사용할 수 없는 볼륨은 해당 목록에 표시되지 않습니다. 볼륨은 다음과 같은 이유로 적합하지 않을 수 있습니다.

* 볼륨은 스냅샷 볼륨과 같이 비표준 볼륨입니다.
* 볼륨이 최적이 아닙니다.
* 볼륨이 이미 미러링 관계에 있습니다.
* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨 간의 씬 볼륨 특성이 일치하지 않습니다.
* DA(Data Assurance)를 사용하는 경우 운영 볼륨과 보조 볼륨의 DA 설정이 동일해야 합니다.
+
** 운영 볼륨이 DA를 사용하는 경우 보조 볼륨은 DA를 활성화해야 합니다.
** 운영 볼륨이 DA를 사용하지 않는 경우 보조 볼륨을 DA로 설정하지 않아야 합니다.

* 비동기식 미러링의 경우 운영 볼륨과 2차 볼륨의 드라이브 보안 기능이 동일해야 합니다.
+
** 기본 볼륨이 FIPS를 지원할 수 있는 경우 보조 볼륨은 FIPS를 지원할 수 있어야 합니다.
** 기본 볼륨이 FDE를 지원할 수 있는 경우 보조 볼륨은 FDE를 지원할 수 있어야 합니다.
** 주 볼륨이 드라이브 보안을 사용하지 않는 경우 보조 볼륨이 드라이브 보안을 사용하지 않아야 합니다.

[[ID7f3c6f2b5aefd525cbe3ef63d5440d31]]
= 동기화 우선 순위가 동기화 속도에 어떤 영향을 미칩니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
동기화 우선 순위는 시스템 성능과 관련하여 동기화 작업에 할당되는 처리 시간을 정의합니다.

운영 볼륨의 컨트롤러 소유자가 이 작업을 백그라운드에서 수행합니다. 동시에 컨트롤러 소유자가 운영 볼륨에 대한 로컬 I/O 쓰기 및 보조 볼륨에 대한 관련 원격 쓰기를 처리합니다. 재동기화는 컨트롤러 처리 리소스를 입출력 작업에서 전환하므로 재동기화는 호스트 애플리케이션의 성능에 영향을 미칠 수 있습니다.

동기화 우선 순위가 얼마나 오래 걸릴 수 있고 동기화 우선 순위가 시스템 성능에 어떤 영향을 미칠 수 있는지 결정할 수 있도록 이 지침을 염두에 두십시오.

다음과 같은 우선 순위가 있습니다.

* 최저
* 낮음
* 중간
* 높음
* 최고

우선 순위가 가장 낮은 속도는 시스템 성능을 지원하지만 재동기화에 더 많은 시간이 걸립니다.
우선 순위가 가장 높은 속도가 재동기화를 지원하지만 시스템 성능이 저하될 수 있습니다.

이 지침은 우선 순위 간의 차이를 대략적으로 나타냅니다.

[cols="45h,~"]
|===
| 전체 동기화의 우선 순위 속도 | 최고 동기화 속도에 비해 경과된 시간입니다

a|
최저
a|
최고 우선 순위인 경우 약 8배

a|
낮음
a|
최고 우선 순위인 경우 약 6배

a|
중간
a|
가장 높은 우선 순위에서 약 3배 반 정도 소요됩니다.

a|
높음
a|
최고 우선 순위보다 약 2배 긴 시간.

|===
볼륨 크기 및 호스트 I/O 속도 로드는 동기화 시간 비교에 영향을 줍니다.

[[IDc35e1ee53332afab10554d9be65eb604]]
= 수동 동기화 정책을 사용하는 것이 권장되는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
수동 재동기화는 재동기화 프로세스를 관리하여 데이터를 복구할 수 있는 최적의 기회를 제공하기 때문에 권장됩니다.

자동 재동기화 정책을 사용하고 재동기화 중에 간헐적인 통신 문제가 발생하는 경우 보조 볼륨의 데이터가 일시적으로 손상될 수 있습니다. 재동기화가 완료되면 데이터가 수정됩니다.

:leveloffset: -1

:leveloffset: -1

= 인증서

:leveloffset: +1

[[IDdc8f46c0bf4b743fde0d03cec58479e9]]
= 인증서 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서 관리를 사용하면 CSR(인증서 서명 요청)을 생성하고 인증서를 가져오고 기존 인증서를 관리할 수 있습니다.

== 인증서란 무엇입니까?

_Certificates_는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다. 인증서 유형에는 두 가지가 있습니다. CA(인증 기관)에서 _signed certificate_를 검증하고, 타사 대신 엔터티의 소유자가 _self-signed certificate_를 확인합니다.

자세한 내용:

* xref:{relative_path}how-certificates-work-unified.html["인증서 작동 방식"]
* xref:{relative_path}certificate-terminology-unified.html["인증서 용어"]

== 인증서를 구성하려면 어떻게 합니까?

인증서 관리에서 Unified Manager를 호스팅하는 관리 스테이션에 대한 인증서를 구성하고 스토리지 시스템의 컨트롤러에 대한 인증서를 가져올 수 있습니다.

자세한 내용:

* xref:{relative_path}use-ca-signed-certificate-um.html["관리 시스템에 CA 서명 인증서를 사용합니다"]
* xref:{relative_path}import-array-certificates-unified.html["스토리지에 대한 인증서를 가져옵니다"]

= 개념

:leveloffset: +1

[[ID05027520f444be9b714795dbe535ade0]]
= 인증서 작동 방식

:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다.

== 서명된 인증서

인증서는 웹 통신이 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지 않도록 합니다. Unified Manager를 사용하면 호스트 관리 시스템의 브라우저 인증서와 검색된 스토리지 시스템의 컨트롤러를 관리할 수 있습니다.

인증서는 신뢰할 수 있는 기관에서 서명할 수도 있고 자체 서명할 수도 있습니다. "서명"은 단순히 누군가가 소유자의 신원을 확인하고 자신의 장치를 신뢰할 수 있다는 것을 확인하는 것을 의미합니다. 스토리지 어레이에는 각 컨트롤러에서 자동으로 생성된 자체 서명 인증서가 함께 제공됩니다. 자체 서명된 인증서를 계속 사용하거나 컨트롤러와 호스트 시스템 간의 보다 안전한 연결을 위해 CA 서명 인증서를 얻을 수 있습니다.

[NOTE]
====
CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간의 공격 방지) 대규모 네트워크를 사용하는 경우 비용이 많이 들 수 있습니다. 반면 자체 서명된 인증서는 보안성이 떨어지지만 무료입니다. 따라서 자체 서명된 인증서는 프로덕션 환경이 아닌 내부 테스트 환경에 가장 많이 사용됩니다.

====
서명된 인증서는 신뢰할 수 있는 타사 조직인 CA(인증 기관)에서 유효성을 검사합니다. 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보, 인증서 발급 및 만료 날짜, 엔터티에 대한 유효한 도메인 및 문자와 숫자로 구성된 디지털 서명이 포함됩니다.

브라우저를 열고 웹 주소를 입력하면 시스템은 백그라운드에서 인증서 확인 프로세스를 수행하여 유효한 CA 서명 인증서가 포함된 웹 사이트에 연결 중인지 확인합니다. 일반적으로 서명된 인증서로 보호되는 사이트에는 자물쇠 아이콘과 주소에 https 지정이 포함되어 있습니다. CA 서명 인증서가 없는 웹 사이트에 연결하려고 하면 브라우저에 사이트가 안전하지 않음을 알리는 경고가 표시됩니다.

CA는 응용 프로그램 프로세스 중에 ID를 확인하는 단계를 수행합니다. 등록된 회사에 이메일을 보내고, 회사 주소를 확인하고, HTTP 또는 DNS 확인을 수행할 수 있습니다. 응용 프로그램 프로세스가 완료되면 CA는 호스트 관리 시스템에 로드할 디지털 파일을 보냅니다. 일반적으로 이러한 파일에는 다음과 같은 신뢰 체인이 포함됩니다.

