SANtricity 솔루션을 사용하십시오

E-Series storage systems

NetApp
March 12, 2026

목차

SANtricity 솔루션을 사용하십시오

웹 서비스 프록시

SANtricity 웹 서비스 프록시에 대해 알아봅니다

SANtricity 웹 서비스 프록시는 호스트 시스템에 별도로 설치되는 RESTful API 서버로, 수백 개의 새로운 NetApp E-Series 스토리지 시스템을 관리합니다. 이 대리인에는 유사한 기능을 제공하는 웹 기반 인터페이스인 SANtricity Unified Manager가 포함되어 있습니다.

설치 개요

웹 서비스 프록시를 설치 및 구성하는 절차는 다음과 같습니다.

1. "설치 및 업그레이드 요구 사항 검토".
2. "웹 서비스 프록시 파일을 다운로드하여 설치합니다".
3. "API 및 Unified Manager에 로그인합니다".
4. "웹 서비스 프록시를 구성합니다".

자세한 내용을 확인하십시오

- Unified Manager — 프록시 설치에는 최신 E-Series 및 EF-Series 스토리지 시스템에 대한 구성 액세스를 제공하는 웹 기반 인터페이스인 SANtricity Unified Manager가 포함됩니다. 자세한 내용은 사용자 인터페이스 또는 에서 제공되는 Unified Manager 온라인 도움말을 참조하십시오 "SANtricity 소프트웨어 문서 사이트입니다".
- REST(Representational State Transfer) — 웹 서비스는 거의 모든 SANtricity 관리 기능에 대한 액세스를 제공하는 RESTful API로, REST 개념에 익숙해야 합니다. 자세한 내용은 을 참조하십시오 "아키텍처 스타일 및 네트워크 기반 소프트웨어 아키텍처의 설계".
- JSON(JavaScript Object Notation) — 웹 서비스 내의 데이터는 JSON을 통해 인코딩되므로 JSON 프로그래밍 개념에 익숙해야 합니다. 자세한 내용은 을 참조하십시오 "JSON을 소개합니다".

웹 서비스에 대해 자세히 알아보십시오

SANtricity 웹 서비스 및 **Unified Manager**에 대해 알아보십시오

웹 서비스 프록시를 설치 및 구성하기 전에 웹 서비스 및 SANtricity 통합 관리자의 개요를 읽어 보십시오.

웹 서비스

웹 서비스는 NetApp E-Series 및 EF-Series 스토리지 시스템을 구성, 관리 및 모니터링할 수 있는 API(Application Programming Interface)입니다. API 요청을 발급하여 E-Series 스토리지 시스템의 구성, 프로비저닝, 성능 모니터링과 같은 워크플로우를 완료할 수 있습니다.

웹 서비스 API를 사용하여 스토리지 시스템을 관리하는 경우 다음 사항에 익숙해야 합니다.

- JSON(JavaScript Object Notation) – 웹 서비스 내의 데이터는 JSON을 통해 인코딩되므로 JSON 프로그래밍

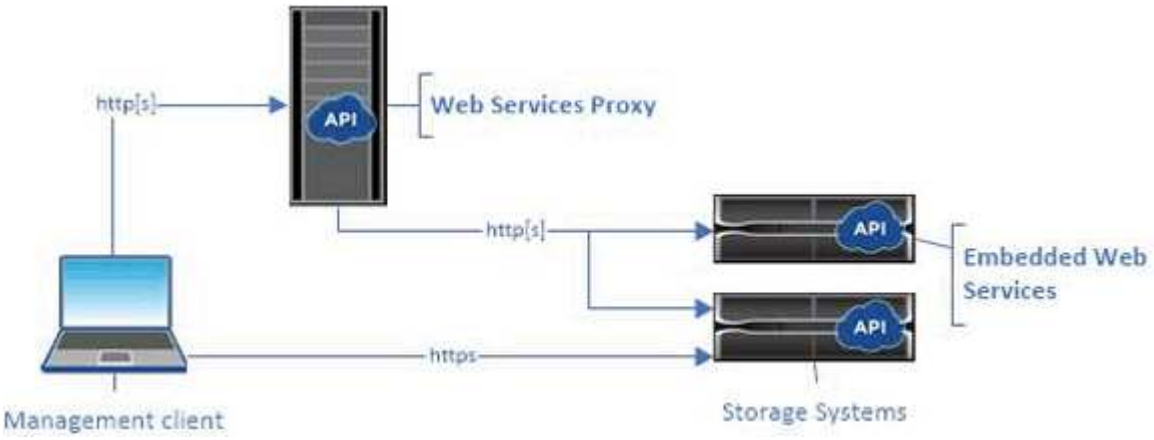
개념에 익숙해야 합니다. 자세한 내용은 을 참조하십시오 "JSON을 소개합니다".

- REST(Representational State Transfer) – 웹 서비스는 거의 모든 SANtricity 관리 기능에 대한 액세스를 제공하는 RESTful API로, REST 개념에 익숙해야 합니다. 자세한 내용은 을 참조하십시오 "아키텍처 스타일 및 네트워크 기반 소프트웨어 아키텍처의 설계".
- 프로그래밍 언어 개념 – Java 및 Python은 웹 서비스 API에서 사용되는 가장 일반적인 프로그래밍 언어이지만, HTTP 요청을 만들 수 있는 모든 프로그래밍 언어는 API 상호 작용에 충분합니다.

웹 서비스는 다음 두 가지 구현 방식으로 제공됩니다.

- * 내장 * — RESTful API 서버는 NetApp SANtricity 11.30 이상 버전을 실행하는 E2800/EF280 스토리지 시스템의 각 컨트롤러, SANtricity 11.40 이상 버전을 실행하는 E5700/EF570, SANtricity 11.60 이상 버전을 실행하는 EF300 또는 EF600, SANtricity 11.90 이상 버전을 실행하는 E4000의 각 컨트롤러에 내장되어 있습니다. 설치가 필요하지 않습니다.
- * 프록시 * — SANtricity 웹 서비스 프록시는 Windows 또는 Linux 서버에 별도로 설치되는 RESTful API 서버입니다. 이 호스트 기반 애플리케이션은 수백 가지의 새로운 기존 NetApp E-Series 스토리지 시스템을 관리할 수 있습니다. 일반적으로 10개 이상의 스토리지 시스템이 있는 네트워크에는 프록시를 사용해야 합니다. 프록시는 포함된 API보다 더 효율적으로 많은 요청을 처리할 수 있습니다.

API의 코어는 두 가지 구축 모두에서 사용할 수 있습니다.



다음 표에서는 프록시와 포함된 버전을 비교하여 보여 줍니다.

고려 사항	프록시	임베디드
설치	호스트 시스템(Linux 또는 Windows)이 필요합니다. 프록시는 에서 다운로드할 수 있습니다 "NetApp Support 사이트" 또는 을 누릅니다 "DockerHub를 참조하십시오".	설치 또는 활성화가 필요하지 않습니다.

고려 사항	프록시	임베디드
보안	기본적으로 최소 보안 설정이 사용됩니다. 개발자가 API를 빠르고 쉽게 시작할 수 있도록 보안 설정이 낮습니다. 필요한 경우 포함된 버전과 동일한 보안 프로필을 사용하여 프록시를 구성할 수 있습니다.	기본적으로 높은 보안 설정이 사용됩니다. API가 컨트롤러에서 직접 실행되므로 보안 설정이 높습니다. 예를 들어, HTTP 액세스를 허용하지 않으며 HTTPS에 대한 모든 SSL 및 이전 TLS 암호화 프로토콜을 비활성화합니다.
중앙 집중식 관리	하나의 서버에서 모든 스토리지 시스템을 관리합니다.	내장된 컨트롤러만 관리합니다.

Unified Manager를 참조하십시오

프록시 설치 패키지에는 E2800, E5700, EF300, EF600과 같은 최신 E-Series 및 EF-Series 스토리지 시스템에 대한 구성 액세스를 제공하는 웹 기반 인터페이스인 Unified Manager가 포함됩니다.

Unified Manager에서 다음 일괄 작업을 수행할 수 있습니다.

- 중앙 보기에서 여러 스토리지 시스템의 상태를 봅니다
- 네트워크에서 여러 스토리지 시스템을 검색합니다
- 한 스토리지 시스템에서 여러 시스템으로 설정을 가져옵니다
- 여러 스토리지 시스템의 펌웨어를 업그레이드합니다

SANtricity 웹 서비스 프록시 호환성 및 제한 사항

웹 서비스 프록시 사용에 적용되는 호환성 및 제한 사항은 다음과 같습니다.

고려 사항	호환성 또는 제한
HTTP 지원	웹 서비스 프록시는 HTTP 또는 HTTPS를 사용할 수 있습니다. (임베디드 버전의 웹 서비스는 보안상의 이유로 HTTPS가 필요합니다.)
기술을 자세히 소개합니다	웹 서비스 프록시를 사용하면 이전 시스템과 최신 E2800, EF280, E5700, EF570, EF300 등의 모든 E-Series 스토리지 시스템을 관리할 수 있습니다. EF600 시리즈 시스템이었습니다.

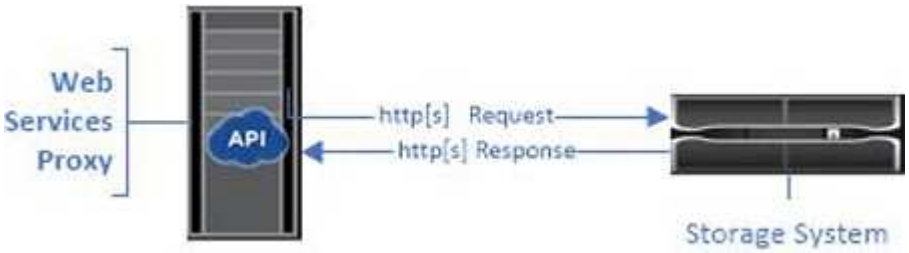
고려 사항	호환성 또는 제한
IP 지원	웹 서비스 프록시는 IPv4 프로토콜 또는 IPv6 프로토콜을 지원합니다. 웹 서비스 프록시가 컨트롤러 구성에서 관리 주소를 자동으로 검색하려고 하면 IPv6 프로토콜이 실패할 수 있습니다. IP 주소 전달 중 또는 IPv6가 서버에 있지 않고 스토리지 시스템에서 활성화되어 있는 동안 발생하는 문제가 오류의 가능한 원인입니다.
NVSRAM 파일 이름 제약 조건	웹 서비스 프록시는 NVSRAM 파일 이름을 사용하여 버전 정보를 정확하게 식별합니다. 따라서 웹 서비스 프록시와 함께 사용되는 NVSRAM 파일 이름은 변경할 수 없습니다. 웹 서비스 프록시는 이름이 바뀐 NVSRAM 파일을 유효한 펌웨어 파일로 인식하지 못할 수 있습니다.
Symbol 웹	Symbol Web은 REST API의 URL입니다. 거의 모든 심볼 호출에 액세스할 수 있습니다. SYMBOL 함수는 다음 URL의 일부입니다. 'http://host:port/devmgr/storage-system/storage 배열 ID/기호/기호 함수' Symbol에서 사용하지 않는 스토리지 시스템은 웹 서비스 프록시를 통해 지원됩니다.

SANtricity 웹 서비스 프록시 **API** 기본 사항에 대해 알아봅니다

웹 서비스 API에서 HTTP 통신에는 요청 응답 주기가 포함됩니다.

요청의 **URL** 요소입니다

사용되는 프로그래밍 언어나 도구에 관계없이 웹 서비스 API에 대한 각 호출은 URL, HTTP 동사 및 Accept 헤더와 유사한 구조를 가집니다.



모든 요청은 다음 예제와 같이 URL을 포함하며 표에 설명된 요소를 포함합니다.

(https://webservices.name.com:8443/devmgr/v2/storage-systems`)

영역	설명
HTTP 전송 'https://'	웹 서비스 프록시를 사용하면 HTTP 또는 HTTPS를 사용할 수 있습니다. 임베디드 웹 서비스는 보안상의 이유로 HTTPS가 필요합니다.
기본 URL 및 포트입니다 "webservices.name.com:8443`	각 요청은 웹 서비스의 활성 인스턴스로 올바르게 라우팅되어야 합니다. 수신 대기 포트와 함께 인스턴스의 FQDN(정규화된 도메인 이름) 또는 IP 주소가 필요합니다. 기본적으로 웹 서비스는 포트 8080(HTTP의 경우) 및 포트 8443(HTTPS의 경우)을 통해 통신합니다. 웹 서비스 프록시의 경우 프록시 설치 중에 또는 wsconfig.xml 파일에서 두 포트를 모두 변경할 수 있습니다. 다양한 관리 애플리케이션을 실행하는 데이터 센터 호스트에서 포트 경합이 흔히 발생합니다. Embedded Web Services의 경우 컨트롤러의 포트를 변경할 수 없습니다. 보안 연결의 경우 기본적으로 포트 8443이 됩니다.
API 경로 devmgr/v2/storage-systems를 선택합니다	Web Services API 내의 특정 REST 리소스 또는 끝점에 대한 요청이 이루어집니다. 대부분의 끝점은 다음과 같습니다. devmgr/v2/<resource>/[id]' API 경로는 다음 세 부분으로 구성됩니다. • Devmgr(장치 관리자)는 웹 서비스 API의 네임스페이스입니다. • v2 는 액세스 중인 API의 버전을 나타낸다. 또한 "utils"를 사용하여 로그인 끝점에 액세스할 수도 있습니다. • 문서내 분류는 스토리지 시스템이다.

지원되는 **HTTP** 동사

지원되는 HTTP 동사에는 GET, POST 및 DELETE가 포함됩니다.

- 가져오기 요청은 읽기 전용 요청에 사용됩니다.
- POST 요청은 개체를 만들고 업데이트하는 데 사용되며, 보안과 관련이 있을 수 있는 읽기 요청에도 사용됩니다.
- 삭제 요청은 일반적으로 관리에서 개체를 제거하거나, 개체를 완전히 제거하거나, 개체의 상태를 다시 설정하는 데 사용됩니다.

현재 웹 서비스 API는 PUT 또는 패치를 지원하지 않습니다. 대신 POST를 사용하여 이러한 동사에 대한 일반적인 기능을 제공할 수 있습니다.

머리글 적용

요청 본문을 반환할 때 Web Services는 달리 지정하지 않는 한 데이터를 JSON 형식으로 반환합니다. 일부 클라이언트는 기본적으로 ""text/html"" 또는 이와 유사한 것을 요청합니다. 이러한 경우 API는 HTTP 코드 406으로 응답하여 이 형식의 데이터를 제공할 수 없음을 나타냅니다. 가장 좋은 방법은 JSON을 응답 유형으로 기대하는 모든 경우에 Accept 헤더를 ""application/json""으로 정의하는 것입니다. 응답 본문이 반환되지 않은 경우(예: 삭제), 수락 헤더를 사용해도 의도하지 않은 효과가 발생하지 않습니다.

응답

API에 대한 요청이 이루어지면 응답이 두 가지 중요한 정보를 반환합니다.

- HTTP 상태 코드 — 요청이 성공했는지 여부를 나타냅니다.
- 선택적 응답 본문 — 일반적으로 실패의 특성에 대한 자세한 정보를 제공하는 리소스 또는 바디의 상태를 나타내는 JSON 바디를 제공합니다.

결과 응답 본문의 모양을 확인하려면 상태 코드와 콘텐츠 형식 헤더를 확인해야 합니다. HTTP 상태 코드 200-203 및 422의 경우 Web Services는 응답으로 JSON 본문을 반환합니다. 다른 HTTP 상태 코드의 경우, Web Services는 일반적으로 추가 JSON 본문을 반환하지 않습니다. 이는 사양이 이를 허용하지 않거나(204) 상태가 자체 설명이기 때문입니다. 이 표에는 일반적인 HTTP 상태 코드 및 정의가 나와 있습니다. 또한 각 HTTP 코드와 관련된 정보가 JSON 본문에서 반환되는지 여부도 나타냅니다.

HTTP 상태 코드입니다	설명	**JSON** 바디
200 정상	성공적인 응답을 나타냅니다.	예
201 생성됨	개체가 생성되었음을 나타냅니다. 이 코드는 200 상태가 아닌 몇 가지 드문 경우에 사용됩니다.	예
202 수락됨	요청이 비동기 요청으로 처리되도록 허용되었지만 실제 결과를 얻으려면 후속 요청을 해야 함을 나타냅니다.	예
203 권한 없는 정보입니다	200개의 응답과 비슷하지만 웹 서비스는 데이터가 최신 데이터임을 보장할 수 없습니다(예: 현재 캐시된 데이터만 사용 가능).	예
204 콘텐츠 없음	작업이 성공했지만 응답 본문이 없음을 나타냅니다.	아니요
400 잘못된 요청	요청에 제공된 JSON 본문이 유효하지 않음을 나타냅니다.	아니요
401 승인되지 않음	인증 실패가 발생했음을 나타냅니다. 자격 증명이 제공되지 않았거나 사용자 이름 또는 암호가 잘못되었습니다.	아니요

HTTP 상태 코드입니다	설명	**JSON** 바디
403 사용 금지	인증 실패 - 인증된 사용자에게 요청된 끝점에 액세스할 수 있는 권한이 없음을 나타냅니다.	아니요
404를 찾을 수 없습니다	요청한 리소스를 찾을 수 없음을 나타냅니다. 이 코드는 존재하지 않는 API 또는 ID에서 요청한 존재하지 않는 리소스에 대해 유효합니다.	아니요
422 처리할 수 없는 엔터티	요청이 일반적으로 제대로 구성되었지만 입력 매개 변수가 잘못되었거나 스토리지 시스템의 상태가 웹 서비스가 요청을 충족시킬 수 없음을 나타냅니다.	예
424 실패한 종속성	웹 서비스 프록시에서 요청된 스토리지 시스템을 현재 액세스할 수 없음을 나타내는 데 사용됩니다. 따라서 웹 서비스가 요청을 충족할 수 없습니다.	아니요
429 요청이 너무 많습니다	요청 한도를 초과했으며 나중에 다시 시도해야 함을 나타냅니다.	아니요

SANtricity 웹 서비스 프록시 용어에 대해 알아봅니다

다음 용어는 웹 서비스 프록시에 적용됩니다.

기간	정의
API를 참조하십시오	API(응용 프로그래밍 인터페이스)는 개발자가 장치와 통신할 수 있도록 하는 프로토콜 및 메서드 집합입니다. 웹 서비스 API는 E-Series 스토리지 시스템과 통신하는 데 사용됩니다.
ASUP	ASUP(AutoSupport) 기능은 고객 지원 번들에서 데이터를 수집하고 원격 문제 해결 및 문제 분석을 위해 메시지 파일을 기술 지원 팀에 자동으로 전송합니다.
엔드포인트	끝점은 API를 통해 사용할 수 있는 기능입니다. 끝점에는 HTTP 동사와 URI 경로가 포함됩니다. 웹 서비스에서 끝점은 스토리지 시스템 검색 및 볼륨 생성과 같은 작업을 실행할 수 있습니다.

기간	정의
HTTP 동사	HTTP 동사는 데이터 검색 및 만들기와 같은 끝점에 대한 해당 작업입니다. 웹 서비스에서 HTTP 동사는 POST, GET 및 DELETE를 포함합니다.
JSON을 참조하십시오	JSON(JavaScript Object Notation)은 XML과 유사한 구조화된 데이터 형식으로, 읽을 수 있는 최소 형식을 사용합니다. 웹 서비스 내의 데이터는 JSON을 통해 인코딩됩니다.
REST/RESTful	REST(Representational State Transfer)는 API의 아키텍처 스타일을 정의하는 느슨한 사양입니다. 대부분의 REST API는 사양을 완전히 따르지 않기 때문에 "restful" 또는 "reST-like"로 묘사됩니다. 일반적으로 "restful" API는 프로그래밍 언어에 상관없이 사용할 수 있으며 다음과 같은 특징이 있습니다. • 프로토콜의 일반적인 의미를 따르는 HTTP 기반 • 정형 데이터의 생산자 및 소비자(JSON, XML 등) • 오브젝트 지향(운영 중심 대신) 웹 서비스는 거의 모든 SANtricity 관리 기능에 대한 액세스를 제공하는 RESTful API입니다.
수행할 수 있습니다	스토리지 시스템은 E-Series 어레이로, 쉘프, 컨트롤러, 드라이브, 소프트웨어 펌웨어를 업데이트할 수 있습니다.
기호 API	Symbol은 E-Series 스토리지 시스템을 관리하기 위한 레거시 API를 제공합니다. 웹 서비스 API의 기본 구현에는 기호가 사용됩니다.
웹 서비스	Web Services는 개발자가 E-Series 스토리지 시스템을 관리하도록 설계된 API입니다. 웹 서비스는 컨트롤러에 내장되어 있고 Linux 또는 Windows에 설치할 수 있는 별도의 프록시와 같은 두 가지 구현이 있습니다.

설치 및 구성

SANtricity 웹 서비스 프록시의 설치 및 업그레이드 요구 사항을 검토합니다

웹 서비스 프록시를 설치하기 전에 설치 요구 사항 및 업그레이드 고려 사항을 검토하십시오.

설치 요구 사항

Windows 또는 Linux 호스트 시스템에 웹 서비스 프록시를 설치 및 구성할 수 있습니다.

프록시 설치에는 다음 요구 사항이 포함됩니다.

요구 사항	설명
호스트 이름 제한	웹 서비스 프록시를 설치할 서버의 호스트 이름에 ASCII 문자, 숫자 및 하이픈(-)만 포함되어 있는지 확인합니다. 이 요구 사항은 서버에 대해 자체 서명된 인증서를 생성하는 데 사용되는 Java Keytool의 제한 사항 때문입니다. 서버의 호스트 이름에 밑줄(_)과 같은 다른 문자가 포함되어 있으면 설치 후 Webserver가 시작되지 않습니다.
운영 체제	다음 운영 체제에 프록시를 설치할 수 있습니다. • 리눅스 • Windows 운영 체제 및 펌웨어 호환성에 대한 전체 목록은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
Linux: 추가 고려 사항	Webserver가 제대로 작동하려면 Linux 표준 기본 라이브러리(init-function)가 필요합니다. 운영 체제용 LSB/insserv 패키지를 설치해야 합니다. 자세한 내용은 Readme 파일의 "추가 패키지 필요" 섹션을 참조하십시오.
다중 인스턴스	서버에 웹 서비스 프록시 인스턴스를 하나만 설치할 수 있지만, 네트워크 내의 여러 서버에 프록시를 설치할 수 있습니다.
용량 계획	웹 서비스 프록시는 로깅에 충분한 공간을 필요로 합니다. 시스템이 다음과 같은 사용 가능한 디스크 공간 요구 사항을 충족하는지 확인합니다. • 필요한 설치 공간 — 275MB • 최소 로깅 공간 — 200MB • 시스템 메모리 — 2GB, 힙 공간은 기본적으로 1Gb입니다 디스크 공간 모니터링 툴을 사용하여 영구 스토리지 및 로깅을 위해 사용 가능한 디스크 드라이브 공간을 확인할 수 있습니다.
라이센스	웹 서비스 프록시는 라이센스 키가 필요하지 않은 독립 실행형 무료 제품입니다. 그러나 해당 저작권 및 서비스 약관이 적용됩니다. 프록시를 그래픽 또는 콘솔 모드로 설치하는 경우 최종 사용자 사용권 계약(EULA)에 동의해야 합니다.

업그레이드 고려 사항

이전 버전에서 업그레이드하는 경우에는 일부 항목이 보존되거나 제거된다는 점에 유의하십시오.

- 웹 서비스 프록시의 경우 이전 구성 설정이 유지됩니다. 이러한 설정에는 사용자 암호, 검색된 모든 스토리지 시스템, 서버 인증서, 신뢰할 수 있는 인증서 및 서버 런타임 구성이 포함됩니다.
- Unified Manager의 경우, 이전에 저장소에 로드된 모든 SANtricity OS 파일이 업그레이드 중에 제거됩니다.

SANtricity 웹 서비스 프록시 및 **SANtricity Unified Manager** 파일 설치 또는 업그레이드

설치에는 파일을 다운로드한 다음 Linux 또는 Windows 서버에 프록시 패키지를 설치하는 과정이 포함됩니다. 이 지침을 사용하여 프록시를 업그레이드할 수도 있습니다.

웹 서비스 프록시 파일을 다운로드합니다

NetApp Support 사이트의 소프트웨어 다운로드 페이지에서 설치 파일과 readme 파일을 다운로드할 수 있습니다.

다운로드 패키지에는 웹 서비스 프록시 및 Unified Manager 인터페이스가 포함되어 있습니다.

단계

1. 로 이동합니다 "NetApp 지원 - 다운로드".
2. E-Series SANtricity 웹 서비스 프록시 * 를 선택합니다.
3. 지침에 따라 파일을 다운로드합니다. 서버에 맞는 올바른 다운로드 패키지를 선택해야 합니다(예: Windows의 경우 EXE, Linux의 경우 bin 또는 RPM).
4. 프록시 및 Unified Manager를 설치할 서버에 설치 파일을 다운로드합니다.

Windows 또는 **Linux** 서버에 설치합니다

세 가지 모드(그래픽, 콘솔 또는 자동) 중 하나를 사용하거나 RPM 파일(Linux만 해당)을 사용하여 웹 서비스 프록시 및 Unified Manager를 설치할 수 있습니다.

시작하기 전에

- "설치 요구 사항을 검토합니다".
- 프록시 및 Unified Manager를 설치할 서버에 올바른 설치 파일(Windows의 경우 EXE, Linux의 경우 BIN)을 다운로드했는지 확인합니다.

그래픽 모드 설치

Windows 또는 Linux의 그래픽 모드에서 설치를 실행할 수 있습니다. 그래픽 모드에서 프롬프트는 Windows 스타일 인터페이스에 나타납니다.

단계

1. 설치 파일을 다운로드한 폴더에 액세스합니다.
2. 다음과 같이 Windows 또는 Linux에 대한 설치를 시작합니다.
   - Windows — 설치 파일을 두 번 클릭합니다.

     'S antricity_webservices - windows_x64-nn.nn.nn.nn.nnnn.exe'

   - Linux — 'santricity_webservices -linux_x64-nn.nn.nn.nn.nn.bin' 명령을 실행합니다

     위의 파일 이름에서 ' nn.nn.nn.nnnn'은 버전 번호를 나타냅니다.

   설치 프로세스가 시작되고 NetApp SANtricity 웹 서비스 프록시 + Unified Manager 시작 화면이 나타납니다.
3. 화면에 표시되는 메시지를 따릅니다.

설치 중에 여러 기능을 활성화하고 일부 구성 매개변수를 입력하라는 메시지가 표시됩니다. 필요한 경우 나중에 구성 파일에서 이러한 선택 항목을 변경할 수 있습니다.

> 업그레이드 중에는 구성 매개 변수를 묻는 메시지가 표시되지 않습니다.

4. Webserver Started 메시지가 나타나면 * OK * 를 클릭하여 설치를 완료합니다.

   설치 완료 대화 상자가 나타납니다.

5. Unified Manager 또는 대화형 API 설명서를 실행하려면 확인란을 클릭한 다음 * 완료 * 를 클릭합니다.

콘솔 모드 설치

Windows 또는 Linux의 경우 콘솔 모드에서 설치를 실행할 수 있습니다. 콘솔 모드에서는 터미널 창에 프롬프트가 나타납니다.

단계

1. '<파일 이름 설치> -i 콘솔' 명령을 실행합니다

   위 명령에서 '<설치 파일 이름>'은 다운로드한 프록시 설치 파일의 이름을 나타냅니다(예: 'santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe').

   > 설치 과정 중 언제든지 설치를 취소하려면 명령 프롬프트에 quit를 입력합니다.

   설치 프로세스가 시작되고 시작 설치 관리자 — 소개 메시지가 나타납니다.

2. 화면에 표시되는 메시지를 따릅니다.

   설치 중에 여러 기능을 활성화하고 일부 구성 매개변수를 입력하라는 메시지가 표시됩니다. 필요한 경우 나중에 구성 파일에서 이러한 선택 항목을 변경할 수 있습니다.

   > 업그레이드 중에는 구성 매개 변수를 묻는 메시지가 표시되지 않습니다.

3. 설치가 완료되면 * Enter * 를 눌러 설치 프로그램을 종료합니다.

자동 모드 설치

Windows 또는 Linux에서 자동 모드로 설치를 실행할 수 있습니다. 무음 모드에서는 터미널 창에 반환 메시지나 스크립트가 나타나지 않습니다.

단계

1. '<파일 이름 설치> -i silent' 명령을 실행합니다

   위 명령에서 '<설치 파일 이름>'은 다운로드한 프록시 설치 파일의 이름을 나타냅니다(예: 'santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe').

2. Enter * 를 누릅니다.

   설치 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 설치가 완료되면 터미널 창에 명령 프롬프트가 나타납니다.

rpm 명령 설치(Linux만 해당)

RPM 패키지 관리 시스템과 호환되는 Linux 시스템의 경우 선택적 RPM 파일을 사용하여 웹 서비스 프록시를 설치할 수 있습니다.

단계

1. RPM 파일을 프록시 및 Unified Manager를 설치할 서버로 다운로드합니다.
2. 터미널 창을 엽니다.
3. 다음 명령을 입력합니다.

```
rpm -U santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
```

> 위 명령에서 nn.nn.nn.nnnn은 버전 번호를 나타냅니다.

설치 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 설치가 완료되면 터미널 창에 명령 프롬프트가 나타납니다.

SANtricity 웹 서비스 프록시 API 및 Unified Manager에 로그인합니다

웹 서비스에는 REST API와 직접 상호 작용할 수 있는 API 설명서가 포함되어 있습니다. 또한 여러 E-Series 스토리지 시스템을 관리하기 위한 브라우저 기반 인터페이스인 Unified Manager도 포함되어 있습니다.

웹 서비스 API에 로그인합니다

웹 서비스 프록시를 설치한 후 브라우저에서 대화형 API 설명서에 액세스할 수 있습니다.

API 설명서는 웹 서비스의 각 인스턴스에서 실행되며 NetApp Support 사이트에서 제공되는 정적 PDF 형식으로도 제공됩니다. 대화형 버전에 액세스하려면 브라우저를 열고 웹 서비스가 있는 위치(포함된 버전의 컨트롤러 또는 프록시의 서버)를 가리키는 URL을 입력합니다.

> 웹 서비스 API는 OpenAPI 사양(원래 Swagger 사양이라고 함)을 구현합니다.

초기 로그인의 경우 "admin" 자격 증명을 사용합니다. "관리자"는 모든 기능 및 역할에 액세스할 수 있는 슈퍼 관리자로 간주됩니다.

단계

1. 브라우저를 엽니다.
2. 포함된 또는 프록시 구현의 URL을 입력합니다.

   - 포함: 'https://<controller>:<port>/devmgr/docs/`

     이 URL에서 "<controller>"는 컨트롤러의 IP 주소 또는 FQDN이며 "<port>"는 컨트롤러의 관리 포트 번호입니다(기본값은 8443임).

   - 프록시: "http[s]://<server>:<port>/devmgr/docs/"

     이 URL에서 '<server>'는 프록시가 설치된 서버의 IP 주소 또는 FQDN이며 수신 포트 번호는 '<port>'입니다

(기본값은 HTTP의 경우 8080, HTTPS의 경우 8443입니다).

> 수신 포트가 이미 사용 중인 경우 프록시는 충돌을 감지하고 다른 수신 포트를 선택하라는 메시지를 표시합니다.

브라우저에서 API 설명서가 열립니다.

3. 대화형 API 문서가 열리면 페이지 오른쪽 상단의 드롭다운 메뉴로 이동하여 * utils * 를 선택합니다.
4. 사용 가능한 끝점을 보려면 * 로그인 * 범주를 클릭합니다.
5. POST:/login * 끝점을 클릭한 다음 * try it out * 을 클릭합니다.
6. 처음 로그인하는 경우 사용자 이름 및 암호에 admin 을 입력합니다.
7. Execute * 를 클릭합니다.
8. 스토리지 관리를 위한 엔드포인트에 액세스하려면 오른쪽 상단의 드롭다운 메뉴로 이동하여 * v2 * 를 선택합니다.

끝점의 상위 수준 범주가 표시됩니다. 표에 설명된 대로 API 설명서를 탐색할 수 있습니다.

영역	설명
드롭다운 메뉴를 선택합니다	페이지 오른쪽 위에 있는 드롭다운 메뉴에서 버전 2의 API 설명서(V2), 기호 인터페이스(기호 V2) 및 로그인할 수 있는 API 유틸리티(유틸리티) 간에 전환할 수 있는 옵션을 제공합니다. API 설명서 버전 1은 사전 릴리스 버전이므로 일반적으로 사용할 수 없으므로 V1은 드롭다운 메뉴에 포함되지 않습니다.
범주	API 설명서는 상위 범주(예: Administration, Configuration)별로 구성되어 있습니다. 관련 끝점을 보려면 범주를 클릭합니다.
엔드포인트	URL이 반환될 가능성이 있는 URL 경로, 필수 매개 변수, 응답 본문 및 상태 코드를 보려면 끝점을 선택합니다.
시도해 보십시오	Try it Out * 을 클릭하여 끝점과 직접 상호 작용할 수 있습니다. 이 버튼은 엔드포인트의 확장 보기 각각에 제공됩니다. 버튼을 클릭하면 파라미터 입력을 위한 필드가 나타납니다(해당하는 경우). 그런 다음 값을 입력하고 * Execute * 를 클릭합니다. 대화형 설명서는 JavaScript를 사용하여 API에 직접 요청을 합니다. 테스트 요청이 아닙니다.

Unified Manager에 로그인합니다

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

Unified Manager에 액세스하려면 브라우저를 열고 프록시가 설치된 위치를 가리키는 URL을 입력합니다. 다음 브라우저 및 버전이 지원됩니다.

브라우저	최소 버전
Google Chrome	79
Microsoft Internet Explorer를 참조하십시오	11
Microsoft Edge를 참조하십시오	79
Mozilla Firefox	70
사파리	12

단계

1. 브라우저를 열고 다음 URL을 입력합니다.

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

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

   Unified Manager 로그인 페이지가 열립니다.

2. 처음 로그인하는 경우 사용자 이름에 admin을 입력한 다음 admin 사용자의 암호를 설정 및 확인합니다.

   암호는 최대 30자까지 입력할 수 있습니다. 사용자 및 암호에 대한 자세한 내용은 Unified Manager 온라인 도움말의 액세스 관리 섹션을 참조하십시오.

SANtricity 웹 서비스 프록시를 구성합니다

사용자 환경의 고유한 운영 및 성능 요구 사항에 맞게 웹 서비스 프록시 설정을 수정할 수 있습니다.

