웹 서비스 프록시

E-Series storage systems

NetApp
January 20, 2026

목차

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 Manager에 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.

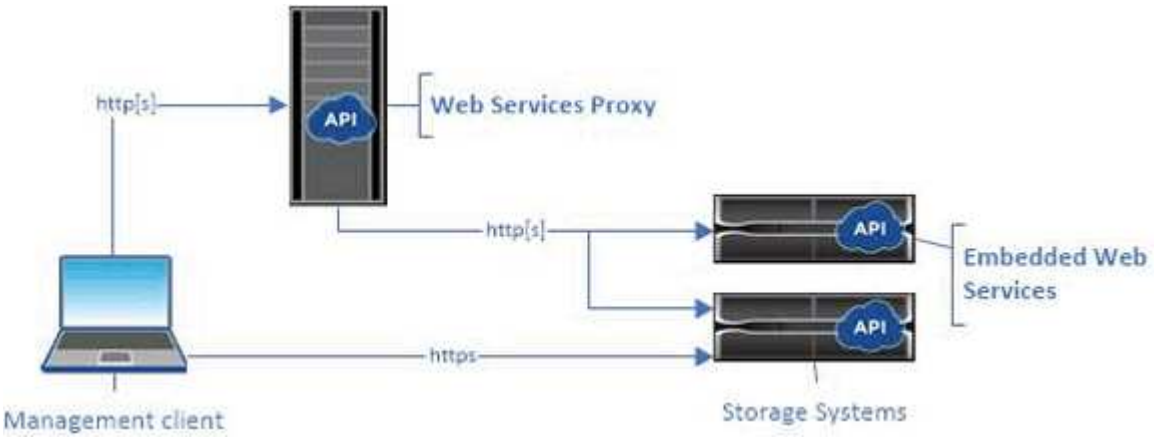
- JSON(JavaScript Object Notation) – 웹 서비스 내의 데이터는 JSON을 통해 인코딩되므로 JSON 프로그래밍 개념에 익숙해야 합니다. 자세한 내용은 을 참조하십시오 "JSON을 소개합니다".

- 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.

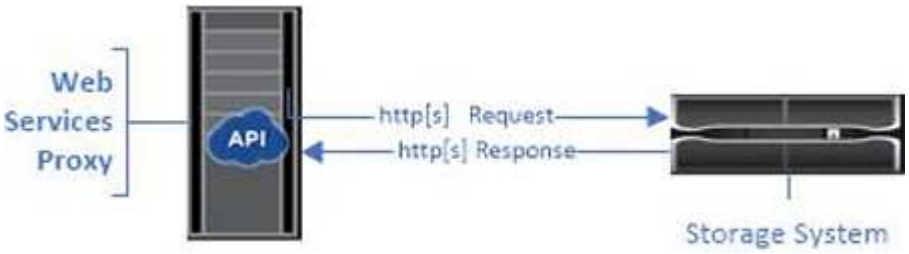
고려 사항	호환성 또는 제한
IP 지원	웹 서비스 프록시는 IPv4 프로토콜 또는 IPv6 프로토콜을 지원합니다. 웹 서비스 프록시가 컨트롤러 구성에서 관리 주소를 자동으로 검색하려고 하면 IPv6 프로토콜이 실패할 수 있습니다. IP 주소 전달 중 또는 IPv6가 서버에 있지 않고 스토리지 시스템에서 활성화되어 있는 동안 발생하는 문제가 오류의 가능한 원인입니다.
NVSRAM 파일 이름 제약 조건	웹 서비스 프록시는 NVSRAM 파일 이름을 사용하여 버전 정보를 정확하게 식별합니다. 따라서 웹 서비스 프록시와 함께 사용되는 NVSRAM 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>`