* * 루트 * -- 계층 구조의 맨 위에 루트 인증서가 있으며, 이 인증서에는 다른 인증서에 서명하는 데 사용되는 개인 키가 들어 있습니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
* * 중급 * -- 루트에서 오프하는 것은 중간 인증서입니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
* * 서버 * -- 체인 하단에 있는 서버 인증서는 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 어레이의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

== 자체 서명된 인증서

스토리지 어레이의 각 컨트롤러에는 사전 설치된 자체 서명된 인증서가 포함되어 있습니다. 자체 서명된 인증서는 타사 대신 개체 소유자가 유효성을 검사한다는 점을 제외하면 CA 서명 인증서와 비슷합니다. CA 서명 인증서와 마찬가지로 자체 서명된 인증서에는 자체 개인 키가 포함되어 있으며, 서버와 클라이언트 간의 HTTPS 연결을 통해 데이터가 암호화되고 전송되도록 합니다.

자체 서명된 인증서는 브라우저에서 "신뢰할 수 있는" 인증서가 아닙니다. 자체 서명된 인증서만 포함된 웹 사이트에 연결할 때마다 브라우저에 경고 메시지가 표시됩니다. 웹 사이트로 이동할 수 있는 경고 메시지의 링크를 클릭해야 합니다. 이렇게 하면 자체 서명된 인증서를 기본적으로 수락하게 됩니다.

== Unified Manager용 인증서

Unified Manager 인터페이스는 호스트 시스템의 웹 서비스 프록시와 함께 설치됩니다. 브라우저를 열고 Unified Manager에 연결하려고 하면 브라우저에서 디지털 인증서를 확인하여 호스트가 신뢰할 수 있는 소스인지 확인합니다. 브라우저에서 서버의 CA 서명 인증서를 찾지 못하면 경고 메시지가 열립니다. 이 페이지에서 웹 사이트로 이동하여 해당 세션에 대해 자체 서명된 인증서를 수락할 수 있습니다. 또는 CA로부터 서명된 디지털 인증서를 받을 수 있으므로 경고 메시지가 더 이상 표시되지 않습니다.

== 컨트롤러의 인증서

Unified Manager 세션 중에 CA 서명된 인증서가 없는 컨트롤러에 액세스하려고 하면 추가 보안 메시지가 표시될 수 있습니다. 이 경우 자체 서명된 인증서를 영구적으로 신뢰하거나 컨트롤러의 CA 서명 인증서를 가져올 수 있습니다. 그러면 웹 서비스 프록시 서버에서 이러한 컨트롤러의 들어오는 클라이언트 요청을 인증할 수 있습니다.

[[ID112059e71407de263f67b81de32a888c]]
= 인증서 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
다음 용어는 인증서 관리에 적용됩니다.

[cols="25h,~"]
|===
| 기간 | 설명

a|
CA
a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.

a|
CSR
a|
CSR(인증서 서명 요청)은 신청자가 CA(인증 기관)로 보내는 메시지입니다. CSR은 CA가 인증서를 발급하는 데 필요한 정보를 확인합니다.

a|
인증서
a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.

a|
인증서 체인
a|
인증서에 보안 계층을 추가하는 파일의 계층 구조입니다. 일반적으로 체인은 계층 맨 위에 루트 인증서 하나, 중간 인증서 하나 이상 및 엔터티를 식별하는 서버 인증서를 포함합니다.

a|
중간 인증서
a|
하나 이상의 중간 인증서가 인증서 체인의 루트에서 분기됩니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.

a|
키 저장소
a|

키 저장소는 해당 공개 키 및 인증서와 함께 개인 키가 들어 있는 호스트 관리 시스템의 리포지토리입니다. 이러한 키와 인증서는 컨트롤러와 같은 사용자 고유의 엔터티를 식별합니다.

a|
루트 인증서입니다
a|
루트 인증서는 인증서 체인의 계층 구조 맨 위에 있으며 다른 인증서에 서명하는 데 사용되는 개인 키를 포함합니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.

a|
서명된 인증서
a|
CA(인증 기관)에서 유효성을 검사하는 인증서입니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 또한 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보와 문자와 숫자로 구성된 디지털 서명이 포함됩니다. 서명된 인증서는 신뢰 체인을 사용하므로 프로덕션 환경에서 가장 많이 사용됩니다. "CA 서명 인증서" 또는 "관리 인증서"라고도 합니다.

a|
자체 서명된 인증서
a|
자체 서명된 인증서는 해당 엔터티의 소유자에 의해 유효성이 검사됩니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 문자와 숫자로 구성된 디지털 서명도 포함되어 있습니다. 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않으므로 테스트 환경에서 가장 많이 사용됩니다. "사전 설치된" 인증서라고도 합니다.

a|
서버 인증서
a|
서버 인증서는 인증서 체인의 맨 아래에 있습니다. 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 시스템의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

a|
트러스토어
a|

Truststore는 CA와 같이 신뢰할 수 있는 타사의 인증서가 포함된 저장소입니다.

|===

:leveloffset: -1

[[IDdaf28d32ca39963aa6f7ae251350303d]]
= 관리 시스템에 CA 서명 인증서를 사용합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
SANtricity Unified Manager를 호스팅하는 관리 시스템에 안전하게 액세스하기 위해 CA 서명 인증서를 얻고 가져올 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.이 작업에 대해
CA 서명 인증서를 사용하는 것은 3단계 절차입니다.

== 1단계: CSR 파일을 완료합니다

먼저 웹 서비스 프록시 및 Unified Manager가 설치된 조직 및 호스트 시스템을 식별하는 인증서 서명 요청(CSR) 파일을 생성해야 합니다.

[NOTE]
====
또는 OpenSSL과 같은 도구를 사용하여 CSR 파일을 생성하고 로 건너뛸 수 있습니다<<2단계: CSR 파일을 제출합니다>>.

====
.단계
. 인증서 관리 * 를 선택합니다.
. 관리 탭에서 * CSR 완료 * 를 선택합니다.
. 다음 정보를 입력하고 * 다음 * 을 클릭합니다.
+

** * 조직 * -- 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
** * 조직 단위(선택 사항) * -- 인증서를 처리하는 조직의 사업부입니다.
** * 시/군/구 * -- 호스트 시스템이나 업무가 위치한 도시.
** * 주/지역(선택 사항) * -- 호스트 시스템 또는 비즈니스가 위치한 주 또는 지역입니다.
** * 국가 ISO 코드 * -- 미국 등 해당 국가의 2자리 ISO(International Organization for Standardization) 코드입니다.

. 웹 서비스 프록시가 설치된 호스트 시스템에 대한 다음 정보를 입력합니다.
+
** * 공통 이름 * -- 웹 서비스 프록시가 설치된 호스트 시스템의 IP 주소 또는 DNS 이름입니다. 주소가 올바른지 확인합니다. 입력한 주소와 정확하게 일치해야 브라우저에서 Unified Manager에 액세스할 수 있습니다. http:// 또는 https://.를 포함하지 마십시오 DNS 이름은 와일드카드로 시작할 수 없습니다.
** * 대체 IP 주소 * -- 공통 이름이 IP 주소인 경우 호스트 시스템에 대한 추가 IP 주소 또는 별칭을 선택적으로 입력할 수 있습니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다.
** * 대체 DNS 이름 * -- 공통 이름이 DNS 이름이면 호스트 시스템에 대한 추가 DNS 이름을 입력합니다. 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다. 대체 DNS 이름이 없지만 첫 번째 필드에 DNS 이름을 입력한 경우 여기에 해당 이름을 복사합니다. DNS 이름은 와일드카드로 시작할 수 없습니다.