Webserver를 중지하거나 다시 시작합니다

Webserver 서비스는 설치 중에 시작되어 백그라운드에서 실행됩니다. 일부 구성 작업 중에 Webserver 서비스를 중지하거나 다시 시작해야 할 수 있습니다.

단계

1. 다음 중 하나를 수행합니다.

   ◦ Windows의 경우 * 시작 * 메뉴로 이동하여 관리 도구 [서비스] 메뉴를 선택하고 * NetApp SANtricity 웹 서비스

* 를 찾은 다음 * 중지 * 또는 * 재시작 * 을 선택합니다.

◦ Linux의 경우 운영 체제 버전의 Webserver를 중지하고 다시 시작하는 방법을 선택합니다. 설치 중에 어떤 데몬이 시작되었는지 팝업 대화 상자가 표시됩니다. 예를 들면 다음과 같습니다.

"web_services_proxy 웹 서버가 설치 및 시작되었습니다. systemctl start | stop | restart | status web_services_proxy.service` 를 사용하여 IT와 상호 작용할 수 있습니다

이 서비스와 상호 작용하는 가장 일반적인 방법은 'emctl' 명령을 사용하는 것입니다.

포트 충돌을 해결합니다

정의된 주소 또는 포트에서 다른 응용 프로그램을 사용할 수 있는 동안 웹 서비스 프록시가 실행되고 있으면 wsconfig.xml 파일에서 포트 충돌을 해결할 수 있습니다.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   ◦ (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   ◦ (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. wsconfig.xml 파일에 다음 줄을 추가합니다. 이 때 _n_은 포트 번호입니다.

```
<sslport clientauth=”request”>*n*</sslport>
<port>n</port>
```

   다음 표에서는 HTTP 포트 및 HTTPS 포트를 제어하는 특성을 보여 줍니다.

이름	설명	상위 노드	속성	필수 요소입니다
구성	구성의 루트 노드입니다	null입니다	버전 - 구성 스키마의 버전은 현재 1.0입니다.	예
슬포트	SSL 요청을 수신 대기하는 TCP 포트. 기본값은 8443입니다.	구성	클라이언트 인증	아니요
포트	HTTP 요청을 수신할 TCP 포트, 기본값은 8080입니다.	구성	-	아니요

3. 파일을 저장하고 닫습니다.
4. Webserver 서비스를 다시 시작하여 변경 사항을 적용합니다.

로드 밸런싱 및/또는 고가용성을 구성합니다

고가용성(HA) 구성에서 웹 서비스 프록시를 사용하려면 로드 밸런싱을 구성할 수 있습니다. HA 구성에서 일반적으로

단일 노드는 모든 요청을 수신하지만 다른 노드는 대기 중이거나 모든 노드에 걸쳐 요청이 로드 밸런싱됩니다.

웹 서비스 프록시는 고가용성(HA) 환경에 존재할 수 있으며, 대부분의 API는 요청 수신자와 관계없이 올바르게 작동합니다. 태그 및 폴더는 로컬 데이터베이스에 저장되고 웹 서비스 프록시 인스턴스 간에 공유되지 않기 때문에 메타데이터 태그와 폴더는 두 가지 예외입니다.

그러나 일부 요청에서는 몇 가지 알려진 타이밍 문제가 발생합니다. 특히 프록시의 한 인스턴스는 작은 창의 두 번째 인스턴스보다 더 빠른 새 데이터를 가질 수 있습니다. 웹 서비스 프록시는 이 타이밍 문제를 제거하는 특수 구성을 포함합니다. 이 옵션은 데이터 일관성을 위해 서비스 요청에 소요되는 시간이 증가하므로 기본적으로 사용되지 않습니다. 이 옵션을 활성화하려면 .INI 파일(Windows의 경우) 또는 .SH 파일(Linux의 경우)에 속성을 추가해야 합니다.

단계

1. 다음 중 하나를 수행합니다.
   - Windows: appserver64.ini 파일을 열고 Dload-balance.enabled=true 속성을 추가합니다.

     예: ``vmarg.7=-Dload-balance.enabled=true’

   - Linux: webserver.sh 파일을 열고 Dload-balance.enabled=true 속성을 추가합니다.

     예: debug_start_options="-dload-balance.enabled=true""
2. 변경 사항을 저장합니다.
3. Webserver 서비스를 다시 시작하여 변경 사항을 적용합니다.

기호 **HTTPS**를 비활성화합니다

기호 명령(기본 설정)을 사용하지 않도록 설정하고 RPC(원격 프로시저 호출)를 통해 명령을 보낼 수 있습니다. 이 설정은 wsconfig.xml 파일에서 변경할 수 있습니다.

기본적으로 웹 서비스 프록시는 SANtricity OS 버전 08.40 이상을 실행하는 모든 E2800 시리즈 및 E5700 시리즈 스토리지 시스템에 대해 HTTPS를 통해 기호 명령을 보냅니다. HTTPS를 통해 전송되는 기호 명령이 스토리지 시스템에 인증됩니다. 필요한 경우 HTTPS 기호 지원을 사용하지 않도록 설정하고 RPC를 통해 명령을 보낼 수 있습니다. RPC를 통한 기호가 구성될 때마다 스토리지 시스템에 대한 모든 수동 명령이 인증 없이 설정됩니다.

RPC를 통한 기호가 사용되는 경우 웹 서비스 프록시는 기호 관리 포트가 비활성화된 시스템에 연결할 수 없습니다.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. 'devic고객전략' 항목에서 'eudemgt Preferred' 값을 rpcOnly로 바꿉니다.

   예를 들면 다음과 같습니다.

   '< env key="devicemgt.symbolclientStrategy">rpcOnly</env>'
3. 파일을 저장합니다.

오리진 간 리소스 공유를 구성합니다

CORS(Cross-origin Resource Sharing)를 구성할 수 있습니다. CORS는 다른 오리진의 서버에서 선택한 리소스에 액세스할 수 있는 권한을 가지도록 하나의 오리진에서 실행되는 웹 애플리케이션을 제공하는 추가 HTTP 헤더를 사용하는 메커니즘입니다.

CORS는 작업 디렉토리에 있는 cors.cfg 파일에 의해 처리됩니다. CORS 구성은 기본적으로 열려 있으므로 도메인 간 액세스는 제한되지 않습니다.

구성 파일이 없으면 CORS가 열려 있는 것입니다. 그러나 cors.cfg 파일이 있으면 이 파일이 사용됩니다. cors.cfg 파일이 비어 있으면 CORS 요청을 할 수 없습니다.

단계

1. 작업 디렉터리에 있는 cors.cfg 파일을 엽니다.
2. 파일에 원하는 선을 추가합니다.

   CORS 구성 파일의 각 줄은 일치시킬 정규식 패턴입니다. 원점 머리글은 cors.cfg 파일의 선과 일치해야 합니다. 오리진 헤더와 일치하는 회선 패턴이 있으면 요청이 허용됩니다. 호스트 요소뿐만 아니라 전체 원점을 비교합니다.

3. 파일을 저장합니다.

요청은 호스트 및 다음과 같은 프로토콜에 따라 일치됩니다.

- localhost를 모든 프로토콜--"\ * localhost *"와 일치시킵니다
- HTTPS에 대해서만 localhost 일치 --'https://localhost*`

SANtricity 웹 서비스 프록시를 제거합니다

웹 서비스 프록시 및 Unified Manager를 제거하려면 프록시를 설치하는 데 사용한 방법에 관계없이 모든 모드(그래픽, 콘솔, 자동 또는 RPM 파일)를 사용할 수 있습니다.

그래픽 모드 제거

Windows 또는 Linux의 그래픽 모드에서 제거를 실행할 수 있습니다. 그래픽 모드에서 프롬프트는 Windows 스타일 인터페이스에 나타납니다.

단계

1. 다음과 같이 Windows 또는 Linux에 대한 제거를 실행합니다.
   - Windows — uninstall_web_services_proxy 제거 파일이 들어 있는 디렉터리로 이동합니다. 기본 디렉토리는 C:/Program Files/NetApp/SANtricity Web Services Proxy/ 입니다. uninstall_web_services_proxy.exe를 두 번 클릭합니다.

     또는 제어판 [프로그램 > 프로그램 제거] 메뉴로 이동한 다음 "NetApp SANtricity 웹 서비스 프록시"를 선택합니다.

   - Linux — 웹 서비스 프록시 제거 파일이 들어 있는 디렉터리로 이동합니다. 기본 디렉토리는 + "/opt/netapp/sSANtricity_web_services_proxy/uninstall_web_services_proxy"에 있습니다
2. 다음 명령을 실행합니다.

uninstall_web_services_proxy-i gui

SANtricity 웹 서비스 프록시 시작 화면이 나타납니다.

3. 제거 대화 상자에서 * 제거 * 를 클릭합니다.

   설치 제거 프로그램 진행 표시줄이 나타나고 진행 상태가 표시됩니다.

4. 제거 완료 메시지가 나타나면 * 완료 * 를 클릭합니다.

콘솔 모드 제거

Windows 또는 Linux의 콘솔 모드에서 제거를 실행할 수 있습니다. 콘솔 모드에서는 터미널 창에 프롬프트가 나타납니다.

단계

1. uninstall_web_services_proxy 디렉토리로 이동합니다.
2. 다음 명령을 실행합니다.

   uninstall_web_services_proxy-i console을 선택합니다

   제거 프로세스가 시작됩니다.

3. 제거가 완료되면 * Enter * 를 눌러 설치 프로그램을 종료합니다.

자동 모드 제거

Windows 또는 Linux의 경우 자동 모드에서 제거를 실행할 수 있습니다. 무음 모드에서는 터미널 창에 반환 메시지나 스크립트가 나타나지 않습니다.

단계

1. uninstall_web_services_proxy 디렉토리로 이동합니다.
2. 다음 명령을 실행합니다.

   'uninstall_web_services_proxy-i silent

   제거 프로세스가 실행되지만 터미널 창에는 반환 메시지 또는 스크립트가 나타나지 않습니다. 웹 서비스 프록시를 성공적으로 제거한 후 터미널 창에 명령 프롬프트가 나타납니다.

rpm 명령 제거**(Linux**만 해당**)**

RPM 명령을 사용하여 Linux 시스템에서 웹 서비스 프록시를 제거할 수 있습니다.

단계

1. 터미널 창을 엽니다.
2. 다음 명령줄을 입력합니다.

   rpm -e sSANtricity_webservices를 나타냅니다

제거 프로세스는 원본 설치에 포함되지 않은 파일을 남겨둘 수 있습니다. 이러한 파일을 수동으로 삭제하여 웹 서비스 프록시를 완전히 제거합니다.

SANtricity 웹 서비스 프록시에서 사용자 액세스를 관리합니다

보안을 위해 웹 서비스 API 및 Unified Manager에 대한 사용자 액세스를 관리할 수 있습니다.

액세스 관리 개요

액세스 관리에는 역할 기반 로그인, 암호 암호화, 기본 인증 및 LDAP 통합이 포함됩니다.

역할 기반 액세스

역할 기반 액세스 제어(RBAC)는 사전 정의된 사용자를 역할에 연결합니다. 각 역할은 특정 수준의 기능에 권한을 부여합니다.

다음 표에서는 각 역할에 대해 설명합니다.

역할	설명
security.admin을 선택합니다	SSL 및 인증서 관리.
storage.admin을 선택합니다	스토리지 시스템 구성에 대한 전체 읽기/쓰기 액세스
Storage.monitor를 선택합니다	스토리지 시스템 데이터를 볼 수 있는 읽기 전용 액세스 권한
support.admin을 클릭합니다	스토리지 시스템의 모든 하드웨어 리소스에 액세스하고 AutoSupport(ASUP) 검색 등의 작업을 지원합니다.

기본 사용자 계정은 users.properties 파일에 정의되어 있습니다. users.properties 파일을 직접 수정하거나 Unified Manager의 액세스 관리 기능을 사용하여 사용자 계정을 변경할 수 있습니다.

다음 표에서는 Web Services 프록시에 사용할 수 있는 사용자 로그인을 보여 줍니다.

사전 정의된 사용자 로그인	설명
관리자	모든 기능에 액세스할 수 있고 모든 역할을 포함하는 슈퍼 관리자. Unified Manager의 경우 처음 로그인할 때 암호를 설정해야 합니다.
스토리지	관리자는 모든 스토리지 프로비저닝을 담당합니다. 이 사용자는 storage.admin, support.admin, storage.monitor 등의 역할을 수행합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
보안	보안 구성을 담당하는 사용자입니다. 이 사용자에게는 security.admin 및 storage.monitor 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.

사전 정의된 사용자 로그인	설명
지원	하드웨어 리소스, 장애 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자에게는 support.admin 및 storage.monitor 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
모니터링	시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자는 storage.monitor 역할만 포함합니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
RW(기존 어레이의 경우)	RW(읽기/쓰기) 사용자에게는 storage.admin, support.admin, storage.monitor 등의 역할이 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.
RO(기존 스토리지의 경우)	ro(읽기 전용) 사용자에게는 storage.monitor 역할만 포함됩니다. 이 계정은 암호를 설정할 때까지 비활성화됩니다.

암호 암호화

각 암호에 기존 SHA256 암호 인코딩을 사용하여 추가 암호화 프로세스를 적용할 수 있습니다. 이 추가 암호화 프로세스는 각 SHA256 해시 암호화에 대해 각 암호(SALT)에 임의의 바이트 세트를 적용합니다. 새로 만든 모든 암호에 소금된 SHA256 암호화가 적용됩니다.

Web Services Proxy 3.0 릴리스 이전에는 SHA256 해싱만 사용하여 암호를 암호화했습니다. 기존 SHA256 해시 전용 암호화된 암호는 이 인코딩을 유지하며 users.properties 파일에서 여전히 유효합니다. 그러나 SHA256 해시 전용 암호화 암호는 SHA256 암호화를 사용하는 암호만큼 안전하지 않습니다.

기본 인증

기본적으로 기본 인증은 활성화되어 있으며, 이는 서버가 기본 인증 과제를 반환함을 의미합니다. 이 설정은 wsconfig.xml 파일에서 변경할 수 있습니다.

LDAP를 지원합니다

분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 응용 프로그램 프로토콜인 LDAP(Lightweight Directory Access Protocol)가 웹 서비스 프록시에 대해 활성화됩니다. LDAP 통합을 통해 사용자 인증 및 역할을 그룹에 매핑할 수 있습니다.

LDAP 기능 구성에 대한 자세한 내용은 Unified Manager 인터페이스 또는 대화형 API 설명서의 LDAP 섹션에서 구성 옵션을 참조하십시오.

사용자 액세스를 구성합니다

암호에 추가 암호화를 적용하고 기본 인증을 설정하며 역할 기반 액세스를 정의하여 사용자 액세스를 관리할 수 있습니다.

암호에 추가 암호화를 적용합니다

최고 수준의 보안을 위해 기존 SHA256 암호 인코딩을 사용하여 암호에 추가 암호화를 적용할 수 있습니다.

이 추가 암호화 프로세스는 각 SHA256 해시 암호화에 대해 각 암호(SALT)에 임의의 바이트 세트를 적용합니다. 새로 만든 모든 암호에 소금된 SHA256 암호화가 적용됩니다.

단계

1. 다음 위치에 있는 users.properties 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\Data\config입니다
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy/data/config
2. 암호화된 암호를 일반 텍스트로 다시 입력합니다.
3. 'ecurepasswds' 명령줄 유틸리티를 실행하여 암호를 다시 암호화하거나 간단히 웹 서비스 프록시를 다시 시작합니다. 이 유틸리티는 웹 서비스 프록시의 루트 설치 디렉터리에 설치됩니다.

> 또는 Unified Manager를 통해 암호를 편집할 때마다 로컬 사용자 암호를 솔트 및 해시 할 수 있습니다.

기본 인증을 구성합니다

기본적으로 기본 인증이 활성화되어 있으며 이는 서버가 기본 인증 과제를 반환함을 의미합니다. 필요한 경우 wsconfig.xml 파일에서 해당 설정을 변경할 수 있습니다.

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. 파일에서 FALSE(사용 안 함) 또는 TRUE(사용 가능)를 지정하여 다음 행을 수정합니다.

   예: "<env key="enable-basic-auth">true</env>"
3. 파일을 저장합니다.
4. Webserver 서비스를 다시 시작하여 변경 사항을 적용합니다.

역할 기반 액세스를 구성합니다

특정 기능에 대한 사용자 액세스를 제한하려면 각 사용자 계정에 대해 지정된 역할을 수정할 수 있습니다.

웹 서비스 프록시는 역할 기반 액세스 제어(RBAC)를 포함하며, 이 역할 기반 액세스 제어(RBAC)는 역할이 미리 정의된 사용자와 연결됩니다. 각 역할은 특정 수준의 기능에 권한을 부여합니다. users.properties 파일을 직접 수정하여 사용자 계정에 할당된 역할을 변경할 수 있습니다.

> Unified Manager에서 Access Management를 사용하여 사용자 계정을 변경할 수도 있습니다. 자세한 내용은 Unified Manager와 함께 제공되는 온라인 도움말을 참조하십시오.

단계

1. 다음 위치에 있는 users.properties 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\Data\config입니다
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy/data/config
2. 수정할 사용자 계정(스토리지, 보안, 모니터, 지원, RW, 또는 ro).

admin 사용자를 수정하지 마십시오. 모든 기능에 액세스할 수 있는 고급 사용자입니다.

3. 필요에 따라 지정된 역할을 추가하거나 제거합니다.

   역할은 다음과 같습니다.

   - Security.admin — SSL 및 인증서 관리.
   - storage.admin — 스토리지 시스템 구성에 대한 전체 읽기/쓰기 액세스 권한.
   - Storage.monitor — 스토리지 시스템 데이터를 볼 수 있는 읽기 전용 액세스입니다.
   - support.admin — 스토리지 시스템의 모든 하드웨어 리소스에 액세스하고 AutoSupport(ASUP) 검색과 같은 작업을 지원합니다.

     관리자를 포함한 모든 사용자는 storage.monitor 역할이 필요합니다.

4. 파일을 저장합니다.

SANtricity 웹 서비스 프록시에서 보안 및 인증서를 관리합니다

웹 서비스 프록시에서 보안을 위해 SSL 포트 지정을 지정하고 인증서를 관리할 수 있습니다. 인증서는 클라이언트와 서버 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.

SSL을 활성화합니다

웹 서비스 프록시는 보안을 위해 SSL(Secure Sockets Layer)을 사용하며, 이 보안 계층은 설치 중에 활성화됩니다. wsconfig.xml 파일에서 SSL 포트 지정을 변경할 수 있습니다.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. 다음 예제와 같이 SSL 포트 번호를 추가하거나 변경합니다.

```
<sslport clientauth="request">8443</sslport>
```

결과

SSL이 구성된 상태로 서버를 시작하면 서버는 키 저장소 및 신뢰 저장소 파일을 찾습니다.

- 서버가 키 저장소를 찾지 못할 경우 서버는 첫 번째로 검색된 비루프백 IPv4 주소의 IP 주소를 사용하여 키 저장소를 생성한 다음 자체 서명된 인증서를 키 저장소에 추가합니다.
- 서버에서 truststore를 찾지 못했거나 truststore를 지정하지 않은 경우 서버는 키 저장소를 truststore로 사용합니다.

인증서 확인을 건너뜁니다

보안 연결을 지원하기 위해 웹 서비스 프록시는 자체 신뢰할 수 있는 인증서에 대해 스토리지 시스템 인증서를

검증합니다. 필요한 경우 스토리지 시스템에 접속하기 전에 프록시에서 해당 확인을 바이패스하도록 지정할 수 있습니다.

시작하기 전에

- 모든 스토리지 시스템 접속이 안전해야 합니다.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. 다음 예와 같이 trust.all.arrays 항목에 true를 입력합니다.

```
<env key="trust.all.arrays">true</env>
```

3. 파일을 저장합니다.

호스트 관리 인증서를 생성하고 가져옵니다

인증서는 클라이언트와 서버 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다. 웹 서비스 프록시가 설치된 호스트 시스템에 대한 CA(인증 기관) 인증서를 생성하고 가져오려면 API 끝점을 사용합니다.

호스트 시스템의 인증서를 관리하려면 API를 사용하여 다음 작업을 수행합니다.

- 호스트 시스템에 대한 인증서 서명 요청(CSR)을 생성합니다.
- CSR 파일을 CA로 보낸 다음 인증서 파일을 보낼 때까지 기다립니다.
- 서명된 인증서를 호스트 시스템으로 가져옵니다.

Unified Manager 인터페이스에서 인증서를 관리할 수도 있습니다. 자세한 내용은 Unified Manager에서 제공되는 온라인 도움말을 참조하십시오.

단계

1. 에 로그인합니다 "대화형 API 설명서".
2. 오른쪽 상단의 드롭다운 메뉴로 이동한 다음 * v2 * 를 선택합니다.
3. Administration * 링크를 확장하고 * /certificates * 엔드포인트로 스크롤합니다.
4. CSR 파일 생성:
   a. POST:/certificates * 를 선택한 다음 * try it out * 을 선택합니다.

      웹 서버가 자체 서명된 인증서를 재생성합니다. 그런 다음 필드에 정보를 입력하여 공통 이름, 조직, 조직 단위, 대체 ID 및 CSR 생성에 사용되는 기타 정보를 정의할 수 있습니다.

   b. 예제 값* 창에 필요한 정보를 추가하여 유효한 CA 인증서를 생성한 다음 명령을 실행합니다.

POST:/certificates * 또는 * POST:/certificates/reset * 을 다시 호출하지 마십시오. 또는 CSR을 다시 생성해야 합니다. POST:/certificates * 또는 * POST:/certificates/reset * 를 호출하면 새 개인 키로 자체 서명된 새 인증서가 생성됩니다. 서버에서 개인 키를 마지막으로 다시 설정하기 전에 생성된 CSR을 보내면 새 보안 인증서가 작동하지 않습니다. 새 CSR을 생성하고 새 CA 인증서를 요청해야 합니다.

c. get:/certificates/server* 끝점을 실행하여 현재 인증서 상태가 **POST:/certificates** 명령에서 추가된 정보와 함께 자체 서명된 인증서인지 확인합니다.

   서버 인증서(별칭으로 "jetty"로 표시됨)는 현재 자체 서명되어 있습니다.

d. POST:/certificates/export * 끝점을 확장하고 * try it * 를 선택한 다음 CSR 파일의 파일 이름을 입력하고 * Execute * 를 클릭합니다.

5. fileUrl을 복사하여 새 브라우저 탭에 붙여 넣어 CSR 파일을 다운로드한 다음 유효한 CA로 보내 새 웹 서버 인증서 체인을 요청합니다.
6. CA에서 새 인증서 체인을 발급하는 경우 인증서 관리자 도구를 사용하여 루트, 중간 및 웹 서버 인증서를 분리한 다음 웹 서비스 프록시 서버로 가져옵니다.
   a. POST:/sslconfig/server * 끝점을 확장하고 * try it out * 을 선택합니다.
   b. alias * 필드에 CA 루트 인증서 이름을 입력합니다.
   c. 치환 MainServerCertificate* 필드에서 * false * 를 선택합니다.
   d. 새 CA 루트 인증서를 찾아 선택합니다.
   e. Execute * 를 클릭합니다.
   f. 인증서 업로드에 성공했는지 확인합니다.
   g. CA 중간 인증서에 대해 CA 인증서 업로드 절차를 반복합니다.
   h. 새 웹 서버 보안 인증서 파일에 대해 인증서 업로드 절차를 반복합니다. 이 단계를 제외하고, * 치환 MainServerCertificate * 드롭다운에서 * true * 를 선택합니다.
   i. 웹 서버 보안 인증서 가져오기가 성공했는지 확인합니다.
   j. 키 저장소에서 새 루트, 중간 및 웹 서버 인증서를 사용할 수 있는지 확인하려면 * get:/certificates/server * 를 실행합니다.
7. POST:/certificates/reload * 엔드포인트를 선택하여 확장한 다음 * try it out * 을 선택합니다. 두 컨트롤러를 모두 재시작할지 묻는 메시지가 나타나면 * false * 를 선택합니다. ("참"은 이중 어레이 컨트롤러의 경우에만 적용됩니다.) Execute * 를 클릭합니다.

   /certificates/reload* 끝점은 대개 성공적인 http 202 응답을 반환합니다. 그러나 웹 서버 truststore 및 keystore 인증서를 다시 로드하면 API 프로세스와 웹 서버 인증서 다시 로드 프로세스 간에 경쟁 조건이 생성됩니다. 드물지만 웹 서버 인증서를 다시 로드하면 API 처리 성능을 능가할 수 있습니다. 이 경우 성공적으로 완료되었더라도 다시 로드가 실패한 것으로 나타납니다. 이 경우 다음 단계를 계속 진행하십시오. 다시 로드가 실제로 실패한 경우 다음 단계도 실패합니다.

8. 웹 서비스 프록시에 대한 현재 브라우저 세션을 닫고 새 브라우저 세션을 연 다음 웹 서비스 프록시에 대한 새로운 보안 브라우저 연결을 설정할 수 있는지 확인합니다.

   익명 또는 개인 탐색 세션을 사용하면 이전 탐색 세션에서 저장된 데이터를 사용하지 않고 서버에 대한 연결을 열 수 있습니다.

로그인 잠금 기능

REST API를 통해서만 구성 가능하며 내장 및 프록시 웹 서비스에 대한 로그인 시도 횟수를 제한할 수 있습니다. 설정에 따라 웹 서비스에 대한 로그인 시도 횟수가 초과되면 잠금 기능이 활성화됩니다.

단계

1. 에 로그인합니다 "대화형 API 설명서".
2. 오른쪽 상단의 드롭다운 메뉴로 이동한 다음 * v2 * 를 선택합니다.
3. get:/settings/lockout * 끝점을 클릭하여 잠금 설정을 가져옵니다.
4. POST:/settings/lockout * 끝점을 클릭한 다음 * Try it out * 을 클릭하여 잠금 설정을 구성합니다.

SANtricity 웹 서비스 프록시를 사용하여 스토리지 시스템을 관리합니다

네트워크에서 스토리지 시스템을 관리하려면 먼저 스토리지 시스템을 검색한 다음 관리 목록에 추가해야 합니다.

스토리지 시스템을 검색합니다

자동 검색을 설정하거나 스토리지 시스템을 수동으로 검색할 수 있습니다.

스토리지 시스템을 자동으로 검색합니다

wsconfig.xml 파일의 설정을 수정하여 네트워크에서 스토리지 시스템이 자동으로 검색되도록 지정할 수 있습니다. 기본적으로 IPv6 자동 검색은 사용되지 않고 IPv4는 사용하도록 설정됩니다.

스토리지 시스템을 추가하려면 관리 IP 또는 DNS 주소를 하나만 제공하면 됩니다. 경로가 구성되어 있지 않거나 경로가 구성되어 있고 회전 가능한 경우 서버가 모든 관리 경로를 자동으로 검색합니다.

> 초기 접속이 이루어진 후 컨트롤러 구성에서 스토리지 시스템을 자동으로 검색하기 위해 IPv6 프로토콜을 사용하려고 하면 프로세스가 실패할 수 있습니다. 스토리지 시스템에서 IP 주소 전달 또는 IPv6를 사용하는 동안 문제가 발생했지만 서버에서 활성화되어 있지 않은 경우 이러한 오류가 발생할 수 있습니다.

시작하기 전에

IPv6 검색 설정을 활성화하기 전에 스토리지 시스템에 대한 IPv6 연결을 지원하는 인프라가 모든 연결 문제를 완화하는지 확인하십시오.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. 자동 검색 문자열에서 원하는 대로 설정을 true에서 false로 변경합니다. 다음 예를 참조하십시오.

```
<env key="autodiscover.ipv6.enable">true</env>
```

서버가 주소로 라우팅할 수 있도록 경로가 구성되었지만 구성되지 않은 경우 간헐적 연결 오류가 발생합니다. 호스트에서 IP 주소를 라우팅할 수 있도록 설정할 수 없는 경우 자동 검색을 해제합니다('false'로 설정 변경).

3. 파일을 저장합니다.

API 엔드포인트를 사용하여 스토리지 시스템을 검색하고 추가합니다

API 엔드포인트를 사용하여 스토리지 시스템을 검색하고 관리 대상 목록에 추가할 수 있습니다. 이 절차를 수행하면 스토리지 시스템과 API 간에 관리 접속이 생성됩니다.

이 작업에서는 REST API를 사용하여 스토리지 시스템을 검색 및 추가하는 방법을 설명합니다. 그러면 대화형 API 설명서에서 이러한 시스템을 관리할 수 있습니다. 하지만 대신 사용하기 쉬운 인터페이스를 제공하는 Unified Manager에서 스토리지 시스템을 관리할 수 있습니다. 자세한 내용은 Unified Manager와 함께 제공되는 온라인 도움말을 참조하십시오.

시작하기 전에

SANtricity 버전 11.30 이상이 있는 스토리지 시스템의 경우 SANtricity 시스템 관리자 인터페이스에서 기호에 대한 기존 관리 인터페이스를 활성화해야 합니다. 그렇지 않으면 검색 엔드포인트가 실패합니다. System Manager를 열고 설정 [시스템 > 추가 설정 > 관리 인터페이스 변경] 메뉴로 이동하여 이 설정을 찾을 수 있습니다.

단계

1. 에 로그인합니다 "대화형 API 설명서".
2. 다음과 같이 스토리지 시스템을 검색합니다.
   a. API 설명서의 드롭다운에서 * V2 * 를 선택한 다음 * Storage-Systems * 범주를 확장합니다.
   b. POST:/discovery * 끝점을 클릭한 다음 * try it * 를 클릭합니다.
   c. 표에 설명된 대로 매개 변수를 입력합니다.

시작 IP입니다 endIP
네트워크에 있는 하나 이상의 스토리지 시스템에 대한 시작 및 끝 IP 주소 범위로 문자열을 바꿉니다.
사용 에이전트
이 값을 다음 중 하나로 설정합니다. • True = 네트워크 스캔에 대역내 에이전트를 사용합니다. • False = 네트워크 스캔에 대역내 에이전트를 사용하지 않습니다.
연결 시간 초과
연결 시간이 초과되기 전에 스캔에 허용되는 초를 입력합니다.

maxPortsToUse 를 선택합니다
네트워크 스캔에 사용되는 최대 포트 수를 입력합니다.

d. Execute * 를 클릭합니다.

API 작업은 사용자 프롬프트 없이 실행됩니다.

검색 프로세스는 백그라운드에서 실행됩니다.

a. 코드가 202를 반환하는지 확인합니다.

b. 응답 본문 * 에서 RequestId에 대해 반환된 값을 찾습니다. 다음 단계에서 결과를 보려면 요청 ID가 필요합니다.

3. 다음과 같이 검색 결과를 봅니다.

a. get:/discovery * 끝점을 클릭한 다음 * try it out * 을 클릭합니다.

b. 이전 단계의 요청 ID를 입력합니다. 요청 ID * 를 비워 두면 끝점의 기본값은 마지막으로 실행된 요청 ID로 설정됩니다.

c. Execute * 를 클릭합니다.

d. 코드가 200을 반환하는지 확인합니다.

e. 응답 본문에서 요청 ID와 storageSystems의 문자열을 찾습니다. 문자열은 다음 예제와 비슷합니다.

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. WWN, 레이블 및 IP 주소 값을 기록합니다. 다음 단계를 위해 필요한 것입니다.

4. 다음과 같이 스토리지 시스템을 추가합니다.

a. POST:/storage-system* 끝점을 클릭한 다음 * try it out * 을 클릭합니다.

b. 표에 설명된 대로 매개 변수를 입력합니다.

ID입니다

이 스토리지 시스템의 고유한 이름을 입력하십시오. 레이블(GET:/DISCOVERY의 응답에 표시됨)을 입력할 수 있지만 이름은 사용자가 선택한 문자열이 될 수 있습니다. 이 필드에 값을 제공하지 않으면 웹 서비스에서 자동으로 고유 식별자를 할당합니다.
제어 주소
GET:/DISCOVERY 응답에 표시된 IP 주소를 입력합니다. 이중 컨트롤러의 경우 IP 주소를 쉼표로 구분합니다. 예를 들면 다음과 같습니다. ""IP 주소 1", "IP 주소 2""
검증
"true"를 입력하면 웹 서비스가 스토리지 시스템에 연결될 수 있다는 확인 메시지를 받을 수 있습니다.
암호
스토리지 시스템의 관리 암호를 입력합니다.
WWN입니다
스토리지 시스템의 WWN을 입력합니다(GET:/DISCOVERY의 응답에 표시됨).

c. 전체 문자열 집합이 다음 예제와 비슷하게 하려면 ""enableTrace":true" 뒤에 있는 모든 문자열을 제거합니다.

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Execute * 를 클릭합니다.

e. 코드 응답이 201인지 확인합니다. 이는 끝점이 성공적으로 실행되었음을 나타냅니다.

Post:/storage-systems * 엔드포인트가 대기열에 추가됩니다. 다음 단계에서 * get:/storage-systems * 끝점을 사용하여 결과를 볼 수 있습니다.

5. 다음과 같이 목록 추가를 확인합니다.

a. get:/storage-system * 끝점을 클릭합니다.