. 호스트 정보가 올바른지 확인합니다. 그렇지 않으면 CA에서 반환된 인증서를 가져오려고 할 때 실패합니다.
. 마침 * 을 클릭합니다.
. 로 이동합니다. <<2단계: CSR 파일을 제출합니다>>

== 2단계: CSR 파일을 제출합니다

CSR(인증서 서명 요청) 파일을 생성한 후 CA(인증 기관)로 보내 Unified Manager 및 웹 서비스 프록시를 호스팅하는 시스템에 대한 서명된 관리 인증서를 받습니다.

NOTE: E-Series 시스템에는 .pem, .crt, .cer 또는 .key 파일 형식을 포함하는 서명된 인증서에 대한 PEM 형식(Base64 ASCII 인코딩)이 필요합니다.

.단계
. 다운로드한 CSR 파일을 찾습니다.
+
다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

. CSR 파일을 CA(예: VeriSign 또는 DigiCert)에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.

+
[CAUTION]
====
* CSR 파일을 CA에 제출한 후에는 다른 CSR 파일을 다시 생성하지 마십시오. * CSR을 생성할 때마다 시스템은 개인 키 및 공개 키 쌍을 생성합니다. 공개 키는 CSR의 일부이며 개인 키는 시스템의 키 저장소에 보관됩니다. 서명된 인증서를 받아서 가져오면 시스템에서 개인 키와 공개 키가 모두 원래 쌍이 되도록 합니다. 키가 일치하지 않으면 서명된 인증서가 작동하지 않으므로 CA에서 새 인증서를 요청해야 합니다.

====
. CA가 서명된 인증서를 반환하면 로 이동합니다<<3단계: 관리 인증서를 가져옵니다>>.

== 3단계: 관리 인증서를 가져옵니다

CA(인증 기관)에서 서명된 인증서를 받은 후 웹 서비스 프록시 및 Unified Manager 인터페이스가 설치된 호스트 시스템으로 인증서를 가져옵니다.

.시작하기 전에
* CA로부터 서명된 인증서를 받았습니다. 이러한 파일에는 루트 인증서, 하나 이상의 중간 인증서 및 서버 인증서가 포함됩니다.
* CA가 체인 인증서 파일(예: .p7b 파일)을 제공한 경우, 루트 인증서, 하나 이상의 중간 인증서 및 서버 인증서 등 개별 파일에 체인 파일의 압축을 풀어야 합니다. Windows 유틸리티를 사용하여 파일의 압축을 풀 수 `certmgr` 있습니다(마우스 오른쪽 버튼을 클릭하고 메뉴: 모든 작업 [내보내기] 선택). base-64 인코딩이 권장됩니다. 내보내기가 완료되면 체인의 각 인증서 파일에 대해 CER 파일이 표시됩니다.
* 웹 서비스 프록시가 실행되고 있는 호스트 시스템에 인증서 파일을 복사했습니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 관리 탭에서 * 가져오기 * 를 선택합니다.
+
인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

. 찾아보기 * 를 클릭하여 먼저 루트 및 중간 인증서 파일을 선택한 다음 서버 인증서를 선택합니다. 외부 도구에서 CSR을 생성한 경우 CSR과 함께 생성된 개인 키 파일도 가져와야 합니다.
+
대화 상자에 파일 이름이 표시됩니다.

. 가져오기 * 를 클릭합니다.

.결과

파일이 업로드되고 검증됩니다. 인증서 정보가 인증서 관리 페이지에 표시됩니다.

[[IDd314e653f15d10fbdab9b02bb8ee0d1f]]
= 관리 인증서를 재설정합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리 인증서를 공장 자체 서명된 원래 상태로 되돌릴 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업은 Web Services Proxy 및 Unified Manager가 설치된 호스트 시스템에서 현재 관리 인증서를 삭제합니다. 인증서가 재설정되면 호스트 시스템은 자체 서명된 인증서를 사용하여 되돌아갑니다.

.단계
. 설정 > 인증서 * 를 선택합니다.
. Array Management * 탭을 선택한 다음 * Reset * 을 선택합니다.
+
관리 인증서 재설정 확인 대화 상자가 열립니다.

. 필드에 입력한 `reset` 다음 * 재설정 * 을 클릭합니다.
+
브라우저가 새로 고쳐지면 브라우저가 대상 사이트에 대한 액세스를 차단하고 사이트가 HTTP Strict Transport Security를 사용하고 있다고 보고할 수 있습니다. 이 조건은 자체 서명된 인증서로 다시 전환하면 발생합니다. 대상에 대한 액세스를 차단하는 조건을 지우려면 브라우저에서 탐색 데이터를 지워야 합니다.

.결과
시스템에서 서버에서 자체 서명된 인증서를 사용하도록 되돌립니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.

= 스토리지 인증서를 사용합니다

```
:leveloffset: +1


[[ID369a66a3e019960739fb1bcc033ffac3]]
= 스토리지에 대한 인증서를 가져옵니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
필요한 경우 스토리지 시스템에 대한 인증서를 가져와 SANtricity Unified Manager를
호스팅하는 시스템에서 인증할 수 있습니다. 인증서는 CA(인증 기관)에서 서명할 수도 있고 자체
서명할 수도 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이
나타나지 않습니다.
* 신뢰할 수 있는 인증서를 가져오는 경우 System Manager를 사용하여 스토리지 배열
컨트롤러에 대한 인증서를 가져와야 합니다.


.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열
인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
+
보기를 제한하려면 * Show certificates that are... * filtering 필드를 사용하거나 열
머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.
+
인증서가 업로드 및 검증됩니다.




[[IDf94e42cfa1bcbf50446dc9d3c183b460]]
= 신뢰할 수 있는 인증서를 삭제합니다
:allow-uri-read:
```

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
만료된 인증서와 같이 더 이상 필요하지 않은 인증서를 하나 이상 삭제할 수 있습니다.

.시작하기 전에
기존 인증서를 삭제하기 전에 새 인증서를 가져옵니다.

[CAUTION]
====
루트 또는 중간 인증서를 삭제하면 여러 스토리지 시스템이 동일한 인증서 파일을 공유할 수 있으므로 여러 스토리지 시스템에 영향을 줄 수 있습니다.

====
.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
. 테이블에서 하나 이상의 인증서를 선택한 다음 * 삭제 * 를 클릭합니다.
+
[NOTE]
====
사전 설치된 인증서에는 * 삭제 * 기능을 사용할 수 없습니다.

====
+
신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

. 삭제를 확인한 다음 * 삭제 * 를 클릭합니다.
+
인증서가 테이블에서 제거됩니다.




[[IDf13dc6870cbed91424beaf5a26bc0f0a]]
= 신뢰할 수 없는 인증서를 확인합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
신뢰할 수 없는 인증서는 스토리지 어레이에서 SANtricity Unified Manager에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다.

인증서 페이지에서는 스토리지 배열에서 자체 서명된 인증서를 가져오거나 신뢰할 수 있는 타사에서 발급한 CA(인증 기관) 인증서를 가져와 신뢰할 수 없는 인증서를 확인할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다.
* CA 서명 인증서를 가져올 계획인 경우:
+
** 스토리지 배열의 각 컨트롤러에 대한 인증서 서명 요청(.csr 파일)을 생성하여 CA로 보냈습니다.
** CA가 신뢰할 수 있는 인증서 파일을 반환했습니다.
** 인증서 파일은 로컬 시스템에서 사용할 수 있습니다.

.이 작업에 대해
다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

* 최근에 스토리지 배열을 추가했습니다.
* 하나 이상의 인증서가 만료되었습니다.
* 하나 이상의 인증서가 해지되었습니다.
* 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 신뢰할 수 있는 * 탭을 선택합니다.
+
이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
+
보기를 제한하려면 * Show certificates that are... * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.

. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.
+
인증서가 업로드 및 검증됩니다.

```
:leveloffset: -1


= 인증서를 관리합니다

:leveloffset: +1


[[ID4358bf0aac93f2ca03e19046e8092b81]]
= 인증서를 봅니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증서를 사용하는 조직, 인증서를 발급한 기관, 유효 기간 및 지문(고유 식별자)을 포함하는 인증서의 요약 정보를 볼 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 다음 탭 중 하나를 선택합니다.
+
** * 관리 * -- 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
** * 신뢰 * -- Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.


. 인증서에 대한 자세한 내용을 보려면 해당 행을 선택하고 행 끝에 있는 줄임표를 선택한 다음 * 보기 * 또는 * 내보내기 * 를 클릭합니다.




[[IDb3f2623996844df931e29f82a7aec24f]]
= 인증서를 내보냅니다
:allow-uri-read:
:icons: font
```

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증서를 내보내 전체 세부 정보를 볼 수 있습니다.

.시작하기 전에
내보낸 파일을 열려면 인증서 뷰어 응용 프로그램이 있어야 합니다.

.단계
. 인증서 관리 * 를 선택합니다.
. 다음 탭 중 하나를 선택합니다.
+
** * 관리 * -- 웹 서비스 프록시를 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. Unified Manager에 안전하게 액세스할 수 있습니다.
** * 신뢰 * -- Unified Manager가 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.


. 페이지에서 인증서를 선택한 다음 행 끝에 있는 줄임표를 클릭합니다.
. 내보내기 * 를 클릭한 다음 인증서 파일을 저장합니다.
. 인증서 뷰어 응용 프로그램에서 파일을 엽니다.




:leveloffset: -1


:leveloffset: -1


= 액세스 관리

:leveloffset: +1


[[ID72d8df5c0a12ee71d1ef8cf92cb33dd7]]
= 액세스 관리 개요
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
액세스 관리는 SANtricity Unified Manager에서 사용자 인증을 구성하는 방법입니다.

== 어떤 인증 방법을 사용할 수 있습니까?

다음과 같은 인증 방법을 사용할 수 있습니다.

* * 로컬 사용자 역할 * -- 인증은 RBAC(역할 기반 액세스 제어) 기능을 통해 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다.
* * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다.
* * SAML * -- 인증은 SAML 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다.

자세한 내용:

* xref:{relative_path}how-access-management-works-unified.html["액세스 관리 작동 방식"]
* xref:{relative_path}access-management-terminology-unified.html["Access Management(액세스 관리) 용어"]
* xref:{relative_path}permissions-for-mapped-roles-unified.html["매핑된 역할에 대한 권한"]
* xref:{relative_path}access-management-with-saml.html["SAML"]

== 액세스 관리를 구성하려면 어떻게 합니까?

SANtricity 소프트웨어는 로컬 사용자 역할을 사용하도록 사전 구성되어 있습니다. LDAP를 사용하려면 액세스 관리 페이지에서 LDAP를 구성할 수 있습니다.

자세한 내용:

* xref:{relative_path}access-management-with-local-user-roles-unified.html["로컬 사용자 역할을 사용하여 액세스 관리"]
* xref:{relative_path}access-management-with-directory-services-unified.html["디렉토리 서비스를 통한 액세스 관리"]
* xref:{relative_path}configure-saml.html["SAML를 구성합니다"]

= 개념

```
:leveloffset: +1


[[IDb2c85df4e21ac154b9db81224d1f03de]]
= 액세스 관리 작동 방식
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
액세스 관리를 사용하여 SANtricity Unified Manager에서 사용자 인증을 설정합니다.



== 구성 워크플로우

Access Management 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에
로그인합니다.
+
[NOTE]
====
처음 로그인하는 경우 사용자 이름이 `admin` 자동으로 표시되며 변경할 수 없습니다.
`admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다. 암호는 처음 로그인할 때 설정해야
합니다.

====
. 관리자는 미리 구성된 로컬 사용자 역할이 포함된 사용자 인터페이스에서 Access
Management로 이동합니다. 이러한 역할은 RBAC(역할 기반 액세스 제어) 기능 구현입니다.
. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
+
** * 로컬 사용자 역할 * -- 인증은 RBAC 기능을 통해 관리됩니다. 로컬 사용자 역할에는 특정
액세스 권한을 가진 사전 정의된 사용자 및 역할이 포함됩니다. 관리자는 이러한 로컬 사용자
역할을 단일 인증 방법으로 사용하거나 디렉터리 서비스와 함께 사용할 수 있습니다. 사용자 암호
설정 이외의 구성은 필요하지 않습니다.
** * 디렉터리 서비스 * -- 인증은 LDAP(Lightweight Directory Access Protocol)
서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다.
관리자가 LDAP 서버에 연결한 다음 LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
** * SAML * -- 인증은 SAML(Security Assertion Markup Language) 2.0을 사용하여
ID 공급자(IDP)를 통해 관리됩니다. 관리자는 IdP 시스템과 스토리지 어레이 간의 통신을 설정한
다음 IdP 사용자를 스토리지 어레이에 포함된 로컬 사용자 역할에 매핑합니다.
```

. 관리자는 Unified Manager에 대한 로그인 자격 증명을 제공합니다.
. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다. 로그인 중에 시스템은 다음과 같은 백그라운드 작업을 수행합니다.
+
** 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
** 할당된 역할에 따라 사용자의 권한을 결정합니다.
** 사용자에게 사용자 인터페이스의 기능에 대한 액세스 권한을 제공합니다.
** 상단 배너에 사용자 이름을 표시합니다.

== 기능은 Unified Manager에서 사용할 수 있습니다

기능에 대한 액세스는 사용자가 할당한 역할에 따라 달라집니다. 여기에는 다음이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용할 수 없는 기능은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.

[[IDc00c2704c59f0c288e6ca2f809a53868]]
= Access Management(액세스 관리) 용어
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리 용어가 SANtricity Unified Manager에 어떻게 적용되는지 알아보십시오.

[cols="25h,~"]
|===
| 기간 | 설명

a|
Active Directory를 클릭합니다
a|
AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.

a|
바인딩
a|
바인딩 작업은 클라이언트를 디렉토리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명이 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.

a|
CA
a|
CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.

a|
인증서
a|
인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.

a|
LDAP를 지원합니다
a|
LDAP(Lightweight Directory Access Protocol)는 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하면 다양한 응용 프로그램 및 서비스를 LDAP 서버에 연결하여 사용자의 유효성을 검사할 수 있습니다.

a|
RBAC
a|
역할 기반 액세스 제어(RBAC)는 개별 사용자의 역할에 따라 컴퓨터 또는 네트워크 리소스에 대한

액세스를 제어하는 방법입니다. Unified Manager에는 사전 정의된 역할이 포함되어 있습니다.

 a|
SAML
 a|
SAML(Security Assertion Markup Language)은 두 개체 간의 인증 및 승인을 위한 XML 기반 표준입니다. SAML을 사용하면 다중 요소 인증을 수행할 수 있습니다. 사용자는 ID를 입증하기 위해 두 개 이상의 항목(예: 암호 및 지문)을 제공해야 합니다. 스토리지의 내장된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.

 a|
SSO
 a|
SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

 a|
웹 서비스 프록시
 a|
표준 HTTPS 메커니즘을 통해 액세스를 제공하는 웹 서비스 프록시를 사용하면 관리자가 스토리지 시스템에 대한 관리 서비스를 구성할 수 있습니다. 프록시는 Windows 또는 Linux 호스트에 설치할 수 있습니다. Unified Manager 인터페이스는 웹 서비스 프록시에서 사용할 수 있습니다.

|===

[[ID186994e663f7772a5d8bc9ed46ebfc50]]
= 매핑된 역할에 대한 권한
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자가 포함됩니다. 각 역할에는 SANtricity Unified Manager의 작업에 액세스할 수 있는 권한이 포함되어 있습니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용자에게 특정 기능에 대한 권한이 없는 경우 해당 기능을 선택할 수 없거나 사용자 인터페이스에 표시되지 않습니다.

[[IDd441aae8e26aa31ff0b6a8923e424fd5]]
= 로컬 사용자 역할을 사용하여 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리자는 SANtricity Unified Manager에서 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.