매개 변수가 필요하지 않습니다.

b. Execute * 를 클릭합니다.

c. 코드 응답이 200인지 확인합니다. 이는 끝점이 성공적으로 실행되었음을 나타냅니다.

d. 응답 본문에서 스토리지 시스템 세부 정보를 찾습니다. 반환된 값은 다음 예제와 같이 관리되는 스토리지 목록에 성공적으로 추가되었음을 나타냅니다.


```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


관리형 스토리지 시스템의 수를 스케일업할 수 있습니다

기본적으로 API는 최대 100개의 스토리지 시스템을 관리할 수 있습니다. 더 많은 를 관리해야 하는 경우에는 서버의 메모리 요구 사항을 높여야 합니다.

서버는 512MB의 메모리를 사용하도록 설정되어 있습니다. 네트워크에 100개의 추가 스토리지 시스템이 추가될 때마다 이 숫자에 250MB를 추가하십시오. 물리적으로 보유한 것보다 더 많은 메모리를 추가하지 마십시오. 운영 체제 및 기타 응용 프로그램에 충분한 추가 공간을 제공합니다.

기본 캐시 크기는 8,192개의 이벤트입니다. MEL 이벤트 캐시의 대략적인 데이터 사용량은 8,192개 이벤트마다 1MB입니다. 따라서 기본값을 유지함으로써 스토리지 시스템의 캐시 사용량을 약 1MB로 설정해야 합니다.

메모리 외에도 프록시는 각 스토리지 시스템에 대해 네트워크 포트를 사용합니다. Linux와 Windows에서는 네트워크 포트를 파일 핸들로 고려합니다. 보안 조치로서 대부분의 운영 체제는 프로세스 또는 사용자가 한 번에 열 수 있는 열린 파일 핸들 수를 제한합니다. 특히 열린 TCP 연결이 파일 처리인 Linux 환경에서는 웹 서비스 프록시가 이 제한을 쉽게 초과할 수 있습니다. 픽스는 시스템에 따라 달라지므로 이 값을 올리는 방법은 운영 체제 설명서를 참조하십시오.

단계

1. 다음 중 하나를 수행합니다.

- Windows에서 appserver64.init 파일로 이동합니다. 'vmarg.3=-Xmx512M' 줄을 찾습니다
- Linux의 경우 webserver.sh 파일로 이동합니다. "java_options="-Xmx512M" 줄을 찾습니다

2. 메모리를 늘리려면 512를 원하는 메모리(MB)로 바꾸십시오.
3. 파일을 저장합니다.

SANtricity 웹 서비스 프록시 통계에 대한 자동 폴링을 관리합니다

검색된 스토리지 시스템의 모든 디스크 및 볼륨 통계에 대한 자동 폴링을 구성할 수 있습니다.

통계 개요

통계는 스토리지 시스템의 데이터 수집 속도 및 성능에 대한 정보를 제공합니다.

웹 서비스 프록시는 다음과 같은 유형의 통계에 대한 액세스를 제공합니다.

- raw statistics — 데이터 수집 시점의 데이터 지점에 대한 총 카운터입니다. 원시 통계는 총 읽기 작업 또는 총 쓰기 작업에 사용할 수 있습니다.
- 분석된 통계 — 간격에 대한 계산된 정보입니다. 분석된 통계의 예로는 초당 읽기 입출력 작업(IOPS) 또는 쓰기 처리량이 있습니다.

원시 통계는 선형이므로 일반적으로 최소 2개의 수집된 데이터 포인트가 가용 데이터를 도출해야 합니다. 분석된 통계는 중요한 메트릭을 제공하는 원시 통계의 파생입니다. 원시 통계에서 파생될 수 있는 많은 값은 사용자의 편의를 위해 분석된 통계에서 사용 가능한 시점 형식으로 표시됩니다.

자동 폴링이 활성화되었는지 여부에 관계없이 원시 통계를 검색할 수 있습니다. URL 끝에 usecache=true 쿼리 문자열을 추가하여 마지막 폴에서 캐시된 통계를 검색할 수 있습니다. 캐시된 결과를 사용하면 통계 검색 성능이 크게 향상됩니다. 그러나 구성된 폴링 간격 캐시와 같거나 작은 속도로 여러 건의 통화가 동일한 데이터를 검색합니다.

통계 기능

웹 서비스 프록시는 지원되는 하드웨어 모델 및 소프트웨어 버전에서 원시 및 분석된 컨트롤러 및 인터페이스 통계를 검색할 수 있는 API 엔드포인트를 제공합니다.

원시 통계 **API**

- '/storage-systems/{system-id}/controller-statistics'
- '/storage-systems/{system-id}/drive-statistics/{디스크 ID 목록}'
- '/storage-systems/{system-id}/interface-statistics/{인터페이스 ID 목록}'
- '/storage-systems/{system-id}/volume-statistics/{볼륨 ID 목록}'

분석된 통계 **API**

- '/storage-systems/{id}/분석됨-controller-statistics/'
- '/storage-systems/{id}/분석됨-drive-statistics/{디스크 ID 목록}'
- '/storage-systems/{id}/분석됨-interface-statistics/{인터페이스 ID의 선택적 목록}'
- '/storage-systems/{id}/분석됨-volume-statistics/{볼륨 ID 목록}'

이러한 URL은 마지막 폴링에서 분석된 통계를 검색하며 폴링이 활성화된 경우에만 사용할 수 있습니다. 이러한 URL에는 다음과 같은 입력 출력 데이터가 포함됩니다.

- 초당 작업 수입니다
- 초당 메가바이트 단위의 처리량
- 응답 시간(밀리초)

이 계산은 가장 일반적인 스토리지 성능 측정인 통계 폴링 반복 간의 차이를 기반으로 합니다. 이러한 통계는 분석되지 않은 통계보다 선호됩니다.

> 시스템이 시작될 때 다양한 메트릭을 계산하는 데 사용할 이전 통계 수집이 없으므로 분석된 통계에는 데이터를 반환하기 위해 시작 후 최소 하나의 폴링 주기가 필요합니다. 또한 누적 카운터가 재설정되는 경우 다음 폴링 주기에 예측할 수 없는 데이터 수가 있습니다.

폴링 간격을 구성합니다

폴링 간격을 구성하려면 wsconfig.xml 파일을 수정하여 폴링 간격을 초 단위로 지정합니다.

> 통계가 메모리에 캐시되기 때문에 각 스토리지 시스템에 대해 약 1.5MB의 메모리 사용량이 증가할 수 있습니다.

시작하기 전에

- 스토리지 시스템은 프록시에서 검색되어야 합니다.

단계

1. 다음 위치에 있는 wsconfig.xml 파일을 엽니다.
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) --/opt/NetApp/SANtricity_web_services_proxy
2. '<env-entries>' 태그 안에 다음 줄을 추가합니다. 이 때 n은 폴링 요청 사이의 간격(초)입니다.

   ```
   <env key="stats.poll.interval">n</env>
   ```

   예를 들어, 60을 입력하면 60초 간격으로 폴링이 시작됩니다. 즉, 이전 폴링 기간이 완료된 후 60초 후에 시스템이 폴링을 시작하도록 요청합니다(이전 폴링 기간의 지속 시간과 상관 없음). 모든 통계는 검색된 정확한 시간에 타임스탬프로 표시됩니다. 시스템은 60초 계산의 기반이 되는 시간 스탬프 또는 시간 차이를 사용합니다.
3. 파일을 저장합니다.

SANtricity 웹 서비스 프록시를 사용하여 AutoSupport를 관리합니다

데이터를 수집한 AutoSupport(ASUP)를 구성하여 원격 문제 해결 및 문제 분석을 위해 해당 데이터를 기술 지원 부서에 자동으로 전송할 수 있습니다.

AutoSupport(ASUP) 개요

ASUP(AutoSupport) 기능은 수동 및 일정 기반의 기준에 따라 메시지를 NetApp에 자동으로 전송합니다.

각 AutoSupport 메시지는 로그 파일, 구성 데이터, 상태 데이터 및 성능 메트릭의 모음입니다. 기본적으로 AutoSupport는 다음 표에 나열된 파일을 매주 한 번씩 NetApp 지원 팀에 전송합니다.

파일 이름	설명
x-headers-data.txt	X-헤더 정보가 포함된 .txt 파일입니다.
manifest.xml	메시지의 내용을 자세히 설명하는 .xml 파일입니다.
arraydata.xml	클라이언트 영구 데이터 목록이 들어 있는 .xml 파일입니다.
appserver-config.txt	응용 프로그램 서버 구성 데이터가 포함된 .txt 파일입니다.
wsconfig.txt	웹 서비스 구성 데이터가 포함된 .txt 파일입니다.
host-info.txt	호스트 환경에 대한 정보가 포함된 .txt 파일입니다.
server-logs.7z	사용 가능한 모든 웹 서버 로그 파일을 포함하는 .7z 파일입니다.
client-info.txt	메서드 및 웹 페이지 적중 횟수와 같은 응용 프로그램별 카운터에 대한 임의의 키/값 쌍이 들어 있는 .txt 파일입니다.
webServices - profile.json	이러한 파일에는 Webservices 프로필 데이터와 Jersey 모니터링 통계 데이터가 포함되어 있습니다. 기본적으로 저지 모니터링 통계가 활성화됩니다. wsconfig.xml 파일에서 다음과 같이 활성화 및 비활성화할 수 있습니다. • Enable:(< env key="enable.jersey.statistics">true</env>) • 비활성화: `<env key="enable.jersey.statistics">false</env>'

AutoSupport를 구성합니다

AutoSupport는 설치 시 기본적으로 활성화되어 있지만, 이 설정을 변경하거나 전송 유형을 수정할 수 있습니다.

AutoSupport를 활성화 또는 비활성화합니다

AutoSupport 기능은 웹 서비스 프록시를 처음 설치하는 동안 활성화 또는 비활성화되지만 ASUPConfig 파일에서 해당 설정을 변경할 수 있습니다.

아래 단계에 설명된 대로 ASUPConfig.xml 파일을 통해 AutoSupport를 활성화하거나 비활성화할 수 있습니다. 또는 * 구성 * 및 * POST/ASUP * 를 사용하여 API를 통해 이 기능을 활성화 또는 비활성화한 다음 "참" 또는 "거짓"을 입력할 수 있습니다.

1. 작업 디렉터리에서 ASUPConfig.xml 파일을 엽니다.
2. <asupdata enable="Boolean_value" timestamp="timestamp">의 행을 찾습니다
3. TRUE(활성화) 또는 FALSE(비활성화)를 입력합니다. 예를 들면 다음과 같습니다.