== 구성 워크플로우

로컬 사용자 역할은 시스템에서 사전 구성됩니다. 로컬 사용자 역할을 인증에 사용하려면 관리자가 다음을 수행할 수 있습니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 사용자 프로파일을 검토합니다. 사용자 프로필은 미리 정의되어 있으며 수정할 수 없습니다.
. 필요에 따라 관리자는 각 사용자 프로필에 대해 새 암호를 할당합니다.
. 사용자는 할당된 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증에 로컬 사용자 역할만 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 암호를 변경합니다.
* 암호의 최소 길이를 설정합니다.
* 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

[[ID25e2035096a1115db31658b603ac05e2]]
= 디렉토리 서비스를 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉터리 서비스를 사용할 수 있습니다.

== 구성 워크플로우

네트워크에서 LDAP 서버 및 디렉토리 서비스를 사용하는 경우 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 LDAP 서버에 대한 구성 설정을 입력합니다. 설정에는 도메인 이름, URL 및 바인딩 계정 정보가 포함됩니다.
. LDAP 서버가 보안 프로토콜(LDAPS)을 사용하는 경우 관리자는 LDAP 서버와 웹 서비스 프록시가 설치된 호스트 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
. 서버 연결이 설정되면 관리자는 사용자 그룹을 로컬 사용자 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
. 관리자는 LDAP 서버와 웹 서비스 프록시 간의 연결을 테스트합니다.

. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 디렉터리 서비스를 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 디렉토리 서버를 추가합니다.
* 디렉토리 서버 설정을 편집합니다.
* LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
* 디렉토리 서버를 제거합니다.
* 암호를 변경합니다.
* 암호의 최소 길이를 설정합니다.
* 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

[[IDe0515a6c15ce607a05c17b306d78052a]]
= SAML을 통한 액세스 관리
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management의 경우 관리자는 스토리지에 포함된 SAML(Security Assertion Markup Language) 2.0 기능을 사용할 수 있습니다.

== 구성 워크플로우

SAML 구성은 다음과 같이 작동합니다.

. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 로그인합니다.
+
[NOTE]
====
 `admin`사용자는 System Manager의 모든 기능에 액세스할 수 있습니다.

====
. 관리자는 액세스 관리 아래의 * SAML * 탭으로 이동합니다.

. 관리자는 ID 공급자(IDP)와의 통신을 구성합니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 스토리지 시스템과의 통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 Unified Manager를 사용하여 파일을 스토리지 어레이에 업로드합니다.
. 관리자는 서비스 공급자와 IDP 간의 신뢰 관계를 설정합니다. 서비스 공급자는 사용자 인증을 제어합니다. 이 경우 스토리지 배열의 컨트롤러는 서비스 공급자 역할을 합니다. 관리자는 Unified Manager를 사용하여 컨트롤러의 서비스 공급자 메타데이터 파일을 내보내어 통신을 구성합니다. 그런 다음 관리자는 IDP 시스템에서 메타데이터 파일을 IDP로 가져옵니다.
+
[NOTE]
====
또한 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하는지 확인해야 합니다.

====
. 관리자는 스토리지 어레이의 역할을 IDP에 정의된 사용자 속성에 매핑합니다. 이를 위해 관리자는 Unified Manager를 사용하여 매핑을 생성합니다.
. 관리자는 IDP URL에 대한 SSO 로그인을 테스트합니다. 이 테스트는 스토리지 배열 및 IDP가 통신할 수 있도록 보장합니다.
+
[CAUTION]
====
SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
. Unified Manager에서 관리자는 스토리지 어레이에 대해 SAML을 활성화합니다.
. 사용자는 SSO 자격 증명을 사용하여 시스템에 로그인합니다.

== 관리

인증을 위해 SAML을 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

* 새 역할 매핑을 수정하거나 작성합니다
* 서비스 공급자 파일을 내보냅니다

== 액세스 제한

SAML이 활성화된 경우 사용자는 기존 Storage Manager 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

또한 다음 클라이언트는 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

* 엔터프라이즈 관리 창(EMW)
* CLI(Command-Line Interface)
* SDK(소프트웨어 개발자 키트) 클라이언트
* 대역내 클라이언트
* HTTP 기본 인증 REST API 클라이언트
* 표준 REST API 끝점을 사용하여 로그인합니다

:leveloffset: -1

= 로컬 사용자 역할을 사용합니다

:leveloffset: +1

[[IDfeac353f17e1ab4aab296e7e3501ba36]]
= 로컬 사용자 역할을 봅니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
로컬 사용자 역할 탭에서 기본 역할에 대한 사용자 매핑을 볼 수 있습니다. 이러한 매핑은 SANtricity Unified Manager용 웹 서비스 프록시에 적용된 RBAC(역할 기반 액세스 제어)의 일부입니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.이 작업에 대해
사용자 및 매핑을 변경할 수 없습니다. 암호만 수정할 수 있습니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
+
사용자는 다음 표에 나와 있습니다.

+

** * admin * -- 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자는 모든 역할을 포함합니다.
** * 스토리지 * -- 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자에게는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다.
** * 보안 * -- 액세스 관리 및 인증서 관리를 포함한 보안 구성을 담당하는 사용자입니다. 이 사용자는 보안 관리자 및 모니터 역할을 포함합니다.
** * 지원 * -- 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자에게는 지원 관리자 및 모니터 역할이 포함됩니다.
** * monitor * -- 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자는 Monitor 역할만 포함합니다.
** * rw * (읽기/쓰기) -- 이 사용자는 스토리지 관리자, 지원 관리자 및 모니터 역할을 포함합니다.
** * ro * (읽기 전용) -- 이 사용자는 Monitor 역할만 포함합니다.

[[IDc4164811419835346c46670a9eb2f2f4]]
= 로컬 사용자 프로필에 대한 암호를 변경합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management에서 각 사용자의 사용자 암호를 변경할 수 있습니다.

.시작하기 전에
* 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
* 로컬 관리자 암호를 알아야 합니다.

.이 작업에 대해
암호를 선택할 때는 다음 지침을 염두에 두십시오.

* 새 로컬 사용자 암호는 최소 암호(보기/편집 설정)에 대한 현재 설정을 충족하거나 초과해야 합니다.
* 암호는 대/소문자를 구분합니다.
* 후행 공백은 암호가 설정되어 있을 때 암호에서 제거되지 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
* 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.

.단계

. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 테이블에서 사용자를 선택합니다.
+
암호 변경 단추를 사용할 수 있게 됩니다.

. 암호 변경 * 을 선택합니다.
+
암호 변경 대화 상자가 열립니다.

. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 사용자가 시스템에 액세스하기 위해 암호를 입력하도록 확인란을 선택할 수 있습니다.
. 두 필드에 선택한 사용자의 새 암호를 입력합니다.
. 이 작업을 확인하려면 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

.결과
사용자가 현재 로그인한 경우 암호 변경으로 인해 사용자의 활성 세션이 종료됩니다.

[[ID6e178355f9f8f17f8d9cdf53791c8ae5]]
= 로컬 사용자 암호 설정을 변경합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
모든 신규 또는 업데이트된 로컬 사용자 암호에 필요한 최소 길이를 설정할 수 있습니다. 또한 로컬 사용자가 암호를 입력하지 않고 시스템에 액세스하도록 허용할 수 있습니다.

.시작하기 전에
루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.

.이 작업에 대해
로컬 사용자 암호의 최소 길이를 설정할 때는 다음 지침을 염두에 두십시오.

* 설정을 변경해도 기존 로컬 사용자 암호에는 영향을 주지 않습니다.
* 로컬 사용자 암호에 필요한 최소 길이 설정은 0자에서 30자 사이여야 합니다.
* 새 로컬 사용자 암호는 현재 최소 길이 설정을 충족하거나 초과해야 합니다.
* 로컬 사용자가 암호를 입력하지 않고 시스템에 액세스하도록 하려면 암호의 최소 길이를 설정하지 마십시오.

.단계

. 액세스 관리 * 를 선택합니다.
. 로컬 사용자 역할 * 탭을 선택합니다.
. 설정 보기/편집 * 을 선택합니다.
+
로컬 사용자 암호 설정 대화 상자가 열립니다.

. 다음 중 하나를 수행합니다.
+
** 로컬 사용자가 암호를 입력하지 않고 _시스템에 액세스할 수 있도록 하려면 "모든 로컬 사용자 암호를 최소한 입력해야 함" 확인란의 선택을 취소합니다.
** 모든 로컬 사용자 암호에 대해 최소 암호 길이를 설정하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란을 선택한 다음 spinner 상자를 사용하여 모든 로컬 사용자 암호에 필요한 최소 길이를 설정합니다.
+
새 로컬 사용자 암호는 현재 설정을 충족하거나 초과해야 합니다.

. 저장 * 을 클릭합니다.

:leveloffset: -1

= 디렉토리 서비스를 사용합니다

:leveloffset: +1

[[IDbec6f1c3869acd5eaff10727cdec441a]]
= 디렉토리 서버를 추가합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
액세스 관리에 대한 인증을 구성하려면 SANtricity Unified Manager용 웹 서비스 프록시를 실행하는 호스트와 LDAP 서버 간의 통신을 설정해야 합니다. 그런 다음 LDAP 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

.이 작업에 대해
디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관이 서명한 경우 인증을 위해 CA 인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명이 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 다음으로 LDAP 서버의 사용자 그룹을 로컬 사용자 역할에 매핑합니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 디렉터리 서비스 * 탭에서 * 디렉터리 서버 추가 * 를 선택합니다.
+
디렉토리 서버 추가 대화 상자가 열립니다.

. 서버 설정 * 탭에서 LDAP 서버의 자격 증명을 입력합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 구성 설정 *

 a|
도메인
 a|
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.

 a|
서버 URL입니다
 a|

LDAP 서버에 액세스하기 위한 URL을 의 형식으로 `ldap[s]://*host*:*port*` 입력합니다.

a|
인증서 업로드(선택 사항)
a|

NOTE: 이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.

찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.

a|
BIND ACCOUNT(선택 사항)
a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어, 바인딩 사용자를 "bindacct"라고 하는 경우와 같은 값을 입력할 수 `CN=bindacct,CN=Users,DC=cpoc,DC=local` 있습니다.

a|
바인딩 암호(선택 사항)
a|

NOTE: 이 필드는 바인딩 계정을 입력할 때 나타납니다.

바인딩 계정의 암호를 입력합니다.

a|
추가하기 전에 서버 연결을 테스트합니다
a|
시스템이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다.

이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.

a|
* 권한 설정 *

a|
검색 기준 DN
a|
사용자를 검색할 LDAP 컨텍스트를 입력합니다(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`).

a|
사용자 이름 특성입니다
a|
인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들면 다음과 `sAMAccountName`같습니다.

a|
그룹 속성
a|
그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들면 다음과 `memberOf, managedObjects`같습니다.

|===
====
. 역할 매핑 * 탭을 클릭합니다.
. 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 매핑 *

a|
그룹 DN
a|
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다. 정규식이 지원됩니다. 이러한 특수

정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다. \. [] {}() <>*+-=!?^$|

 a|
역할
 a|
필드를 클릭하고 그룹 DN에 매핑할 로컬 사용자 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor 역할이 다른 역할과 함께 필요합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====
+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 매핑을 마쳤으면 * 추가 * 를 클릭합니다.
+
시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

[[IDb08a1d98226363bfe8a539d828d164f8]]
= 디렉토리 서버 설정 및 역할 매핑을 편집합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 Access Management에서 디렉터리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수

있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 디렉토리 서버를 정의해야 합니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 디렉터리 서비스 * 탭을 선택합니다.
. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
. 설정 보기/편집 * 을 선택합니다.
+
Directory Server Settings(디렉터리 서버 설정) 대화 상자가 열립니다.

. 서버 설정 * 탭에서 원하는 설정을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

a|
* 구성 설정 *

a|
도메인
a|
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(_username_@_domain_)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.

a|
서버 URL입니다
a|
의 형식으로 LDAP 서버에 액세스하기 위한 URL `ldap[s]://host:port`입니다.

a|
BIND ACCOUNT(선택 사항)
a|
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.

a|
바인딩 암호(선택 사항)
a|
바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)

a|
저장하기 전에 서버 연결을 테스트합니다
a|
시스템이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 테스트는 * 저장 * 을 클릭한 후에 수행됩니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 테스트를 건너뛰고 구성을 다시 편집하려면 오류를 해결하거나 확인란을 선택 해제해야 합니다.

a|
* 권한 설정 *

a|
검색 기준 DN
a|
사용자를 검색하는 LDAP 컨텍스트(일반적으로 의 형식 `CN=Users, DC=cpoc, DC=local`)

a|
사용자 이름 특성입니다
a|
인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들면 다음과 `sAMAccountName`같습니다.

a|
그룹 속성
a|
그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들면 다음과

`memberOf, managedObjects`같습니다.

|===
====
. 역할 매핑 * 탭에서 원하는 매핑을 변경합니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 매핑 *

 a|
그룹 DN
 a|
매핑할 LDAP 사용자 그룹의 도메인 이름입니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 정규식 패턴의 일부가 아닌 경우 백슬래시(\)로 이스케이프되어야 합니다.

\.[]{}() <> * +-=!?^$|

 a|
역할
 a|
그룹 DN에 매핑할 역할입니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. SANtricity Unified Manager에 로그인하려면 Monitor 역할이 다른 역할과 함께 필요합니다. 역할은 다음과 같습니다.

** * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

|===
====

+

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.

.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

[[IDa0e4370f0011dbc2d91b39420ceccf90]]
= 디렉토리 서버를 제거합니다
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
디렉터리 서버와 웹 서비스 프록시 간의 연결을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

.시작하기 전에
보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

.이 작업에 대해
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

.단계
. 액세스 관리 * 를 선택합니다.
. 디렉터리 서비스 * 탭을 선택합니다.
. 목록에서 삭제할 디렉토리 서버를 선택합니다.
. 제거 * 를 클릭합니다.
+
디렉터리 서버 제거 대화 상자가 열립니다.

. 필드에 입력한 `remove` 다음 * 제거 * 를 클릭합니다.
+
디렉토리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.

```
:leveloffset: -1


= SAML을 사용합니다

:leveloffset: +1


[[ID739d613a03de21b9555f200219a11134]]
= SAML를 구성합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
액세스 관리에 대한 인증을 구성하려면 스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용할 수 있습니다. 이 구성은 ID 공급자와 스토리지 공급자 간의 연결을 설정합니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* 스토리지 배열에 있는 컨트롤러의 IP 주소 또는 도메인 이름을 알아야 합니다.
* IDP 관리자가 IDP 시스템을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클록이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 Unified Manager 액세스에 사용되는 로컬 시스템에서 제공됩니다.


.이 작업에 대해
IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다. 서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다. IDP와 스토리지 어레이 간의 연결을 설정하려면 이 두 엔터티 간에 메타데이터 파일을 공유합니다. 다음으로 IDP 사용자 엔터티를 스토리지 어레이 역할에 매핑합니다. 마지막으로 SAML을 활성화하기 전에 연결 및 SSO 로그인을 테스트합니다.
```

[NOTE]
====
* SAML 및 디렉토리 서비스 *. 디렉터리 서비스가 인증 방법으로 구성되어 있을 때 SAML을 설정하면 SAML이 Unified Manager의 디렉터리 서비스를 대체합니다. 나중에 SAML을 사용하지 않도록 설정하면 Directory Services 구성이 이전 구성으로 돌아갑니다.

====
[CAUTION]
====
* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
SAML 인증 구성은 다단계 절차입니다.

== 1단계: IDP 메타데이터 파일을 업로드합니다

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 Unified Manager로 가져옵니다. IDP 시스템은 인증 요청을 올바른 URL로 리디렉션하고 받은 응답을 검증하려면 이 메타데이터가 필요합니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
+
구성 단계의 개요가 페이지에 표시됩니다.