```
<asupdata enabled="false" timestamp="0">
```

타임스탬프 항목이 불필요합니다.

4. 파일을 저장합니다.

AutoSupport 전달 방법을 구성합니다

AutoSupport 기능을 구성하여 HTTPS 또는 SMTP 배달 방법을 사용할 수 있습니다. HTTPS는 기본 전송 방법입니다.

1. 작업 디렉터리에서 ASUPConfig.xml 파일에 액세스합니다.
2. 문자열, "<delivery type="n">"에 표에 설명된 대로 1, 2 또는 3을 입력합니다.

값	설명
1	• HTTPS * (기본값) 전달 유형="1">

2	SMTP * — SMTP에 AutoSupport 전달 유형을 올바르게 구성하려면 다음 예와 같이 보낸 사람 및 받는 사람 사용자 이메일과 함께 SMTP 메일 서버 주소를 포함해야 합니다.
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

원격 볼륨 미러링

SANtricity 원격 스토리지 볼륨에 대해 알아보십시오

SANtricity ® 원격 스토리지 볼륨 기능을 사용하여 원격 스토리지 장치에서 로컬 E-Series 볼륨으로 직접 데이터를 가져올 수 있습니다. 이 기능은 장비 업그레이드 프로세스를 간소화하고, 비 E-Series 장치에서 E-Series 시스템으로 데이터를 이동할 수 있는 데이터 마이그레이션 기능을 제공합니다.

구성 개요

원격 스토리지 볼륨 기능은 선택된 하위 모델 ID에서 SANtricity System Manager에서 사용할 수 있습니다. 이 기능을

사용하려면 원격 스토리지 시스템과 E-Series 스토리지 시스템이 서로 통신하도록 구성해야 합니다.

다음 워크플로를 사용합니다.

1. "요건 및 제한 사항 검토".
2. "하드웨어를 구성합니다".
3. "원격 저장소 가져오기".

SANtricity 원격 저장소 볼륨은 현재 E4000 시스템에서 지원되지 않습니다.

자세한 내용을 확인하십시오

- 온라인 도움말: System Manager 사용자 인터페이스 또는 에서 사용할 수 있습니다 "SANtricity 소프트웨어 문서 사이트입니다".
- 원격 스토리지 볼륨 기능에 대한 자세한 기술 정보는 를 참조하십시오 "원격 스토리지 볼륨 기술 보고서".

SANtricity 원격 스토리지 볼륨 사용에 대한 요구 사항 및 제한 사항

원격 스토리지 볼륨 기능을 구성하기 전에 다음 요구 사항 및 제한 사항을 검토하십시오.

하드웨어 요구 사항

지원되는 프로토콜

원격 스토리지 볼륨 기능의 초기 릴리스의 경우 iSCSI 및 IPv4 프로토콜에서만 지원을 사용할 수 있습니다.

을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴" 원격 스토리지 볼륨 기능에 사용되는 호스트와 E-Series(대상) 어레이 간의 최신 지원 및 구성 정보를 확인할 수 있습니다.

수행할 수 있습니다

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. iSCSI 지원 인터페이스를 포함해야 합니다.

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. 하지만 가져오기를 시작한 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.

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.

생산 수입 준비

프로덕션을 가져오기 전에 테스트 또는 "dry run" 가져오기를 수행하여 스토리지 및 Fabric 구성이 올바른지 확인해야 합니다.

많은 변수가 가져오기 작업 및 완료 시간에 영향을 줄 수 있습니다. 프로덕션 가져오기가 성공하고 예상 기간을 가져오려면 이러한 테스트 가져오기를 사용하여 모든 연결이 예상대로 작동하고 가져오기 작업이 적절한 시간 내에 완료되는지 확인할 수 있습니다. 그런 다음 원하는 결과를 얻기 위해 조정을 수행한 후 생산 가져오기를 시작할 수 있습니다.

SANtricity 원격 스토리지 볼륨의 하드웨어를 구성합니다

E-Series 스토리지 시스템은 지원되는 iSCSI 프로토콜을 통해 원격 스토리지 시스템과 통신하도록 구성해야 합니다.

원격 스토리지 장치 및 **E-Series** 어레이를 구성합니다

SANtricity 시스템 관리자로 넘어가기 전에 원격 스토리지 볼륨 기능을 구성하려면 다음을 수행하십시오.

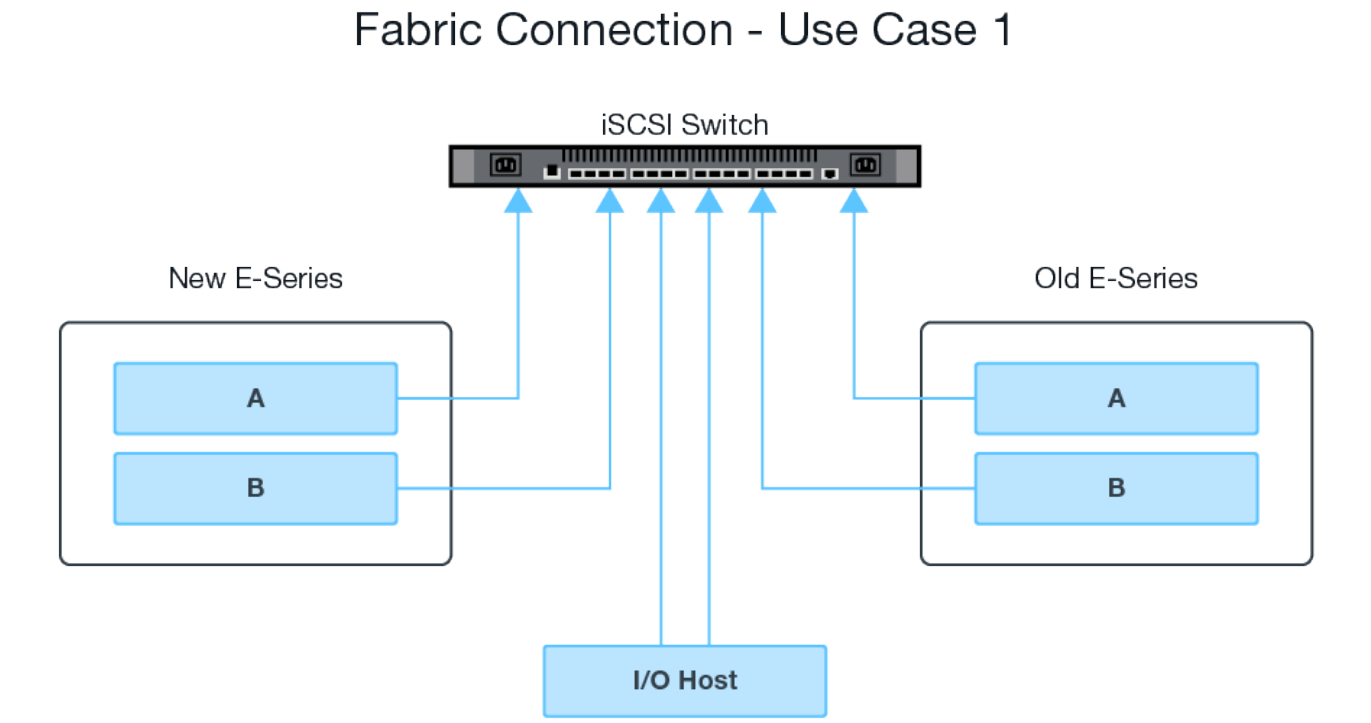
1. E-Series 시스템과 원격 스토리지 시스템 간에 케이블로 연결된 연결을 수동으로 설정하여 두 시스템이 iSCSI를 통해 통신하도록 구성할 수 있습니다.
2. E-Series 시스템과 원격 스토리지 시스템이 서로 통신할 수 있도록 iSCSI 포트를 구성합니다.
3. E-Series 시스템의 IQN을 가져옵니다.
4. E-Series 시스템이 원격 스토리지 시스템에 보이도록 설정합니다. 원격 스토리지 시스템이 E-Series 시스템인 경우 대상 E-Series 시스템의 IQN을 호스트 포트의 연결 정보로 사용하여 호스트를 생성합니다.
5. 호스트/애플리케이션에서 원격 스토리지 디바이스를 사용 중인 경우
   - 원격 스토리지 디바이스에 대한 입출력을 중지합니다.
   - 원격 스토리지 디바이스의 매핑을 해제/마운트 해제합니다.
6. 원격 스토리지 장치를 E-Series 스토리지 시스템에 정의된 호스트에 매핑합니다.
7. 매핑에 사용되는 디바이스의 LUN 번호를 가져옵니다.

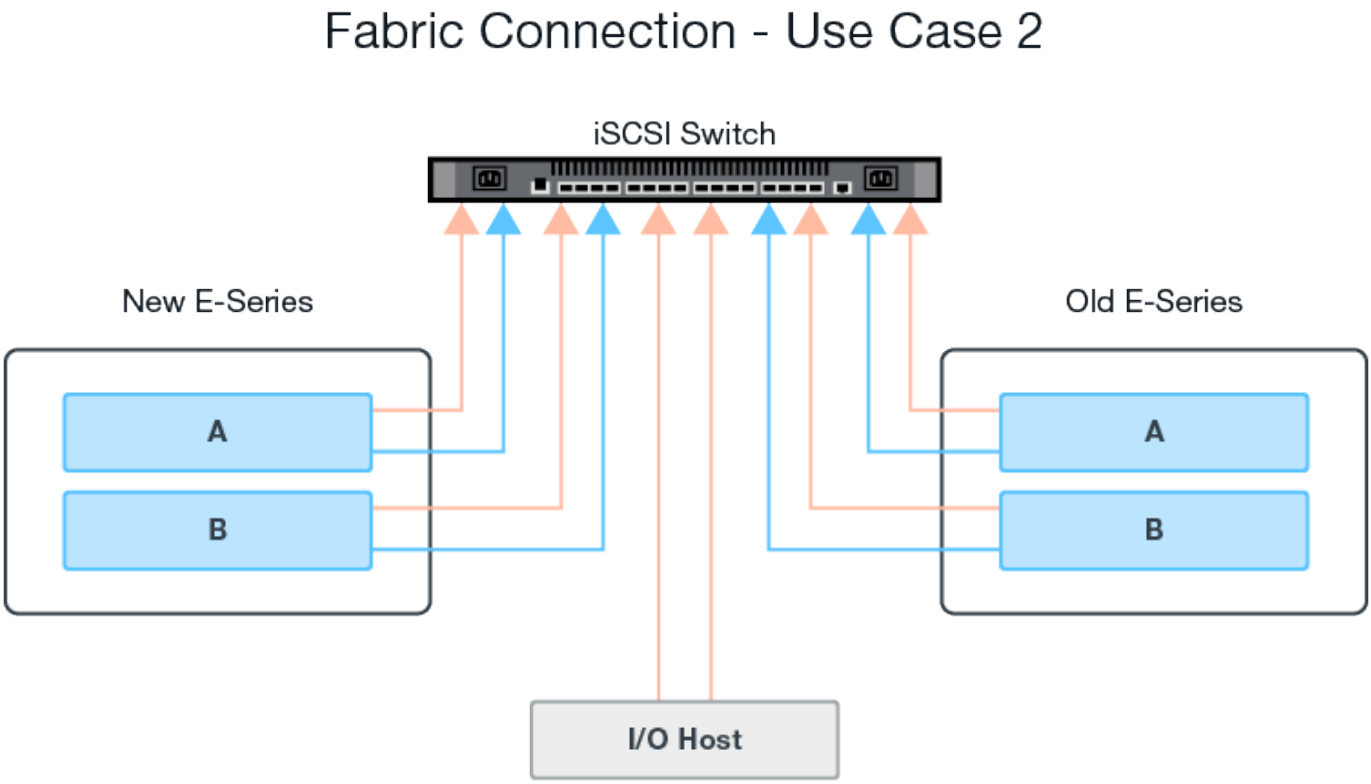
권장: 가져오기 프로세스를 시작하기 전에 원격 소스 볼륨을 백업합니다.

스토리지 어레이에 케이블을 연결합니다

설정 프로세스 중에 스토리지 어레이와 I/O 호스트를 iSCSI 호환 인터페이스에 케이블로 연결해야 합니다.

다음 다이어그램은 iSCSI 연결을 통해 원격 저장소 볼륨 작업을 수행하도록 시스템에 케이블을 연결하는 방법의 예를 제공합니다.





iSCSI 포트를 구성합니다

타겟(로컬 E-Series 스토리지 어레이)과 소스(원격 스토리지 어레이) 간의 통신을 보장하기 위해 iSCSI 포트를 구성해야 합니다.

iSCSI 포트는 서브넷에 따라 여러 방법으로 구성할 수 있습니다. 다음은 원격 스토리지 볼륨 기능과 함께 사용할 iSCSI 포트를 구성하는 방법에 대한 몇 가지 예입니다.

소스 **A**	소스 **B**	타겟 **A**	타겟 **B**
10.10.1.100.22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

소스 **A**	소스 **B**	타겟 **A**	타겟 **B**
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

SANtricity 원격 스토리지 볼륨의 원격 스토리지를 가져옵니다

원격 시스템에서 로컬 E-Series 스토리지 시스템으로 스토리지 가져오기를 시작하려면 SANtricity System Manager 사용자 인터페이스에서 원격 스토리지 가져오기 마법사를 사용합니다.

필요한 것

- E-Series 스토리지 시스템은 원격 스토리지 시스템과 통신하도록 구성해야 합니다. 을 참조하십시오 "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. 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 참조하십시오 "요구 사항 및 제한 사항".
- 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 작업 및 완료 시간에 영향을 줄 수 있으므로 먼저 더 작은 "테스트" 가져오기를 수행해야 합니다. 이 테스트를 사용하여 모든 연결이 예상대로 작동하는지, 가져오기 작업이 적절한 시간 내에 완료되는지 확인합니다.

단계

1. SANtricity 시스템 관리자에서 * 스토리지 > 원격 스토리지 * 를 클릭합니다.
2. 원격 저장소 가져오기 * 를 클릭합니다.

   원격 스토리지 가져오기 마법사가 표시됩니다.

3. 소스 구성 패널의 1a단계에서 연결 정보를 입력합니다.

   a. 이름 * 필드에 원격 저장 장치의 이름을 입력합니다.

   b. iSCSI 접속 속성 * 에서 원격 스토리지 디바이스에 대해 IQN, IP 주소 및 포트 번호(기본값 3260)를 입력합니다.

      다른 iSCSI 연결을 추가하려면 * + 다른 IP 주소 추가 * 를 클릭하여 원격 스토리지에 대한 추가 IP 주소를 포함합니다. 완료되면 * 다음 * 을 클릭합니다.

   Next(다음)를 클릭하면 Configure Source(소스 구성) 패널의 1b단계가 표시됩니다.

4. LUN * 필드에서 원격 스토리지 디바이스에 대해 원하는 소스 LUN을 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 '계속'을 입력한 다음 * 계속 * 을 클릭하여 작업을 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) 화면에서 지정된 원격 스토리지 디바이스, 타겟 및 가져오기 설정이 정확한지 확인합니다. 마침 * 을 클릭하여 원격 스토리지 생성을 완료합니다.

   다른 가져오기를 시작할지 묻는 다른 대화 상자가 열립니다.

7. 필요한 경우 * 예 * 를 클릭하여 다른 원격 스토리지 가져오기를 생성합니다. Yes(예)를 클릭하면 Configure Source(소스 구성) 패널의 1a단계로 돌아가서 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.

   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.

9. 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.

SANtricity 원격 스토리지 볼륨에 대한 가져오기 진행률을 관리합니다

가져오기 프로세스가 시작된 후 진행 상황을 확인하고 조치를 취할 수 있습니다.

각 가져오기 작업에 대해 작업 진행 중 페이지에는 완료율과 남은 예상 시간이 표시됩니다. 작업에는 가져오기 우선 순위 변경, 작업 중지 및 다시 시작, 작업 연결 해제 등이 있습니다.

홈 페이지(* 홈 > 진행 중인 작업 표시 *)에서 진행 중인 작업을 볼 수도 있습니다.

단계

1. SANtricity 시스템 관리자에서 원격 스토리지 페이지로 이동하여 * 작업 보기 * 를 선택합니다.

   작업 진행 중 대화 상자가 표시됩니다.

2. 필요한 경우 작업 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.
   - * Stop * (중지 *) – 원격 저장 장치에서 데이터 복사를 일시 중지하려면 * Stop * (중지 *)을 선택합니다. 가져오기 쌍 간의 관계는 그대로 유지되며 가져오기 작업을 계속할 준비가 되면 * Resume * 을 선택할 수 있습니다.
   - * Resume * – 중지된 위치에서 중지되거나 실패한 프로세스를 시작하려면 * Resume * 을 선택합니다. 그런 다음 Resume 작업에 우선 순위를 적용하고 * OK * 를 클릭합니다.

     재시작 작업은 처음부터 가져오기를 다시 시작하지 * 않습니다 *. 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.

SANtricity 원격 스토리지 볼륨에 대한 원격 스토리지 연결 설정을 수정합니다

설정 보기/편집 옵션을 통해 원격 저장소 구성에 대한 연결 설정을 편집, 추가 또는 삭제할 수 있습니다.

연결 속성을 변경하면 진행 중인 가져오기에 영향을 줍니다. 중단을 방지하려면 가져오기가 실행되지 않을 때만 연결 속성을 변경합니다.

단계

1. SANtricity 시스템 관리자의 원격 스토리지 화면에서 결과 목록 섹션 아래에서 원하는 원격 스토리지 객체를 선택합니다.
2. 설정 보기/편집 * 을 클릭합니다.

   Remote Storage Settings(원격 저장소 설정) 화면이 표시됩니다.

3. 연결 속성 * 탭을 클릭합니다.

원격 스토리지 가져오기에 대해 구성된 IP 주소 및 포트 설정이 표시됩니다.

4. 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 '삭제'를 입력한 다음 * 삭제 * 를 클릭하여 작업을 확인합니다. 원격 스토리지 객체 목록에서 연결이 제거됩니다.
5. 저장 * 을 클릭합니다.

   수정된 접속 설정이 원격 스토리지 객체에 적용됩니다.

SANtricity 원격 스토리지 볼륨의 원격 스토리지 객체를 제거합니다

가져오기가 완료된 후 로컬 디바이스와 원격 디바이스 간에 더 이상 데이터를 복사하지 않으려면 원격 스토리지 객체를 제거할 수 있습니다.

단계

1. 제거하려는 원격 스토리지 객체와 연결된 가져오기가 없는지 확인합니다.
2. SANtricity 시스템 관리자의 원격 스토리지 화면에서 결과 목록 섹션 아래에서 원하는 원격 스토리지 객체를 선택합니다.
3. 제거 * 를 클릭합니다.

   원격 스토리지 연결 제거 확인 대화 상자가 표시됩니다.

4. 'remove'를 입력한 다음 * Remove * 를 클릭하여 작업을 확인합니다.

   선택한 원격 스토리지 객체가 제거됩니다.

vCenter용 스토리지 플러그인

vCenter용 SANtricity 스토리지 플러그인에 대해 자세히 알아보십시오

vCenter용 SANtricity 스토리지 플러그인은 VMware vSphere 클라이언트 세션 내에서 E-Series 스토리지 어레이에 대한 통합 관리 기능을 제공합니다.

사용 가능한 작업

플러그인을 사용하여 다음 작업을 수행할 수 있습니다.

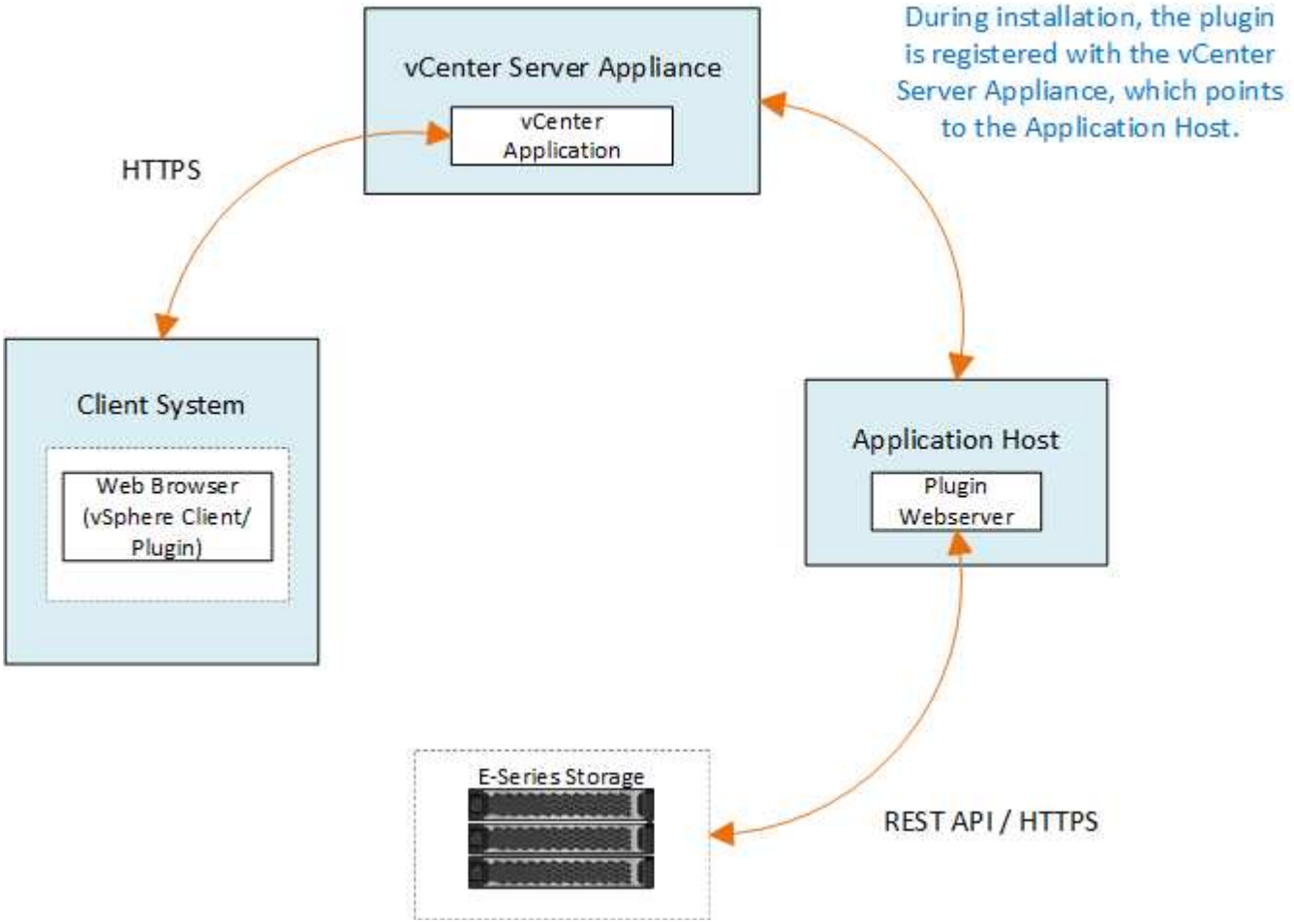
- 네트워크에서 검색된 스토리지 어레이를 보고 관리합니다.
- 여러 스토리지 시스템 그룹에 대해 배치 작업을 수행합니다.
- 소프트웨어 OS에서 업그레이드를 수행합니다.

- 한 스토리지 어레이에서 다른 스토리지 어레이로 설정을 가져옵니다.
- 볼륨, SSD 캐시, 호스트, 호스트 클러스터, 풀 구성 볼륨 그룹:
- 어레이에 대한 추가 관리 작업을 위해 System Manager 인터페이스를 시작합니다.

> 플러그인은 스토리지 어레이에 대한 각 컨트롤러에 내장되어 있는 System Manager 인터페이스를 직접 대체하는 것이 아닙니다. System Manager는 추가 관리 기능을 제공합니다. 필요한 경우 플러그인의 주 보기에서 스토리지 어레이를 선택한 다음 * Launch * 를 클릭하여 System Manager를 열 수 있습니다.

플러그인을 사용하려면 VMware 환경에 구축된 VMware vCenter Server Appliance와 플러그인 웹 서버를 설치하고 실행하기 위한 애플리케이션 호스트가 필요합니다.

vCenter 환경의 통신에 대한 자세한 내용은 다음 그림을 참조하십시오.



인터페이스 개요

플러그인에 로그인하면 기본 페이지가 * Manage - All * 로 열립니다. 이 페이지에서는 네트워크에서 검색된 모든 스토리지 어레이를 보고 관리할 수 있습니다.

탐색 사이드바

탐색 사이드바에 다음이 표시됩니다.

- * 관리 * — 네트워크에서 스토리지 어레이를 검색, 어레이에 대한 시스템 관리자 실행, 한 어레이에서 여러 어레이로

설정 가져오기, 어레이 그룹 관리, SANtricity OS 업그레이드 및 스토리지 용량 할당 등의 작업을 수행합니다.

- * 인증서 관리 * — 브라우저와 클라이언트 간 인증을 위해 인증서를 관리합니다.
- * Operations * — 한 어레이에서 다른 어레이로 설정을 가져오는 것과 같은 배치 작업의 진행률을 봅니다.

> 스토리지 배열의 상태가 최적이 아닌 경우 일부 작업을 사용할 수 없습니다.

- * 지원 * — 기술 지원 옵션, 리소스 및 연락처를 봅니다.

지원되는 브라우저

vCenter용 Storage Plugin은 여러 유형의 브라우저에서 액세스할 수 있습니다. 다음 브라우저 및 버전이 지원됩니다.

- Google Chrome 89 이상
- Mozilla Firefox 80 이상
- Microsoft Edge 90 이상

사용자 역할 및 권한

vCenter용 Storage Plugin의 작업에 액세스하려면 사용자에게 읽기-쓰기 권한이 있어야 합니다. 기본적으로 정의된 모든 VMware vCenter 사용자 ID에는 플러그인에서 작업을 수행할 수 있는 권한이 없습니다.

구성 개요

구성에는 다음 단계가 포함됩니다.

1. "플러그인을 설치하고 등록합니다".
2. "플러그인 액세스 권한을 구성합니다".
3. "플러그인 인터페이스에 로그인합니다".
4. "스토리지 시스템을 검색합니다".
5. "스토리지 프로비저닝".

자세한 내용을 확인하십시오

vSphere Client에서 데이터 저장소를 관리하는 방법에 대한 자세한 내용은 를 참조하십시오 "VMware vSphere 설명서".

시작하십시오

vCenter용 **SANtricity** 스토리지 플러그인의 설치 및 업그레이드 요구 사항

vCenter용 SANtricity 스토리지 플러그인을 설치 또는 업그레이드하기 전에 설치 요구 사항 및 업그레이드 고려 사항을 검토하십시오.

설치 요구 사항

Windows 호스트 시스템에서 vCenter용 Storage Plugin을 설치 및 구성할 수 있습니다. 플러그인 설치에는 다음 요구 사항이 포함됩니다.

요구 사항	설명
지원되는 버전	• VMware vCenter Server Appliance 지원 버전: 6.7U3J, 7.0U1, 7.0U2, 7.0U3 및 8.0. • NetApp SANtricity OS 버전: 11.60.2 이상 • 지원되는 애플리케이션 호스트 버전: Windows 2016, Windows 2019, Windows 2022. 호환성에 대한 자세한 내용은 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
다중 인스턴스	Windows 호스트에 vCenter용 Storage Plugin 인스턴스를 하나만 설치할 수 있으며 하나의 vCSA에만 등록할 수 있습니다.
용량 계획	vCenter용 Storage Plugin을 실행하려면 실행 및 로깅을 위한 충분한 공간이 필요합니다. 시스템이 다음과 같은 사용 가능한 디스크 공간 요구 사항을 충족하는지 확인합니다. • 필요한 설치 공간 — 275MB • 스토리지 공간 — 275MB + 200MB(로깅) • 시스템 메모리 — 1.5GB
라이센스	vCenter용 Storage Plugin은 라이센스 키가 필요하지 않은 독립 실행형 무료 제품입니다. 그러나 해당 저작권 및 서비스 약관이 적용됩니다.

업그레이드 고려 사항

이전 버전에서 업그레이드하는 경우 업그레이드하기 전에 vCSA에서 플러그인을 등록 해제해야 합니다.

- 업그레이드 중에는 플러그인의 이전 구성 설정 대부분이 보존됩니다. 이러한 설정에는 사용자 암호, 검색된 모든 스토리지 시스템, 서버 인증서, 신뢰할 수 있는 인증서 및 서버 런타임 구성이 포함됩니다.
- 업그레이드 프로세스에서 * vcenter.properties* 파일이 보존되지 않으므로 업그레이드하기 전에 플러그 인을 등록 취소해야 합니다. 업그레이드가 완료되면 플러그인을 vCSA에 다시 등록할 수 있습니다.
- 이전에 리포지토리에 로드된 모든 SANtricity OS 파일이 업그레이드 중에 제거됩니다.

vCenter용 **SANtricity** 스토리지 플러그인을 설치하거나 업그레이드합니다

다음 단계에 따라 vCenter용 Storage Plugin을 설치하고 플러그인 등록을 확인합니다. 다음 지침을 사용하여 플러그인을 업그레이드할 수도 있습니다.

설치 사전 요구 사항을 검토합니다

시스템이 의 요구 사항을 충족하는지 확인합니다 "설치 및 업그레이드 요구 사항 검토".

업그레이드 프로세스에서 * vcenter.properties* 파일은 보존되지 않습니다. 업그레이드 중인 경우 업그레이드 전에 플러그 인을 등록 취소해야 합니다. 업그레이드가 완료되면 플러그인을 vCSA에 다시 등록할 수 있습니다.

플러그인 소프트웨어를 설치합니다

플러그인 소프트웨어를 설치하려면:

1. 설치 관리자 파일을 응용 프로그램 서버로 사용할 호스트에 복사한 다음 설치 프로그램을 다운로드한 폴더에 액세스합니다.
2. 설치 파일을 두 번 클릭합니다.

   'S antricity_storage_vcenterplugin-windows_x64—nn.nn.nn.nnnn.exe'

   위 파일 이름에서 ' nn.nn.nn.nnnn'은 버전 번호를 나타냅니다.

3. 설치가 시작되면 화면의 지시에 따라 여러 기능을 활성화하고 일부 구성 매개 변수를 입력합니다. 필요한 경우 나중에 구성 파일에서 이러한 선택 항목을 변경할 수 있습니다.

   업그레이드 중에는 구성 매개 변수를 묻는 메시지가 표시되지 않습니다.

   설치하는 동안 인증서 유효성 검사를 묻는 메시지가 표시됩니다. 플러그인과 스토리지 시스템 간에 인증서 유효성 검사를 적용하려면 이 확인란을 선택한 상태로 유지합니다. 이렇게 하면 스토리지 배열 인증서가 플러그인에 대해 신뢰되도록 확인됩니다. 인증서를 신뢰할 수 없는 경우 플러그인에 인증서를 추가할 수 없습니다. 인증서 유효성 검사를 재정의하려면 자체 서명된 인증서를 사용하여 모든 스토리지 어레이를 플러그인에 추가할 수 있도록 확인란을 선택 취소합니다. 인증서에 대한 자세한 내용은 플러그인 인터페이스에서 사용할 수 있는 온라인 도움말을 참조하십시오.

4. Webserver Started 메시지가 나타나면 * OK * 를 클릭하여 설치를 완료한 다음 * Done * 을 클릭합니다.
5. services.msc * 명령을 실행하여 응용 프로그램 서버가 성공적으로 설치되었는지 확인합니다.
6. VCP(Application Server) 서비스 * vCenter * 용 NetApp SANtricity 스토리지 플러그인 이 설치되어 있고 서비스가 시작되었는지 확인합니다.

   필요한 경우 설치 후 인증서 유효성 검사 및 웹 서비스 포트 설정을 변경할 수 있습니다. 설치 디렉터리에서 wsconfig.xml 파일을 엽니다. 스토리지 배열에서 인증서 유효성 검사를 제거하려면 env 키 trust.all.arrays를 true로 변경합니다. 웹 서비스 포트를 변경하려면 'slport' 값을 0에서 65535 사이의 원하는 포트 값으로 수정합니다. 사용된 포트 번호가 다른 프로세스에 바인딩되어 있지 않은지 확인합니다. 완료되면 변경 사항을 저장하고 플러그인 웹 서버를 다시 시작합니다. 플러그인을 vCSA에 등록한 후 플러그인 웹 서버의 포트 값이 변경되면 vCSA가 변경된 포트에서 플러그인 웹서버로 통신하도록 플러그인을 등록 취소하고 다시 등록해야 합니다.

vCenter Server Appliance에 플러그인을 등록합니다

플러그인 소프트웨어가 설치되면 vCSA에 플러그인을 등록합니다.

플러그인은 한 번에 하나의 vCSA에만 등록할 수 있습니다. 다른 vCSA에 등록하려면 현재 vCSA에서 플러그인을 등록 취소하고 애플리케이션 호스트에서 제거해야 합니다. 그런 다음 플러그인을 다시 설치하고 다른 vCSA에 등록할 수 있습니다.

1. 명령줄을 통해 프롬프트를 열고 다음 디렉토리로 이동합니다.

   "<설치 디렉토리>\vcenter-register\bin"

2. vcenter-register.bat * 파일: 'vcenter-register.bat^ - action registerPlugin^ - vcenter Hostname <vcenter FQDN>^ - username <Administrator username>^'을 실행합니다
3. 스크립트가 성공했는지 확인합니다.

로그는 "%install_dir%/working/logs/vc-registration.log"에 저장됩니다.

플러그인 등록을 확인합니다

플러그인을 설치하고 등록 스크립트를 실행한 후 플러그인이 vCenter Server Appliance에 성공적으로 등록되었는지 확인합니다.

1. vCenter Server Appliance에 대한 vSphere Client를 엽니다.
2. 메뉴 표시줄에서 Administrator[Client Plugins] 메뉴를 선택합니다.
3. vCenter용 Storage Plugin이 * Enabled * 로 표시되는지 확인합니다.

   응용 프로그램 서버와 통신할 수 없다는 오류 메시지와 함께 플러그인이 사용 안 함 으로 표시되면 응용 프로그램 서버에 대해 정의된 포트 번호가 사용 중인 방화벽을 통과할 수 있도록 설정되어 있는지 확인합니다. 기본 애플리케이션 서버 TCP(Transmission Control Protocol) 포트 번호는 8445입니다.

SANtricity Storage Plugin for vCenter 액세스 권한을 구성합니다

사용자, 역할 및 권한이 포함된 vCenter용 Storage Plugin에 대한 액세스 권한을 구성할 수 있습니다.

필요한 **vSphere** 권한을 검토합니다

vSphere Client 내에서 플러그인에 액세스하려면 적절한 vSphere 권한이 있는 역할에 할당해야 합니다. "Configure datastore" vSphere 권한이 있는 사용자는 플러그인에 대한 읽기/쓰기 액세스 권한을 가지고 있는 반면 "Browse datastore" 권한이 있는 사용자는 읽기 전용 액세스 권한을 갖습니다. 사용자에게 이러한 권한이 없는 경우 플러그인에는 "권한 부족" 메시지가 표시됩니다.

플러그인 액세스 유형입니다	**vSphere** 권한이 필요합니다
읽기-쓰기(구성)	데이터 저장소. 구성
읽기 전용(보기)	데이터 저장소. 찾아보기

스토리지 관리자 역할을 구성합니다

플러그인 사용자에게 읽기/쓰기 권한을 제공하려면 역할을 생성, 복제 또는 편집할 수 있습니다. vSphere Client에서 역할을 구성하는 방법에 대한 자세한 내용은 VMware Doc Center에서 다음 항목을 참조하십시오.

- "사용자 지정 역할을 만듭니다"

역할 작업에 액세스합니다

1. vSphere Client의 홈 페이지에서 액세스 제어 영역에서 * Administrator * 를 선택합니다.
2. 액세스 제어 영역에서 * 역할 * 을 클릭합니다.
3. 다음 작업 중 하나를 수행합니다.
   - * 새 역할 생성 *: * 역할 생성 * 작업 아이콘을 클릭합니다.
   - * 클론 역할 *: 기존 역할을 선택하고 * 클론 역할 * 작업 아이콘을 클릭합니다.
   - * 기존 역할 편집 *: 기존 역할을 선택하고 * 역할 편집 * 작업 아이콘을 클릭합니다.

관리자 역할은 편집할 수 없습니다.

위의 선택에 따라 적절한 마법사가 나타납니다.

새 역할을 만듭니다

1. 권한 목록에서 이 역할에 할당할 액세스 권한을 선택합니다.

   플러그인에 대한 읽기 전용 액세스를 허용하려면 Datastore [Browse datastore] 메뉴를 선택합니다. 읽기-쓰기 액세스를 허용하려면 Datastore [Configure Datastore] 메뉴를 선택합니다.

2. 필요한 경우 목록에 다른 권한을 할당한 후 * 다음 * 을 클릭합니다.
3. 역할의 이름을 지정하고 설명을 입력합니다.
4. 마침 * 을 클릭합니다.

역할을 복제합니다

1. 역할의 이름을 지정하고 설명을 입력합니다.
2. 마법사를 마치려면 * 확인 * 을 클릭합니다.
3. 목록에서 복제된 역할을 선택한 다음 * 역할 편집 * 을 클릭합니다.
4. 권한 목록에서 이 역할에 할당할 액세스 권한을 선택합니다.

   플러그인에 대한 읽기 전용 액세스를 허용하려면 Datastore [Browse datastore] 메뉴를 선택합니다. 읽기-쓰기 액세스를 허용하려면 Datastore [Configure Datastore] 메뉴를 선택합니다.

5. 다음 * 을 클릭합니다.
6. 필요한 경우 이름과 설명을 업데이트합니다.
7. 마침 * 을 클릭합니다.

기존 역할을 편집합니다

1. 권한 목록에서 이 역할에 할당할 액세스 권한을 선택합니다.

   플러그인에 대한 읽기 전용 액세스를 허용하려면 Datastore [Browse datastore] 메뉴를 선택합니다. 읽기-쓰기 액세스를 허용하려면 Datastore [Configure Datastore] 메뉴를 선택합니다.

2. 다음 * 을 클릭합니다.
3. 필요한 경우 이름 또는 설명을 업데이트합니다.
4. 마침 * 을 클릭합니다.

vCenter Server 어플라이언스에 대한 권한을 설정합니다

역할에 대한 권한을 설정한 후 vCenter Server 어플라이언스에 권한을 추가해야 합니다. 이 권한을 사용하면 지정된 사용자 또는 그룹이 플러그인에 액세스할 수 있습니다.

1. 메뉴 드롭다운 목록에서 * 호스트 및 클러스터 * 를 선택합니다.
2. 액세스 제어 영역에서 * vCenter Server Appliance * 를 선택합니다.
3. 사용 권한 * 탭을 클릭합니다.
4. 권한 추가 * 작업 아이콘을 클릭합니다.
5. 적절한 도메인 및 사용자/그룹을 선택합니다.
6. 읽기/쓰기 플러그인 권한을 허용하는 생성된 역할을 선택합니다.
7. 필요한 경우 * Propagate to Children * 옵션을 활성화합니다.
8. 확인 * 을 클릭합니다.

> ⓘ 기존 권한을 선택하고 생성된 역할을 사용하도록 수정할 수 있습니다. * 단, 권한이 다시 발생하는 것을 방지하기 위해서는 역할이 읽기/쓰기 플러그인 권한과 동일한 권한을 가져야 합니다. *

플러그인에 액세스하려면 플러그인에 대한 읽기/쓰기 권한이 있는 사용자 계정으로 vSphere Client에 로그인해야 합니다.

사용 권한 관리에 대한 자세한 내용은 VMware Doc Center에서 다음 항목을 참조하십시오.

- "vCenter 구성 요소에 대한 권한 관리"
- "역할 및 권한에 대한 모범 사례"

로그인하여 **vCenter**용 **SANtricity** 스토리지 플러그인을 탐색합니다

vCenter용 Storage Plugin에 로그인하여 사용자 인터페이스를 탐색할 수 있습니다.

1. 플러그인에 로그인하기 전에 다음 브라우저 중 하나를 사용하고 있는지 확인합니다.
   - Google Chrome 89 이상
   - Mozilla Firefox 80 이상
   - Microsoft Edge 90 이상
2. 플러그인에 대한 읽기/쓰기 권한이 있는 사용자 계정으로 vSphere Client에 로그인합니다.
3. vSphere 클라이언트 홈 페이지에서 * vCenter * 용 SANtricity 스토리지 플러그인 을 클릭합니다.

   vSphere Client 창에서 플러그인이 열립니다. 플러그인의 기본 페이지가 * Manage - All * 로 열립니다.
4. 왼쪽의 탐색 사이드바에서 스토리지 관리 작업에 액세스합니다.

- * 관리 * – 네트워크에서 스토리지 어레이를 검색, 어레이에 대한 System Manager 열기, 한 어레이에서 여러 어레이로 설정 가져오기, 어레이 그룹 관리, OS 소프트웨어 업그레이드 및 스토리지 용량 할당 등의 작업을 수행합니다.
- * 인증서 관리 * – 브라우저와 클라이언트 간 인증을 위해 인증서를 관리합니다.
- * Operations * – 한 어레이에서 다른 어레이로 설정을 가져오는 등의 배치 작업 진행률을 봅니다.
- * 지원 * – 기술 지원 옵션, 리소스 및 연락처를 볼 수 있습니다.

스토리지 배열의 상태가 최적이 아닌 경우 일부 작업을 사용할 수 없습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 시스템을 검색합니다

스토리지 리소스를 표시하고 관리하려면 vCenter용 Storage Plugin 인터페이스를 사용하여 네트워크에 있는 어레이의 IP 주소를 검색해야 합니다.

시작하기 전에

- 어레이 컨트롤러의 네트워크 IP 주소(또는 주소 범위)를 알아야 합니다.
- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 하며 스토리지 배열 로그인 자격 증명(사용자 이름 및 암호)을 알고 있어야 합니다.

1단계**:** 검색할 네트워크 주소를 입력합니다

단계

1. 관리 페이지에서 * 추가/검색 * 을 선택합니다.

   네트워크 주소 범위 입력 대화 상자가 나타납니다.

2. 다음 중 하나를 수행합니다.
   - 하나의 어레이를 검색하려면 * 단일 스토리지 어레이 검색 * 라디오 버튼을 선택한 다음 스토리지 어레이에 있는 컨트롤러 중 하나의 IP 주소를 입력합니다.
   - 여러 스토리지 어레이를 검색하려면 * 네트워크 범위 내의 모든 스토리지 배열 검색 * 라디오 버튼을 선택한 다음 시작 네트워크 주소와 끝 네트워크 주소를 입력하여 로컬 하위 네트워크를 검색합니다.
3. 검색 시작 * 을 클릭합니다.

   검색 프로세스가 시작되면 검색된 스토리지 시스템이 대화 상자에 표시됩니다. 검색 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

   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. 관리 도메인에 추가할 스토리지 배열 옆의 확인란을 선택합니다.

   시스템은 관리 도메인에 추가할 각 스토리지에 대해 자격 증명 검사를 수행합니다. 계속하기 전에 신뢰할 수 없는 인증서의 문제를 해결해야 할 수 있습니다.

5. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

   스토리지 배열에 유효한 인증서가 있는 경우 로 이동합니다 3단계: 암호를 입력합니다.

스토리지 배열에 유효한 인증서가 없는 경우 자체 서명된 인증서 확인 대화 상자가 나타납니다. 로 이동합니다 2 단계: 검색 중에 신뢰할 수 없는 인증서를 해결합니다.

CA 서명 인증서를 가져오려면 검색 마법사에서 취소하고 왼쪽 패널에서 * 인증서 관리 * 를 클릭합니다. 자세한 지침은 온라인 도움말을 참조하십시오.

2단계**:** 검색 중에 신뢰할 수 없는 인증서를 해결합니다

검색 프로세스를 진행하기 전에 인증서 문제를 해결해야 합니다.

1. 자체 서명된 인증서 확인 대화 상자가 열리면 신뢰할 수 없는 인증서에 대해 표시되는 정보를 검토합니다. 자세한 내용을 보려면 표의 맨 끝에 있는 줄임표를 클릭하고 팝업 메뉴에서 * 보기 * 를 선택하십시오.
2. 다음 중 하나를 수행합니다.
   - 검색된 스토리지 배열에 대한 접속을 신뢰할 수 있는 경우 * Next * (다음 *)를 클릭한 다음 * Yes * (예 *)를 클릭하여 확인하고 마법사의 다음 대화 상자로 이동합니다. 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 배열이 플러그인에 추가됩니다.
   - 스토리지 배열에 대한 연결을 신뢰하지 않는 경우, * Cancel * 을 선택하고 각 스토리지 배열의 보안 인증서 전략을 확인한 후 추가하십시오.
3. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.

3단계**:** 암호를 입력합니다

검색을 위한 마지막 단계로 관리 도메인에 추가할 스토리지 배열에 대한 암호를 입력해야 합니다.

1. 검색된 각 스토리지 시스템의 필드에 관리자 암호를 입력합니다.
2. 마침 * 을 클릭합니다.

   시스템이 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다. 프로세스가 완료되면 스토리지 어레이가 관리 도메인에 추가되고 선택한 그룹에 연결됩니다(지정된 경우).

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지를 프로비저닝합니다

스토리지를 프로비저닝하려면 볼륨을 생성하고 호스트에 볼륨을 할당한 다음 볼륨을 데이터 저장소에 할당합니다.

1단계**:** 볼륨 생성

볼륨은 스토리지 어레이에서 스토리지 공간을 관리하고 구성하는 데이터 컨테이너입니다. 스토리지 배열에서 사용 가능한 스토리지 용량에서 볼륨을 생성하여 시스템 리소스를 구성할 수 있습니다. "볼륨"의 개념은 빠른 액세스를 위해 파일을 구성하기 위해 컴퓨터의 폴더/디렉토리를 사용하는 것과 비슷합니다.

볼륨은 호스트에서 볼 수 있는 유일한 데이터 계층입니다. SAN 환경에서는 볼륨이 LUN(논리 유닛 번호)에 매핑됩니다. 이러한 LUN은 스토리지 시스템에서 지원하는 하나 이상의 호스트 액세스 프로토콜을 사용하여 액세스할 수 있는 사용자 데이터를 저장합니다.

단계

1. 관리 페이지에서 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.

3. 메뉴: Create [Volumes](볼륨 생성)를 선택합니다.

   호스트 선택 대화 상자가 나타납니다.

4. 드롭다운 목록에서 볼륨을 할당할 특정 호스트 또는 호스트 클러스터를 선택하거나 나중에 호스트 또는 호스트 클러스터를 할당하도록 선택합니다.
5. 선택한 호스트 또는 호스트 클러스터에 대한 볼륨 생성 순서를 계속하려면 * 다음 * 을 클릭합니다.

   워크로드 선택 대화 상자가 나타납니다. 워크로드에는 유사한 특성의 볼륨이 포함되어 있으며 이 볼륨은 워크로드가 지원하는 애플리케이션의 유형에 따라 최적화됩니다. 워크로드를 정의하거나 기존 워크로드를 선택할 수 있습니다.

6. 다음 중 하나를 수행합니다.
   - 기존 워크로드에 대한 볼륨 생성 * 옵션을 선택한 다음 드롭다운 목록에서 워크로드를 선택합니다.
   - 새 작업 부하 생성 * 옵션을 선택하여 지원되는 응용 프로그램 또는 “기타” 응용 프로그램에 대한 새 작업 부하를 정의한 다음 다음 다음 단계를 수행합니다.
     i. 드롭다운 목록에서 새 워크로드를 생성할 애플리케이션의 이름을 선택합니다. 이 스토리지 배열에서 사용하려는 애플리케이션이 나열되지 않은 경우 "기타" 항목 중 하나를 선택합니다.
     ii. 생성할 워크로드의 이름을 입력합니다.
7. 다음 * 을 클릭합니다. 워크로드가 지원되는 애플리케이션 유형과 연결되어 있는 경우 요청된 정보를 입력하고, 그렇지 않으면 다음 단계로 이동합니다.

   볼륨 추가/편집 대화 상자가 나타납니다. 이 대화 상자에서는 적합한 풀 또는 볼륨 그룹에서 볼륨을 생성합니다. 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.

8. 볼륨 추가를 시작하기 전에 다음 표의 지침을 읽으십시오.

필드에 입력합니다	설명
여유 용량	볼륨이 풀 또는 볼륨 그룹에서 생성되기 때문에 선택한 풀 또는 볼륨 그룹에 충분한 가용 용량이 있어야 합니다.
DA(Data Assurance)	DA 지원 볼륨을 생성하려면 사용하려는 호스트 연결이 DA를 지원해야 합니다. • DA 지원 볼륨을 생성하려면 DA를 지원하는 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "DA" 옆에 * Yes * 가 표시됨). • DA 기능은 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.

필드에 입력합니다	설명
드라이브 보안	보안이 설정된 볼륨을 생성하려면 스토리지 배열에 대한 보안 키를 생성해야 합니다. • 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 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 읽기 중에 고유 암호화 키를 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 프로비저닝	리소스 프로비저닝된 볼륨을 만들려면 모든 드라이브가 DULBE(할당 취소 또는 기록되지 않은 논리적 블록 오류) 옵션이 있는 NVMe 드라이브여야 합니다.

9. 이전 단계에서 "기타" 또는 애플리케이션별 워크로드를 선택했는지 여부에 따라 다음 작업 중 하나를 선택합니다.
   - * 기타 * – 하나 이상의 볼륨을 생성하는 데 사용할 각 풀 또는 볼륨 그룹에서 * 새 볼륨 추가 * 를 클릭합니다.
   - * 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.

     다음 필드가 나타납니다.

필드에 입력합니다	설명
볼륨 이름	볼륨 생성 시퀀스 중에 볼륨에 기본 이름이 할당됩니다. 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. 풀의 용량은 4GiB 단위로 할당됩니다. 4GiB의 배수에 포함되지 않은 용량은 할당되지만 사용할 수 없습니다. 전체 용량을 사용할 수 있도록 용량을 4GiB 단위로 지정합니다. 사용할 수 없는 용량이 있는 경우, 볼륨을 다시 얻을 수 있는 유일한 방법은 볼륨의 용량을 늘리는 것입니다.
볼륨 유형	"애플리케이션별 워크로드"를 선택한 경우 볼륨 유형 필드가 나타납니다. 애플리케이션별 워크로드를 위해 생성된 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. • 허용된 세그먼트 크기 전환 * – 시스템이 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 암호화 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.

10. 선택한 응용 프로그램에 대한 볼륨 생성 순서를 계속하려면 * 다음 * 을 클릭합니다.
11. 마지막 단계에서는 생성하려는 볼륨의 요약을 검토하고 필요한 내용을 변경합니다. 변경하려면 * 뒤로 * 를 클릭합니다. 볼륨 구성이 만족스러우면 * 마침 * 을 클릭합니다.

2단계**:** 호스트 액세스를 생성하고 볼륨을 할당합니다

호스트를 수동으로 생성할 수 있습니다.

- * 수동 * – 수동 호스트 생성 중에 호스트 포트 식별자를 목록에서 선택하거나 수동으로 입력하여 연결합니다. 호스트를 생성한 후 볼륨에 대한 액세스를 공유하려는 경우 호스트에 볼륨을 할당하거나 호스트 클러스터에 추가할 수 있습니다.

호스트를 수동으로 생성합니다

시작하기 전에

다음 지침을 읽으십시오.

- 사용자 환경 내에 이미 스토리지 시스템을 추가하거나 검색한 상태여야 합니다.
- 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. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

3. MENU: Create [Host] 를 클릭합니다.

   Create Host 대화 상자가 나타납니다.

4. 필요에 따라 호스트 설정을 선택합니다.

필드에 입력합니다	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.

필드에 입력합니다	설명
호스트 포트	다음 중 하나를 수행합니다. • * I/O 인터페이스 선택 * — 일반적으로 호스트 포트는 로그인되어 있고 드롭다운 목록에서 사용할 수 있어야 합니다. 목록에서 호스트 포트 식별자를 선택할 수 있습니다. • * 수동 추가 * — 호스트 포트 식별자가 목록에 표시되지 않으면 호스트 포트가 로그인되어 있지 않은 것입니다. HBA 유틸리티 또는 iSCSI 이니시에이터 유틸리티를 사용하여 호스트 포트 식별자를 찾아 호스트에 연결할 수 있습니다. 호스트 포트 식별자를 수동으로 입력하거나 유틸리티에서 호스트 포트 필드로 복사/붙여 넣을 수 있습니다(한 번에 하나씩). 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 이니시에이터 암호를 설정합니다	(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 * Set CHAP initiator secret * 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 사용되는 유일한 iSCSI 인증 방법은 CHAP입니다.

5. Create * 를 클릭합니다.
6. 호스트 정보를 업데이트해야 하는 경우 테이블에서 호스트를 선택하고 * 설정 보기/편집 * 을 클릭합니다.

   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, 호스트 IPT에 대해 생성된 첫 번째 포트의 기본 별칭은 "ipt_1"입니다.

7. 다음으로, I/O 작업에 사용할 수 있도록 호스트 또는 호스트 클러스터에 볼륨을 할당해야 합니다. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

8. 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 열을 정렬하거나 필터 상자에 원하는 항목을 입력할 수 있습니다.

9. 할당할 각 볼륨 옆의 확인란을 선택하거나 표 머리글에서 확인란을 선택하여 모든 볼륨을 선택합니다.
10. 작업을 완료하려면 * 배정 * 을 클릭하십시오.

    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.

3단계**: vSphere Client**에서 데이터 저장소를 생성합니다

vSphere Client에서 데이터 저장소를 생성하려면 를 참조하십시오 "vSphere Client에서 VMFS 데이터 저장소를 생성합니다" 항목을 참조하십시오.

볼륨 용량을 늘려 기존 데이터 저장소의 용량을 늘립니다

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

시작하기 전에

다음을 확인합니다.

- 볼륨의 연결된 풀 또는 볼륨 그룹에서 충분한 가용 용량을 사용할 수 있습니다.
- 볼륨은 최적이며 수정 상태가 아닙니다.
- 볼륨에서 사용 중인 핫 스페어 드라이브가 없습니다. (볼륨 그룹의 볼륨에만 적용됩니다.)

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

단계

1. vSphere Client 내에서 플러그인으로 이동합니다.
2. 플러그인 내에서 원하는 스토리지 배열을 선택합니다.
3. Provisioning * 을 클릭하고 * Manage Volumes * 를 선택합니다.
4. 용량을 늘릴 볼륨을 선택한 다음 * 용량 증가 * 를 선택합니다.

   용량 증가 확인 대화 상자가 나타납니다.

5. 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.

6. 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.

7. 증가 * 를 클릭합니다.
8. 선택한 볼륨에 대해 현재 실행 중인 용량 증가 작업의 진행 상황에 대한 최근 작업 창을 봅니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.
9. 볼륨 용량이 완료되면 에 설명된 대로 VMFS 크기를 수동으로 늘려야 합니다 "vSphere Client에서 VMFS 데이터 저장소 용량을 늘립니다" 항목을 참조하십시오.

볼륨을 추가하여 기존 데이터 저장소의 용량을 늘립니다

1. 볼륨을 추가하여 데이터 저장소의 용량을 늘릴 수 있습니다. 의 단계를 따릅니다 1단계: 볼륨 생성.
2. 그런 다음 원하는 호스트에 볼륨을 할당하여 데이터 저장소의 용량을 늘립니다.

   를 참조하십시오 "vSphere Client에서 VMFS 데이터 저장소 용량을 늘립니다" 자세한 내용은 VMware Doc Center의 항목을 참조하십시오.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 시스템 상태를 확인합니다

Storage Plugin for vCenter 또는 vSphere Client에서 시스템 상태를 볼 수 있습니다.

1. vSphere Client 내에서 플러그인을 엽니다.
2. 다음 패널에서 상태를 봅니다.
   - * 스토리지 배열 상태 * — * Manage - All * 패널로 이동합니다. 검색된 각 배열에 대해 이 행은 상태 열을 제공합니다.
   - * 작업 진행 중 * — 측면 패널에서 * 작업 * 을 클릭하여 설정 가져오기와 같은 장기 실행 작업을 모두 봅니다. Provisioning 드롭다운에서 장기 실행 작업을 볼 수도 있습니다. 진행 중인 작업 대화 상자에 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. 필요한 경우 작업 열의 링크를 사용하여 작업의 우선 순위를 중지하거나 변경합니다.

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

플러그인에 대해 나타날 수 있는 작업은 다음 표에 나와 있습니다. System Manager 인터페이스에 추가 작업도 표시될 수 있습니다.

작동	작업의 가능한 상태입니다	수행할 수 있는 작업
볼륨 생성(64TiB보다 큰 일반 풀 볼륨만 해당)	진행 중입니다	없음
볼륨 삭제(64TiB보다 큰 일반 풀 볼륨만 해당)	진행 중입니다	없음
풀 또는 볼륨 그룹에 용량을 추가합니다	진행 중입니다	없음
볼륨의 RAID 레벨을 변경합니다	진행 중입니다	없음
풀의 용량을 줄입니다	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
볼륨을 초기화합니다	진행 중입니다	없음
볼륨의 용량을 늘립니다	진행 중입니다	없음
볼륨의 세그먼트 크기를 변경합니다	진행 중입니다	없음

인증서를 관리합니다

vCenter용 **SANtricity** 스토리지 플러그인에서 인증서 관리에 대해 자세히 알아보십시오

vCenter용 저장소 플러그인에서 인증서 관리를 사용하면 CSR(인증서 서명 요청)을 생성하고 인증서를 가져오고 기존 인증서를 관리할 수 있습니다.

인증서란 무엇입니까**?**

인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다. 웹 통신은 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지 않은 상태로 전송됩니다. vCenter용 저장소 플러그인을 사용하면 호스트 관리 시스템의 브라우저 인증서와 검색된 스토리지 배열의 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 있음을 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.

> 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.

자체 서명된 인증서는 브라우저에서 "신뢰"되지 않습니다. 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.

관리 인증서

플러그인을 열면 브라우저에서 디지털 인증서를 확인하여 관리 호스트가 신뢰할 수 있는 소스인지 확인합니다. 브라우저에서 CA 서명 인증서를 찾지 못하면 경고 메시지가 열립니다. 이 페이지에서 웹 사이트로 이동하여 해당 세션에 대해 자체 서명된 인증서를 수락할 수 있습니다. 또한 CA로부터 서명된 디지털 인증서를 받을 수 있으므로 경고 메시지가 더 이상 표시되지 않습니다.

신뢰할 수 있는 인증서

플러그인 세션 중에 CA 서명 인증서가 없는 컨트롤러에 액세스하려고 하면 추가 보안 메시지가 표시될 수 있습니다. 이 경우 자체 서명된 인증서를 영구적으로 신뢰하거나 컨트롤러에 대해 CA 서명 인증서를 가져올 수 있으므로 플러그인이 이러한 컨트롤러에서 들어오는 클라이언트 요청을 인증할 수 있습니다.

vCenter용 SANtricity 스토리지 플러그인에서 CA 서명 인증서를 사용합니다

Storage Plugin for vCenter를 호스팅하는 관리 시스템에 안전하게 액세스하기 위해 CA 서명 인증서를 얻고 가져올 수 있습니다.

CA 서명 인증서를 사용하는 절차는 3단계로 구성됩니다.

- 1단계: CSR 파일을 완료합니다.
- 2단계: CSR 파일을 제출합니다.
- 3단계: 관리 인증서를 가져옵니다.

1단계: CSR 파일을 완료합니다

먼저 인증서 서명 요청(CSR) 파일을 생성해야 합니다. 이 파일은 사용자의 조직과 플러그인이 실행 중인 호스트 시스템을 식별합니다. 또는 OpenSSL과 같은 도구를 사용하여 CSR 파일을 생성하고 로 건너뛸 수 있습니다 2단계: CSR 파일을 제출합니다.

단계

1. 인증서 관리 * 를 선택합니다.

2. 관리 * 탭에서 * CSR 완료 * 를 선택합니다.
3. 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.
4. 플러그인이 실행되고 있는 호스트 시스템에 대한 다음 정보를 입력합니다.
   - * 공통 이름 * — 플러그인이 실행되고 있는 호스트 시스템의 IP 주소 또는 DNS 이름입니다. 이 주소가 올바른지 확인합니다. 입력한 주소와 정확히 일치해야 브라우저에서 플러그인에 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.
5. 호스트 정보가 올바른지 확인합니다. 그렇지 않으면 CA에서 반환된 인증서를 가져오려고 할 때 실패합니다.
6. 마침 * 을 클릭합니다.

2단계: CSR 파일을 제출합니다

CSR(인증서 서명 요청) 파일을 생성한 후 생성된 CSR 파일을 CA에 전송하여 플러그인을 호스팅하는 시스템에 대한 서명된 관리 인증서를 받습니다.

E-Series 시스템에는 .pem, .crt, .cer 또는 .key 파일 형식을 포함하는 서명된 인증서에 대한 PEM 형식(Base64 ASCII 인코딩)이 필요합니다.

단계

1. 다운로드한 CSR 파일을 찾습니다.

   다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

2. CSR 파일을 CA(예: VeriSign 또는 DigiCert)에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.

> CSR 파일을 CA에 제출한 후 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.

3단계: 관리 인증서를 가져옵니다

CA(인증 기관)에서 서명된 인증서를 받은 후 플러그인이 설치된 호스트 시스템으로 인증서를 가져옵니다.

시작하기 전에

- CA의 서명된 인증서가 있어야 합니다. 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 certmgr 유틸리티를 사용하여 파일의 압축을 풀 수 있습니다(마우스 오른쪽 단추를 클릭하고 All Tasks(모든 작업) [Export(내보내기)] 메뉴를 선택합니다). base-64 인코딩이 권장됩니다. 내보내기가 완료되면 체인의 각 인증서 파일에 대해 CER 파일이 표시됩니다.
- 플러그인이 실행 중인 호스트 시스템에 인증서 파일을 복사해야 합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 관리 * 탭에서 * 가져오기 * 를 선택합니다.

   인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 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.

4. 가져오기 * 를 클릭합니다.

결과

파일이 업로드되고 검증됩니다. 인증서 정보가 인증서 관리 페이지에 표시됩니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 관리 인증서를 재설정합니다

vCenter용 Storage Plugin을 호스팅하는 관리 시스템의 경우 관리 인증서를 공장 자체 서명된 원래 상태로 되돌릴 수 있습니다.

이 작업에 대해

이 작업은 Storage Plugin for vCenter가 실행 중인 호스트 시스템에서 현재 관리 인증서를 삭제합니다. 인증서가 재설정되면 호스트 시스템은 자체 서명된 인증서를 사용하여 되돌아갑니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 관리 * 탭에서 * 재설정 * 을 선택합니다.

   관리 인증서 재설정 확인 대화 상자가 열립니다.

3. 필드에 reset을 입력한 다음 * Reset * 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.

vCenter용 SANtricity 스토리지 플러그인에서 스토리지의 인증서를 가져옵니다

필요한 경우 스토리지 배열에 대한 인증서를 가져와 vCenter용 Storage Plugin을 호스팅하는 시스템에서 인증할 수 있습니다. 인증서는 CA(인증 기관)에서 서명할 수도 있고 자체 서명할 수도 있습니다.

시작하기 전에

신뢰할 수 있는 인증서를 가져오는 경우 System Manager를 사용하여 스토리지 배열 컨트롤러에 대한 인증서를 가져와야 합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

   이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

3. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
4. 보기를 제한하려면 * Show certificates that are… * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.
5. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.

   인증서가 업로드 및 검증됩니다.

vCenter용 SANtricity 스토리지 플러그인에서 인증서를 봅니다

인증서를 사용하는 조직, 인증서를 발급한 기관, 유효 기간 및 지문(고유 식별자)을 포함하는 인증서의 요약 정보를 볼 수 있습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 다음 탭 중 하나를 선택합니다.
   - * Management * — 플러그인을 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. 플러그인에 대한 보안 액세스를 허용합니다.
   - * 신뢰 * — 플러그인이 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.
3. 인증서에 대한 자세한 내용을 보려면 해당 행을 선택하고 행 끝에 있는 줄임표를 선택한 다음 * 보기 * 또는 * 내보내기 * 를 클릭합니다.

vCenter용 SANtricity 스토리지 플러그인에서 인증서를 내보냅니다

인증서를 내보내 전체 세부 정보를 볼 수 있습니다.

시작하기 전에

내보낸 파일을 열려면 인증서 뷰어 응용 프로그램이 있어야 합니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 다음 탭 중 하나를 선택합니다.
   - * Management * — 플러그인을 호스팅하는 시스템의 인증서를 표시합니다. 관리 인증서는 CA(인증 기관)에서 자체 서명하거나 승인할 수 있습니다. 플러그인에 대한 보안 액세스를 허용합니다.
   - * 신뢰 * — 플러그인이 스토리지 시스템 및 LDAP 서버와 같은 기타 원격 서버에 액세스할 수 있는 인증서를 표시합니다. 인증서는 CA(인증 기관)에서 발급하거나 자체 서명할 수 있습니다.
3. 페이지에서 인증서를 선택한 다음 행 끝에 있는 줄임표를 클릭합니다.
4. 내보내기 * 를 클릭한 다음 인증서 파일을 저장합니다.
5. 인증서 뷰어 응용 프로그램에서 파일을 엽니다.

vCenter용 SANtricity 스토리지 플러그인에서 신뢰할 수 있는 인증서를 삭제합니다

만료된 인증서와 같이 더 이상 필요하지 않은 인증서를 하나 이상 삭제할 수 있습니다.

시작하기 전에

기존 인증서를 삭제하기 전에 새 인증서를 가져옵니다.

> 루트 또는 중간 인증서를 삭제하면 여러 스토리지 시스템이 동일한 인증서 파일을 공유할 수 있으므로 여러 스토리지 시스템에 영향을 줄 수 있습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.
3. 테이블에서 하나 이상의 인증서를 선택한 다음 * 삭제 * 를 클릭합니다.

   > 사전 설치된 인증서에는 삭제 기능을 사용할 수 없습니다.

   신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.
4. 삭제를 확인한 다음 * 삭제 * 를 클릭합니다.

   인증서가 테이블에서 제거됩니다.

vCenter용 SANtricity 스토리지 플러그인에서 신뢰할 수 없는 인증서를 해결합니다

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

CA 서명 인증서를 가져오려면 다음을 확인합니다.

- 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

신뢰할 수 없는 인증서는 스토리지 배열이 플러그인에 대한 보안 연결을 설정하려고 시도하지만 연결이 보안으로 확인하지 못할 때 발생합니다. 다음 중 하나라도 해당되는 경우 신뢰할 수 있는 CA 인증서를 추가로 설치해야 할 수 있습니다.

- 최근에 스토리지 배열을 추가했습니다.
- 하나 이상의 인증서가 만료되었거나 해지되었습니다.
- 하나 이상의 인증서에 루트 또는 중간 인증서가 없습니다.

단계

1. 인증서 관리 * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

   이 페이지에는 스토리지 배열에 대해 보고된 모든 인증서가 표시됩니다.

3. [인증서] 가져오기 메뉴를 선택하여 CA 인증서를 가져오거나 메뉴: 자체 서명된 [스토리지 배열 인증서] 가져오기 를 선택하여 자체 서명된 인증서를 가져옵니다.
4. 보기를 제한하려면 * Show certificates that are… * filtering 필드를 사용하거나 열 머리글 중 하나를 클릭하여 인증서 행을 정렬할 수 있습니다.
5. 대화 상자에서 인증서를 선택한 다음 * 가져오기 * 를 클릭합니다.

   인증서가 업로드 및 검증됩니다.

스토리지 관리

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 시스템 관리에 대해 자세히 알아보십시오

Add/Discover 기능을 사용하여 vCenter용 Storage 플러그인에서 관리할 스토리지 시스템을 찾아 추가합니다. 관리 페이지에서 검색된 이러한 스토리지에 대한 새 암호를 이름 변경, 제거 및 제공할 수도 있습니다.

스토리지 검색 시 고려 사항

플러그인이 스토리지 리소스를 표시하고 관리하려면 조직의 네트워크에서 관리할 스토리지 어레이를 검색해야 합니다. 단일 어레이 또는 여러 어레이를 검색하고 추가할 수 있습니다.

제공합니다

여러 어레이를 검색하도록 선택한 경우 네트워크 IP 주소 범위를 입력한 다음 시스템이 해당 범위의 각 IP 주소에 대한 개별 연결을 시도합니다. 성공적으로 도달한 스토리지 배열이 플러그인에 표시되면 이를 관리 도메인에 추가할 수 있습니다.

단일 스토리지 어레이

단일 어레이를 검색하도록 선택한 경우 스토리지 어레이에 있는 컨트롤러 중 하나의 IP 주소를 입력한 다음 해당 어레이를 관리 도메인에 추가합니다.

플러그인은 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 플러그인이 컨트롤러를 검색 또는 표시하지 않습니다. 그러나 스토리지 배열을 추가하면 연결된 모든 IP 주소가 검색되어 관리 보기에 표시됩니다.

사용자 자격 증명

추가할 각 스토리지 배열에 대해 관리자 암호를 제공해야 합니다.

인증서

검색 프로세스의 일부로 검색된 스토리지 시스템이 신뢰할 수 있는 소스의 인증서를 사용하고 있는지 확인합니다. 시스템은 브라우저를 사용하여 에서 설정하는 모든 연결에 대해 두 가지 유형의 인증서 기반 인증을 사용합니다.

- * 신뢰할 수 있는 인증서 * — 하나 이상의 컨트롤러 인증서가 만료되었거나 해지되었거나 체인에 인증서가 없는 경우 인증 기관에서 제공하는 신뢰할 수 있는 인증서를 추가로 설치해야 할 수 있습니다.
- * 자체 서명된 인증서 * — 어레이도 자체 서명된 인증서를 사용할 수 있습니다. 서명된 인증서를 가져오지 않고 어레이를 검색할 경우 플러그인은 자체 서명된 인증서를 수락할 수 있는 추가 단계를 제공합니다. 스토리지 배열의 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 배열이 플러그인에 추가됩니다. 스토리지 배열에 대한 연결을 신뢰하지 않는 경우, 스토리지 배열을 플러그인에 추가하기 전에 * Cancel * 을 선택하고 스토리지 배열의 보안 인증서 전략을 확인합니다.

스토리지 배열 상태입니다

vCenter용 Storage Plugin을 열면 각 스토리지 배열과의 통신이 설정되고 각 스토리지 배열의 상태가 표시됩니다.

Manage-All * 페이지에서 스토리지 배열의 상태 및 스토리지 배열 연결 상태를 볼 수 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. 이 문제는 플러그인이 시작되고 아직 스토리지 어레이와 연결되지 않았거나 스토리지 어레이가 오프라인 상태이며 플러그인을 시작한 이후 연락이 되지 않은 경우에 발생할 수 있습니다.
오프라인	이전에 플러그인이 스토리지 어레이에 연결했지만 지금은 모든 연결이 끊어졌습니다.

스토리지 배열의 기본 운영 작업에 vCenter용 저장소 플러그인 을 사용할 수 있습니다. 그러나 플러그인에서 사용할 수 없는 작업을 수행하기 위해 System Manager를 시작해야 하는 경우가 있습니다.

System Manager는 이더넷 관리 포트를 통해 네트워크에 연결되는 스토리지 어레이 컨트롤러에 내장된 애플리케이션입니다. System Manager에는 모든 어레이 기반 기능이 포함되어 있습니다.

다음 표를 참조하여 특정 스토리지 어레이 작업에 플러그인 인터페이스나 System Manager 인터페이스를 사용할 수 있는지 여부를 결정할 수 있습니다.

기능	플러그인 인터페이스	**System Manager** 인터페이스
여러 스토리지 시스템의 그룹에 대한 배치 작업	예	아니요 작업은 단일 어레이에서 수행됩니다.
SANtricity OS 펌웨어의 업그레이드	예. 일괄 작업에서 하나 이상의 어레이	예. 단일 스토리지 전용.
한 어레이에서 여러 어레이로 설정을 가져옵니다	예	아니요
호스트 및 호스트 클러스터 관리(볼륨 생성, 할당, 업데이트 및 삭제)	예	예
풀 및 볼륨 그룹 관리(생성, 업데이트, 보안 활성화 및 삭제)	예	예
볼륨 관리(생성, 크기 조정, 업데이트 및 삭제)	예	예
SSD Cache 관리(생성, 업데이트 및 삭제)	예	예
미러링 및 스냅샷 관리	아니요	예
하드웨어 관리(컨트롤러 상태 보기, 포트 연결 구성, 컨트롤러 오프라인, 핫 스페어 활성화, 드라이브 지우기, 등)	아니요	예
알림(e-메일, SNMP, syslog) 관리	아니요	예
보안 키 관리	아니요	예
컨트롤러의 인증서 관리	아니요	예
컨트롤러의 액세스 관리(LDAP, SAML 등)	아니요	예
AutoSupport 관리	아니요	예

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 시스템을 검색합니다

vCenter용 저장소 플러그인에서 저장소 리소스를 표시하고 관리하려면 네트워크에 있는 어레이의 IP 주소를 검색해야 합니다.

시작하기 전에

- 어레이 컨트롤러의 네트워크 IP 주소(또는 주소 범위)를 알아야 합니다.
- 스토리지 배열이 올바르게 설정 및 구성되어 있어야 합니다.

- 스토리지 배열 암호는 System Manager의 액세스 관리 타일을 사용하여 설정해야 합니다.

이 작업에 대해

스토리지 검색은 다단계 절차입니다.

- 1단계: 검색할 네트워크 주소를 입력합니다
- 2단계: 검색 중에 신뢰할 수 없는 인증서를 해결합니다
- 3단계: 암호를 입력합니다

1단계**:** 검색할 네트워크 주소를 입력합니다

스토리지 어레이를 검색하는 첫 번째 단계로, 로컬 하위 네트워크에서 검색할 단일 IP 주소 또는 IP 주소 범위를 입력합니다. 추가/검색 기능은 검색 프로세스를 안내하는 마법사를 엽니다.

단계

1. Manage * 페이지에서 * Add/Discover * 를 선택합니다.

   네트워크 주소 범위 입력 대화 상자가 나타납니다.

2. 다음 중 하나를 수행합니다.
   - 하나의 어레이를 검색하려면 * 단일 스토리지 어레이 검색 * 라디오 버튼을 선택한 다음 스토리지 어레이에 있는 컨트롤러 중 하나의 IP 주소를 입력합니다.
   - 여러 스토리지 어레이를 검색하려면 * 네트워크 범위 내의 모든 스토리지 배열 검색 * 라디오 버튼을 선택한 다음 시작 네트워크 주소와 끝 네트워크 주소를 입력하여 로컬 하위 네트워크를 검색합니다.
3. 검색 시작 * 을 클릭합니다.

   검색 프로세스가 시작되면 검색된 스토리지 시스템이 대화 상자에 표시됩니다. 검색 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

   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. 관리 도메인에 추가할 스토리지 배열 옆의 확인란을 선택합니다.

   시스템은 관리 도메인에 추가할 각 스토리지에 대해 자격 증명 검사를 수행합니다. 계속하기 전에 신뢰할 수 없는 인증서의 문제를 해결해야 할 수 있습니다.

5. 마법사의 다음 단계로 진행하려면 * Next * (다음 *)를 클릭합니다.
6. 스토리지 배열에 유효한 인증서가 있는 경우 로 이동합니다 3단계: 암호를 입력합니다. 스토리지 배열에 유효한 인증서가 없는 경우 자체 서명된 인증서 확인 대화 상자가 나타납니다. 로 이동합니다 2단계: 검색 중에 신뢰할 수 없는 인증서를 해결합니다. CA 서명 인증서를 가져오려면 검색 대화 상자에서 취소하고 로 이동합니다 "스토리지에 대한 인증서를 가져옵니다".

2단계**:** 검색 중에 신뢰할 수 없는 인증서를 해결합니다

필요한 경우 검색 프로세스를 진행하기 전에 모든 인증서 문제를 해결해야 합니다.

검색 중에 스토리지 배열에 "신뢰할 수 없는 인증서" 상태가 표시되는 경우 자체 서명된 인증서 확인 대화 상자가

나타납니다. 이 대화 상자에서 신뢰할 수 없는 인증서를 확인하거나 CA 인증서를 가져올 수 있습니다(참조) "스토리지에 대한 인증서를 가져옵니다")를 클릭합니다.

단계

1. 자체 서명된 인증서 확인 대화 상자가 열리면 신뢰할 수 없는 인증서에 대해 표시되는 정보를 검토합니다. 자세한 내용을 보려면 표의 맨 끝에 있는 줄임표를 클릭하고 팝업 메뉴에서 * 보기 * 를 선택하십시오.
2. 다음 중 하나를 수행합니다.
   - 검색된 스토리지 배열에 대한 연결을 신뢰할 수 있는 경우 * Next * (다음 *)를 클릭한 다음 * Yes * (예 *)를 클릭하여 확인하고 마법사의 다음 카드로 계속 진행합니다. 자체 서명된 인증서가 신뢰할 수 있는 것으로 표시되고 스토리지 배열이 플러그인에 추가됩니다.
   - 스토리지 배열에 대한 연결을 신뢰하지 않는 경우, 플러그인에 스토리지 배열을 추가하기 전에 * Cancel * 을 선택하고 각 스토리지 배열의 보안 인증서 전략을 확인합니다.

3단계**:** 암호를 입력합니다

검색을 위한 마지막 단계로 관리 도메인에 추가할 스토리지 배열에 대한 암호를 입력해야 합니다.

단계

1. 필요한 경우 이전에 어레이에 그룹을 구성한 경우 드롭다운을 사용하여 검색된 어레이에 대한 그룹을 선택할 수 있습니다.
2. 검색된 각 스토리지 시스템의 필드에 관리자 암호를 입력합니다.
3. 마침 * 을 클릭합니다.

시스템이 지정된 스토리지 어레이에 연결하는 데 몇 분 정도 걸릴 수 있습니다.

결과

스토리지 배열이 관리 도메인에 추가되고 선택한 그룹에 연결됩니다(지정된 경우).

실행 옵션을 사용하면 관리 작업을 수행하려는 경우 하나 이상의 스토리지 어레이에 대한 브라우저 기반 System Manager를 열 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 배열 이름을 바꿉니다

vCenter용 Storage Plugin의 관리 페이지에 표시되는 스토리지 배열의 이름을 변경할 수 있습니다.

단계

1. Manage * 페이지에서 스토리지 배열 이름 왼쪽에 있는 확인란을 선택합니다.
2. 행의 맨 오른쪽에 있는 줄임표를 선택한 다음 팝업 메뉴에서 * 스토리지 배열 이름 바꾸기 * 를 선택합니다.
3. 새 이름을 입력하고 * 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 배열 암호를 변경합니다

vCenter용 Storage Plugin에서 스토리지 배열을 보고 액세스하는 데 사용되는 암호를 업데이트할 수 있습니다.

시작하기 전에

System Manager에서 설정된 스토리지 어레이의 현재 암호를 알아야 합니다.

이 작업에 대해

이 작업에서는 플러그인에서 액세스할 수 있도록 스토리지 배열의 현재 암호를 입력합니다. System Manager에서 어레이 암호를 변경한 경우 이 방법이 필요할 수 있습니다.

단계

1. Manage * 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 배열을 제거합니다

vCenter용 저장소 플러그인에서 더 이상 스토리지를 관리하지 않으려는 경우 하나 이상의 저장소 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 * 페이지에서 제거할 스토리지 배열을 하나 이상 선택합니다.
2. Uncommon Tasks [Remove storage arrays] 메뉴를 선택합니다.

   스토리지 배열이 플러그인 인터페이스의 모든 보기에서 제거됩니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 **System Manager**를 시작합니다

단일 어레이를 관리하려면 시작 옵션을 사용하여 새 브라우저 창에서 SANtricity System Manager를 엽니다.

System Manager는 이더넷 관리 포트를 통해 네트워크에 연결되는 스토리지 어레이 컨트롤러에 내장된 애플리케이션입니다. System Manager에는 모든 어레이 기반 기능이 포함되어 있습니다. System Manager에 액세스하려면 웹 브라우저를 통해 네트워크 관리 클라이언트에 대역외 연결이 있어야 합니다.

단계

1. Manage * 페이지에서 관리할 스토리지 어레이를 하나 이상 선택합니다.
2. 시작 * 을 클릭합니다.

   브라우저에서 새 탭이 열리면 System Manager 로그인 페이지가 표시됩니다.

3. 사용자 이름과 암호를 입력한 다음 * 로그인 * 을 클릭합니다.

설정을 가져옵니다

vCenter용 SANtricity 스토리지 플러그인의 가져오기 설정 기능에 대해 알아봅니다

설정 가져오기 기능은 단일 스토리지 배열(소스)의 설정을 vCenter용 Storage Plugin의 여러 스토리지(대상)로 복제할 수 있는 일괄 작업입니다.

가져올 수 있는 설정입니다

다음 구성을 한 어레이에서 다른 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.
- * 시스템 설정 * — 다음과 관련된 구성:
  - 볼륨에 대한 미디어 스캔 설정입니다
  - SSD 설정
  - 자동 로드 밸런싱(호스트 연결 보고 포함 안 함)
- * 스토리지 구성 * — 다음과 관련된 구성:
  - 볼륨(일반 및 비리포지토리 볼륨만 해당)
  - 볼륨 그룹 및 풀
  - 핫 스페어 드라이브 할당

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. 플러그인 인터페이스에서 * 관리 * 페이지로 이동하여 설정을 가져옵니다.
4. 작업 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 소스와 대상 어레이 간에 다를 수 있지만 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.

vCenter용 SANtricity 스토리지 플러그인에서 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

다음을 확인합니다.

- 알림은 소스로 사용할 스토리지 어레이에 대한 System Manager(메뉴: 설정 [경고])에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.
- 에서 스토리지 구성을 복제하는 데 필요한 요구 사항을 검토했습니다 "설정 가져오기 개요".

이 작업에 대해

가져오기 작업에 대해 e-메일, SNMP 또는 syslog 알림을 선택할 수 있습니다.

- * 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 작업 [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 플러그인이 해당 어레이와 통신할 수 없는 경우(예: 오프라인이거나 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.

vCenter용 SANtricity 스토리지 플러그인에서 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

다음을 확인합니다.

- AutoSupport는 소스로 사용할 스토리지 어레이에 대한 시스템 관리자(메뉴: 지원 [지원 센터])에 구성되어 있습니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.
- 에서 스토리지 구성을 복제하는 데 필요한 요구 사항을 검토했습니다 "설정 가져오기 개요".

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 작업 [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 플러그인이 해당 어레이와 통신할 수 없는 경우(예: 오프라인이거나 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.

vCenter용 SANtricity 스토리지 플러그인에서 디렉토리 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

다음을 확인합니다.

- 디렉토리 서비스는 소스로 사용할 스토리지 어레이에 대한 System Manager(메뉴: 설정 [액세스 관리])에서 구성됩니다.
- 대상 스토리지 배열에 대한 기존 구성은 System Manager(시스템 설정) [System(시스템) > Save Storage Array Configuration(스토리지 배열 구성 저장)] 메뉴에서 백업됩니다.
- 에서 스토리지 구성을 복제하는 데 필요한 요구 사항을 검토했습니다 "설정 가져오기 개요".

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 작업 [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 플러그인이 해당 어레이와 통신할 수 없는 경우(예: 오프라인이거나 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.

vCenter용 SANtricity 스토리지 플러그인에서 시스템 설정을 가져옵니다

한 스토리지 어레이에서 다른 스토리지 어레이로 시스템 설정을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

다음을 확인합니다.

- 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.
- 에서 스토리지 구성을 복제하는 데 필요한 요구 사항을 검토했습니다 "설정 가져오기 개요".

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 작업 [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 플러그인이 해당 어레이와 통신할 수 없는 경우(예: 오프라인이거나 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.

한 스토리지 어레이에서 다른 스토리지 어레이로 스토리지 구성을 가져올 수 있습니다. 이 배치 작업은 네트워크에서 여러 어레이를 구성해야 하는 시간을 절약합니다.

시작하기 전에

다음을 확인합니다.

- 스토리지는 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.
- 에서 스토리지 구성을 복제하는 데 필요한 요구 사항을 검토했습니다 "설정 가져오기 개요".
- 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.

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 작업 [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 플러그인이 해당 어레이와 통신할 수 없는 경우(예: 오프라인이거나 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.

스토리지 그룹을 관리합니다

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 그룹을 관리하는 방법에 대해 알아봅니다

스토리지 시스템 집합을 그룹화하여 vCenter용 Storage Plugin에서 물리적 인프라와 가상화 인프라를 관리할 수 있습니다. 모니터링 또는 보고 작업을 보다 쉽게 실행할 수 있도록 스토리지 어레이를 그룹화할 수 있습니다.

스토리지 그룹 유형:

- * 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 그룹을 생성합니다

스토리지 그룹을 생성한 다음 스토리지 시스템을 그룹에 추가합니다. 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 그룹에 스토리지 어레이를 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 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.

vCenter용 **SANtricity** 스토리지 플러그인의 그룹에서 스토리지 어레이를 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 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.

OS 소프트웨어를 업그레이드합니다

vCenter용 스토리지 플러그인을 사용하여 **SANtricity** 소프트웨어 업그레이드를 관리하는 방법에 대해 알아봅니다

vCenter용 스토리지 플러그인에서 같은 유형의 여러 스토리지 어레이에 대한 SANtricity 소프트웨어 및 NVSRAM 업그레이드를 관리할 수 있습니다.

워크플로우 업그레이드

다음 단계에서는 소프트웨어 업그레이드를 수행하기 위한 높은 수준의 워크플로우를 제공합니다.

1. 지원 사이트에서 최신 SANtricity OS 파일을 다운로드합니다(지원 페이지에서 링크 제공). 관리 호스트 시스템(브라우저에서 플러그인에 액세스하는 호스트)에 파일을 저장한 다음 파일의 압축을 풉니다.
2. 플러그인에서 SANtricity OS 소프트웨어 파일과 NVSRAM 파일을 리포지토리(파일이 저장되는 서버 영역)에 로드할 수 있습니다.
3. 저장소에 파일이 로드되면 업그레이드에 사용할 파일을 선택할 수 있습니다. SANtricity OS 소프트웨어 업그레이드 페이지에서 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 플러그인은 다음 작업을 수행합니다.
   - 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.
   - 각 컨트롤러로 업그레이드 파일을 전송합니다.
   - 컨트롤러를 재부팅하고 한 번에 하나의 컨트롤러인 새 OS 소프트웨어를 활성화합니다. 활성화 중에 기존 OS 파일이 새 파일로 대체됩니다.

나중에 소프트웨어가 활성화되도록 지정할 수도 있습니다.

업그레이드 고려 사항

여러 스토리지 시스템을 업그레이드하기 전에 계획의 일환으로 주요 고려 사항을 검토하십시오.

현재 버전

검색된 각 스토리지 배열에 대한 vCenter용 저장소 플러그인 의 관리 페이지에서 현재 SANtricity OS 소프트웨어 버전을 볼 수 있습니다. 이 버전은 SANtricity OS 소프트웨어 열에 표시됩니다. 각 행에서 OS 버전을 클릭하면 컨트롤러 펌웨어 및 NVSRAM 정보가 팝업 대화 상자에 표시됩니다.

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 참조하십시오 "상호 운용성 매트릭스 툴".

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.

vCenter용 **SANtricity** 스토리지 플러그인에서 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.

vCenter용 스토리지 플러그인을 사용하여 **SANtricity** 소프트웨어 및 **NVSRAM**을 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

다음을 확인합니다.

- 플러그인이 실행 중인 호스트 시스템에서 최신 SANtricity OS 파일을 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.

* 데이터 손실 또는 스토리지 배열 손상 위험 * — 업그레이드 중에 스토리지 배열을 변경하지 마십시오. 스토리지 어레이에 대한 전원을 유지합니다.

단계

1. 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.
2. 기본 보기에서 * 관리 * 를 선택한 다음 업그레이드할 스토리지 어레이를 하나 이상 선택합니다.
3. 업그레이드 센터 [업그레이드 > SANtricity OS > 소프트웨어]를 선택합니다.

   SANtricity OS 소프트웨어 업그레이드 페이지가 나타납니다.

4. 지원 사이트에서 로컬 컴퓨터로 최신 SANtricity OS 소프트웨어 패키지를 다운로드합니다.
   a. 소프트웨어 저장소에 새 파일 추가 를 클릭합니다
   b. 최신 SANtricity OS 다운로드를 찾기 위한 링크를 클릭합니다.
   c. 최신 릴리스 다운로드 * 링크를 클릭합니다.
   d. 나머지 지침에 따라 OS 파일과 NVSRAM 파일을 로컬 컴퓨터에 다운로드합니다.

      버전 8.42 이상에서는 디지털 서명된 펌웨어가 필요합니다. 서명되지 않은 펌웨어를 다운로드하려고 하면 오류가 표시되고 다운로드가 중단됩니다.

5. 컨트롤러를 업그레이드하는 데 사용할 OS 소프트웨어 파일과 NVSRAM 파일을 선택합니다.
   a. 드롭다운에서 로컬 시스템으로 다운로드한 OS 파일을 선택합니다.

      여러 개의 파일을 사용할 수 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.

      소프트웨어 리포지토리는 플러그인과 관련된 모든 소프트웨어 파일을 나열합니다. 사용할 파일이 표시되지 않으면 * 소프트웨어 리포지토리에 새 파일 추가 * 링크를 클릭하여 추가할 OS 파일이 있는 위치를 찾을 수 있습니다.

   a. NVSRAM 파일 선택 * 드롭다운에서 사용할 컨트롤러 파일을 선택합니다.

      파일이 여러 개 있는 경우 파일이 최신 날짜부터 가장 오래된 날짜순으로 정렬됩니다.

6. 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.
7. (선택 사항) 소프트웨어 파일을 활성화하지 않고 스토리지 어레이로 전송하려면 * OS 소프트웨어를 스토리지 어레이로 전송, 스테이징으로 표시 및 나중에 활성화 * 확인란을 선택합니다.
8. 시작 * 을 클릭합니다.
9. 지금 활성화할지 아니면 나중에 활성화할지 여부에 따라 다음 중 하나를 수행합니다.
   - 업그레이드하려는 어레이에 제안된 OS 소프트웨어 버전을 전송하려면 "전송"을 입력하고 * 전송 * 을 클릭합니다. 전송된 소프트웨어를 활성화하려면 업그레이드 센터 [스테이징된 SANtricity OS 소프트웨어 활성화] 메뉴를 선택합니다.
   - 업그레이드를 선택한 어레이에서 제안된 OS 소프트웨어 버전을 전송 및 활성화하려면 "업그레이드"를 입력하고 * 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 클릭할 수 있습니다. 그리고 * 로그 저장 * 을 선택하여 오류를 검토합니다. 상태 점검 오류를 재정의하도록 선택한 다음 * 계속 * 을 클릭하여 업그레이드를 진행할 수도 있습니다.
   - 업그레이드 전 상태 점검 후 업그레이드 작업을 취소할 수 있습니다.
10. (선택 사항) 업그레이드가 완료되면 줄임표(…)를 클릭하여 특정 스토리지 배열에 대해 업그레이드된 항목 목록을 볼 수 있습니다. 그런 다음 * 로그 저장 * 을 선택합니다.

    이 파일은 브라우저의 다운로드 폴더에 'upgrade_log-<date>'라는 이름으로 저장됩니다. Json’이라고 합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 스테이징된 **OS** 소프트웨어를 활성화합니다

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.

활성화 프로세스가 시작된 후에는 중지할 수 없습니다.

단계

1. 기본 보기에서 * 관리 * 를 선택합니다. 필요한 경우 페이지 맨 위에서 * Status * 열을 클릭하여 "OS Upgrade(활성화 대기 중)" 상태의 모든 스토리지 어레이를 정렬합니다.
2. 소프트웨어를 활성화할 스토리지 어레이를 하나 이상 선택한 다음 메뉴: 업그레이드 센터 [스테이징된 SANtricity 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 클릭할 수 있습니다. 그리고 * 로그 저장 * 을 선택하여 오류를 검토합니다. 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.
3. (선택 사항) 활성화가 완료된 후 줄임표(…)를 클릭하여 특정 스토리지 배열에 대해 활성화된 항목 목록을 볼 수 있습니다. 그런 다음 * 로그 저장 * 을 선택합니다.

   파일은 브라우저의 Downloads 폴더에 "activate_log-<date>"라는 이름으로 저장됩니다. Json'이라고 합니다.

vCenter용 SANtricity 스토리지 플러그인에서 스테이징된 OS 소프트웨어를 지웁니다

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

1. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [스테이징된 SANtricity 소프트웨어 지우기] 를 선택합니다.

   Clear Staged SANtricity Software(스테이징된 소프트웨어 지우기) 대화 상자가 열리고 보류 중인 소프트웨어 또는 NVSRAM이 있는 검색된 모든 스토리지 시스템이 나열됩니다.
2. 필요한 경우 스테이징된 소프트웨어가 있는 모든 시스템을 볼 수 있도록 목록에서 스토리지 시스템을 필터링하거나 정렬합니다.
3. 선택 취소할 보류 중인 소프트웨어가 있는 스토리지 시스템의 확인란을 선택합니다.
4. 지우기 * 를 클릭합니다.

   작업 상태가 대화 상자에 표시됩니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 소프트웨어 저장소를 관리합니다

vCenter용 Storage Plugin과 관련된 모든 소프트웨어 파일이 나열된 소프트웨어 저장소를 보고 관리할 수 있습니다.

시작하기 전에

리포지토리를 사용하여 SANtricity OS 파일을 추가하는 경우 로컬 시스템에서 OS 파일을 사용할 수 있는지 확인합니다.

이 작업에 대해

SANtricity OS 소프트웨어 저장소 관리 옵션을 사용하여 플러그인이 실행 중인 호스트 시스템으로 하나 이상의 OS 파일을 가져올 수 있습니다. 소프트웨어 저장소에서 사용 가능한 하나 이상의 OS 파일을 삭제하도록 선택할 수도 있습니다.

단계

1. 기본 보기에서 * 관리 * 를 선택한 다음 메뉴: 업그레이드 센터 [SANtricity 소프트웨어 저장소 관리] 를 선택합니다.

   SANtricity OS 소프트웨어 저장소 관리 대화 상자가 나타납니다.

2. 다음 작업 중 하나를 수행합니다.
   - * 가져오기: *
     i. 가져오기 * 를 클릭합니다.
     ii. 찾아보기 * 를 클릭한 다음 추가할 OS 파일이 있는 위치로 이동합니다. OS 파일의 파일 이름은 N2800-830000-000.DLP와 비슷합니다.
     iii. 추가할 OS 파일을 하나 이상 선택한 다음 * 가져오기 * 를 클릭합니다.
   - * 삭제: *
     i. 소프트웨어 저장소에서 제거할 OS 파일을 하나 이상 선택합니다.
     ii. 삭제 * 를 클릭합니다.

결과

가져오기를 선택한 경우 파일이 업로드되고 확인됩니다. 삭제를 선택하면 소프트웨어 저장소에서 파일이 제거됩니다.

스토리지 프로비저닝

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 용량 할당에 대해 자세히 알아보십시오

vCenter용 저장소 플러그인에서 볼륨이라는 데이터 컨테이너를 생성하여 호스트가 스토리지의 저장소에 액세스할 수 있도록 할 수 있습니다.

볼륨 유형 및 특성

볼륨은 스토리지 어레이에서 스토리지 공간을 관리하고 구성하는 데이터 컨테이너입니다.

스토리지 배열에서 사용 가능한 스토리지 용량에서 볼륨을 생성하여 시스템 리소스를 구성할 수 있습니다. "볼륨"의 개념은 빠른 액세스를 위해 파일을 구성하기 위해 컴퓨터의 폴더/디렉토리를 사용하는 것과 비슷합니다.

볼륨은 호스트에서 볼 수 있는 유일한 데이터 계층입니다. SAN 환경에서는 볼륨이 LUN(논리 유닛 번호)에 매핑됩니다. 이러한 LUN은 FC, iSCSI 및 SAS를 비롯한 스토리지 어레이에서 지원하는 하나 이상의 호스트 액세스 프로토콜을 사용하여 액세스할 수 있는 사용자 데이터를 저장합니다.

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 단일 컨트롤러로 볼륨의 워크로드를 관리할 수 있습니다. 이중 컨트롤러 어레이에서 볼륨에는 볼륨을 "소유"하는 기본 컨트롤러(A 또는 B)가 있습니다. 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.

- * 리소스 프로비저닝 * — EF600 또는 EF300 스토리지 어레이의 경우 백그라운드 초기화 프로세스 없이 즉시 볼륨을 사용하도록 지정할 수 있습니다. 리소스 프로비저닝된 볼륨은 SSD 볼륨 그룹 또는 풀의 일반 볼륨으로, 볼륨이 생성될 때 드라이브 용량이 할당되지만 드라이브 블록이 할당 해제(매핑 해제)됩니다.
- * 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.

볼륨에 대한 용량입니다

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.

생성 및 확장 용량

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 생성하는 경우 이미 존재하는 풀 또는 볼륨 그룹에 추가 볼륨을 생성하고 있습니다. 볼륨 용량을 확장한 후 파일 시스템 크기를 수동으로 늘려야 합니다. 이 방법은 사용 중인 파일 시스템에 따라 다릅니다. 자세한 내용은 호스트 운영 체제 설명서를 참조하십시오.

플러그인 인터페이스에서는 씬 볼륨을 생성하는 옵션을 제공하지 않습니다.

볼륨에 대해 보고된 용량입니다

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

일반적으로 볼륨의 보고된 용량을 볼륨이 커질 것으로 생각되는 최대 용량으로 설정합니다. 볼륨은 애플리케이션에 예측 가능하고 우수한 성능을 제공합니다. 이는 생성 시 모든 가용 용량이 예약되고 할당되기 때문입니다.

용량 제한

볼륨의 최소 용량은 1MiB이고 최대 용량은 풀 또는 볼륨 그룹에 있는 드라이브의 수와 용량에 따라 결정됩니다.

볼륨에 대해 보고된 용량을 늘릴 경우 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.

애플리케이션별 워크로드

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 작업 부하 사용에 대한 질문에 답하라는 메시지가 표시됩니다. 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 * — 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 Server를 참조하십시오
  - Microsoft Exchange Server를 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 System Manager를 시작합니다. 이 인터페이스를 통해 다음과 같은 몇 가지 방법으로 애플리케이션별 워크로드와 관련된 정보를 볼 수 있습니다.

- Volumes(볼륨) 타일에서 Applications & Workload(애플리케이션 및 워크로드) 탭을 선택하여 워크로드별로 그룹화된 스토리지 어레이의 볼륨과 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지를 생성합니다

vCenter용 저장소 플러그인에서 먼저 특정 애플리케이션 유형에 대한 워크로드를 생성하여 저장소를 생성합니다. 다음으로, 기본 볼륨 특성이 유사한 볼륨을 생성하여 스토리지 용량을 워크로드에 추가합니다.

1단계**:** 워크로드 생성

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

이 작업에 대해

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.

시스템에서는 다음 애플리케이션 유형에 대해서만 최적화된 볼륨 구성을 권장합니다.

- Microsoft SQL Server를 참조하십시오
- Microsoft Exchange Server를 참조하십시오
- 비디오 감시
- VMware ESXi(가상 머신 파일 시스템과 함께 사용할 볼륨용)

단계

1. 관리 페이지에서 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 메뉴: Create [Workload](워크로드 생성)를 선택합니다.

애플리케이션 워크로드 생성 대화 상자가 나타납니다.

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

2단계**:** 볼륨 생성

볼륨을 생성하여 애플리케이션별 워크로드에 스토리지 용량을 추가하고 생성된 볼륨을 특정 호스트 또는 호스트 클러스터에 표시할 수 있습니다.

이 작업에 대해

대부분의 애플리케이션 유형은 사용자 정의 볼륨 구성으로 기본 설정되지만, 다른 유형은 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. 시스템에서는 이 정보를 사용하여 최적의 볼륨 구성을 생성합니다. 이 구성은 필요에 따라 편집할 수 있습니다.

메뉴에서 볼륨을 생성할 수 있습니다. Provisioning [Manage Volumes > Create > Volumes] 또는 메뉴에서 Provisioning [Configure Pools and Volume Groups > Create > Volumes]. 이 절차는 두 선택 항목에 대해 동일합니다.

볼륨을 생성하는 프로세스는 여러 단계로 이루어집니다.

2a단계**:** 볼륨의 호스트를 선택합니다

첫 번째 단계에서는 볼륨에 대한 특정 호스트 또는 호스트 클러스터를 선택하거나 호스트를 나중에 할당하도록 선택할 수 있습니다.

시작하기 전에

다음을 확인합니다.

- 유효한 호스트 또는 호스트 클러스터가 정의되었습니다(메뉴: Provisioning [Configure Hosts](호스트 구성)로 이동).
- 호스트에 대한 호스트 포트 식별자가 정의되었습니다.
- DA 지원 볼륨을 생성하려는 경우 호스트 접속에서 DA(Data Assurance)를 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. 관리 페이지에서 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 메뉴: Create [Volumes](볼륨 생성)를 선택합니다.

   호스트 선택 대화 상자가 나타납니다.
4. 드롭다운 목록에서 볼륨을 할당할 특정 호스트 또는 호스트 클러스터를 선택하거나 나중에 호스트 또는 호스트 클러스터를 할당하도록 선택합니다.
5. 선택한 호스트 또는 호스트 클러스터에 대한 볼륨 생성 순서를 계속하려면 * 다음 * 을 클릭합니다

   워크로드 선택 대화 상자가 나타납니다.

2b단계**:** 볼륨에 대한 워크로드를 선택합니다

두 번째 단계에서는 VMware와 같은 특정 애플리케이션에 맞게 스토리지 시스템 구성을 사용자 지정할 워크로드를 선택합니다.

이 작업에 대해

이 작업에서는 워크로드에 대한 볼륨을 생성하는 방법에 대해 설명합니다. 일반적으로 워크로드에는 유사한 특징이 있는 볼륨이 포함되어 있으며, 이러한 볼륨은 워크로드가 지원하는 애플리케이션의 유형에 따라 최적화됩니다. 이 단계에서 워크로드를 정의하거나 기존 워크로드를 선택할 수 있습니다.

다음 지침을 염두에 두십시오.

- 애플리케이션별 워크로드를 사용하는 경우, 시스템에서는 애플리케이션 워크로드 I/O와 애플리케이션 인스턴스의 기타 트래픽 간의 경합을 최소화하기 위해 최적화된 볼륨 구성을 권장합니다. 볼륨 추가/편집 대화 상자(다음 단계에서 사용 가능)를 사용하여 권장 볼륨 구성을 검토한 다음 시스템 권장 볼륨 및 특성을 편집, 추가 또는 삭제할 수 있습니다.
- 다른 애플리케이션 유형을 사용할 경우 볼륨 추가/편집 대화 상자(다음 단계에서 사용 가능)를 사용하여 볼륨 구성을 수동으로 지정합니다.

단계

1. 다음 중 하나를 수행합니다.
   - 기존 워크로드에 대한 볼륨 생성 * 옵션을 선택한 다음 드롭다운 목록에서 워크로드를 선택합니다.
   - 지원되는 애플리케이션 또는 "기타" 애플리케이션의 새 워크로드를 정의하려면 * 새 워크로드 생성 * 옵션을 선택한 후 다음 단계를 수행합니다.
     - 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 않으면 다음 단계로

이동합니다.

단계 **2c:** 볼륨 추가 또는 편집

세 번째 단계에서는 볼륨 구성을 정의합니다.

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.
  - DA 지원 볼륨을 생성하려면 DA를 지원하는 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "DA" 옆에 * Yes * 가 표시됨).
  - DA 기능은 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.
  - 보안이 설정된 볼륨을 생성하려면 보안이 가능한 풀 또는 볼륨 그룹을 선택합니다(풀 및 볼륨 그룹 후보 테이블에서 "보안 가능" 옆에 있는 예 확인).
  - 드라이브 보안 기능은 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 읽기 중에 고유 암호화 키를 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

볼륨 추가/편집 대화 상자에 표시된 적합한 풀 또는 볼륨 그룹에서 볼륨을 생성합니다. 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. 이전 단계에서 다른 워크로드를 선택했는지 또는 애플리케이션별 워크로드를 선택했는지의 여부에 따라 다음 작업 중 하나를 선택합니다.
   - * 기타 * — 하나 이상의 볼륨을 생성하는 데 사용할 각 풀 또는 볼륨 그룹에서 * 새 볼륨 추가 * 를 클릭합니다.

필드 세부 정보

필드에 입력합니다	설명
볼륨 이름	볼륨 생성 시퀀스 중에 볼륨에 기본 이름이 할당됩니다. 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 4GiB 단위로 할당됩니다. 4GiB의 배수에 포함되지 않은 용량은 할당되지만 사용할 수 없습니다. 전체 용량을 사용할 수 있도록 용량을 4GiB 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
세그먼트 크기	에는 볼륨 그룹의 볼륨에만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. * 허용된 세그먼트 크기 전환 * — 시스템이 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.

◦ * 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 세부 정보

필드에 입력합니다	설명
볼륨 이름	볼륨 생성 시퀀스 중에 볼륨에 기본 이름이 할당됩니다. 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 4GiB 단위로 할당됩니다. 4GiB의 배수에 포함되지 않은 용량은 할당되지만 사용할 수 없습니다. 전체 용량을 사용할 수 있도록 용량을 4GiB 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
세그먼트 크기	에는 볼륨 그룹의 볼륨에만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. * 허용된 세그먼트 크기 전환 * — 시스템이 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 대한 볼륨 생성 순서를 계속하려면 * 다음 * 을 클릭합니다.

2D 단계**:** 체적 구성을 검토합니다

마지막 단계에서는 생성하려는 볼륨의 요약을 검토하고 필요한 내용을 변경합니다.

단계

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

작업을 마친 후

- vSphere Client에서 볼륨에 대한 데이터 저장소를 생성합니다.
- 응용 프로그램이 볼륨을 사용할 수 있도록 응용 프로그램 호스트에서 필요한 모든 운영 체제 수정을 수행합니다.
- 운영 체제 특정 유틸리티(타사 공급업체에서 제공)를 실행한 다음 SMcli 명령을 실행합니다 `-identifyDevices` 볼륨 이름과 호스트 스토리지 배열 이름을 서로 연관시킵니다.

  SMcli는 SANtricity OS에 포함되어 있으며 SANtricity System Manager를 통해 다운로드할 수 있습니다. SANtricity System Manager를 통해 SMcli를 다운로드하는 방법에 대한 자세한 내용은 를 참조하십시오 "SANtricity System Manager 온라인 도움말에서 CLI(Command Line Interface) 항목을 다운로드하십시오".

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨 용량을 늘립니다

볼륨의 크기를 조정하여 보고된 용량을 늘릴 수 있습니다.

시작하기 전에

다음을 확인합니다.

- 볼륨의 연결된 풀 또는 볼륨 그룹에서 충분한 가용 용량을 사용할 수 있습니다.
- 볼륨은 최적이며 수정 상태가 아닙니다.
- 볼륨에서 사용 중인 핫 스페어 드라이브가 없습니다. (볼륨 그룹의 볼륨에만 적용됩니다.)

이 작업에 대해

이 작업에서는 풀 또는 볼륨 그룹에서 사용 가능한 용량을 사용하여 볼륨의 보고된 용량(호스트에 보고된 용량)을 늘리는 방법에 대해 설명합니다. 이 풀 또는 볼륨 그룹의 다른 볼륨에 대해 가질 수 있는 향후 용량 요구 사항을 고려하십시오.

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. Manage * 페이지에서 크기를 조정할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 용량을 늘릴 볼륨을 선택한 다음 * 용량 증가 * 를 선택합니다.

   용량 증가 확인 대화 상자가 나타납니다.

4. 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.

5. 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.
6. 증가 * 를 클릭합니다.

   선택한 항목에 따라 볼륨 용량이 증가합니다. 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨 설정을 변경합니다

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

시작하기 전에

변경할 볼륨이 최적 상태인지 확인합니다.

단계

1. 관리 페이지에서 변경할 볼륨이 포함된 스토리지 배열을 선택합니다.

2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 변경할 볼륨을 선택한 다음 * 설정 보기/편집 * 을 선택합니다.

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

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

   필드 세부 정보

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.
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)입니다. 볼륨의 고유한 16진수 식별자입니다. • 확장 고유 식별자(EUI)입니다. 볼륨의 EUI-64 식별자입니다. • 하위 시스템 식별자(SSID)입니다. 볼륨의 스토리지 배열 하위 시스템 식별자입니다.

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

필드 세부 정보

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.
세그먼트 크기 조정	에는 볼륨 그룹의 볼륨에 대해서만 표시되는 세그먼트 크기 조정 설정이 나와 있습니다. 세그먼트 크기를 변경하여 성능을 최적화할 수 있습니다. * 허용된 세그먼트 크기 전환 * — 시스템이 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.

설정	설명
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.
SSD 캐시	EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다. 에는 SSD 캐시 설정이 나와 있습니다. 이 설정은 호환 볼륨에서 읽기 전용 성능을 향상하는 방법으로 활성화할 수 있습니다. 볼륨은 동일한 드라이브 보안 및 데이터 보증 기능을 공유하는 경우 호환됩니다. SSD Cache 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.

6. 저장 * 을 클릭합니다.

결과

선택한 사항에 따라 볼륨 설정이 변경됩니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 워크로드에 볼륨을 추가합니다

할당되지 않은 볼륨을 기존 또는 새로운 워크로드에 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. 관리 페이지에서 추가할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 애플리케이션 및 워크로드 * 탭을 선택합니다.

   애플리케이션 및 워크로드 보기가 나타납니다.

4. 워크로드에 추가 * 를 선택합니다.

   워크로드 선택 대화 상자가 나타납니다.

5. 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.

6. 작업 순서에 추가를 계속하려면 * 다음 * 을 선택합니다.

   볼륨 선택 대화 상자가 나타납니다.

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

vCenter용 **SANtricity** 스토리지 플러그인에서 워크로드 설정을 변경합니다

워크로드의 이름을 변경하고 관련 애플리케이션 유형을 볼 수 있습니다.

단계

1. 관리 페이지에서 변경할 워크로드가 포함된 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 애플리케이션 및 워크로드 * 탭을 선택합니다.

   애플리케이션 및 워크로드 보기가 나타납니다.

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

   애플리케이션 및 워크로드 설정 대화 상자가 나타납니다.

5. (선택 사항) 사용자가 제공한 워크로드 이름을 변경합니다.
6. 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨을 초기화합니다

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 최적 상태이며 볼륨에서 수정 작업이 진행 중이지 않습니다. * 주의: * 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.

다음 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 절차는 풀 또는 볼륨 그룹에서 생성된 표준 볼륨에만 적용됩니다.

단계

1. 관리 페이지에서 초기화할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 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.

4. 초기화하려는 볼륨을 하나 이상 선택하고 작업을 수행할지 확인합니다.

결과

시스템은 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).

이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 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, 애플리케이션 오류를 방지하기 위해 재배포가 진행되는 동안 볼륨에 대한 모든 I/O 작업을 중지해야 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. 관리 페이지에서 재배포할 볼륨이 포함된 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 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.

4. 재배포할 볼륨을 하나 이상 선택하고 작업을 수행할지 확인합니다.

결과

선택한 볼륨이 기본 컨트롤러 소유자로 이동하거나 Redistribute Volumes Unnessary(볼륨 재분산 불필요) 대화 상자가 나타날 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 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. 관리 페이지에서 컨트롤러 소유권을 변경할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 볼륨을 선택한 다음 메뉴 추가 [소유권 변경]을 선택합니다.

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

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

결과

- 시스템에서 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.

vCenter용 SANtricity 스토리지 플러그인에서 볼륨에 대한 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 볼륨의 캐시 설정을 동시에 변경할 수 있습니다.

단계

1. 관리 페이지에서 캐시 설정을 변경할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 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.

4. 기본 * 탭을 선택하여 읽기 캐싱 및 쓰기 캐싱 설정을 변경합니다.

   필드 세부 정보

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 쓰기 캐시가 해제된 후 캐시가 자동으로 플러시됩니다.

5. 고급 * 탭을 선택하여 일반 볼륨의 고급 설정을 변경합니다. 고급 캐시 설정은 일반 볼륨에만 사용할 수 있습니다.

필드 세부 정보

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.
배터리가 없는 쓰기 캐싱	배터리가 없는 쓰기 캐싱 설정을 사용하면 배터리가 없거나, 오류가 발생했거나, 완전히 방전되었거나, 완전히 충전되지 않은 경우에도 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. 주의: * 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.
미러링을 사용한 쓰기 캐싱	미러링을 사용한 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.

6. 캐시 설정을 변경하려면 * 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨에 대한 미디어 검사 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. 관리 페이지에서 미디어 스캔 설정을 변경할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 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.

4. 미디어 스캔을 활성화하려면 * 다음 과정을 통해 미디어 스캔 * 확인란을 선택합니다. 미디어 스캔 확인란을 비활성화하면 모든 미디어 스캔 설정이 일시 중단됩니다.
5. 미디어 검사를 실행할 일 수를 지정합니다.
6. 미디어 스캔을 수행하려는 각 볼륨에 대해 * Media Scan * (미디어 스캔 *) 확인란을 선택합니다. 시스템은 미디어 스캔을 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.
7. 저장 * 을 클릭합니다.

결과

선택한 내용에 따라 백그라운드 미디어 검사에 변경 사항이 적용됩니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨을 삭제합니다

하나 이상의 볼륨을 삭제하여 풀 또는 볼륨 그룹의 사용 가능한 용량을 늘릴 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

일반적으로 볼륨이 잘못된 매개 변수 또는 용량으로 생성되었거나, 더 이상 스토리지 구성 요구사항을 충족하지 않은 경우 볼륨을 삭제합니다. 볼륨을 삭제하면 풀 또는 볼륨 그룹의 사용 가능한 용량이 증가합니다.

볼륨을 삭제하면 해당 볼륨의 모든 데이터가 손실됩니다.

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.

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

단계

1. Manage * 페이지에서 삭제할 볼륨이 포함된 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Manage Volumes](볼륨 관리)를 선택합니다.
3. 삭제 * 를 클릭합니다.

   Delete Volumes(볼륨 삭제) 대화 상자가 나타납니다.

4. 삭제할 볼륨을 하나 이상 선택한 다음 작업을 수행할지 확인합니다.
5. 삭제 * 를 클릭합니다.

호스트를 구성합니다

vCenter용 **SANtricity** 스토리지 플러그인에서 호스트 생성에 대해 자세히 알아봅니다

vCenter용 Storage Plugin을 사용하여 스토리지를 관리하려면 네트워크에서 각 호스트를 검색 또는 정의해야 합니다. 호스트는 스토리지 배열의 볼륨에 입출력을 전송하는 서버입니다.

수동 호스트 생성

호스트를 생성하는 것은 스토리지 어레이가 호스트에 연결된 호스트를 파악하고 볼륨에 대한 I/O 액세스를 허용하는 데 필요한 단계 중 하나입니다. 호스트를 수동으로 생성할 수 있습니다.

- * 수동 * — 수동 호스트 생성 중에 호스트 포트 식별자를 목록에서 선택하거나 수동으로 입력하여 연결합니다. 호스트를 생성한 후 볼륨에 대한 액세스를 공유하려는 경우 호스트에 볼륨을 할당하거나 호스트 클러스터에 추가할 수 있습니다.

볼륨이 할당되는 방법입니다

호스트에서 볼륨에 I/O를 보내려면 볼륨을 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 중 호스트와 컨트롤러 사이의 주소 역할을 합니다. 볼륨이 생성된 후 LUN을 변경할 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 호스트 액세스를 생성합니다

vCenter용 Storage Plugin을 사용하여 스토리지를 관리하려면 네트워크에서 각 호스트를 검색 또는 정의해야 합니다.

이 작업에 대해

호스트를 생성하면 스토리지 시스템에 대한 접속 및 볼륨에 대한 입출력 액세스를 제공하는 호스트 매개 변수를 정의할 수 있습니다.

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. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

3. MENU: Create [Host] 를 클릭합니다.

   Create Host 대화 상자가 나타납니다.

4. 필요에 따라 호스트 설정을 선택합니다.

필드 세부 정보

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 선택 * — 일반적으로 호스트 포트는 로그인되어 있고 드롭다운 목록에서 사용할 수 있어야 합니다. 목록에서 호스트 포트 식별자를 선택할 수 있습니다. • * 수동 추가 * — 호스트 포트 식별자가 목록에 표시되지 않으면 호스트 포트가 로그인되어 있지 않은 것입니다. HBA 유틸리티 또는 iSCSI 이니시에이터 유틸리티를 사용하여 호스트 포트 식별자를 찾아 호스트에 연결할 수 있습니다. 호스트 포트 식별자를 수동으로 입력하거나 유틸리티에서 호스트 포트 필드로 복사/붙여 넣을 수 있습니다(한 번에 하나씩). 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 이니시에이터 암호를 설정합니다	(선택 사항) iSCSI IQN을 사용하여 호스트 포트를 선택하거나 수동으로 입력한 경우, CHAP(Challenge Handshake Authentication Protocol)를 사용하여 인증하기 위해 스토리지 배열에 액세스를 시도하는 호스트를 요구하려면 “Set CHAP initiator secret(CHAP 초기자 암호 설정)” 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 사용되는 유일한 iSCSI 인증 방법은 CHAP입니다.

5. Create * 를 클릭합니다.
6. 호스트 정보를 업데이트해야 하는 경우 테이블에서 호스트를 선택하고 * 설정 보기/편집 * 을 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, 호스트 IPT에 대해 생성된 첫 번째 포트의 기본 별칭은 "ipt_1"입니다.

작업을 마친 후

I/O 작업에 사용할 수 있도록 볼륨을 호스트에 할당해야 합니다. 로 이동합니다 "호스트에 볼륨을 할당합니다".

vCenter용 **SANtricity** 스토리지 플러그인에서 호스트 클러스터를 생성합니다

두 개 이상의 호스트에서 동일한 볼륨에 대한 I/O 액세스가 필요한 경우 호스트 클러스터를 생성할 수 있습니다.

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. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.
3. 메뉴 선택: Create [Host cluster](호스트 클러스터 생성)를 선택합니다.

   Create Host Cluster 대화상자가 나타납니다.
4. 호스트 클러스터에 대한 설정을 적절히 선택합니다.

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.

5. 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.

작업을 마친 후

I/O 작업에 사용할 수 있도록 볼륨을 호스트 클러스터에 할당해야 합니다. 로 이동합니다 "호스트에 볼륨을 할당합니다".

vCenter용 **SANtricity** 스토리지 플러그인에서 호스트에 볼륨을 할당합니다

I/O 작업에 사용할 수 있도록 호스트 또는 호스트 클러스터에 볼륨을 할당해야 합니다.

시작하기 전에

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 모든 볼륨이 느린 초기화로 돌아갑니다.

이 작업에 대해

볼륨 할당은 스토리지 배열의 해당 볼륨에 대한 호스트 또는 호스트 클러스터 액세스 권한을 부여합니다.

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.

  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.

단계

1. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

호스트 구성 페이지가 열립니다.

3. 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 열을 정렬하거나 필터 상자에 원하는 항목을 입력할 수 있습니다.

4. 할당할 각 볼륨 옆의 확인란을 선택하거나 표 머리글에서 확인란을 선택하여 모든 볼륨을 선택합니다.
5. 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.

vCenter용 SANtricity 스토리지 플러그인에서 볼륨 할당을 취소합니다

볼륨에 대한 I/O 액세스가 더 이상 필요하지 않은 경우 호스트 또는 호스트 클러스터에서 해당 볼륨의 할당을 취소할 수 있습니다.

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. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

3. 편집할 호스트 또는 호스트 클러스터를 선택하고 * 볼륨 할당 해제 * 를 클릭합니다.

   현재 할당된 모든 볼륨이 표시된 대화 상자가 나타납니다.

4. 할당 취소할 각 볼륨 옆의 확인란을 선택하거나 표 머리글에서 확인란을 선택하여 모든 볼륨을 선택합니다.
5. 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 클러스터의 이름, 호스트 운영 체제 유형 및 관련 호스트 클러스터를 변경할 수 있습니다.

단계

1. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

3. 편집할 호스트를 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   현재 호스트 설정을 보여주는 대화 상자가 나타납니다.

4. 호스트 속성을 변경하려면 * 속성 * 탭이 선택되어 있는지 확인한 다음 필요에 따라 설정을 변경합니다.

   필드 세부 정보

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. 포트 설정을 변경하려면 * 호스트 포트 * 탭을 클릭한 다음 필요에 따라 설정을 변경합니다.

필드 세부 정보

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. Fibre Channel 및 Infiniband 호스트 포트 식별자 이름은 16자여야 합니다. iSCSI 호스트 포트 식별자 이름은 최대 223자입니다. 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. 시스템은 CHAP(Challenge Handshake Authentication Protocol) 방법을 사용하여 초기 링크 중에 대상 및 초기자의 ID를 확인합니다. 인증은 CHAP 암호라는 공유 보안 키를 기반으로 합니다.

6. 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 호스트 또는 호스트 클러스터를 삭제합니다

호스트 또는 호스트 클러스터를 제거하여 볼륨이 더 이상 해당 호스트에 연결되지 않도록 할 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. 관리 페이지에서 호스트 연결이 있는 스토리지 배열을 선택합니다.

2. 메뉴: Provisioning [Configure Hosts](호스트 구성)를 선택합니다.

   호스트 구성 페이지가 열립니다.

3. 삭제할 호스트 또는 호스트 클러스터를 선택하고 * Delete * 를 클릭합니다.

   확인 대화 상자가 나타납니다.

4. 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.

풀 및 볼륨 그룹을 구성합니다

vCenter용 **SANtricity** 스토리지 플러그인에서 스토리지 풀 및 볼륨 그룹에 대해 자세히 알아보십시오

vCenter용 저장소 플러그인에서 스토리지를 프로비저닝하려면 스토리지 배열에서 사용할 HDD(하드 디스크 드라이브) 또는 SSD(Solid State Disk) 드라이브가 포함될 풀 또는 볼륨 그룹을 만듭니다.

프로비저닝

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

- 풀
- 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.

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 시스템은 모든 활성 드라이브에 걸쳐 데이터를 동적으로 재조정합니다.

풀은 또 다른 RAID 레벨로 작동하며, 기본 RAID 아키텍처를 가상화하여 재구축, 드라이브 확장, 드라이브 손실 처리 등의 작업을 수행할 때 성능과 유연성을 최적화합니다. 시스템은 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 1개의 드라이브 용량이 예약됩니다. 이 여유 용량을 "보존 용량"이라고 합니다.

풀을 생성할 때 비상 사용을 위해 특정 용량이 보존됩니다. 이 용량은 여러 드라이브의 관점에서 표현되지만 실제 구현은 전체 드라이브 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.

풀 또는 볼륨 그룹을 사용할지 여부를 결정합니다

풀을 선택합니다

- 더 빠른 드라이브 리빌드 및 단순화된 스토리지 관리 또는 높은 수준의 랜덤 워크로드가 필요한 경우
- 풀을 구성하는 드라이브 집합에 각 볼륨의 데이터를 무작위로 분산하려는 경우 풀의 RAID 레벨 또는 풀의 볼륨을 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.

자동 및 수동 풀 생성

스토리지 구성에 따라 시스템에서 자동으로 풀을 생성하도록 허용하거나 직접 풀을 생성할 수 있습니다. 풀은 논리적으로 그룹화된 드라이브 집합입니다.

풀을 생성 및 관리하기 전에 풀을 자동으로 생성하는 방법과 풀을 수동으로 생성해야 하는 시기에 대한 다음 섹션을 검토하십시오.

자동 작성

시스템에서 스토리지 시스템에서 할당되지 않은 용량을 감지하면 스토리지 시스템에서 할당되지 않은 용량을 감지하면 자동 풀 생성이 시작됩니다. 하나 이상의 풀을 생성하거나 기존 풀에 할당되지 않은 용량을 추가하라는 메시지가 자동으로 표시됩니다.

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 같아야 합니다. 다음 작업을 완료하라는 메시지가 표시됩니다.
- 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 셸프 손실 방지 또는 드로어 손실 보호 상태를 유지할 수 없습니다. 스토리지 어레이에 여러 애플리케이션이 있고 동일한 드라이브 리소스를 두고 경합하지 않으려는 경우에도 풀을 수동으로 생성할 수 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 풀을 자동으로 생성합니다

시스템에서 할당되지 않은 드라이브 11개 이상을 감지하거나 기존 풀에 적합한 할당되지 않은 드라이브 1개를 감지하면 자동으로 풀을 생성할 수 있습니다. 풀은 논리적으로 그룹화된 드라이브 집합입니다.

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

자동 풀 생성을 사용하여 스토리지 어레이에서 할당되지 않은 모든 드라이브를 하나의 풀로 쉽게 구성하고 기존 풀에 드라이브를 추가할 수 있습니다.

다음 사항에 유의하십시오.

- 스토리지 배열에 드라이브를 추가하면 시스템에서 드라이브를 자동으로 감지하고 드라이브 유형 및 현재 구성에 따라 단일 풀 또는 다중 풀을 생성하라는 메시지를 표시합니다.
- 풀이 이전에 정의된 경우 시스템에서 호환 가능한 드라이브를 기존 풀에 추가하는 옵션을 자동으로 표시합니다. 새 드라이브를 기존 풀에 추가하면 시스템에서 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. 풀을 생성하려면 스토리지 배열의 모든 드라이브를 사용해야 합니다.

단계

1. 관리 페이지에서 풀의 스토리지 시스템을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 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.

   시스템에서 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.
4. 새 풀의 이름을 변경하려면 * 편집 * 아이콘(연필)을 클릭합니다.
5. 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.
6. Accept * 를 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 풀을 수동으로 생성합니다

설정이 자동 풀 구성에 대한 요구 사항을 충족하지 않는 경우 풀을 수동으로 생성할 수 있습니다. 풀은 논리적으로 그룹화된 드라이브 집합입니다.

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. 풀을 생성하려면 스토리지 배열의 모든 드라이브를 사용해야 합니다.

이 작업에 대해

풀을 생성하는 동안 드라이브 유형, 보안 기능, DA(Data Assurance) 기능, 쉘프 손실 보호, 서랍 손실 보호와 같은 특성을 확인합니다.

EF600 및 EF300 스토리지 어레이의 경우 리소스 프로비저닝과 볼륨 블록 크기도 설정에 포함됩니다.

단계

1. 관리 페이지에서 풀의 스토리지 시스템을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. MENU: Create [Pool] 를 클릭합니다.

   풀 생성 대화 상자가 나타납니다.

4. 풀의 이름을 입력합니다.
5. (선택 사항) 스토리지 배열에 둘 이상의 드라이브 유형이 있는 경우 사용할 드라이브 유형을 선택합니다.

   결과 테이블에는 생성할 수 있는 모든 풀이 나열됩니다.

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

필드 세부 정보

특징	사용
사용 가능한 용량	에는 GiB 단위의 풀 후보 가용 용량이 나와 있습니다. 애플리케이션 스토리지 요구 사항에 맞는 용량을 갖춘 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. 시스템은 보존 용량을 위해 가능한 한 많은 드라이브를 자동으로 예약합니다(풀에 있는 6개 드라이브마다 시스템이 보존 용량을 위해 1개의 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.
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.
DA 가능	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. DA를 사용하려면 DA를 지원하는 풀을 선택합니다. 이 옵션은 DA 기능이 활성화된 경우에만 사용할 수 있습니다. 풀에는 DA를 사용할 수 있거나 DA를 사용할 수 없는 드라이브가 포함될 수 있지만 이 기능을 사용하려면 모든 드라이브가 DA를 지원해야 합니다.

특징	사용
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.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨 그룹을 생성합니다

호스트에서 액세스할 수 있는 하나 이상의 볼륨에 대해 볼륨 그룹을 생성할 수 있습니다. 볼륨 그룹은 RAID 레벨 및 용량과 같은 공유 특성을 가진 볼륨의 컨테이너입니다.

시작하기 전에

다음 지침을 검토하십시오.

- 할당되지 않은 드라이브가 하나 이상 필요합니다.
- 단일 볼륨 그룹에 포함할 수 있는 드라이브 용량에 제한이 있습니다. 이러한 제한은 호스트 유형에 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 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 시스템은 볼륨 그룹을 생성할 때 Advanced(고급) 기능에서 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.

이 작업에 대해

볼륨 그룹을 생성하는 동안 드라이브 수, 보안 기능, DA(Data Assurance) 기능, 쉘프 손실 보호, 서랍 손실 보호와 같은 그룹 특성을 확인합니다.

EF600 및 EF300 스토리지 어레이의 설정에는 리소스 프로비저닝, 드라이브 블록 크기, 볼륨 블록 크기도 포함됩니다.

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

단계

1. 관리 페이지에서 볼륨 그룹의 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 메뉴 [Volume group](볼륨 그룹)을 클릭합니다.

   Create Volume Group 대화상자가 나타납니다.
4. 볼륨 그룹의 이름을 입력합니다.
5. 데이터 스토리지 및 보호 요구사항에 가장 적합한 RAID 레벨을 선택합니다. 볼륨 그룹 후보 테이블이 나타나고 선택한 RAID 레벨을 지원하는 후보만 표시됩니다.
6. (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.
7. (선택 사항) 자동 방법 또는 수동 방법을 선택하여 볼륨 그룹에서 사용할 드라이브를 정의할 수 있습니다. 자동 방법이 기본 선택 항목입니다.

   드라이브 중복성과 최적의 드라이브 구성을 이해하는 전문가가 아니라면 수동 방법을 사용하지 마십시오.

   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.
8. 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. 자세한 내용은 SANtricity 시스템 관리자 설명서를 참조하십시오. "볼륨 그룹을 생성합니다".

vCenter용 SANtricity 스토리지 플러그인에서 풀 또는 볼륨 그룹에 용량을 추가합니다

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

시작하기 전에

- 드라이브가 최적 상태여야 합니다.

- 드라이브는 드라이브 유형(HDD 또는 SSD)이 동일해야 합니다.
- 풀 또는 볼륨 그룹이 Optimal 상태여야 합니다.
- 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

이 작업에서는 풀 또는 볼륨 그룹에 포함할 가용 용량을 추가할 수 있습니다. 이 여유 용량을 사용하여 추가 볼륨을 생성할 수 있습니다. 이 작업 중에 볼륨의 데이터에 액세스할 수 있습니다.

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 배열의 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. 관리 페이지에서 풀 또는 볼륨 그룹이 있는 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 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.

4. 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 세부 정보

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 보호할 수 있지만 이 기능을 사용하려면 모든 드라이브가 안전해야 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 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.
DA 가능	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.

5. 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 손실 방지
   - 서랍 손실 방지
   - 전체 디스크 암호화 기능
   - Data Assurance입니다
   - DULBE 기능

6. 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 **SSD** 캐시를 생성합니다

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.

EF600 또는 EF300 스토리지 시스템에서는 SSD Cache를 사용할 수 없습니다.

이 작업에 대해

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.

SSD Cache를 생성할 때는 다음 지침을 따르십시오.

- SSD Cache는 나중에 생성하지 않을 때만 보안을 설정할 수 있습니다.
- 스토리지 어레이당 하나의 SSD Cache만 지원됩니다.
- 스토리지 배열의 최대 가용 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. 관리 페이지에서 캐시의 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 메뉴: 생성 [SSD Cache] 를 클릭합니다.

   SSD 캐시 생성 대화 상자가 나타납니다.

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

   필드 세부 정보

특징	사용
용량	에는 사용 가능한 용량이 GiB 단위로 표시됩니다. 애플리케이션의 스토리지 요구 사항에 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 Cache를 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 캐시를 생성하려면 * 보안 활성화 * 확인란을 선택합니다. 참고: 한 번 설정하면 보안을 비활성화할 수 없습니다. SSD Cache는 나중에 생성하지 않을 때만 보안을 설정할 수 있습니다.
DA 가능	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.

6. 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.

7. Create * 를 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 풀에 대한 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.

> 플러그인 인터페이스를 사용하여 풀의 RAID 레벨을 변경할 수 없습니다. 플러그인은 풀을 자동으로 RAID 6으로 구성합니다.

단계

1. 관리 페이지에서 풀이 있는 스토리지 시스템을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 편집할 풀을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   풀 설정 대화 상자가 나타납니다.

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

필드 세부 정보

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 플러그인이 메시지를 보내 더 많은 스토리지 공간을 추가하거나 불필요한 객체를 삭제할 수 있도록 합니다. 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) 및 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.

5. 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨 그룹에 대한 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. 관리 페이지에서 볼륨 그룹이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 편집할 볼륨 그룹을 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   볼륨 그룹 설정 대화 상자가 나타납니다.

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

필드 세부 정보

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 중요한 데이터를 기업 또는 개인 차원에서 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 사용 가능한 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.

5. 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 플러그인은 볼륨 그룹을 구성하는 모든 볼륨의 RAID 레벨을 변경합니다. 작업 중에 성능이 약간 영향을 받을 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 **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.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

단계

1. 관리 페이지에서 SSD Cache가 포함된 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 편집할 SSD Cache를 선택한 다음 * 설정 보기/편집 * 을 클릭합니다.

   SSD Cache Settings 대화상자가 나타납니다.

4. SSD Cache 설정을 적절하게 검토 또는 편집합니다.

필드 세부 정보

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.

5. 저장 * 을 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 **SSD** 캐시 통계를 확인합니다

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

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

이 작업에 대해

상세 통계의 하위 집합인 공칭 통계가 SSD 캐시 통계 보기 대화 상자에 표시됩니다. 모든 SSD 통계를 .csv 파일로 내보낼 때만 SSD Cache에 대한 자세한 통계를 볼 수 있습니다.

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

단계

1. 관리 페이지에서 SSD Cache가 포함된 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 통계를 보려는 SSD Cache를 선택하고 메뉴: 추가 [SSD Cache 보기] 통계 를 클릭합니다.

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

   필드 세부 정보

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.

4. 대화 상자를 닫으려면 * 취소 * 를 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 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. 풀은 RAID 6로만 구성됩니다.

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. 관리 페이지에서 풀 또는 볼륨 그룹이 있는 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. Uncommon Tasks [Check volume redundancy] 메뉴를 선택합니다.

   Check Redundancy 대화상자가 나타납니다.

4. 확인할 볼륨을 선택한 다음 check 를 입력하여 이 작업을 수행할지 확인합니다.
5. 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 상태가 Status 열에 표시됩니다.
   - 미디어 또는 패리티 오류가 발생하면 검사가 중지되고 오류가 보고됩니다. 다음 표에는 이중화 검사 상태에 대한 자세한 정보가 나와 있습니다.

필드 세부 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.

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

vCenter용 **SANtricity** 스토리지 플러그인에서 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. 관리 페이지에서 풀 또는 볼륨 그룹이 있는 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 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.

4. Uncommon Tasks[삭제] 메뉴를 선택하고 확인합니다.

결과

시스템은 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.

vCenter용 **SANtricity** 스토리지 플러그인에서 볼륨 그룹의 사용 가능한 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 가용 용량 통합 권장 사항이 나타납니다. 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. 관리 페이지에서 볼륨 그룹이 있는 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 통합할 여유 용량이 있는 볼륨 그룹을 선택한 다음, Uncommon Tasks [Consolidate volume group free capacity] 메뉴를 선택합니다.

여유 용량 통합 대화 상자가 나타납니다.

4. 이 작업을 수행하려면 '통합'을 입력하십시오.
5. 통합 * 을 클릭합니다.

결과

시스템은 볼륨 그룹의 여유 용량 영역을 이후 스토리지 구성 작업을 위해 인접한 하나의 용량으로 통합(조각 모음)하기 시작합니다.

작업을 마친 후

탐색 사이드바에서 * Operations * 를 선택하여 통합 가용 용량 작업의 진행률을 확인합니다. 이 작업은 시간이 오래 걸릴 수 있으며 시스템 성능에 영향을 줄 수 있습니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 드라이브의 **LED** 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. 관리 페이지에서 스토리지 배열을 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 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.

4. 드라이브를 찾은 후 * 끄기 * 를 클릭합니다.

vCenter용 **SANtricity** 스토리지 플러그인에서 기존 풀 또는 **SSD** 캐시의 용량을 줄입니다

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.

다음은 성능에 영향을 미칠 수 있는 잠재적 영향입니다.

- 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.

다음은 보안 가능 드라이브에 미치는 영향입니다.

- 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. 관리 페이지에서 스토리지 배열을 선택합니다.

   메뉴: Provisioning [Configure Pools and Volume Groups]를 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.

결과

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

vCenter용 **SANtricity** 스토리지 플러그인에서 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. 관리 페이지에서 풀 또는 볼륨 그룹이 있는 스토리지 어레이를 선택합니다.
2. 메뉴: Provisioning [Configure Pools and Volume Groups]를 선택합니다.
3. 보안을 설정할 풀 또는 볼륨 그룹을 선택한 다음 MENU: More [Enable security] 를 클릭합니다.

   보안 활성화 확인 대화 상자가 나타납니다.

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

vCenter용 SANtricity 스토리지 플러그인을 제거합니다

vCenter Server Appliance에서 플러그인을 제거하고 애플리케이션 호스트에서 플러그인 웹 서버를 제거할 수 있습니다.

이러한 단계는 순서에 관계없이 수행할 수 있는 두 가지 고유 단계입니다. 그러나 플러그인 등록을 취소하기 전에 응용 프로그램 호스트에서 플러그인 웹서버를 제거하도록 선택하면 등록 스크립트가 해당 프로세스 중에 제거되고 방법 1을 사용하여 등록을 취소할 수 없습니다.

vCenter Server Appliance에서 플러그인 등록을 취소합니다

vCenter Server Appliance에서 플러그인 등록을 취소하려면 다음 방법 중 하나를 선택합니다.

- 방법 1: 등록 스크립트를 실행합니다
- 방법 2: vCenter Server Mob 페이지를 사용합니다

방법 1: 등록 스크립트를 실행합니다

1. 명령줄을 통해 프롬프트를 열고 다음 디렉토리로 이동합니다.

   "<설치 디렉토리>\vcenter-register\bin"

2. "vcenter-register.bat" 파일을 실행합니다.

   vcenter-register.bat ^

   '-action unregisterPlugin^'

   "-vCenterHostname <vCenter FQDN>^"

   '-사용자 이름 <관리자 사용자 이름>^'

3. 스크립트가 성공했는지 확인합니다.

   로그는 "%install_dir%/working/logs/vc-registration.log"에 저장됩니다.

방법 **2: vCenter Server Mob** 페이지를 사용합니다

1. 웹 브라우저를 열고 다음 URL을 입력합니다.

   https://<FQDN[] vCenter Server>/MOB의

2. 관리자 자격 증명 아래에 로그인합니다.
3. 'extensionManager'의 속성 이름을 찾아 해당 속성과 관련된 링크를 클릭합니다.
4. 자세히 * 를 클릭하여 속성 목록을 확장합니다. 링크 를 클릭합니다.
5. 확장자 plugin.netapp.eseries` 가 목록에 있는지 확인합니다.
6. 이 경우 UnregisterExtension 메서드 를 클릭합니다.
7. 대화 상자에 plugin.netapp.eseries` 값을 입력하고 * Invoke Method * 를 클릭합니다.
8. 대화 상자를 닫고 웹 브라우저를 새로 고칩니다.
9. plugin.netapp.eseries` 확장자가 목록에 없는지 확인합니다.

> 이 절차에서는 vCenter Server Appliance에서 플러그인 등록을 해제하지만 서버에서 플러그인 패키지 파일은 제거하지 않습니다. 패키지 파일을 제거하려면 SSH를 사용하여 vCenter Server Appliance에 액세스하고 "etc/vmware/vsphere-ui/vc-packages/vsphere-client-environment/" 디렉토리로 이동합니다. 그런 다음 플러그인과 연결된 디렉터리를 제거합니다.

애플리케이션 호스트에서 플러그인 웹 서버를 제거합니다

애플리케이션 호스트에서 플러그인 소프트웨어를 제거하려면 다음 단계를 수행하십시오.

1. 응용 프로그램 서버에서 * 제어판 * 으로 이동합니다.
2. 앱 및 기능 * 으로 이동한 다음 * vCenter * 용 SANtricity 스토리지 플러그인 을 선택합니다.
3. 제거/변경 * 을 클릭합니다.

   확인 대화 상자가 열립니다.

4. 제거 * 를 클릭합니다.

   제거가 완료되면 확인 메시지가 표시됩니다.

5. 완료 * 를 클릭합니다.

vCenter용 SANtricity 스토리지 플러그인에 대한 FAQ

이 FAQ는 질문에 대한 간단한 답변을 찾는 경우에 도움이 될 수 있습니다.

어떤 설정을 가져올까요?

설정 가져오기 기능은 하나의 스토리지 어레이에서 여러 스토리지 어레이로 구성을 로드하는 일괄 작업입니다.

이 작업 중에 가져오는 설정은 소스 스토리지 배열이 System Manager에 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 표시되지 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).

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 워크로드가 볼륨 생성에 어떤 영향을 미칩니까**?**

볼륨을 생성하는 동안 작업 부하 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 Server를 참조하십시오
  - Microsoft Exchange Server를 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.

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.

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. 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.

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.

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(또는 "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 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 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

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 Technology, Inc., 다중 경로 드라이버를 사용하는 Mac OS 버전을 지원합니다.
Windows(ATTO)	ATTO Technology, Inc., 다중 경로 드라이버를 사용하는 Windows 운영 체제를 지원합니다.
IBM SVC	IBM SAN Volume Controller 구성을 지원합니다.
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.

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.

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 액세스 권한을 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 경우에만 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.

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.

보존 용량이란?

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.

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 수준이라는 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
- 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.

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.

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 그룹에서 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.

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 * Yes * 가 표시됨).

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.

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.

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.

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

공칭 통계

SSD 캐시 통계를 보려면 * 관리 * 페이지로 이동하십시오. 메뉴: Provisioning [Configure Pools & Volume Groups]를 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.

EF600 또는 EF300 스토리지 시스템에서는 이 기능을 사용할 수 없습니다.

이 목록에는 상세 통계의 하위 집합인 공칭 통계가 포함됩니다.

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 .csv 파일로 내보낸 후에만 자세한 통계를 볼 수 있습니다.

세부 통계는 공칭 통계 다음에 나열됩니다.

선반 손실 방지 및 서랍 손실 방지란 무엇입니까?

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.

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.

레벨	쉘프 손실 방지 기준	필요한 최소 쉘프 수입니다
수영장	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 보호를 참조하십시오.	5
RAID 6	볼륨 그룹은 단일 드로어에 2개 이상의 드라이브를 포함하지 않습니다.	3
RAID 3 또는 RAID 5	볼륨 그룹의 각 드라이브는 별도의 쉘프에 있습니다.	3
RAID 1	RAID 1 쌍의 각 드라이브는 별도의 쉘프에 있어야 합니다.	2
RAID 0	선반 손실 보호를 달성할 수 없습니다.	해당 없음

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.

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.

레벨	서랍 손실 방지 기준	필요한 최소 드로어 수입니다
수영장	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.	5
RAID 6	볼륨 그룹은 단일 드로어에 2개 이상의 드라이브를 포함하지 않습니다.	3
RAID 3 또는 5	볼륨 그룹의 각 드라이브는 별도의 드로어에 있습니다	3
RAID 1	미러링된 쌍의 각 드라이브는 별도의 드로어에 위치해야 합니다.	2
RAID 0	문서함 손실 방지를 달성할 수 없습니다.	해당 없음

선반 및 서랍 손실 방지를 어떻게 유지합니까**?**

풀 또는 볼륨 그룹의 쉘프 및 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.	6 서랍용 쉘프 5의 경우
RAID 6	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

레벨	선반/서랍 손실 방지 기준	필요한 최소 쉘프/서랍 수
RAID 1	미러링된 쌍의 각 드라이브는 별도의 쉘프 또는 드로어에 위치해야 합니다.	2
RAID 0	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.

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) 및 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 사용 가능한 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 Dataset Management 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.

> 현재 리소스 프로비저닝 기능을 사용할 수 없습니다. 일부 보기에서는 구성 요소가 리소스 프로비저닝 가능 상태로 보고될 수 있지만 나중에 업데이트할 때 다시 활성화될 때까지 리소스 프로비저닝된 볼륨을 생성하는 기능이 비활성화되었습니다.

리소스가 프로비저닝된 볼륨

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 Dataset Management 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.

기능 활성화 및 비활성화

드라이브가 DULBE를 지원하는 시스템에서는 리소스 프로비저닝이 기본적으로 사용됩니다. 풀 및 볼륨 그룹에서 기본 설정을 해제할 수 있습니다. 리소스 프로비저닝을 해제하는 작업은 기존 볼륨에 대해 영구적으로 수행되므로 되돌릴 수 없습니다. 즉, 이러한 볼륨 그룹 및 풀에 대해 리소스 프로비저닝을 다시 설정할 수 없습니다.

그러나 새로 생성한 모든 볼륨에 대해 리소스 프로비저닝을 다시 활성화하려면 설정 [시스템] 메뉴에서 다시 활성화할 수 있습니다. 리소스 프로비저닝을 다시 설정하면 새로 생성한 볼륨 그룹 및 풀만 영향을 받습니다. 기존 볼륨 그룹 및 풀은 변경되지 않습니다. 필요한 경우 설정 [시스템] 메뉴에서 자원 프로비저닝을 다시 비활성화할 수도 있습니다.

내부 보안 키와 외부 보안 키 관리의 차이점은 무엇입니까?

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.

보안 키를 생성하기 전에 알아야 할 사항은 무엇입니까?

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 메모리에서 액세스할 수 없는 위치에 유지 및 "숨김"됩니다. 내부 보안 키를 생성하기 전에 다음을 수행해야 합니다.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
2. 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.

1. 스토리지 배열에 보안 가능 드라이브를 설치합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
2. 드라이브 보안 기능이 활성화되어 있는지 확인합니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오
3. 서명된 클라이언트 인증서 파일을 가져옵니다. 클라이언트 인증서가 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP 요청을 신뢰할 수 있습니다.
   a. 먼저 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 설정 [인증서 > 키 관리 > CSR 완료] 메뉴로 이동합니다.
   b. 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.)
   c. 클라이언트 인증서 파일이 있는 경우 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.
4. 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.

암호문을 정의해야 하는 이유는 무엇입니까**?**

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.

기능과 이점을 설명할 수 있습니다

클라우드 커넥터

SANtricity ® Cloud Connector 개요

SANtricity Cloud Connector는 호스트 기반 Linux 애플리케이션으로, E-Series 볼륨을 S3 불만 계정(예: Amazon Simple Storage Service 및 NetApp StorageGRID) 및 NetApp AltaVault 어플라이언스로 전체 블록 기반 및 파일 기반 백업 및 복구를 수행할 수 있습니다.

RedHat 및 SUSE Linux 플랫폼에 설치할 수 있는 SANtricity 클라우드 커넥터는 패키지 솔루션(.bin 파일)입니다. SANtricity 클라우드 커넥터를 설치한 후 애플리케이션을 구성하여 E-Series 볼륨의 백업 및 복원 작업을 AltaVault 어플라이언스 또는 기존 Amazon S3 또는 StorageGRID 계정에 수행할 수 있습니다. SANtricity 클라우드 커넥터를 통해 수행되는 모든 작업은 REST 기반 API를 사용합니다.

SANtricity 클라우드 커넥터 도구는 더 이상 사용되지 않으며 다운로드할 수 없습니다.

고려 사항

이러한 절차를 사용할 때는 다음 사항에 유의하십시오.

- 이 절차에서 설명하는 구성 및 백업/복원 작업은 SANtricity 클라우드 커넥터의 그래픽 사용자 인터페이스 버전에 적용됩니다.
- SANtricity 클라우드 커넥터 애플리케이션의 REST API 워크플로우는 이 절차에 설명되어 있지 않습니다. 숙련된 개발자의 경우 API 설명서에서 각 SANtricity 클라우드 커넥터 작업에 대해 엔드포인트를 사용할 수 있습니다. API 설명서는 브라우저를 통해 "http://<hostname.domain>:<port>/docs``으로 이동하여 액세스할 수 있습니다.

백업 유형

SANtricity 클라우드 커넥터는 이미지 기반 백업과 파일 기반 백업의 두 가지 백업 유형을 제공합니다.

- * 이미지 기반 백업 *

  이미지 기반 백업은 스냅샷 볼륨에서 원시 데이터 블록을 읽고 이를 이미지라고 하는 파일에 백업합니다. 스냅샷 볼륨의 모든 데이터 블록은 빈 블록, 삭제된 파일이 차지하는 블록, 파티셔닝과 관련된 블록, 파일 시스템 메타데이터 등을 포함하여 백업됩니다. 이미지 백업에서는 파티션 구성이나 파일 시스템에 관계없이 스냅샷 볼륨에 모든 정보를 저장할 수 있습니다.

  이미지는 백업 타겟에 단일 파일로 저장되지 않고 대신 64MB 크기의 일련의 데이터 청크로 분할됩니다. 데이터 청크를 통해 SANtricity Cloud Connector는 백업 타겟에 대한 여러 연결을 사용할 수 있으므로 백업 프로세스의 성능이 향상됩니다.

  StorageGRID 및 Amazon Web Services(S3)로 백업하는 경우 각 데이터 청크는 별도의 암호화 키를 사용하여 청크를 암호화합니다. 키는 사용자가 제공한 암호와 사용자 데이터의 SHA256 해시의 조합으로 구성된 SHA256 해시입니다. AltaVault로 백업할 경우 AltaVault가 이 작업을 수행하므로 SANtricity 클라우드 커넥터는 데이터 청크를 암호화하지 않습니다.

- * 파일 기반 백업 *

파일 기반 백업은 파일 시스템 파티션에 포함된 파일을 읽고 64MB 크기의 일련의 데이터 청크로 백업합니다. 파일 기반 백업은 삭제된 파일 또는 파티션 분할과 파일 시스템 메타데이터를 백업하지 않습니다. 이미지 기반 백업과 마찬가지로 데이터 청크를 통해 SANtricity Cloud Connector는 백업 타겟에 대한 여러 연결을 사용할 수 있으므로 백업 프로세스의 성능이 향상됩니다.

StorageGRID 및 Amazon Web Services에 백업하는 경우 각 데이터 청크는 별도의 암호화 키를 사용하여 청크를 암호화합니다. 키는 사용자 제공 암호문과 사용자 데이터의 SHA256 해시의 조합으로 구성된 SHA256 해시입니다. AltaVault로 백업하는 경우 AltaVault가 이 작업을 수행하기 때문에 SANtricity 클라우드 커넥터에 의해 데이터 청크가 암호화되지 않습니다.

SANtricity Cloud Connector의 시스템 요구 사항

시스템은 SANtricity 클라우드 커넥터의 호환성 요구 사항을 충족해야 합니다.

호스트 하드웨어 요구 사항

하드웨어는 다음 최소 요구 사항을 충족해야 합니다.

- 최소 5GB의 메모리, 구성된 최대 힙 크기에 대해 4GB
- 소프트웨어 설치 시 최소 5GB의 사용 가능한 디스크 공간이 필요합니다

SANtricity 클라우드 커넥터를 사용하려면 SANtricity 웹 서비스 프록시를 설치해야 합니다. 웹 서비스 프록시를 로컬로 설치하거나 다른 서버에서 응용 프로그램을 원격으로 실행할 수 있습니다. SANtricity 웹 서비스 프록시 설치에 대한 자세한 내용은 를 참조하십시오 "웹 서비스 프록시 항목".

지원되는 브라우저

다음 브라우저는 SANtricity 클라우드 커넥터 응용 프로그램에서 지원됩니다(최소 버전 표시).

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

Microsoft Internet Explorer v11 브라우저 내에서 호환성 보기 설정을 사용할 때 SANtricity 클라우드 커넥터 응용 프로그램에 대한 API 문서가 로드되지 않습니다. Microsoft Internet Explorer v11 브라우저에서 API 문서가 제대로 표시되도록 하려면 호환성 보기 설정을 사용하지 않는 것이 좋습니다.

호환되는 스토리지 어레이 및 컨트롤러 펌웨어입니다

SANtricity 클라우드 커넥터 애플리케이션을 사용하기 전에 스토리지 어레이와 펌웨어의 호환성을 확인해야 합니다.

SANtricity 클라우드 커넥터의 호환 가능한 모든 스토리지 어레이 및 펌웨어의 전체 최신 목록은 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

호환되는 운영 체제

SANtricity 클라우드 커넥터 4.0 응용 프로그램은 다음 운영 체제와 호환되고 지원됩니다.

운영 체제	버전	있습니다
Red Hat Enterprise Linux(RHEL)	7.x	64비트
SUSE Linux Enterprise Server(SLES)	12.x	64비트

지원되는 파일 시스템

SANtricity Cloud Connector 애플리케이션을 통해 백업 및 복구를 수행하려면 지원되는 파일 시스템을 사용해야 합니다.

SANtricity 클라우드 커넥터 애플리케이션에서 백업 및 복구 작업을 지원하는 파일 시스템은 다음과 같습니다.

- ext2
- ext3
- ext4

SANtricity 클라우드 커넥터를 설치합니다

SANtricity 클라우드 커넥터 패키지 솔루션(.bin 파일)은 RedHat 및 SUSE Linux 플랫폼에서만 사용할 수 있습니다.

호환되는 Linux 운영 체제에서 그래픽 모드 또는 콘솔 모드를 통해 SANtricity 클라우드 커넥터 응용 프로그램을 설치할 수 있습니다. 설치 프로세스 중에 SANtricity 클라우드 커넥터에 대한 비 SSL 및 SSL 포트 번호를 지정해야 합니다. SANtricity 클라우드 커넥터가 설치되면 데몬 프로세스로 실행됩니다.

SANtricity 클라우드 커넥터 도구는 더 이상 사용되지 않으며 다운로드할 수 없습니다.

시작하기 전에

다음 참고 사항을 검토하십시오.

- SANtricity 웹 서비스 프록시가 SANtricity 클라우드 커넥터와 동일한 서버에 이미 설치되어 있는 경우 비 SSL 포트 번호와 SSL 포트 번호 충돌 간에 충돌이 발생합니다. 이 경우 SANtricity 클라우드 커넥터 설치 중에 SSL이 아닌 포트와 SSL 포트에 적절한 번호를 선택합니다.
- 호스트에서 하드웨어 변경이 수행되는 경우 암호화 일관성을 보장하기 위해 SANtricity 클라우드 커넥터 애플리케이션을 다시 설치합니다.
- SANtricity 클라우드 커넥터 애플리케이션의 버전 3.1을 통해 생성된 백업은 SANtricity 클라우드 커넥터 애플리케이션의 버전 4.0과 호환되지 않습니다. 이러한 백업을 유지 관리하려면 이전 버전의 SANtricity 클라우드 커넥터를 계속 사용해야 합니다. SANtricity Cloud Connector의 3.1 및 4.0 릴리즈를 성공적으로 설치하려면 애플리케이션의 각 버전에 대해 고유한 포트 번호를 할당해야 합니다.

장치 매퍼 다중 경로**(DM-MP)** 설치

SANtricity 클라우드 커넥터를 실행하는 모든 호스트는 Linux 장치 매퍼 다중 경로(DM-MP)를 실행하고 다중 경로 도구 패키지를 설치해야 합니다.

SANtricity 클라우드 커넥터 검색 프로세스는 백업 또는 복원할 볼륨 및 파일을 검색하고 인식하기 위해 다중 경로 툴

패키지를 사용합니다. 장치 매퍼를 설정하고 구성하는 방법에 대한 자세한 내용은 에서 사용 중인 SANtricity 릴리스에 대한 _SANtricity 저장소 관리자 다중 경로 드라이버 안내서_를 참조하십시오 "E-Series 및 SANtricity 문서 리소스".

Cloud Connector를 설치합니다

Linux 운영 체제에 SANtricity 클라우드 커넥터를 그래픽 모드 또는 콘솔 모드로 설치할 수 있습니다.

그래픽 모드

그래픽 모드를 사용하여 Linux 운영 체제에 SANtricity 클라우드 커넥터를 설치할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 설치를 위한 호스트 위치를 지정합니다.

단계

1. SANtricity 클라우드 커넥터 설치 파일을 원하는 호스트 위치로 다운로드합니다.
2. 터미널 창을 엽니다.
3. SANtricity 클라우드 커넥터 설치 파일이 포함된 디렉토리 파일로 이동합니다.
4. SANtricity 클라우드 커넥터 설치 프로세스를 시작합니다.

   ```
   ./cloudconnector-xxxx.bin -i gui
   ```

   이 명령에서 xxxx는 애플리케이션의 버전 번호를 지정합니다.

   설치 프로그램 창이 표시됩니다.

5. Introduction 문을 검토한 후 * Next * 를 클릭합니다.

   NetApp, Inc. 소프트웨어에 대한 라이센스 계약은 설치 프로그램 창에 표시됩니다.

6. 사용권 계약 조건에 동의하고 * 다음 * 을 클릭합니다.

   이전 릴리스의 SANtricity 클라우드 커넥터 페이지에서 생성된 백업이 표시됩니다.

7. 이전 릴리스의 SANtricity 클라우드 커넥터 메시지로 생성된 백업을 확인하려면 * 다음 * 을 클릭합니다.

   > ⓘ 이전 버전을 유지하면서 SANtricity 클라우드 커넥터 버전 4.0을 설치하려면 각 응용 프로그램 버전에 대해 고유한 포트 번호를 할당해야 합니다.

   설치 선택 페이지가 설치 프로그램 창에 표시됩니다. 설치할 위치 필드에는 기본 설치 폴더 'opt/netapp/sSANtricity_cloud_connector4/'가 표시됩니다

8. 다음 옵션 중 하나를 선택합니다.
   - 기본 위치를 그대로 사용하려면 * 다음 * 을 클릭합니다.
   - 기본 위치를 변경하려면 새 폴더 위치를 입력합니다. 비 SSL Jetty 포트 번호 입력 페이지가 표시됩니다. 기본값이 8080인 경우 비 SSL 포트에 할당됩니다.
9. 다음 옵션 중 하나를 선택합니다.

◦ 기본 SSL 포트 번호를 적용하려면 * 다음 * 을 클릭합니다.

◦ 기본 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다.

10. 다음 옵션 중 하나를 선택합니다.

◦ 기본 비 SSL 포트 번호를 그대로 사용하려면 * 다음 * 을 클릭합니다.

◦ 기본 비 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다. 사전 설치 요약 페이지가 표시됩니다.

11. 표시된 설치 전 요약을 검토하고 * 설치 * 를 클릭합니다.

SANtricity 클라우드 커넥터 설치가 시작되고 Webserver 데몬 설정 프롬프트가 표시됩니다.

12. OK * 를 클릭하여 Webserver Daemon Setup 프롬프트를 확인합니다.

Installation Complete(설치 완료) 메시지가 표시됩니다.

13. Done * 을 클릭하여 SANtricity 클라우드 커넥터 설치 프로그램을 종료합니다.

콘솔 모드

콘솔 모드를 사용하여 Linux 운영 체제에 SANtricity 클라우드 커넥터를 설치할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 설치를 위한 호스트 위치를 지정합니다.

단계

1. SANtricity 클라우드 커넥터 설치 파일을 원하는 IO 호스트 위치로 다운로드합니다.
2. 터미널 창을 엽니다.
3. SANtricity 클라우드 커넥터 설치 파일이 포함된 디렉토리 파일로 이동합니다.
4. SANtricity 클라우드 커넥터 설치 프로세스를 시작합니다.