. IdP(ID 공급자 가져오기) 파일 * 링크를 클릭합니다.
+
ID 공급자 파일 가져오기 대화 상자가 열립니다.

. 로컬 시스템에 복사한 IDP 메타데이터 파일을 선택하여 업로드하려면 * 찾아보기 * 를 클릭합니다.
+
파일을 선택하면 IDP 엔티티 ID가 표시됩니다.

. 가져오기 * 를 클릭합니다.

== 2단계: 서비스 제공업체 파일 내보내기

IDP와 스토리지 어레이 간의 신뢰 관계를 설정하려면 서비스 공급자 메타데이터를 IDP로

가져옵니다. IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 서비스 공급자와 통신할 수 있도록 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. Export Service Provider files *(서비스 제공자 파일 내보내기 *) 링크를 클릭합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 컨트롤러 A * 필드에 컨트롤러 IP 주소 또는 DNS 이름을 입력한 다음 * 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.
+
내보내기 * 를 클릭하면 서비스 공급자 메타데이터가 로컬 시스템에 다운로드됩니다. 파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 XML 형식의 서비스 공급자 메타데이터 파일을 찾습니다.
. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져와 트러스트 관계를 설정합니다. 파일을 직접 가져오거나 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.

== 3단계: 역할 매핑

사용자에게 Unified Manager에 대한 권한 부여 및 액세스 권한을 제공하려면 IDP 사용자 특성 및 그룹 멤버쉽을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

.시작하기 전에
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.

.단계
. Unified Manager * 역할 매핑 링크를 클릭합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

```
 a|
* 매핑 *



 a|
사용자 속성
 a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.



 a|
속성 값
 a|
매핑할 그룹의 속성 값을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는
(`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다



 a|
역할
 a|
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 포함할 각 역할을
개별적으로 선택해야 합니다. Monitor 역할은 Unified Manager에 로그인하기 위한 다른
역할과 함께 필요합니다. 하나 이상의 그룹에 보안 관리자 역할도 필요합니다.

매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기
액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스
(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및
컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이
없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한
액세스는 없습니다.


|===
====
+
[NOTE]
====
```

Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.

====
. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
+
[NOTE]
====
역할 매핑은 SAML이 활성화된 후에 수정할 수 있습니다.

====
. 매핑을 마치면 * 저장 * 을 클릭합니다.

== 4단계: SSO 로그인을 테스트합니다

IDP 시스템 및 스토리지 어레이가 통신할 수 있도록 SSO 로그인을 선택적으로 테스트할 수 있습니다. 이 테스트는 SAML을 활성화하기 위한 마지막 단계에서도 수행됩니다.

.시작하기 전에
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.

.단계
. Test SSO Login * 링크를 선택합니다.
+
SSO 자격 증명을 입력하기 위한 대화 상자가 열립니다.

. 보안 관리자 권한과 모니터 권한이 모두 있는 사용자의 로그인 자격 증명을 입력합니다.
+
시스템에서 로그인을 테스트하는 동안 대화 상자가 열립니다.

. 테스트 성공 메시지를 찾습니다. 테스트가 성공적으로 완료되면 SAML 활성화를 위한 다음 단계로 이동합니다.
+
테스트가 성공적으로 완료되지 않으면 추가 정보와 함께 오류 메시지가 나타납니다. 다음을 확인합니다.

+
** 사용자는 보안 관리자 및 모니터 권한이 있는 그룹에 속합니다.
** IDP 서버에 대해 업로드한 메타데이터가 정확합니다.
** SP 메타데이터 파일의 컨트롤러 주소가 올바릅니다.

== 5단계: SAML을 활성화합니다

마지막 단계는 사용자 인증을 위해 SAML 구성을 완료하는 것입니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.

.시작하기 전에
* IDP 메타데이터 파일을 Unified Manager로 가져옵니다.
* 컨트롤러의 서비스 공급자 메타데이터 파일은 신뢰 관계를 위해 IDP 시스템으로 가져옵니다.
* 하나 이상의 Monitor 및 Security Admin 역할 매핑이 구성되어 있습니다.

[CAUTION]
====
* 편집 및 사용 안 함. * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

====
.단계
. SAML * 탭에서 * SAML * 활성화 링크를 선택합니다.
+
Confirm Enable SAML(SAML 활성화 확인) 대화 상자가 열립니다.

. 을 입력하고 `enable` * 사용 * 을 클릭합니다.
. SSO 로그인 테스트에 대한 사용자 자격 증명을 입력합니다.

.결과
시스템에서 SAML을 활성화하면 모든 활성 세션이 종료되고 SAML을 통해 사용자 인증이 시작됩니다.

[[ID4acc02a26965e30b6f9d5b8c87313f1b]]
= SAML 역할 매핑을 변경합니다
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
이전에 Access Management에 SAML을 구성한 경우 IDP 그룹과 스토리지 배열의 사전 정의된 역할 간의 역할 매핑을 변경할 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* SAML이 구성 및 활성화되었습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 역할 매핑 * 을 선택합니다.
+
역할 매핑 대화 상자가 열립니다.

. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.
+
[CAUTION]
====
SAML이 활성화되어 있는 동안에는 권한을 제거하지 않도록 주의하십시오. 그렇지 않으면 Unified Manager에 액세스할 수 없게 됩니다.

====
+
.필드 상세정보
[%collapsible]
====
[cols="25h,~"]
|===
| 설정 | 설명

 a|
* 매핑 *

 a|
사용자 속성
 a|
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.

```
 a|
```
속성 값
```
 a|
```
매핑할 그룹의 속성 값을 지정합니다.

```
 a|
```
역할
```
 a|
```
필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 이 그룹에 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 Unified Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 보안 관리자 역할은 하나 이상의 그룹에 할당해야 합니다. 매핑된 역할에는 다음 권한이 포함됩니다.

** * 스토리지 관리자 * -- 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
** * 보안 관리자 * -- 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
** * 지원 관리자 * -- 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
** * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

```
|===
====
+
```

NOTE: Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.

. 선택적으로 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
. 저장 * 을 클릭합니다.

.결과
이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

```
[[ID65b86508a906ad5f27dce71ebe7b23a6]]
= SAML 서비스 공급자 파일을 내보냅니다
:allow-uri-read:
:experimental:
```

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
필요한 경우 스토리지 배열에 대한 서비스 공급자 메타데이터를 내보내고 해당 파일을 IdP(Identity Provider) 시스템으로 다시 가져올 수 있습니다.

.시작하기 전에
* 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
* SAML이 구성 및 활성화되었습니다.


.이 작업에 대해
이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다. IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 요청을 보내는 데 사용할 수 있는 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

.단계
. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
. SAML * 탭을 선택합니다.
. 내보내기 * 를 선택합니다.
+
서비스 공급자 파일 내보내기 대화 상자가 열립니다.

. 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.
+
[NOTE]
====
도메인 이름 필드는 읽기 전용입니다.

====
+
파일이 저장된 위치를 기록해 둡니다.

. 로컬 시스템에서 내보낸 XML 형식의 서비스 공급자 메타데이터 파일을 찾습니다.
. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져옵니다. 파일을 직접 가져오거나 컨트롤러 정보를 수동으로 입력할 수 있습니다.
. 닫기 * 를 클릭합니다.