```
./cloudconnector-xxxx.bin –i console
```

이 명령에서 xxxx는 애플리케이션의 버전 번호를 나타냅니다.

SANtricity 클라우드 커넥터 설치 프로세스가 초기화됩니다.

5. 설치 프로세스를 진행하려면 * Enter * 를 누르십시오.

NetApp, Inc. 소프트웨어에 대한 최종 사용자 라이센스 계약은 설치 프로그램 창에 표시됩니다.

설치 프로세스를 취소하려면 설치 프로그램 창 아래에 quit를 입력합니다.

6. 최종 사용자 사용권 계약의 각 부분을 진행하려면 * Enter * 를 누르십시오.

사용권 계약 수락 진술은 설치 프로그램 창 아래에 표시됩니다.

7. 최종 사용자 사용권 계약 조건에 동의하고 SANtricity 클라우드 커넥터 설치를 계속하려면 설치 프로그램 창에서 'Y'를 입력하고 * Enter * 를 누르십시오.

   이전 릴리스의 SANtricity 클라우드 커넥터 페이지에서 생성된 백업이 표시됩니다.

   최종 사용자 계약 조건에 동의하지 않으면 "N"을 입력하고 * Enter * 를 눌러 SANtricity 클라우드 커넥터의 설치 프로세스를 종료합니다.

8. 이전 릴리스의 SANtricity 클라우드 커넥터 메시지로 생성된 백업을 확인하려면 * Enter * 를 누르십시오.

   이전 버전을 유지하면서 SANtricity 클라우드 커넥터 버전 4.0을 설치하려면 각 응용 프로그램 버전에 대해 고유한 포트 번호를 할당해야 합니다.

   SANtricity 클라우드 커넥터에 대한 다음 기본 설치 폴더가 있는 설치 폴더 선택 메시지가 표시됩니다. ""/opt/netapp/sSANtricity_cloud_connector4/".

9. 다음 옵션 중 하나를 선택합니다.
   - 기본 설치 위치를 그대로 사용하려면 * Enter * 를 누릅니다.
   - 기본 설치 위치를 변경하려면 새 폴더 위치를 입력합니다. 비 SSL Jetty 포트 번호 입력 메시지가 표시됩니다. 기본값이 8080인 경우 비 SSL 포트에 할당됩니다.
10. 다음 옵션 중 하나를 선택합니다.
    - 기본 SSL 포트 번호를 그대로 사용하려면 * 다음 * 을 누릅니다.
    - 기본 SSL 포트 번호를 변경하려면 원하는 새 포트 번호 값을 입력합니다.
11. 다음 옵션 중 하나를 선택합니다.
    - 기본 비 SSL 포트 번호를 그대로 사용하려면 * Enter * 를 누릅니다.
    - 기본 비 SSL 포트 번호를 변경하려면 새 포트 번호 값을 입력합니다. SANtricity 클라우드 커넥터의 사전 설치 요약이 표시됩니다.
12. 표시된 사전 설치 요약을 검토하고 * Enter * 를 누릅니다.
13. Enter * 를 눌러 Webserver Daemon Setup 프롬프트를 확인합니다.

    Installation Complete(설치 완료) 메시지가 표시됩니다.

14. SANtricity 클라우드 커넥터 설치 프로그램을 종료하려면 * Enter * 를 누릅니다.

서버 인증서와 **CA** 인증서를 키 저장소에 추가합니다

브라우저에서 SANtricity 클라우드 커넥터 호스트로의 보안 https 연결을 사용하려면 SANtricity 클라우드 커넥터 호스트에서 자체 서명된 인증서를 수락하거나 브라우저와 SANtricity 클라우드 커넥터 응용 프로그램에서 인식되는 인증서와 신뢰 체인을 추가할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터 애플리케이션이 호스트에 설치되어 있어야 합니다.

단계

1. 'stemctl' 명령을 사용하여 서비스를 중지합니다.

2. 기본 설치 위치에서 작업 디렉토리에 액세스합니다.

> SANtricity 클라우드 커넥터의 기본 설치 위치는 '/opt/netapp/SANtricity_cloud_connector4'입니다.

3. 'keytool' 명령을 사용하여 서버 인증서 및 인증서 서명 요청(CSR)을 생성합니다.

◦ 예 *

```
keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
-sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
keystore_cloudconnect.jks -storepass changeit
keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
-storepass changeit -file cloudconnect.csr
```

4. 생성된 CSR을 선택한 CA(인증 기관)에 보냅니다.

인증 기관이 인증서 요청에 서명하고 서명된 인증서를 반환합니다. 또한 CA 자체로부터 인증서를 받습니다. 이 CA 인증서를 키 저장소로 가져와야 합니다.

5. 인증서와 CA 인증서 체인을 "/<설치 경로>/작업/키 저장소" 응용 프로그램 키 저장소로 가져옵니다

◦ 예 *

```
keytool -import -alias ca-root -file root-ca.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
keystore_cloudconnect.jks -storepass <password> -noprompt
keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
-keystore keystore_cloudconnect.jks -storepass <password>
```

6. 서비스를 다시 시작합니다.

StorageGRID 인증서를 키 저장소에 추가합니다

StorageGRID를 SANtricity 클라우드 커넥터 응용 프로그램의 대상 유형으로 구성하는 경우 먼저 SANtricity 클라우드 커넥터 키 저장소에 StorageGRID 인증서를 추가해야 합니다.

시작하기 전에

- 서명된 StorageGRID 인증서가 있습니다.
- 호스트에 SANtricity 클라우드 커넥터 애플리케이션이 설치되어 있습니다.

단계

1. 'stemctl' 명령을 사용하여 서비스를 중지합니다.
2. 기본 설치 위치에서 작업 디렉토리에 액세스합니다.

SANtricity 클라우드 커넥터의 기본 설치 위치는 '/opt/netapp/SANtricity_cloud_connector4'입니다.

3. StorageGRID 인증서를 "/<설치 경로>/작업/키 저장소" 응용 프로그램 키 저장소로 가져옵니다

◦ 예 *