:leveloffset: -1
```

= FAQ 를 참조하십시오

:leveloffset: +1

[[IDcd71403a420398f5a05fe4ff89cece3b]]
= 로그인할 수 없는 이유는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
로그인을 시도할 때 오류가 발생하면 다음과 같은 가능한 원인을 검토하십시오.

다음과 같은 이유 중 하나로 인해 로그인 오류가 발생할 수 있습니다.

* 잘못된 사용자 이름 또는 암호를 입력했습니다.
* 권한이 부족합니다.
* 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 다시 로그인하려면 10분 정도 기다립니다.
* SAML 인증이 활성화되었습니다. 로그인하려면 브라우저를 새로 고치십시오.

[[IDf0e52d61f624d7f952cf185e5b3f9b7a]]
= 디렉토리 서버를 추가하기 전에 알아야 할 사항은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
Access Management에서 디렉터리 서버를 추가하기 전에 특정 요구 사항을 충족해야 합니다.

* 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
* 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
* 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

```
[[ID4c4bd16d8c567550e3fe8e4ff40c77fb]]
= 스토리지 어레이 역할에 매핑하는 방법에 대해 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
그룹을 역할에 매핑하기 전에 지침을 검토하십시오.

RBAC(역할 기반 액세스 제어) 기능에는 다음 역할이 포함됩니다.

* * 스토리지 관리자 * -- 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
* * 보안 관리자 * -- 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
* * 지원 관리자 * -- 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
* * Monitor * -- 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.


[NOTE]
====
Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다.

====
LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스를 사용하는 경우 다음 사항을 확인하십시오.

* 관리자가 디렉토리 서비스에 사용자 그룹을 정의했습니다.
* LDAP 사용자 그룹의 그룹 도메인 이름을 알고 있습니다.




== SAML

스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하는 경우 다음 사항을 확인하십시오.

* IDP(Identity Provider) 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
* 그룹 구성원 이름을 알고 있습니다.
* 매핑할 그룹의 속성 값을 알고 있습니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 (`\`정규식 패턴의 일부가 아닌 경우 백슬래시를 사용하여 이스케이프해야 합니다.
```

```
+
[listing]
----
\.[]{}()<>*+-=!?^$|
----
* Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 모든 사용자는 Unified Manager가 올바르게 작동하지 않습니다.




[[ID7abe56a2cd2ff61b3aa7c93259539793]]
= SAML을 구성 및 활성화하기 전에 알아야 할 내용은 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
인증을 위해 SAML(Security Assertion Markup Language) 기능을 구성 및 활성화하기 전에 다음 요구 사항을 충족하고 SAML 제한 사항을 이해해야 합니다.



== 요구 사항

시작하기 전에 다음 사항을 확인하십시오.

* ID 공급자(IDP)가 네트워크에 구성되어 있습니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
* IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹을 구성했습니다.
* IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
* 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클록이 동기화되도록 했습니다.
* IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 Unified Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.
* 스토리지 배열의 컨트롤러에 있는 IP 주소 또는 도메인 이름을 알고 있습니다.



== 제한 사항

위의 요구 사항 외에 다음과 같은 제한 사항을 이해해야 합니다.
```

* SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오. 최종 구성 단계에서 SAML을 활성화하기 전에 SSO 로그인을 테스트하는 것이 좋습니다. (SAML을 활성화하기 전에 SSO 로그인 테스트도 수행합니다.)
* 나중에 SAML을 사용하지 않도록 설정하면 이전 구성(로컬 사용자 역할 및/또는 디렉터리 서비스)이 자동으로 복원됩니다.
* 디렉토리 서비스가 현재 사용자 인증을 위해 구성된 경우 SAML은 해당 구성을 재정의합니다.
* SAML이 구성된 경우 다음 클라이언트가 스토리지 시스템 리소스에 액세스할 수 없습니다.
+
** 엔터프라이즈 관리 창(EMW)
** CLI(Command-Line Interface)
** SDK(소프트웨어 개발자 키트) 클라이언트
** 대역내 클라이언트
** HTTP 기본 인증 REST API 클라이언트
** 표준 REST API 끝점을 사용하여 로그인합니다

[[IDbd70f6e5020cfce1ec267df564557db7]]
= 로컬 사용자는 무엇입니까?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
로컬 사용자는 시스템에 미리 정의되어 있으며 특정 권한을 포함합니다.

로컬 사용자는 다음과 같습니다.

* * admin * -- 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자는 모든 역할을 포함합니다. 암호는 처음 로그인할 때 설정해야 합니다.
* * 스토리지 * -- 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자에게는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * 보안 * -- 액세스 관리 및 인증서 관리를 포함한 보안 구성을 담당하는 사용자입니다. 이 사용자는 보안 관리자 및 모니터 역할을 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * 지원 * -- 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자에게는 지원 관리자 및 모니터 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * monitor * -- 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자는 Monitor 역할만 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.

* * rw * (읽기/쓰기) -- 이 사용자는 스토리지 관리자, 지원 관리자 및 모니터 역할을 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
* * ro * (읽기 전용) -- 이 사용자는 Monitor 역할만 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

[[IDe50e89bccc455daa4242c175a32f95c9]]
= 이전 버전
:allow-uri-read:

[role="lead"]
아래 링크를 통해 E-Series 하드웨어 및 SANtricity 소프트웨어의 이전 버전 설명서에 액세스하십시오. 이 링크를 클릭하면 다른 문서 사이트로 이동합니다.

== 이전 릴리즈에 대한 하드웨어 설명서

* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484026["E2712, E2724, E5612, E5624 컨트롤러 드라이브 트레이 및 DE1600 및 DE5600 확장 드라이브 트레이를 설치합니다"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484072["E2760 및 E5660 컨트롤러-드라이브 트레이 및 DE6600 확장 드라이브 트레이를 설치합니다"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2484108["EF560 Flash Array 및 DE5600 플래시 확장 트레이를 설치합니다"^]
* https://mysupport.netapp.com/info/web/ECMP11392380.html["이전 시스템을 설치합니다"^]
* https://mysupport.netapp.com/info/web/ECMP11751516.html["이전 시스템 유지 관리"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1394872["E2600 및 E2700에 두 번째 컨트롤러를 추가합니다"^]
* https://library.netapp.com/ecm/ecm_download_file/ECMLP2353447["호스트 프로토콜을 변경하거나 추가합니다"^]
* https://mysupport.netapp.com/ecm/ecm_download_file/ECMP1656638["AC 전원에서 DC 전원으로 변환합니다"^]

```
== 이전 릴리스에 대한 소프트웨어 문서


=== SANtricity 릴리스 11.7

* https://docs.netapp.com/us-en/e-series-santricity-117/index.html["System
Manager 도움말"^]
* https://docs.netapp.com/us-en/e-series-santricity-
117/index.html["Unified Manager 도움말"^]




=== SANtricity 릴리스 11.6

* https://docs.netapp.com/us-en/e-series-santricity-116/index.html["System
Manager 도움말"^]
* https://docs.netapp.com/us-en/e-series-santricity-
116/index.html["Unified Manager 도움말"^]




=== SANtricity 릴리스 11.5

* https://docs.netapp.com/us-en/e-series-santricity-115/index.html["System
Manager 도움말"^]




=== SANtricity 릴리스 11.4

* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862590["AMW(E2700,
E5600/EF560) 도움말"^]
* https://mysupport.netapp.com/ecm/ecm_get_file/ECMLP2862588["EMW(E2700,
E5600/EF560) 도움말"^]




[[ID8be8ccd0bb9d620033c0822d04ea159b]]
```

```
= 법적 고지
:hardbreaks:
:allow-uri-read:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: {root_path}{relative_path}./media/


[role="lead lead"]
법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.



== 저작권

link:https://www.netapp.com/company/legal/copyright/["https://www.netapp.com/company/legal/copyright/"^]



== 상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

link:https://www.netapp.com/company/legal/trademarks/["https://www.netapp.com/company/legal/trademarks/"^]



== 특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

link:https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf["https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf"^]



== 개인 정보 보호 정책

link:https://www.netapp.com/company/legal/privacy-policy/["https://www.netapp.com/company/legal/privacy-policy/"^]
```

== 오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이센스에 대한 정보를 제공합니다.

https://library.netapp.com/ecm/ecm_download_file/ECMLP2885978["E-Series/EF-Series SANtricity OS에 대한 알림"]

:leveloffset: -1

<<<
저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로

가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 link:http://www.netapp.com/TM[http://www.netapp.com/TM^]에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.