```
opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
-trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
/home/ictlabsg01.cer -keystore
/opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
```

4. 서비스를 다시 시작합니다.

SANtricity 클라우드 커넥터를 처음으로 구성합니다

설치가 완료되면 구성 마법사를 통해 SANtricity 클라우드 커넥터 응용 프로그램을 설정할 수 있습니다. SANtricity 클라우드 커넥터에 처음 로그인하면 구성 마법사가 표시됩니다.

SANtricity 클라우드 커넥터에 처음으로 로그인합니다

SANtricity 클라우드 커넥터를 처음으로 초기화하는 경우 응용 프로그램에 액세스하려면 기본 암호를 입력해야 합니다.

시작하기 전에

인터넷에 연결된 브라우저에 액세스할 수 있는지 확인합니다.

단계

1. 지원되는 브라우저를 엽니다.
2. 구성된 SANtricity 클라우드 커넥터 서버에 연결합니다(예: 'http://localhost:8080/`).

   SANtricity 클라우드 커넥터 애플리케이션의 초기 로그인 페이지가 표시됩니다.

3. Administrator Password(관리자 암호) 필드에 기본 암호 "password(암호)"를 입력합니다.
4. 로그인 * 을 클릭합니다.

   SANtricity 클라우드 커넥터 구성 마법사가 표시됩니다.

구성 마법사 사용

SANtricity 클라우드 커넥터에 처음 로그인하면 구성 마법사가 표시됩니다.

구성 마법사를 통해 관리자 암호, 웹 서비스 프록시 로그인 관리 자격 증명, 원하는 백업 대상 유형 및 SANtricity 클라우드 커넥터의 암호화 암호 구문을 설정합니다.

1단계**:** 관리자 암호를 설정합니다

관리자 암호 설정 페이지를 통해 SANtricity 클라우드 커넥터에 대한 후속 로그인에 사용되는 암호를 사용자 지정할 수 있습니다.

관리자 암호 설정 페이지를 통해 암호를 설정하면 SANtricity 클라우드 커넥터 응용 프로그램의 초기 로그인 중에 사용되는 기본 암호가 효과적으로 대체됩니다.

단계

1. 관리자 암호 설정 페이지의 * 새 관리자 암호 입력 * 필드에 SANtricity 클라우드 커넥터에 대해 원하는 로그인 암호를 입력합니다.
2. 새 관리자 암호 * 필드를 다시 입력하십시오. 필드에 첫 번째 필드의 암호를 다시 입력하십시오.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터의 암호 설정이 수락되고 암호 설정 페이지가 구성 마법사 아래에 표시됩니다.

   사용자 정의 관리자 암호는 구성 마법사를 완료할 때까지 설정되지 않습니다.

2단계**:** 암호문 설정

암호화 암호 입력 페이지에서 8자에서 32자 사이의 영숫자 암호를 지정할 수 있습니다.

SANtricity 클라우드 커넥터 응용 프로그램에서 사용하는 데이터 암호화 키의 일부로 사용자 지정 암호가 필요합니다.

단계

1. 암호 정의 * 필드에 원하는 암호를 입력합니다.
2. 암호 구문 * 필드를 다시 입력하십시오. 필드에 첫 번째 필드의 암호를 다시 입력하십시오.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터 애플리케이션에 대해 입력한 암호문이 수락되고 구성 마법사의 대상 유형 선택 페이지가 표시됩니다.

3단계**:** 대상 유형을 선택합니다

백업 및 복원 기능은 SANtricity 클라우드 커넥터를 통해 Amazon S3, AltaVault 및 StorageGRID 타겟 유형에 사용할 수 있습니다. 대상 유형 선택 페이지에서 SANtricity 클라우드 커넥터 애플리케이션에 대해 원하는 스토리지 타겟 유형을 지정할 수 있습니다.

시작하기 전에

AltaVault 마운트 지점, Amazon AWS 계정 또는 StorageGRID 계정 중 하나가 있는지 확인합니다.

단계

1. 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.
   - Amazon AWS
   - AltaVault
   - StorageGRID

   선택한 옵션의 대상 유형 페이지가 구성 마법사에 표시됩니다.
2. AltaVault, Amazon AWS 또는 StorageGRID에 대한 적절한 구성 지침을 참조하십시오.

AltaVault 어플라이언스를 구성합니다

대상 유형 선택 페이지에서 AltaVault 어플라이언스 옵션을 선택하면 AltaVault 대상 유형의 구성 옵션이 표시됩니다.

시작하기 전에

- AltaVault 어플라이언스에 대한 NFS 마운트 경로가 있습니다.
- AltaVault 어플라이언스를 대상 유형으로 지정했습니다.

단계

1. NFS 마운트 경로 * 필드에 AltaVault 타겟 유형의 마운트 지점을 입력합니다.

   NFS 마운트 경로 * 필드의 값은 Linux 경로 형식을 따라야 합니다.

2. 선택한 타겟 유형에 구성 데이터베이스의 백업을 만들려면 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

   연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사 아래에 입력된 새 백업 정보로 대체할 수 있습니다.

3. 지정된 AltaVault 설정에 대한 연결을 테스트하려면 * 연결 테스트 * 를 클릭합니다.
4. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사에 표시됩니다.

5. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

Amazon AWS 계정을 구성합니다

대상 유형 선택 페이지에서 Amazon AWS 옵션을 선택하면 Amazon AWS 타겟 유형에 대한 구성 옵션이 표시됩니다.

시작하기 전에

- Amazon AWS 계정이 설정되었습니다.
- Amazon AWS를 타겟 유형으로 지정했습니다.

단계

1. 액세스 키 ID * 필드에 Amazon AWS 타겟의 액세스 ID를 입력합니다.
2. 비밀 액세스 키 * 필드에 대상의 비밀 액세스 키를 입력합니다.
3. [버킷 이름] * 필드에 대상의 버킷 이름을 입력합니다.
4. 선택한 타겟 유형에 구성 데이터베이스의 백업을 생성하려면 * 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

   데이터베이스를 잃어버린 경우 백업 대상의 데이터를 복원할 수 있도록 이 설정을 사용하는 것이 좋습니다.

연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사 아래에 입력된 새 백업 정보로 대체할 수 있습니다.

5. Test Connection * 을 클릭하여 입력된 Amazon AWS 자격 증명을 확인합니다.
6. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사 아래에 표시됩니다.

7. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

StorageGRID 계정을 구성합니다

대상 유형 선택 페이지에서 StorageGRID 옵션을 선택하면 StorageGRID 대상 유형에 대한 구성 옵션이 표시됩니다.

시작하기 전에

- StorageGRID 계정이 설정되어 있습니다.
- SANtricity 클라우드 커넥터 키 저장소에 서명된 StorageGRID 인증서가 있습니다.
- 대상 유형으로 StorageGRID를 지정했습니다.

단계

1. URL * 필드에 Amazon S3 클라우드 서비스의 URL을 입력합니다
2. 액세스 키 ID * 필드에 S3 대상의 액세스 ID를 입력합니다.
3. 비밀 액세스 키 * 필드에 S3 대상의 비밀 액세스 키를 입력합니다.
4. Bucket Name * 필드에 S3 타겟의 버킷 이름을 입력합니다.
5. 경로 스타일 액세스를 사용하려면 * 경로 스타일 액세스 사용 * 확인란을 선택합니다.

   이 옵션을 선택하지 않으면 가상 호스트 스타일 액세스가 사용됩니다.

6. 선택한 타겟 유형에 구성 데이터베이스의 백업을 생성하려면 * 이 대상에 구성 데이터베이스의 백업 저장 * 확인란을 선택합니다.

   데이터베이스를 잃어버린 경우 백업 대상의 데이터를 복원할 수 있도록 이 설정을 사용하는 것이 좋습니다.

   연결을 테스트할 때 지정된 대상 유형에서 기존 데이터베이스 구성이 감지되면 SANtricity 클라우드 커넥터 호스트의 기존 데이터베이스 구성 정보를 구성 마법사에 입력한 새 백업 정보로 바꿀 수 있습니다.

7. Test Connection * 을 클릭하여 입력한 S3 자격 증명을 확인합니다.

   일부 S3 호환 계정에는 보안 HTTP 연결이 필요할 수 있습니다. StorageGRID 인증서를 키 저장소에 배치하는 방법에 대한 자세한 내용은 를 참조하십시오 "StorageGRID 인증서를 키 저장소에 추가합니다".

8. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 지정된 대상 유형이 허용되고 웹 서비스 프록시 페이지가 구성 마법사 아래에 표시됩니다.

9. "4단계: 웹 서비스 프록시에 연결"을 진행합니다.

4단계**:** 웹 서비스 프록시에 연결합니다

SANtricity 클라우드 커넥터와 함께 사용되는 웹 서비스 프록시의 로그인 및 연결 정보는 웹 서비스 프록시 URL 및 자격 증명 입력 페이지를 통해 입력됩니다.

시작하기 전에

SANtricity 웹 서비스 프록시에 대한 연결이 설정되어 있는지 확인합니다.

단계

1. URL* 필드에 SANtricity 클라우드 커넥터에 사용되는 웹 서비스 프록시의 URL을 입력합니다.
2. 사용자 이름 * 필드에 웹 서비스 프록시 연결의 사용자 이름을 입력합니다.
3. 암호 * 필드에 웹 서비스 프록시 연결의 암호를 입력합니다.
4. 입력한 웹 서비스 프록시 자격 증명에 대한 연결을 확인하려면 * 연결 테스트 * 를 클릭합니다.
5. 테스트 연결을 통해 입력한 웹 서비스 프록시 자격 증명을 확인한 후
6. 다음 * 을 클릭합니다

   SANtricity 클라우드 커넥터에 대한 웹 서비스 프록시 자격 증명이 수락되고 스토리지 배열 선택 페이지가 구성 마법사에 표시됩니다.

5단계**:** 스토리지 배열을 선택합니다

구성 마법사를 통해 입력한 SANtricity 웹 서비스 프록시 자격 증명을 기반으로 사용 가능한 스토리지 배열 목록이 스토리지 배열 선택 페이지에 표시됩니다. 이 페이지에서는 SANtricity 클라우드 커넥터가 백업 및 복원 작업에 사용하는 스토리지 어레이를 선택할 수 있습니다.

시작하기 전에

SANtricity 웹 서비스 프록시 응용 프로그램에 스토리지 배열이 구성되어 있는지 확인합니다.

> SANtricity 클라우드 커넥터 애플리케이션에서 확인할 수 없는 스토리지 스토리지는 로그 파일에서 API 예외를 발생하게 됩니다. 이는 연결할 수 없는 스토리지에서 볼륨 목록을 가져올 때마다 SANtricity Cloud Connector 애플리케이션의 의도된 동작입니다. 로그 파일에서 이러한 API 예외를 방지하려면 스토리지 배열에서 직접 루트 문제를 해결하거나 SANtricity 웹 서비스 프록시 응용 프로그램에서 영향을 받는 스토리지 배열을 제거할 수 있습니다.

단계

1. 백업 및 복원 작업을 위해 SANtricity 클라우드 커넥터 애플리케이션에 할당할 스토리지 어레이 옆의 각 확인란을 선택합니다.
2. 다음 * 을 클릭합니다.

   선택한 스토리지 배열이 수락되고 호스트 선택 페이지가 구성 마법사에 표시됩니다.

스토리지 배열 선택 페이지에서 선택한 스토리지 배열에 대해 유효한 암호를 구성해야 합니다. SANtricity 웹 서비스 프록시 API 설명서를 통해 스토리지 배열 암호를 구성할 수 있습니다.

6단계**:** 호스트를 선택합니다

구성 마법사를 통해 선택한 웹 서비스 프록시 호스팅 스토리지 어레이를 기반으로 사용 가능한 호스트를 선택하여 호스트 선택 페이지를 통해 백업 및 복구 대상 볼륨을 SANtricity 클라우드 커넥터 애플리케이션에 매핑할 수 있습니다.

시작하기 전에

SANtricity 웹 서비스 프록시를 통해 사용할 수 있는 호스트가 있는지 확인합니다.

단계

1. 나열된 스토리지 배열의 드롭다운 메뉴에서 원하는 호스트를 선택합니다.
2. 호스트 선택 페이지에 나열된 추가 스토리지 시스템에 대해 1단계를 반복합니다.
3. 다음 * 을 클릭합니다.

   SANtricity 클라우드 커넥터에 대해 선택한 호스트가 수락되고 검토 페이지가 구성 마법사에 표시됩니다.

7단계**:** 초기 구성을 검토합니다

SANtricity 클라우드 커넥터 구성 마법사의 마지막 페이지에는 검토를 위해 입력된 결과가 요약되어 있습니다.

검증된 구성 데이터의 결과를 검토합니다.

- 모든 구성 데이터의 유효성을 성공적으로 확인 및 설정한 경우 * Finish * 를 클릭하여 구성 프로세스를 완료합니다.
- 구성 데이터의 섹션을 확인할 수 없는 경우 * Back * 을 클릭하여 구성 마법사의 해당 페이지로 이동하여 제출된 데이터를 수정합니다.

SANtricity 클라우드 커넥터에 로그인합니다

지원되는 브라우저에서 구성된 서버를 통해 SANtricity 클라우드 커넥터 응용 프로그램의 그래픽 사용자 인터페이스에 액세스할 수 있습니다. SANtricity 클라우드 커넥터 계정이 설정되어 있는지 확인합니다.

단계

1. 지원되는 브라우저에서 구성된 SANtricity 클라우드 커넥터 서버에 연결합니다(예: "http://localhost:8080/`).

   SANtricity 클라우드 커넥터 애플리케이션의 로그인 페이지가 표시됩니다.

2. 구성된 관리자 암호를 입력합니다.
3. 로그인 * 을 클릭합니다.

   SANtricity 클라우드 커넥터 애플리케이션의 랜딩 페이지가 표시됩니다.

SANtricity 클라우드 커넥터 응용 프로그램의 왼쪽 탐색 패널에서 백업 옵션에 액세스할 수 있습니다. 백업 옵션은 새 이미지 기반 또는 파일 기반 백업 작업을 생성할 수 있는 백업 페이지를 표시합니다.

SANtricity Cloud Connector 애플리케이션의 * 백업 * 페이지를 사용하여 E-Series 볼륨의 백업을 생성 및 처리합니다. 이미지 기반 백업이나 파일 기반 백업을 만든 다음 이러한 작업을 즉시 또는 나중에 수행할 수 있습니다. 또한 마지막으로 수행된 전체 백업을 기준으로 전체 백업 또는 증분 백업을 수행하도록 선택할 수 있습니다. SANtricity 클라우드 커넥터 애플리케이션을 통해 수행된 마지막 전체 백업을 기준으로 최대 6개의 증분 백업을 수행할 수 있습니다.

SANtricity 클라우드 커넥터 애플리케이션에 나열된 백업 및 복원 작업에 대한 모든 타임스탬프는 현지 시간을 사용합니다.

새 이미지 기반 백업을 생성합니다

SANtricity 클라우드 커넥터 애플리케이션의 백업 페이지에 있는 생성 기능을 통해 새 이미지 기반 백업을 생성할 수 있습니다.

시작하기 전에

웹 서비스 프록시에서 SANtricity 클라우드 커넥터에 등록된 스토리지 배열이 있는지 확인합니다.

단계

1. 백업 페이지에서 * 생성 * 을 클릭합니다.

   백업 생성 창이 표시됩니다.

2. 이미지 기반 백업 생성 * 을 선택합니다.
3. 다음 * 을 클릭합니다.

   사용 가능한 E-Series 볼륨 목록이 백업 생성 창에 표시됩니다.

4. 원하는 E-Series 볼륨을 선택하고 * Next * 를 클릭합니다.

   백업 생성 확인 창의 * 백업 이름 지정 및 설명 * 페이지가 표시됩니다.

5. 자동 생성된 백업 이름을 수정하려면 * Job Name * 필드에 원하는 이름을 입력합니다.
6. 필요한 경우 * Job Description * 필드에 백업에 대한 설명을 추가합니다.

   백업 내용을 쉽게 식별할 수 있는 작업 설명을 입력해야 합니다.

7. 다음 * 을 클릭합니다.

   선택한 이미지 기반 백업의 요약이 Create Backup 창의 * Review backup information * 페이지에 표시됩니다.

8. 선택한 백업을 검토하고 * Finish * 를 클릭합니다.

   Create Backup 창의 확인 페이지가 표시됩니다.

9. 다음 옵션 중 하나를 선택합니다.
   - * 예 * — 선택한 백업에 대한 전체 백업을 시작합니다.
   - * 아니요 * — 선택한 이미지 기반 백업에 대한 전체 백업이 수행되지 않습니다.

   선택한 이미지 기반 백업에 대한 전체 백업은 나중에 백업 페이지의 실행 기능을 통해 수행할 수 있습니다.

10. 확인 * 을 클릭합니다.

    선택한 E-Series 볼륨에 대한 백업이 시작되고 백업 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

새 폴더/파일 기반 백업을 생성합니다

SANtricity 클라우드 커넥터 애플리케이션의 백업 페이지에 있는 생성 기능을 통해 새 폴더/파일 기반 백업을 생성할 수 있습니다.

시작하기 전에

웹 서비스 프록시에서 SANtricity 클라우드 커넥터에 등록된 스토리지 배열이 있는지 확인합니다.

파일 기반 백업은 지정한 파일 시스템의 모든 파일을 무조건 백업합니다. 그러나 파일 및 폴더의 선택적 복원을 수행할 수 있습니다.

단계

1. 백업 페이지에서 * 생성 * 을 클릭합니다.

   백업 생성 창이 표시됩니다.

2. 폴더/파일 기반 백업 생성 * 을 선택합니다.
3. 다음 * 을 클릭합니다.

   백업에 사용할 수 있는 파일 시스템이 포함된 볼륨 목록이 백업 생성 창에 표시됩니다.

4. 원하는 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   선택한 볼륨에서 사용 가능한 파일 시스템 목록이 Create Backup 창에 표시됩니다.

   파일 시스템이 나타나지 않으면 SANtricity 클라우드 커넥터 애플리케이션이 파일 시스템 유형을 지원하는지 확인하십시오. 자세한 내용은 을 참조하십시오 "지원되는 파일 시스템".

5. 백업할 폴더나 파일이 들어 있는 원하는 파일 시스템을 선택하고 * 다음 * 을 클릭합니다.

   백업 생성 확인 창의 * 백업 이름 지정 및 설명 * 페이지가 표시됩니다.

6. 자동 생성된 백업 이름을 수정하려면 * Job Name * 필드에 원하는 이름을 입력합니다.
7. 필요한 경우 * Job Description * 필드에 백업에 대한 설명을 추가합니다.

   백업 내용을 쉽게 식별할 수 있는 작업 설명을 입력해야 합니다.

8. 다음 * 을 클릭합니다.

   선택한 폴더/파일 기반 백업에 대한 요약이 Create Backup 창의 * Review backup information * 페이지에 표시됩니다.

9. 선택한 폴더/파일 기반 백업을 검토하고 * 마침 * 을 클릭합니다.

   Create Backup 창의 확인 페이지가 표시됩니다.

10. 다음 옵션 중 하나를 선택합니다.
    - * 예 * — 선택한 백업에 대한 전체 백업을 시작합니다.
    - * 아니요 * — 선택한 백업에 대한 전체 백업이 수행되지 않습니다.

    > 선택한 파일 기반 백업에 대한 전체 백업은 나중에 백업 페이지의 실행 기능을 통해 수행할 수도 있습니다.

11. 닫기 * 를 클릭합니다.

    선택한 E-Series 볼륨에 대한 백업이 시작되고 백업 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

전체 및 증분 백업을 실행합니다

백업 페이지의 실행 기능을 통해 전체 및 증분 백업을 수행할 수 있습니다. 증분 백업은 파일 기반 백업에만 사용할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 백업 작업을 생성했는지 확인합니다.

단계

1. 백업 탭에서 원하는 백업 작업을 선택하고 * 실행 * 을 클릭합니다.

   > 이전에 수행된 초기 백업 없이 이미지 기반 백업 작업 또는 백업 작업을 선택할 때마다 전체 백업이 자동으로 수행됩니다.

   백업 실행 창이 표시됩니다.

2. 다음 옵션 중 하나를 선택합니다.
   - * 전체 * — 선택한 파일 기반 백업에 대한 모든 데이터를 백업합니다.
   - * Incremental * — 마지막으로 수행된 백업 이후 변경된 내용만 백업합니다.

   > SANtricity 클라우드 커넥터 애플리케이션을 통해 수행된 마지막 전체 백업을 기준으로 최대 6개의 증분 백업을 수행할 수 있습니다.

3. Run * 을 클릭합니다.

   백업 요청이 시작됩니다.

백업 작업을 삭제합니다

삭제 기능은 백업 세트와 함께 선택한 백업의 지정된 타겟 위치에서 백업된 데이터를 삭제합니다.

시작하기 전에

완료, 실패 또는 취소 상태의 백업이 있는지 확인합니다.

단계

1. 백업 페이지에서 원하는 백업을 선택하고 * 삭제 * 를 클릭합니다.

   전체 기본 백업을 삭제하도록 선택하면 관련된 모든 증분 백업도 삭제됩니다.

   Confirm Delete(삭제 확인) 창이 표시됩니다.

2. 삭제 작업을 확인하려면 * 유형 삭제 * 필드에 '삭제'를 입력합니다.
3. 삭제 * 를 클릭합니다.

   선택한 백업이 삭제됩니다.

SANtricity Cloud Connector에서 새 이미지 기반 또는 파일 기반 복원을 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 왼쪽 탐색 패널에서 복원 옵션에 액세스할 수 있습니다. 복원 옵션은 새 이미지 기반 또는 파일 기반 복원 작업을 만들 수 있는 복원 페이지를 표시합니다.

SANtricity 클라우드 커넥터는 작업 개념을 사용하여 E-Series 볼륨의 실제 복원을 수행합니다. 복원을 수행하기 전에 작업에 사용할 E-Series 볼륨을 확인해야 합니다. 복원을 위해 E-Series 볼륨을 SANtricity 클라우드 커넥터 호스트에 추가한 후 SANtricity 클라우드 커넥터 애플리케이션의 '복원' 페이지를 사용하여 복원을 생성 및 처리할 수 있습니다.

SANtricity 클라우드 커넥터 애플리케이션에 나열된 백업 및 복원 작업에 대한 모든 타임스탬프는 현지 시간을 사용합니다.

새 이미지 기반 복원을 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에 있는 만들기 기능을 통해 새 이미지 기반 복원을 만들 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 이미지 기반 백업을 사용할 수 있는지 확인합니다.

단계

1. SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에서 * 생성 * 을 클릭합니다.

   Restore(복원) 창이 표시됩니다.

2. 원하는 백업을 선택합니다.
3. 다음 * 을 클릭합니다.

백업 지점 선택 페이지가 복원 창에 표시됩니다.

4. 원하는 완료된 백업을 선택합니다.
5. 다음 * 을 클릭합니다.

   Restore(복원) 창에 Select Restore Target(대상 복원 선택) 페이지가 표시됩니다.

6. 복원 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   Restore(복원) 창에 Review(검토) 페이지가 표시됩니다.

7. 선택한 복원 작업을 검토하고 * Finish * 를 클릭합니다.

   선택한 타겟 호스트 볼륨에 대한 복구가 시작되고 복구 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

새 파일 기반 복구를 생성합니다

SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에 있는 만들기 기능을 통해 새 파일 기반 복원을 만들 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터를 통해 파일 기반 백업을 사용할 수 있는지 확인합니다.

단계

1. SANtricity 클라우드 커넥터 응용 프로그램의 복원 페이지에서 * 생성 * 을 클릭합니다.

   Restore(복원) 창이 표시됩니다.

2. Restore 창에서 원하는 파일 기반 백업을 선택합니다.
3. 다음 * 을 클릭합니다.

   백업 지점 선택 페이지가 복원 작업 생성 창에 표시됩니다.

4. 백업 지점 선택 페이지에서 원하는 완료된 백업을 선택합니다.
5. 다음 * 을 클릭합니다.

   복구 창에 사용 가능한 파일 시스템 또는 폴더/파일 목록이 표시됩니다.

6. 복원할 폴더 또는 파일을 선택하고 * 다음 * 을 클릭합니다.

   Restore(복원) 창에 Select Restore Target(대상 복원 선택) 페이지가 표시됩니다.

7. 복원 볼륨을 선택하고 * 다음 * 을 클릭합니다.

   Restore(복원) 창에 Review(검토) 페이지가 표시됩니다.

8. 선택한 복원 작업을 검토하고 * Finish * 를 클릭합니다.

   선택한 타겟 호스트 볼륨에 대한 복구가 시작되고 복구 페이지의 결과 목록 섹션에 작업 상태가 표시됩니다.

복원을 삭제합니다

삭제 기능을 사용하여 복원 페이지의 결과 목록 섹션에서 선택한 복원 항목을 삭제할 수 있습니다.

시작하기 전에

완료, 실패 또는 취소 상태의 복원 작업이 있는지 확인합니다.

단계

1. 복원 페이지에서 * 삭제 * 를 클릭합니다.

   Confirm Delete(삭제 확인) 창이 표시됩니다.

2. 삭제 작업을 확인하려면 * 유형 삭제 * 필드에 삭제 를 입력합니다.
3. 삭제 * 를 클릭합니다.

   > 일시 중지된 복구는 삭제할 수 없습니다.

   선택한 복원이 삭제됩니다.

SANtricity 클라우드 커넥터 설정을 수정합니다

설정 옵션을 사용하면 S3 계정, 관리되는 스토리지 배열 및 호스트, 웹 서비스 프록시 자격 증명에 대한 응용 프로그램의 현재 구성을 수정할 수 있습니다. 설정 옵션을 통해 SANtricity 클라우드 커넥터 응용 프로그램의 암호를 변경할 수도 있습니다.

S3 계정 설정을 수정합니다

S3 계정 설정 창에서 SANtricity 클라우드 커넥터 응용 프로그램에 대한 기존 S3 설정을 수정할 수 있습니다.

시작하기 전에

URL 또는 S3 버킷 레이블 설정을 수정할 때 SANtricity 클라우드 커넥터를 통해 구성된 기존 백업에 대한 액세스가 영향을 받는다는 점에 유의하십시오.

단계

1. 왼쪽 도구 모음에서 * 설정 > 구성 * 을 클릭합니다.

   설정 - 구성 페이지가 표시됩니다.

2. S3 계정 설정에 대한 * 설정 보기/편집 * 을 클릭합니다.

   S3 계정 설정 페이지가 표시됩니다.

3. URL 파일에 S3 클라우드 서비스의 URL을 입력합니다.
4. 액세스 키 ID * 필드에 S3 대상의 액세스 ID를 입력합니다.
5. 비밀 액세스 키 * 필드에 S3 대상의 액세스 키를 입력합니다.
6. S3 버킷 이름 * 필드에 S3 타겟의 버킷 이름을 입력합니다.
7. 필요한 경우 * 경로 스타일 액세스 사용 * 확인란을 선택합니다.

8. Test Connection * 을 클릭하여 입력한 S3 자격 증명에 대한 연결을 확인합니다.
9. 저장 * 을 클릭하여 수정 사항을 적용합니다.

   수정된 S3 계정 설정이 적용됩니다.

스토리지 시스템을 관리합니다

스토리지 배열 관리 페이지의 SANtricity 클라우드 커넥터 호스트에 등록된 웹 서비스 프록시에서 스토리지 배열을 추가하거나 제거할 수 있습니다.

스토리지 배열 관리 페이지에는 SANtricity 클라우드 커넥터 호스트에 등록할 수 있는 웹 서비스 프록시의 스토리지 배열 목록이 표시됩니다.

단계

1. 왼쪽 도구 모음에서 * 설정 > 스토리지 배열 * 을 클릭합니다.

   Settings - Storage Arrays(설정 - 스토리지 배열) 화면이 표시됩니다.

2. SANtricity 클라우드 커넥터에 스토리지 어레이를 추가하려면 * 추가 * 를 클릭합니다.
   a. Add Storage Arrays 창의 결과 목록에서 원하는 스토리지 배열 옆에 있는 각 확인란을 선택합니다.
   b. 추가 * 를 클릭합니다.

      선택한 스토리지 배열이 SANtricity 클라우드 커넥터에 추가되고 설정 - 스토리지 배열 화면의 결과 목록 섹션에 표시됩니다.

3. 추가된 스토리지 배열에 대한 호스트를 수정하려면 Settings(설정) - Storage Arrays(스토리지 배열) 화면의 Result list(결과 목록) 섹션에서 라인 항목에 대해 * Edit(편집) * 를 클릭합니다.
   a. Associated Host(연결된 호스트) 드롭다운 메뉴에서 스토리지 배열에 대해 원하는 호스트를 선택합니다.
   b. 저장 * 을 클릭합니다.

      선택한 호스트가 스토리지 배열에 할당됩니다.

4. SANtricity 클라우드 커넥터 호스트에서 기존 스토리지 배열을 제거하려면 하단 결과 목록에서 원하는 스토리지 배열을 선택하고 * Remove * 를 클릭합니다.
   a. 스토리지 배열 제거 확인 필드에 remove를 입력합니다.
   b. 제거 * 를 클릭합니다.

      선택한 스토리지 배열이 SANtricity 클라우드 커넥터 호스트에서 제거됩니다.

웹 서비스 프록시 설정을 수정합니다

웹 서비스 프록시 설정 창에서 SANtricity 클라우드 커넥터 응용 프로그램에 대한 기존 웹 서비스 프록시 설정을 수정할 수 있습니다.

시작하기 전에

SANtricity 클라우드 커넥터와 함께 사용되는 웹 서비스 프록시는 적절한 어레이가 추가되고 해당 암호가 설정되어 있어야 합니다.

단계

1. 왼쪽 도구 모음에서 * 메뉴: 설정 [구성] * 을 클릭합니다.

   설정 - 구성 화면이 표시됩니다.

2. 웹 서비스 프록시에 대한 * 설정 보기/편집 * 을 클릭합니다.

   웹 서비스 프록시 설정 화면이 표시됩니다.

3. URL 필드에 SANtricity 클라우드 커넥터에 사용되는 웹 서비스 프록시의 URL을 입력합니다.
4. 사용자 이름 필드에 웹 서비스 프록시 연결의 사용자 이름을 입력합니다.
5. 암호 필드에 웹 서비스 프록시 연결의 암호를 입력합니다.
6. 입력한 웹 서비스 프록시 자격 증명에 대한 연결을 확인하려면 * 연결 테스트 * 를 클릭합니다.
7. 저장 * 을 클릭하여 수정 사항을 적용합니다.

SANtricity 클라우드 커넥터 암호를 변경합니다

암호 변경 화면에서 SANtricity 클라우드 커넥터 응용 프로그램의 암호를 변경할 수 있습니다.

단계

1. 왼쪽 도구 모음에서 * 메뉴: 설정 [구성] * 을 클릭합니다.

   설정 - 구성 화면이 표시됩니다.

2. SANtricity 클라우드 커넥터의 * 암호 변경 * 을 클릭합니다.

   암호 변경 화면이 표시됩니다.

3. 현재 암호 필드에 SANtricity 클라우드 커넥터 응용 프로그램의 현재 암호를 입력합니다.
4. 새 암호 필드에 SANtricity 클라우드 커넥터 응용 프로그램의 새 암호를 입력합니다.
5. 새 암호 확인 필드에 새 암호를 다시 입력합니다.
6. 새 암호를 적용하려면 * 변경 * 을 클릭합니다.

   수정된 암호는 SANtricity 클라우드 커넥터 응용 프로그램에 적용됩니다.

SANtricity 클라우드 커넥터를 제거합니다

그래픽 제거 프로그램 또는 콘솔 모드를 통해 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

그래픽 모드를 사용하여 제거합니다

그래픽 모드를 사용하여 Linux 운영 체제에서 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

단계

1. 터미널 창에서 SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉터리로 이동합니다.

   SANtricity 클라우드 커넥터의 제거 파일은 다음 기본 디렉토리 위치에서 사용할 수 있습니다.

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉토리에서 다음 명령을 실행합니다.

```
./uninstall_cloud_connector4 -i gui
```

SANtricity 클라우드 커넥터의 제거 프로세스가 초기화됩니다.

3. 제거 창에서 * 제거 * 를 클릭하여 SANtricity 클라우드 커넥터 제거를 계속합니다.

제거 프로세스가 완료되고 SANtricity 클라우드 커넥터 응용 프로그램이 Linux 운영 체제에서 제거됩니다.

콘솔 모드를 사용하여 제거합니다

콘솔 모드를 사용하여 Linux 운영 체제에서 SANtricity 클라우드 커넥터를 제거할 수 있습니다.

단계

1. 터미널 창에서 SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉터리로 이동합니다.

SANtricity 클라우드 커넥터의 제거 파일은 다음 기본 디렉토리 위치에서 사용할 수 있습니다.

```
/opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
```

2. SANtricity 클라우드 커넥터 제거 파일이 포함된 디렉토리에서 다음 명령을 실행합니다.

```
./uninstall_cloud_connector4 -i console
```

SANtricity 클라우드 커넥터의 제거 프로세스가 초기화됩니다.

3. 제거 창에서 * Enter * 를 눌러 SANtricity 클라우드 커넥터 제거를 계속합니다.

제거 프로세스가 완료되고 SANtricity 클라우드 커넥터 응용 프로그램이 Linux 운영 체제에서 제거됩니다.